Прим. № __

ЗАТВЕРДЖЕНО

Наказ Адміністрації Держспецзв'язку
25 жовтня 2022 року № 715

Професійний стандарт
«Аналітик з безпеки інформаційно-телекомунікаційних систем»

1. Загальні відомості професійного стандарту

1.1. Основна мета професійної діяльності

Збирання, оброблення, аналізування та поширення результатів оцінювання кіберзагроз/сигналів попередження. Дослідження, аналіз та участь у реагуванні на кіберінциденти в кіберпросторі.

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

Секція J	Інформація та телекомунікації	**Розділ 61**	Телекомунікації (електрозв'язок)	**Група 61.1**	Діяльність у сфері 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 61.9	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.

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

Розділ	**Клас**	**Підклас**
2	**213**	**2139**
Професіонали	Професіонали в галузі обчислень (комп'ютеризації)	Професіонали в інших галузях обчислень (комп'ютеризації)

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

Аналітик з безпеки інформаційно-телекомунікаційних систем 2139.2.

1.5. Професійна кваліфікація

Аналітик з безпеки інформаційно-телекомунікаційних систем (трудові функції А, Б, В, Г).

Провідний аналітик з безпеки інформаційно-телекомунікаційних систем (трудові функції А, Б, В, Г, Д).

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

Обіймає посаду аналітика з безпеки інформаційно-телекомунікаційних систем, провідного аналітика з безпеки інформаційно-телекомунікаційних систем.

Аналітик з безпеки інформаційно-телекомунікаційних систем, провідний аналітик з безпеки інформаційно-телекомунікаційних систем безпосередньо підпорядкований керівнику профільного структурного підрозділу (або уповноваженій особі) в структурних підрозділах підприємства/організації, профільних структурних підрозділах підприємства/організації із захисту інформації та кібербезпеки, профільних науково-дослідних установах, підприємствах/організаціях, які реалізовують або застосовують функції захисту інформації, збирання, оброблення, аналізування та поширення результатів оцінювання кіберзагроз/сигналів попередження, досліджують та аналізують кіберінциденти, беруть участь у реагуванні на кіберінциденти в кіберпросторі.

Робоче місце розташовано у приміщенні (кабінеті, кімнаті, лабораторії, приміщенні обчислювального центру) відповідного підприємства/організації/ установи.

1.7. Умови праці

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

Відпустки надаються відповідно до законодавства, умов колективного договору, графіків надання відпусток та за результатами атестації відповідності робочого місця умовам праці.

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

Для кваліфікацій «Аналітик з безпеки інформаційно-телекомунікаційних систем», «Провідний аналітик з безпеки інформаційно-телекомунікаційних систем»:

диплом магістра за будь-якою із шести спеціальностей галузі знань 12 «Інформаційні технології» або за спеціальностями 171 «Електроніка», 172 «Телекомунікації та радіотехніка» галузі знань 17 «Електроніка та телекомунікації» (7 рівень НРК), а також свідоцтво про присвоєння (підвищення) кваліфікації «Аналітик з безпеки інформаційно-телекомунікаційних систем» або інший документ, що підтверджує професійну кваліфікацію «Аналітик з безпеки інформаційно-телекомунікаційних систем»;

або свідоцтво про присвоєння (підвищення) кваліфікації «Провідний аналітик з безпеки інформаційно-телекомунікаційних систем» або інший документ, що підтверджує професійну кваліфікацію «Провідний аналітик з безпеки інформаційно-телекомунікаційних систем».

Аналітик з безпеки інформаційно-телекомунікаційних систем – 7 рівень НРК.

Провідний аналітик з безпеки інформаційно-телекомунікаційних систем – 7 рівень НРК.

2. Навчання та професійний розвиток

2.1. Первинна професійна підготовка (назва кваліфікації)

Для професійних кваліфікацій «Аналітик з безпеки інформаційно-телекомунікаційних систем» і «Провідний аналітик з безпеки інформаційно-телекомунікаційних систем» – підготовка на другому (магістерському) рівні вищої освіти галузі знань 12 «Інформаційні технології». Стаж роботи за спеціальністю не менше трьох років.

2.2 Підвищення кваліфікації без присвоєння нового рівня освіти

Підвищення професійної кваліфікації «Аналітик з безпеки інформаційно-телекомунікаційних систем» для отримання професійної кваліфікації «Провідний аналітик з безпеки інформаційно-телекомунікаційних систем». Стаж роботи за спеціальністю не менше трьох років.

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

Кодекс законів про працю України.

Закон України «Про захист прав споживачів».

Закон України «Про інформацію».

Закон України «Про державну таємницю».

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

Закон України «Про захист персональних даних».

Закон України «Про доступ до публічної інформації»;

Закон України «Про основні засади забезпечення кібербезпеки України».

Закон України «Про електронні довірчі послуги».

Закон України «Про національну безпеку України».

Закон України «Про електронні комунікації».

Закон України «Про публічні електронні реєстри».

Закон України «Про критичну інфраструктуру».

Постанова Кабінету Міністрів України від 29.03.2006 р. № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах».

Постанова Кабінету Міністрів України від 16.11.2002 р. № 1772 «Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах».

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

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

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

Постанова Кабінету Міністрів України від 09.10.2020 р. № 943 «Деякі питання об'єктів критичної інформаційної інфраструктури».

Постанова Кабінету Міністрів України від 16.12.2020 р. № 1358 «Деякі питання функціонування Національної телекомунікаційної мережі».

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

Наказ Адміністрації Держспецзв'язку від 02.12.2014 р. № 660 «Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», зареєстрований в Міністерстві юстиції України 28.01.2015 р. за № 90/26535.

Наказ Адміністрації Держспецзв'язку від 15.01.2016 р. № 20 «Про затвердження Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті», зареєстрований в Міністерстві юстиції України 05.02.2016 р. за № 196/28326.

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

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

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

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

Нормативні документи в галузі технічного захисту інформації (далі – НД ТЗІ) щодо створення комплексних систем захисту інформації.

Державні стандарти України (далі – ДСТУ) щодо впровадження систем керування інформаційною безпекою.

Галузеві стандарти в сфері інформаційної та кібербезпеки.

Стандарти Національного інституту стандартів і технологій (далі – NIST) в сфері інформаційної та кібербезпеки.

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

4. Загальні компетентності

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

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

Умовне позначення	Трудові функції	Професійні компетентності (за трудовою дією або групою трудових дій)	Умовне позначення
А	Організація аналітичної діяльності з безпеки інформаційно-телекомунікаційних систем	Здатність перевіряти наявність мінімальних вимог безпеки до всього програмного забезпечення	**А1**
		Здатність здійснювати контроль за тим, щоб усі операції з безпеки та обслуговування системи (застосування виправлень безпеки) відповідали термінам, встановленим органом управління для передбачуваного операційного середовища	**А2**
		Здатність застосовувати заходи безпеки для усунення вразливостей, здійснювати контроль за тим, що продукти з підтримкою функцій кібербезпеки або компенсаційні технології контролю безпеки знижують ідентифікований ризик до прийнятного рівня та рекомендувати зміни щодо безпеки	**А3**
		Здатність інтегрувати автоматизовані можливості для оновлення або виправлення системного програмного забезпечення та розробляти процеси і процедури для ручного оновлення та виправлення системного програмного забезпечення	**А4**
		Здатність до вивчення топології мережі для усвідомлення потоків даних через мережу, забезпечувати інтеграцію та впровадження	**А5**

		міждоменних рішень у безпечному середовищі	
		Здатність усувати/мінімізувати недоліки безпеки, виявлені під час тестування безпеки/сертифікації, інформувати відповідальних працівників (відповідального керівника або уповноваженого представника) про підозрілі кіберінциденти та формалізувати історію події, статус і потенційний вплив для подальших дій відповідно до плану реагування на кіберінциденти організації (прийняти або обробити ризик)	**А6**
		Здатність забезпечувати виконання аварійного відновлення та безперервність роботи, зокрема розробляти процедури та здійснювати тестування передачі операцій системи на альтернативний сайт на основі вимог доступності системи	**А7**
		Здатність впроваджувати заходи безпеки системи відповідно до встановлених процедур, визначених тактик, технік для наборів вторгнень, для забезпечення конфіденційності, цілісності, доступності, аутентифікації та невідмовності	**А8**
Б	Аналіз заходів і ситуації з безпекою інформаційно-телекомунікаційних систем	Здатність характеризувати та аналізувати мережевий трафік для виявлення аномальної активності (метадані), шкідливих дій, потенційних загроз мережевим ресурсам, слабких місць, методів експлуатації, впливу на систему та інформацію	**Б1**
		Здатність виконувати огляди безпеки та виявляти прогалини в архітектурі безпеки, що є приводом для розроблення рекомендацій щодо включення до стратегії зменшення ризику та розроблення плану управління ризиками безпеки	**Б2**
		Здатність аналізувати тенденції кіберзахисту та звітувати про отримання мережевих сповіщень з різних джерел в організації, вказуючи можливі причини таких повідомлень	**Б3**

		Здатність забезпечувати своєчасне виявлення, ідентифікацію та попередження про можливі атаки/вторгнення, аномальні події та дії зі зловживання та відрізняти ці інциденти та події від штатної діяльності, проводячи дослідження, аналізування і кореляцію в широкому діапазоні всіх наборів вихідних даних (показання та попередження)	**Б4**
		Здатність перевіряти попередження системи виявлення вторгнень щодо мережевого трафіку за допомогою інструментів аналізування пакетів для локалізації та видалення шкідливого програмного забезпечення	**Б5**
		Здатність відновлювати втрачені дані чи інформацію про зловмисну атаку або дію на основі інформації щодо мережевого трафіку	**Б6**
		Здатність надавати допомогу в створенні сигнатур, які можна реалізувати в мережевих інструментах кіберзахисту у відповідь на нові або спостережувані загрози в мережевому середовищі	**Б7**
В	Аналіз упереджувальних/ розвідувальних заходів з безпеки інформаційно-телекомунікаційних систем	Здатність застосовувати принципи сервісно-орієнтованої архітектури безпеки, щоб відповідати вимогам організації до конфіденційності, цілісності та доступності	**В1**
		Здатність впроваджувати конкретні контрзаходи з кіберзахисту (операцій і технічного обслуговування системи) для систем та/або програм, їх документування та оновлення, у разі потреби	**В2**
		Здатність документувати та передавати інформацію про інциденти, які можуть спричинити поточний і негайний вплив на навколишнє середовище; рекомендувати та планувати заходи з усунення вразливостей комп'ютерного середовища за результатами оцінювання наявних заходів та/або поведінки системного середовища	**В3**
		Здатність виконувати кореляцію подій, використовуючи інформацію, зібрану з різних джерел на підприємстві, щоб досягти усвідомлення ситуації та визначити ефективність спостережуваної атаки	**В4**
		Здатність проводити тестування кібербезпеки розроблених додатків та/або систем, надавати вхідні дані для технологічних процесів системи управління ризиками	**В5**

		Здатність перевіряти та оновлювати документацію з безпеки, яка відображає особливості проєктування безпеки програми/системи	**В6**
		Здатність визначати програмне забезпечення та операційні системи мережевого пристрою на основі мережевого трафіку, визначати відображення мережі та дії операційної системи	**В7**
		Здатність відстежувати зовнішні джерела даних (сайти постачальників послуг кіберзахисту, команди реагування на комп'ютерні надзвичайні події, фокус безпеки) для підтримання актуальності стану системи з урахуванням загроз кіберзахисту та визначати, які проблеми безпеки можуть вплинути на організацію	**В8**
Г	Проведення моніторингу та оцінювання діяльності із забезпечення безпеки інформаційно-телекомунікаційних систем	Здатність розробляти контент для засобів кіберзахисту	**Г1**
		Здатність надавати щоденні зведені звіти про мережеві події та діяльність, що стосуються практичних заходів кіберзахисту	**Г2**
		Здатність використовувати інструменти кіберзахисту для постійного моніторингу та аналізування системної активності для виявлення зловмисної діяльності	**Г3**
		Здатність оцінювати ефективність заходів з контролю безпеки	**Г4**
		Здатність оцінювати всі процеси керування конфігурацією	**Г5**
		Здатність оцінювати адекватні засоби контролю доступу на основі принципів найменших привілеїв і необхідності отримання відповідної інформації	**Г6**
		Здатність оцінювати та контролювати процеси кібербезпеки, пов'язані з впровадженням системи та її тестуванням	**Г7**
Д	Координація діяльності із забезпечення безпеки інформаційно-телекомунікаційних систем	Здатність координувати роботу з персоналом із забезпечення кібербезпеки всієї організації для перевірки мережевих сповіщень	**Д1**
		Здатність надавати керівникам рекомендації щодо кібербезпеки	**Д2**
		Здатність надавати керівникам рекомендації щодо кібербезпеки на основі інформації про значні загрози та вразливості	**Д3**
		Здатність працювати із заінтересованими сторонами для усунення інцидентів	**Д4**

		кібербезпеки та забезпечення захисту відповідно до вимог щодо усунення вразливостей	
		Здатність надавати рекомендації до планів аварійного відновлення, непередбачених випадків та забезпечення безперервності операцій	**Д5**

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

Трудові функції	Предмети і засоби праці (обладнання, устаткування, матеріали, продукти, інструменти)	Професійні компетентності (за трудовою дією або групою трудових дій)	Знання	Уміння та навички
А. Організація аналітичної діяльності з безпеки інформаційно-телекомунікаційних систем	Нормативні акти, протоколи, стандарти та сертифікати відповідного спрямування; комп'ютерне, програмне та техніко-технологічне забезпечення; операційні системи; інтерпретовані і компільовані комп'ютерні мови; комп'ютерні алгоритми, алгоритми шифрування; бази даних; фізичні та логічні мережеві пристрої та інфраструктура, включно з концентраторами, комутаторами, маршрутизаторами,	**А1.** Здатність перевіряти наявність мінімальних вимог безпеки до всього програмного забезпечення.	**А1.31.** Концепції комп'ютерних мереж і протоколів, а також методології мережевої безпеки **А1.32.** Концепції архітектури мережевої безпеки, включно з топологією, протоколами, компонентами та принципами (застосування глибинного захисту) **А1.33.** Принципи кібербезпеки та приватності/конфіденційності **А1.34.** Принципи та методи безпеки інформаційних технологій (далі – ІТ) (брандмауери, демілітаризовані зони, шифрування) **А1.35.** Принципи глибинного захисту та архітектури мережевої безпеки **А1.36.** Принципи, моделі, методи управління мережевими системами (наскрізний моніторинг продуктивності систем) та інструменти **А1.37.** Принципи взаємодії людини з комп'ютером	**А1.У1.** Визначати, як має працювати система безпеки (включно з її стійкістю і надійністю) і вплив змін умов, операцій або середовища на ці результати **А1.У2.** Виявляти вторгнення на базі хоста та мережі за допомогою технологій виявлення вторгнень (Snort)

	брандмауерами, бездротові технології та засоби зв'язку (стільникові, супутникові, GSM-системи); IP-адреси, маршрутизація на основі безкласових IP-адрес, система нумерації TCP/UDP-портів, модель OSI і базові мережеві протоколи (протоколи TCP/IP), системи управління контентом Web-сайтів (CMS), SCADA системи, списки контролю доступу, списки повноважень, обладнання апаратного забезпечення мереж, засоби безпеки на хостах, прикладні програми (Open Web Application Security Project Top 10 list)		**А1.38.** Процеси управління ризиками (методи оцінювання та зменшення ризику) **А1.39.** Процеси встановлення, інтегрування, оптимізації компонентів системи **А1.310.** Конкретні операційні впливи за недостатності заходів з кібербезпеки **А1.311.** Категорії кіберзловмисників (дії зі сценаріями, інсайдерські загрози, фінансовані іншою державою) **А1.312.** Кіберзагрози та вразливості **А1.313.** Операційні системи **А1.314.** Методи системного адміністрування, мережевих та операційних систем **А1.315.** Моделі безпеки (модель Белла-ЛаПадули, модель цілісності Біби, модель цілісності Кларка-Вілсона) **А1.316.** Різні типи комп'ютерних архітектур **А1.317.** Загальні вектори атак на мережевому рівні **А1.318.** Політики, процедури та правила кіберзахисту та інформаційної безпеки **А1.319.** Стандарти безпеки персональних даних (PII) **А1.320.** Стандарти безпеки даних індустрії платіжних карток (PCI) **А1.321.** Стандарти безпеки даних персональної медичної інформації (PHI) **А1.322.** Закони, нормативні акти, політики та етика, які стосуються кібербезпеки та конфіденційності	

			А1.323. Закони, статути (Укази Президента, керівні принципи виконавчої влади та/або адміністративних/ кримінальних правових інструкцій та процедур) **А1.324.** Закони, правові повноваження, обмеження та правила, що стосуються діяльності з кіберзахисту **А1.325.** Алгоритми шифрування даних **А1.326.** Криптографія та концепції управління криптографічними ключами **А1.327.** Комп'ютерні мови, що інтерпретуються та компілюються **А1.328.** Процеси управління наборами, можливостей та обмежень **А1.329.** Методології шифрування даних **А1.330.** Ризики безпеки додатків (Open Web Application Security Project Top 10 list)	
		А2. Здатність здійснювати контроль за тим, щоб усі операції з безпеки та обслуговування системи (застосування виправлень безпеки) відповідали термінам, встановленим органом управління для передбачуваного операційного середовища	**А1.312.** Кіберзагрози та вразливості **А1.322.** Закони, нормативні акти, політики та етика, які стосуються кібербезпеки та конфіденційності **А1.323.** Закони, статути (Укази Президента, керівні принципи виконавчої влади та/або адміністративних/кримінальних правових інструкцій та процедур) **А2.31.** Концепції в управлінні безпекою (Release Management, Patch Management) **А2.32.** Результати дослідження внутрішніх загроз, звітності, інструментів дослідження та законів/норм **А2.33.** Нові IT та технології кібербезпеки	**А2.У1.** Розпізнавати та класифікувати типи вразливостей і пов'язаних з ними атак **А2.У2.** Використовувати методику обробки інцидентів

			А2.34. Структури звітності постачальника послуг кіберзахисту та процесів у власній організації	
		А3. Здатність застосовувати заходи безпеки для усунення вразливостей, здійснювати контроль за тим, що продукти з підтримкою функцій кібербезпеки або компенсаційні технології контролю безпеки знижують ідентифікований ризик до прийнятного рівня та рекомендувати зміни щодо безпеки	**А1.34.** Принципи та методи безпеки ІТ (брандмауери, демілітаризовані зони, шифрування) **А1.37.** Принципи взаємодії людини з комп'ютером **А1.38.** Процеси управління ризиками (методи оцінювання та зменшення ризику) **А1.312.** Кіберзагрози та вразливості **А1.318.** Політики, процедури та правила кіберзахисту та інформаційної безпеки **А2.31.** Концепції в управлінні безпекою (Release Management, Patch Management) **А3.31.** Системи управління базами даних **А3.32.** Загрози і вразливості безпеки системи та додатків (переповнення буфера, мобільний код, міжсайтові скрипти, мова процедур/структурована мова запитів [PL/SQL] та ін'єкції, умови протидії, прихований канал, повторення, атаки, орієнтовані на повернення, шкідливий код) **А3.33.** Процес розробки систем	**А2.У1.** Розпізнавати та класифікувати типи вразливостей і пов'язаних з ними атак **А3.У1.** Виявляти вторгнення на базі хоста та мережі з урахуванням місць ризику їх появи
		А4. Здатність інтегрувати автоматизовані можливості для оновлення або виправлення системного програмного забезпечення та розробляти процеси і	**А1.34.** Принципи та методи безпеки ІТ (брандмауери, демілітаризовані зони, шифрування) **А1.31.** Концепції комп'ютерних мереж і протоколів, а також методології мережевої безпеки **А1.312.** Кіберзагрози та вразливості **А1.313.** Операційні системи	**А4.У1.** Проєктувати, здійснювати інтеграцію апаратних та програмних рішень **А4.У2.** Писати код мовою програмування, що підтримується

		процедури для ручного оновлення та виправлення системного програмного забезпечення	**А1.330.** Ризики безпеки додатків (Open Web Application Security Project Top 10 list) **А2.33.** Нові ІТ та технології кібербезпеки **А4.31.** Інструменти, методи та прийоми проєктування систем безпеки **А4.32.** Процеси розробки систем **А4.33.** Розширення файлів (.dll, .bat, .zip, .pcap, .gzip)	
		А5. Здатність до вивчення топології мережі для усвідомлення потоків даних через мережу, забезпечувати інтеграцію та впровадження міждоменних рішень у безпечному середовищі	**А1.31.** Концепції комп'ютерних мереж і протоколів, а також методології мережевої безпеки **А1.32.** Концепції архітектури мережевої безпеки, включно з топологією, протоколами, компонентами та принципами (застосування глибинного захисту) **А1.34.** Принципи та методи безпеки ІТ (брандмауери, демілітаризовані зони, шифрування) **А1.35.** Принципи глибинного захисту та архітектури мережевої безпеки **А1.36.** Принципи, моделі, методи управління мережевими системами (наскрізний моніторинг продуктивності систем) та інструменти **А1.314.** Методи системного адміністрування, мережевих та операційних систем **А1.317.** Загальні вектори атак на мережевому рівні **А4.31.** Інструменти, методи та прийоми проєктування систем безпеки	**А2.У1.** Розпізнавати та класифікувати типи вразливостей і пов'язаних з ними атак **А5.У1.** Використовувати аналізатори протоколів

			А5.31. Телекомунікаційні концепції (канал зв'язку, наповнення системних каналів, спектральна ефективність, мультиплексування) **А5.32.** Безпека віртуальної приватної мережі (VPN) **А5.33.** Мережеві інструменти (ping, traceroute, nslookup) **А5.34.** Типи мережевого зв'язку (LAN, WAN, MAN, WLAN, WWAN) **А5.35.** Порти і служби Windows/Unix **А5.36.** Модель OSI та базові мережеві протоколи (TCP/IP) **А5.37.** Мережеві протоколи, такі як TCP/IP, динамічна конфігурація хоста, системи доменних імен (DNS) і служби каталогів	
		А6. Здатність усувати/мінімізувати недоліки безпеки, виявлені під час тестування безпеки/сертифікації, інформувати відповідальних працівників (відповідального керівника або уповноваженого представника) про підозрілі кіберінциденти та формалізувати історію	**А1.38.** Процеси управління ризиками (методи оцінювання та зменшення ризику) **А1.310.** Конкретні операційні впливи за недостатності заходів з кібербезпеки **А1.312.** Кіберзагрози та вразливості **А1.317.** Загальні вектори атак на мережевому рівні **А1.318.** Політики, процедури та правила кіберзахисту та інформаційної безпеки **А2.31.** Концепції в управлінні безпекою (Release Management, Patch Management) **А5.33.** Мережеві інструменти (ping, traceroute, nslookup)	**А1.У1.** Визначати, як має працювати система безпеки (включно з її стійкістю і надійністю) і вплив зміни умов, операцій або середовища на ці результати **А2.У1.** Розпізнавати та класифікувати типи вразливостей і пов'язаних із ними атак **А2.У2.** Використовувати методику обробки інцидентів

		події, статус і потенційний вплив для подальших дій відповідно до плану реагування на кіберінциденти організації (прийняти або обробити ризик)	**А6.31.** Механізми контролю доступу хоста/мережі (список контролю доступу, списки привілеїв) **А6.32.** Політики, вимоги та процедури управління ризиками інформаційних технологій (ІТ) **А6.33.** Принципи, інструменти та методи тестування на проникнення **А6.34.** Інструменти кіберзахисту та оцінювання вразливостей, їх можливостей **А6.35.** Джерела поширення інформації про вразливості (попередження, рекомендації, помилки та бюлетені) **А6.36.** Методології реагування на інциденти та їх обробки	
		А7. Здатність забезпечувати виконання аварійного відновлення та безперервність роботи, зокрема розробляти процедури та здійснювати тестування передачі операцій системи на альтернативний сайт на основі вимог доступності системи	**А1.31.** Концепції комп'ютерних мереж і протоколів, а також методології мережевої безпеки **А1.34.** Принципи та методи безпеки ІТ (брандмауери, демілітаризовані зони, шифрування) **А1.37.** Принципи взаємодії людини з комп'ютером **А1.310.** Конкретні операційні впливи за недостатності заходів з кібербезпеки **А1.313.** Операційні системи **А1.322.** Закони, нормативні акти, політики та етика, які стосуються кібербезпеки та конфіденційності **А3.31.** Системи управління базами даних **А5.31.** Телекомунікаційні концепції (канал зв'язку, наповнення системних каналів,	**А7.У1.** Читати та визначати приналежність електронних підписів **А7.У2.** Розробляти та розгортати інфраструктуру електронних підписів

			спектральна ефективність, мультиплексування) **А6.31.** Механізми контролю доступу хоста/мережі (список контролю доступу, списки привілеїв) **А7.31.** Методи тестування та оцінювання безпеки систем	
		А8. Здатність впроваджувати заходи безпеки системи відповідно до встановлених процедур, визначених тактик, технік для наборів вторгнень, для забезпечення конфіденційності, цілісності, доступності, аутентифікації та невідмовності	**А1.31.** Концепції комп'ютерних мереж і протоколів, а також методології мережевої безпеки **А1.34.** Принципи та методи безпеки ІТ (брандмауери, демілітаризовані зони, шифрування) **А1.35.** Принципи глибинного захисту та архітектури мережевої безпеки **А1.37.** Принципи взаємодії людини з комп'ютером **А1.310.** Конкретні операційні впливи за недостатності заходів з кібербезпеки **А1.311.** Категорії кіберзловмисників (дії зі сценаріями, інсайдерські загрози, фінансовані іншою державою) **А1.312.** Кіберзагрози та вразливості **А1.318.** Політики, процедури та правила кіберзахисту та інформаційної безпеки **А1.322.** Закони, нормативні акти, політики та етика, які стосуються кібербезпеки та конфіденційності **А2.31.** Концепції в управлінні безпекою (Release Management, Patch Management)	**А2.У1.** Розпізнавати та класифікувати типи вразливостей і пов'язаних з ними атак **А7.У2.** Розробляти та розгортати інфраструктуру електронних підписів **А8.У1.** Визначати, як має працювати система безпеки в умовах впровадження заходів безпеки системи відповідно до встановлених процедур, визначених тактик, технік для наборів вторгнень

			А6.31. Механізми контролю доступу хоста/мережі (список контролю доступу, списки привілеїв) **А6.34.** Інструменти кіберзахисту та оцінювання вразливостей, їх можливостей **А8.31.** Методи аутентифікації, авторизації та контролю доступу **А8.32.** Механізми доступу до мережі, ідентифікації та управління доступом (інфраструктура відкритих ключів, Oauth, OpenID, SAML, SPML) **А8.33.** Методології і прийоми виявлення вторгнень для виявлення вторгнень на базі хоста та мережі **А8.34.** Мережеві атаки, зв'язок мережевої атаки із загрозами та вразливими місцями **А8.35.** Вектори атаки на мережевому рівні **А8.36.** Етапи кібератак (розвідка, сканування, вибір вектору проникнення, отримання доступу, ескалація привілеїв, підтримка доступу, експлуатація мережі, приховування слідів)	
Б. Аналіз заходів і ситуації з безпекою інформаційно-телекомунікаційних систем	Нормативні акти, протоколи, стандарти та сертифікати відповідного спрямування; комп'ютерне, програмне та техніко-технологічне забезпечення; операційні системи; інтерпретовані	**Б1.** Здатність характеризувати та аналізувати мережевий трафік для виявлення аномальної активності (метадані), шкідливих дій, потенційних загроз мережевим ресурсам, слабких місць, методів	**А1.31.** Концепції комп'ютерних мереж і протоколів, а також методології мережевої безпеки **А1.34.** Принципи та методи безпеки ІТ (брандмауери, демілітаризовані зони, шифрування) **А1.312.** Кіберзагрози та вразливості **А1.313.** Операційні системи **А3.31.** Системи управління базами даних	**А2.У1.** Розпізнавати та класифікувати типи вразливостей і пов'язаних з ними атак **А5.У1.** Використовувати аналізатори протоколів **Б1.У1.** Виявляти вторгнення на базі хоста та мережі на основі

	і компільовані комп'ютерні мови; комп'ютерні алгоритми, алгоритми шифрування; бази даних; фізичні та логічні мережеві пристрої та інфраструктура, включно з концентраторами, комутаторами, маршрутизаторами, брандмауерами, бездротові технології та засоби зв'язку (стільникові, супутникові, GSM-системи); IP-адреси, маршрутизація на основі безкласових IP-адрес, система нумерації TCP/UDP-портів, модель OSI і базові мережеві протоколи (протоколи TCP/IP), системи управління контентом Web-сайтів (CMS), SCADA системи, списки контролю доступу, списки повноважень, обладнання апаратного	експлуатації, впливу на систему та інформацію	**А5.33.** Мережеві інструменти (ping, traceroute, nslookup) **А5.34.** Типи мережевого зв'язку (LAN, WAN, MAN, WLAN, WWAN) **А8.33.** Методології і прийоми виявлення вторгнень для виявлення вторгнень на базі хоста та мережі **А8.35.** Вектори атаки на мережевому рівні **Б1.32.** Методи аналізування мережевого трафіку	аналізування аномалій трафіку
		Б2. Здатність виконувати огляди безпеки та виявляти прогалини в архітектурі безпеки, що є приводом для розроблення рекомендацій щодо включення до стратегії зменшення ризику та розроблення плану управління ризиками безпеки	**А1.31.** Концепції комп'ютерних мереж і протоколів, а також методології мережевої безпеки **А1.35.** Принципи глибинного захисту та архітектури мережевої безпеки **А1.38.** Процеси управління ризиками (методи оцінювання та зменшення ризику) **А1.310.** Конкретні операційні впливи за недостатності заходів з кібербезпеки **А1.311.** Категорії кіберзловмисників (дії зі сценаріями, інсайдерські загрози, фінансовані іншою державою) **А1.312.** Кіберзагрози та вразливості **А1.317.** Загальні вектори атак на мережевому рівні **А1.318.** Політики, процедури та правила кіберзахисту та інформаційної безпеки **А6.31.** Механізми контролю доступу хоста/мережі (список контролю доступу, списки привілеїв) **А6.34.** Інструменти кіберзахисту та оцінювання вразливостей, їх можливостей	**А2.У1.** Розпізнавати та класифікувати типи вразливостей і пов'язаних з ними атак **Б2.У1.** Збирати дані з різноманітних ресурсів кіберзахисту **Б2.У2.** Знаходити вразливості в системах безпеки (перевірка вразливостей та відповідності)

	забезпечення мереж, засоби безпеки на хостах, прикладні програми (Open Web Application Security Project Top 10 list)		**А6.35.** Джерела поширення інформації про вразливості (попередження, рекомендації, помилки та бюлетні) **Б2.31.** Засоби управління доступом, що ґрунтуються на політиках та ризиках	
		Б3. Здатність аналізувати тенденції кіберзахисту та звітувати про отримання мережевих сповіщень з різних джерел в організації, вказуючи можливі причини таких повідомлень	**А1.31.** Концепції комп'ютерних мереж і протоколів, а також методології мережевої безпеки **А1.312.** Кіберзагрози та вразливості **А1.318.** Політики, процедури та правила кіберзахисту та інформаційної безпеки **А1.322.** Закони, нормативні акти, політики та етика, які стосуються кібербезпеки та конфіденційності **А2.33.** Нові IT та технології кібербезпеки **А3.32.** Загрози і вразливості безпеки системи та додатків (переповнення буфера, мобільний код, міжсайтові скрипти, мова процедур / структурована мова запитів [PL/SQL] та ін'єкції, умови протидії, прихований канал, повторення, атаки, орієнтовані на повернення, шкідливий код) **А6.35.** Джерела поширення інформації про вразливості (попередження, рекомендації, помилки та бюлетні) **А6.36.** Методології реагування на інциденти та їх обробки **А8.33.** Методології і прийоми виявлення вторгнень для виявлення вторгнень на базі хоста та мережі **Б1.32.** Методи аналізування мережевого трафіку	**А5.У1.** Використовувати аналізатори протоколів **Б2.У1.** Збирати дані з різноманітних ресурсів кіберзахисту **Б3.У1.** Проводити аналізування тенденцій

			Б3.31. Поняття мережевої атаки і зв'язок мережевої атаки із загрозами та вразливими місцями	
		Б4. Здатність забезпечувати своєчасне виявлення, ідентифікацію та попередження про можливі атаки/вторгнення, аномальні події та дії зі зловживання та відрізняти ці інциденти та події від штатної діяльності, проводячи дослідження, аналізування і кореляцію в широкому діапазоні всіх наборів вихідних даних (показання та попередження)	**А1.31.** Концепції комп'ютерних мереж і протоколів, а також методології мережевої безпеки **А1.34.** Принципи та методи безпеки ІТ (брандмауери, демілітаризовані зони, шифрування) **А1.312.** Кіберзагрози та вразливості **А1.313.** Операційні системи **А1.317.** Загальні вектори атак на мережевому рівні **А2.32.** Результати дослідження внутрішніх загроз, звітності, інструментів дослідження та законів/норм **А3.32.** Загрози і вразливості безпеки системи та додатків (переповнення буфера, мобільний код, міжсайтові скрипти, мова процедур / структурована мова запитів [PL/SQL] та ін'єкції, умови протидії, прихований канал, повторення, атаки, орієнтовані на повернення, шкідливий код) **А6.34.** Інструменти кіберзахисту та оцінювання вразливостей, їх можливостей **А6.35.** Джерела поширення інформації про вразливості (попередження, рекомендації, помилки та бюлетні) **А6.36.** Методології реагування на інциденти та їх обробки **А8.31.** Методи аутентифікації, авторизації та контролю доступу	**А1.У2.** Виявляти вторгнення на базі хоста та мережі за допомогою технологій виявлення вторгнень (Snort) **А2.У1.** Розпізнавати та класифікувати типи вразливостей і пов'язаних із ними атак **А2.У2.** Використовувати методику обробки інцидентів

			А8.33. Методології і прийоми виявлення вторгнень для виявлення вторгнень на базі хоста та мережі **А8.36.** Етапи кібератак (розвідка, сканування, вибір вектору проникнення, отримання доступу, ескалація привілеїв, підтримка доступу, експлуатація мережі, приховування слідів) **Б1.32.** Методи аналізування мережевого трафіку **Б4.31.** Тактики, прийоми і процедури протидії кіберінцидентам	
		Б5. Здатність перевіряти попередження системи виявлення вторгнень щодо мережевого трафіку за допомогою інструментів аналізування пакетів для локалізації та видалення шкідливого програмного забезпечення	**А1.31.** Концепції комп'ютерних мереж і протоколів, а також методології мережевої безпеки **А1.34.** Принципи та методи безпеки ІТ (брандмауери, демілітаризовані зони, *шифрування*) **А1.312.** Кіберзагрози та вразливості **А1.313.** Операційні системи **А3.32.** Загрози і вразливості безпеки системи та додатків (переповнення буфера, мобільний код, міжсайтові скрипти, мова процедур/структурована мова запитів [*PL/SQL*] та ін'єкції, умови протидії, прихований канал, повторення, атаки, орієнтовані на повернення, шкідливий код) **А4.33.** Розширення файлів (.dll, .bat, .zip, .pcap, .gzip) **А5.35.** Порти і служби Windows/Unix **А6.34.** Інструменти кіберзахисту та оцінювання вразливостей, їх можливостей	**А2.У2.** Використовувати методику обробки інцидентів **А5.У1.** Використовувати аналізатори протоколів **Б5.У1.** Виконувати аналізування трафіку на рівні пакетів

			А6.36. Методології реагування на інциденти та їх обробки **А8.33.** Методології і прийоми виявлення вторгнень для виявлення вторгнень на базі хоста та мережі **Б1.32.** Методи аналізування мережевого трафіку **Б5.31.** Методи аналізування трафіку на рівні пакетів з використанням відповідних інструментів (Wireshark, tcpdump) **Б5.32.** Інструменти і програми системи виявлення вторгнень (IDS)/системи попередження вторгнень (IPS) **Б5.33.** Комп'ютерні алгоритми **Б5.34.** Програмна інженерія **Б5.35.** Вбудовані системи	
		Б6. Здатність відновлювати втрачені дані чи інформацію про зловмисну атаку або дію на основі інформації щодо мережевого трафіку	**А1.31.** Концепції комп'ютерних мереж і протоколів, а також методології мережевої безпеки **А1.35.** Принципи глибинного захисту та архітектури мережевої безпеки **А1.310.** Конкретні операційні впливи за недостатності заходів з кібербезпеки **А1.312.** Кіберзагрози та вразливості **А6.34.** Інструменти кіберзахисту та оцінювання вразливостей, їх можливостей **А6.36.** Методології реагування на інциденти та їх обробки **А8.35.** Вектори атаки на мережевому рівні **А8.36.** Етапи кібератак (розвідка, сканування, вибір вектору проникнення, отримання доступу, ескалація привілеїв,	**А2.У1.** Розпізнавати та класифікувати типи вразливостей і пов'язаних із ними атак **Б1.У1.** Виявляти вторгнення на базі хоста та мережі на основі інформації щодо мережевого трафіку

			підтримка доступу, експлуатація мережі, приховування слідів) **Б3.31.** Поняття мережевої атаки і зв'язок мережевої атаки із загрозами та вразливими місцями	
		Б7. Здатність надавати допомогу в створенні сигнатур, які можна реалізувати в мережевих інструментах кіберзахисту у відповідь на нові або спостережувані загрози в мережевому середовищі	**А1.31.** Концепції комп'ютерних мереж і протоколів, а також методології мережевої безпеки **А1.312.** Кіберзагрози та вразливості **А1.313.** Операційні системи **А1.325.** Алгоритми шифрування даних **А1.329.** Методології шифрування даних **А2.34.** Структури звітності постачальника послуг кіберзахисту та процесів у власній організації **А6.35.** Джерела поширення інформації про вразливості (попередження, рекомендації, помилки та бюлетні) **А8.33.** Методології і прийоми виявлення вторгнень для виявлення вторгнень на базі хоста та мережі **А8.36.** Етапи кібератак (розвідка, сканування, вибір вектору проникнення, отримання доступу, ескалація привілеїв, підтримка доступу, експлуатація мережі, приховування слідів) **Б5.33.** Комп'ютерні алгоритми **Б7.31.** Вплив реалізації сигнатур для вірусів, шкідливих програм і атак **Б7.32.** Криптографія та концепції управління криптографічними ключами	**Б7.У1.** Проєктувати, інтегрувати апаратні та програмні рішення

В. Аналіз упереджувальних/ розвідувальних заходів з безпеки інформаційно-телекомунікаційних систем	Нормативні акти, протоколи, стандарти та сертифікати відповідного спрямування; комп'ютерне, програмне та техніко-технологічне забезпечення; операційні системи; інтерпретовані і компільовані комп'ютерні мови; комп'ютерні алгоритми, алгоритми щифрування; бази даних; фізичні та логічні мережеві пристрої та інфраструктура, включно з концентраторами, комутаторами, маршрутизаторами, брандмауерами, бездротові технології та засоби зв'язку (стільникові, супутникові, GSM-системи); IP-адреси, маршрутизація на основі безкласових IP-адрес, система нумерації TCP/UDP-портів, модель	**В1.** Здатність застосовувати принципи сервісно-орієнтованої архітектури безпеки, щоб відповідати вимогам організації до конфіденційності, цілісності та доступності	**А1.312.** Кіберзагрози та вразливості **А1.315.** Моделі безпеки (модель Белла-ЛаПадули, модель цілісності Біби, модель цілісності Кларка-Вілсона) **А1.318.** Політики, процедури та правила кіберзахисту та інформаційної безпеки **А1.319.** Стандарти безпеки персональних даних (PII) **А1.320.** Стандарти безпеки даних індустрії платіжних карток (PCI) **А1.321.** Стандарти безпеки даних персональної медичної інформації (PHI) **А2.33.** Нові IT та технології кібербезпеки **А3.31.** Системи управління базами даних **А4.31.** Інструменти, методи та прийоми проєктування систем безпеки **А6.31.** Механізми контролю доступу хоста/мережі (список контролю доступу, списки привілеїв) **А8.31.** Методи аутентифікації, авторизації та контролю доступу	**А7.У2.** Розробляти та розгортати інфраструктуру електронних підписів **Б7.У1.** Проєктувати, інтегрувати апаратні та програмні рішення
		В2. Здатність впроваджувати конкретні контрзаходи з кіберзахисту (операцій і технічного обслуговування системи) для систем та/або програм, їх документування та оновлення, у разі потреби	**А1.310.** Конкретні операційні впливи за недостатності заходів з кібербезпеки **А1.312.** Кіберзагрози та вразливості **А1.313.** Операційні системи **А1.322.** Закони, нормативні акти, політики та етика, які стосуються кібербезпеки та конфіденційності **А3.32.** Загрози і вразливості безпеки системи та додатків (переповнення буфера, мобільний код, міжсайтові скрипти, мова процедур / структурована мова запитів	**А7.У2.** Розробляти та розгортати інфраструктуру електронних підписів **Б7.У1.** Проєктувати, інтегрувати апаратні та програмні рішення **В2.У1.** Визначати, як має працювати система безпеки за впровадження

	OSI і базові мережеві протоколи (протоколи TCP/IP), системи управління контентом Web-сайтів (CMS), SCADA системи, списки контролю доступу, списки повноважень, обладнання апаратного забезпечення мереж, засоби безпеки на хостах, прикладні програми (Open Web Application Security Project Top 10 list)		[PL/SQL] та ін'єкції, умови протидії, прихований канал, повторення, атаки, орієнтовані на повернення, шкідливий код) **А4.33.** Розширення файлів (.dll, .bat, .zip, .pcap, .gzip) **А6.34.** Інструменти кіберзахисту та оцінювання вразливостей, їх можливостей **А8.31.** Методи аутентифікації, авторизації та контролю доступу **А8.32.** Механізми доступу до мережі, ідентифікації та управління доступом (інфраструктура відкритих ключів, Oauth, OpenID, SAML, SPML) **А8.36.** Етапи кібератак (розвідка, сканування, вибір вектору проникнення, отримання доступу, ескалація привілеїв, підтримка доступу, експлуатація мережі, приховування слідів) **Б3.31.** Поняття мережевої атаки і зв'язок мережевої атаки із загрозами та вразливими місцями **В2.31.** Процеси розробки контрзаходів для виявлених ризиків безпеки	конкретних контрзаходів з кіберзахисту (операцій та технічного обслуговування системи) **В2.У2.** Використовувати структуру та процеси звітності постачальника послуг кіберзахисту у власній організації
		В3. Здатність документувати та передавати інформацію про інциденти, які можуть спричинити поточний і негайний вплив на навколишнє середовище; рекомендувати та	**А1.35.** Принципи глибинного захисту та архітектури мережевої безпеки **А1.38.** Процеси управління ризиками (методи оцінювання та зменшення ризику) **А1.310.** Конкретні операційні впливи за недостатності заходів з кібербезпеки **А1.312.** Кіберзагрози та вразливості **А1.318.** Політики, процедури та правила кіберзахисту та інформаційної безпеки	**А2.У1.** Розпізнавати та класифікувати типи вразливостей і пов'язаних із ними атак **Б7.У1.** Проєктувати, інтегрувати апаратні та програмні рішення **В2.У2.** Використовувати структуру та процеси

		планувати заходи з усунення вразливостей комп'ютерного середовища за результатами оцінювання наявних заходів та/або поведінки системного середовища	**А1.322.** Закони, нормативні акти, політики та етика, які стосуються кібербезпеки та конфіденційності **А1.323.** Закони, статути (Укази Президента, керівні принципи виконавчої влади та/або адміністративних/ кримінальних правових інструкцій та процедур) **А6.35.** Джерела поширення інформації про вразливості (попередження, рекомендації, помилки та бюлетні) **А6.36.** Методології реагування на інциденти та їх обробки	звітності постачальника послуг кіберзахисту у власній організації **В3.У1.** Визначати, як має працювати система безпеки за наявності факторів, які можуть спричинити поточний і негайний вплив на навколишнє середовище
		В4. Здатність виконувати кореляцію подій, використовуючи інформацію, зібрану з різних джерел на підприємстві, щоб досягти усвідомлення ситуації та визначити ефективність спостережуваної атаки	**А1.34.** Принципи та методи безпеки ІТ (брандмауери, демілітаризовані зони, шифрування) **А1.38.** Процеси управління ризиками (методи оцінювання та зменшення ризику) **А2.34.** Структури звітності постачальника послуг кіберзахисту та процесів у власній організації **А8.33.** Методології і прийоми виявлення вторгнень для виявлення вторгнень на базі хоста та мережі	**Б2.У1.** Збирати дані з різноманітних ресурсів кіберзахисту **Б5.У1.** Виконувати аналізування трафіку на рівні пакетів
		В5. Здатність проводити тестування кібербезпеки розроблених додатків та/або систем, надавати вхідні дані для технологічних процесів системи управління ризиками	**А1.35.** Принципи глибинного захисту та архітектури мережевої безпеки **А1.38.** Процеси управління ризиками (методи оцінювання та зменшення ризику) **А1.310.** Конкретні операційні впливи за недостатності заходів з кібербезпеки **А1.312.** Кіберзагрози та вразливості **А1.313.** Операційні системи	**Б2.У1.** Збирати дані з різноманітних ресурсів кіберзахисту **В5.У1.** Виявляти вторгнення на базі хоста та мережі шляхом тестування кібербезпеки розроблених додатків та/або систем

			А1.318. Політики, процедури та правила кіберзахисту та інформаційної безпеки **А1.327.** Комп'ютерні мови, що інтерпретуються та компілюються **А2.34.** Структури звітності постачальника послуг кіберзахисту та процесів у власній організації **А3.31.** Системи управління базами даних **А3.32.** Загрози і вразливості безпеки системи та додатків (переповнення буфера, мобільний код, міжсайтові скрипти, мова процедур/структурована мова запитів [PL/SQL] та ін'єкції, умови протидії, прихований канал, повторення, атаки, орієнтовані на повернення, шкідливий код) **А6.31.** Механізми контролю доступу хоста/мережі (список контролю доступу, списки привілеїв) **А6.34.** Інструменти кіберзахисту та оцінювання вразливостей, їх можливостей **А6.35.** Джерела поширення інформації про вразливості (попередження, рекомендації, помилки та бюлетні) **Б3.31.** Поняття мережевої атаки і зв`язок мережевої атаки із загрозами та вразливими місцями **Б5.33.** Комп'ютерні алгоритми **Б5.34.** Програмна інженерія	
		В6. Здатність перевіряти та оновлювати документацію з безпеки, яка відображає	**А1.322.** Закони, нормативні акти, політики та етика, які стосуються кібербезпеки та конфіденційності	**А1.У1.** Визначати, як має працювати система безпеки (включно з її стійкістю і надійністю) і

		особливості проєктування безпеки програми/системи	**А4.31.** Інструменти, методи та прийоми проєктування систем безпеки	вплив зміни умов, операцій або середовища на ці результати **В2.У2.** Використовувати структуру та процеси звітності постачальника послуг кіберзахисту у власній організації
		В7. Здатність визначати програмне забезпечення та операційні системи мережевого пристрою на основі мережевого трафіку, визначати відображення мережі та дії операційної системи	**А1.31.** Концепції комп'ютерних мереж і протоколів, а також методології мережевої безпеки **А1.34.** Принципи та методи безпеки ІТ (брандмауери, демілітаризовані зони, шифрування) **А2.33.** Нові ІТ та технології кібербезпеки **А8.33.** Методології і прийоми виявлення вторгнень для виявлення вторгнень на базі хоста та мережі **В7.31.** Методи формалізації відображення мережі та відтворення мережевих топологій **В7.32.** Інструменти командного рядка операційної системи	**А5.У1.** Використовувати аналізатори протоколів **Б5.У1.** Виконувати аналізування трафіку на рівні пакетів
		В8. Здатність відстежувати зовнішні джерела даних (сайти постачальників послуг кіберзахисту, команди реагування на комп'ютерні надзвичайні події, фокус безпеки) для	**А1.31.** Концепції комп'ютерних мереж і протоколів, а також методології мережевої безпеки **А1.38.** Процеси управління ризиками (методи оцінювання та зменшення ризику) **А1.310.** Конкретні операційні впливи за недостатності заходів з кібербезпеки **А1.312.** Кіберзагрози та вразливості	**Б2.У1.** Збирати дані з різноманітних ресурсів кіберзахисту **Б3.У1.** Проводити аналізування тенденцій **В8.У1** Визначати, як має працювати система

		підтримання актуальності стану системи з урахуванням загроз кіберзахисту та визначати, які проблеми безпеки можуть вплинути на організацію	**А2.34.** Структури звітності постачальника послуг кіберзахисту та процесів у власній організації **А6.34.** Інструменти кіберзахисту та оцінювання вразливостей, їх можливостей **А6.35.** Джерела поширення інформації про вразливості (попередження, рекомендації, помилки та бюлетні) **В8.31.** Зовнішні системи збору даних, включно зі збором, фільтрацією та вибором трафіку	безпеки з урахуванням загроз кіберзахисту
Г. Проведення моніторингу та оцінювання діяльності із забезпечення безпеки інформаційно-телекомунікаційних систем	Нормативні акти, протоколи, стандарти та сертифікати відповідного спрямування; комп'ютерне, програмне та техніко-технологічне забезпечення; операційні системи; інтерпретовані і компільовані комп'ютерні мови; комп'ютерні алгоритми, алгоритми шифрування; бази даних; фізичні та логічні мережеві пристрої та інфраструктура, включно з концентраторами, комутаторами, маршрутизаторами,	**Г1.** Здатність розробляти контент для засобів кіберзахисту	**А1.35.** Принципи глибинного захисту та архітектури мережевої безпеки **А1.310.** Конкретні операційні впливи за недостатності заходів з кібербезпеки **А1.312.** Кіберзагрози та вразливості **А1.317.** Загальні вектори атак на мережевому рівні **А2.32.** Результати дослідження внутрішніх загроз, звітності, інструментів дослідження та законів/норм **А3.31.** Системи управління базами даних **А6.34.** Інструменти кіберзахисту та оцінювання вразливостей, їх можливостей **А6.35.** Джерела поширення інформації про вразливості (попередження, рекомендації, помилки та бюлетні) **Б5.33.** Комп'ютерні алгоритми **Б5.34.** Програмна інженерія **В8.31.** Зовнішні системи збору даних, включно зі збором, фільтрацією та вибором трафіку	**А5.У1.** Використовувати аналізатори протоколів

	брандмауерами, бездротові технології та засоби зв'язку (стільникові, супутникові, GSM-системи); IP-адреси, маршрутизація на основі безкласових IP-адрес, система нумерації TCP/UDP-портів, модель OSI і базові мережеві протоколи (протоколи TCP/IP), системи управління контентом Web-сайтів (CMS), SCADA системи, списки контролю доступу, списки повноважень, обладнання апаратного забезпечення мереж, засоби безпеки на хостах, прикладні програми (Open Web Application Security Project Top 10 list)	**Г2.** Здатність надавати щоденні зведені звіти про мережеві події та діяльність, що стосуються практичних заходів кіберзахисту	**А1.31.** Концепції комп'ютерних мереж і протоколів, а також методології мережевої безпеки **А1.318.** Політики, процедури та правила кіберзахисту та інформаційної безпеки **А8.33.** Методології і прийоми виявлення вторгнень для виявлення вторгнень на базі хоста та мережі	**А5.У1.** Використовувати аналізатори протоколів **Б2.У1.** Збирати дані з різноманітних ресурсів кіберзахисту **Б5.У1.** Виконувати аналізування трафіку на рівні пакетів
		Г3. Здатність використовувати інструменти кіберзахисту для постійного моніторингу та аналізування системної активності для виявлення зловмисної діяльності	**А1.31.** Концепції комп'ютерних мереж і протоколів, а також методології мережевої безпеки **А1.34.** Принципи та методи безпеки IT (брандмауери, демілітаризовані зони, шифрування) **А1.313.** Операційні системи **А6.34.** Інструменти кіберзахисту та оцінювання вразливостей, їх можливостей **А8.33.** Методології і прийоми виявлення вторгнень для виявлення вторгнень на базі хоста та мережі **А8.35.** Вектори атаки на мережевому рівні **А8.36.** Етапи кібератак (розвідка, сканування, вибір вектору проникнення, отримання доступу, ескалація привілеїв, підтримка доступу, експлуатація мережі, приховування слідів) **Б2.31.** Засоби управління доступом, що ґрунтуються на політиках та ризиках **Г3.31.** Використання методів та процедур моніторингу в рамках підмережі	**А5.У1.** Використовувати аналізатори протоколів

		Г4. Здатність оцінювати ефективність заходів з контролю безпеки	**А1.37.** Принципи взаємодії людини з комп'ютером **А1.38.** Процеси управління ризиками (методи оцінювання та зменшення ризику) **А1.310.** Конкретні операційні впливи за недостатності заходів з кібербезпеки **А1.312.** Кіберзагрози та вразливості **А1.318.** Політики, процедури та правила кіберзахисту та інформаційної безпеки **А6.31.** Механізми контролю доступу хоста/мережі (список контролю доступу, списки привілеїв) **А6.33.** Принципи, інструменти та методи тестування на проникнення **А6.34.** Інструменти кіберзахисту та оцінювання вразливостей, їх можливостей **А7.31.** Методи тестування та оцінювання безпеки систем **А8.31.** Методи аутентифікації, авторизації та контролю доступу **Г4.31.** Різні класи атак (пасивні, активні, інсайдерські, суміжні, розподільні атаки)	**Г4.У1.** Оцінювати адекватність проєктів безпеки **Г4.У2.** Оцінювати системи безпеки **Г4.У3.** Оцінювати засоби контролю безпеки на основі принципів кібербезпеки. (CIS, NIST SP 800-53, Cybersecurity Framework)
		Г5. Здатність оцінювати всі процеси керування конфігурацією	**А1.38.** Процеси управління ризиками (методи оцінювання та зменшення ризику) **А1.312.** Кіберзагрози та вразливості **А1.313.** Операційні системи **А2.31.**Концепції в управлінні безпекою (Release Management, Patch Management) **А2.33.** Нові IT та технології кібербезпеки **Б5.33.** Комп'ютерні алгоритми	**Г4.У3.** Оцінювати засоби контролю безпеки на основі принципів кібербезпеки. (CIS, NIST SP 800-53, Cybersecurity Framework) **Г5.У1.** Оцінювати адекватність проєктів безпеки стосовно

				процесів керування конфігурацією
		Г6. Здатність оцінювати адекватні засоби контролю доступу на основі принципів найменших привілеїв і необхідності отримання відповідної інформації	**А1.315.** Моделі безпеки (модель Белла-ЛаПадули, модель цілісності Біби, модель цілісності Кларка-Вілсона) **А1.325.** Алгоритми шифрування даних **А3.31.** Системи управління базами даних **А6.34.** Інструменти кіберзахисту та оцінювання вразливостей, їх можливостей **А8.31.** Методи аутентифікації, авторизації та контролю доступу **Б7.32.** Криптографія та концепції управління криптографічними ключами **Г4.31.** Різні класи атак (пасивні, активні, інсайдерські, суміжні, розподільні атаки)	**Г4.У1.** Оцінювати адекватність проєктів безпеки **Г4.У3.** Оцінювати засоби контролю безпеки на основі принципів кібербезпеки. (CIS, NIST SP 800-53, Cybersecurity Framework)
		Г7. Здатність оцінювати та контролювати процеси кібербезпеки, пов'язані з впровадженням системи та її тестуванням	**А1.38.** Процеси управління ризиками (методи оцінювання та зменшення ризику) **А1.310.** Конкретні операційні впливи за недостатності заходів з кібербезпеки **А1.312.** Кіберзагрози та вразливості **А1.322.** Закони, нормативні акти, політики та етика, які стосуються кібербезпеки та конфіденційності **А6.33.** Принципи, інструменти та методи тестування на проникнення **А6.34.** Інструменти кіберзахисту та оцінювання вразливостей, їх можливостей **А7.31.** Методи тестування та оцінювання безпеки систем	**Г4.У1.** Оцінювати адекватність проєктів безпеки **Г7.У2.** Оцінювати засоби контролю безпеки на основі принципів кібербезпеки. (CIS CIS, NIST SP 800-53, Cybersecurity Framework)
Д. Координація діяльності із забезпечення	Нормативні акти, протоколи, стандарти та сертифікати	**Д1.** Здатність координувати роботу з персоналом із	**А1.310.** Конкретні операційні впливи за недостатності заходів з кібербезпеки	**В2.У2.** Використовувати структуру та процеси звітності постачальника

безпеки інформаційно-телекомунікаційних систем	відповідного спрямування; комп'ютерне, програмне та техніко-технологічне забезпечення; операційні системи; інтерпретовані і компільовані комп'ютерні мови; комп'ютерні алгоритми, алгоритми шифрування; бази даних; фізичні та логічні мережеві пристрої та інфраструктура, включно з концентраторами, комутаторами, маршрутизаторами, брандмауерами, бездротові технології та засоби зв'язку (стільникові, супутникові, GSM-системи); IP-адреси, маршрутизація на основі безкласових IP-адрес, система нумерації TCP/UDP-портів, модель OSI і базові мережеві протоколи (протоколи	забезпечення кібербезпеки всієї організації для перевірки мережевих сповіщень	**А1.315.** Моделі безпеки (модель Белла-ЛаПадули, модель цілісності Біби, модель цілісності Кларка-Вілсона) **А1.322.** Закони, нормативні акти, політики та етика, які стосуються кібербезпеки та конфіденційності **А1.323.** Закони, статути (Укази Президента, керівні принципи виконавчої влади та/або адміністративних/ кримінальних правових інструкцій та процедур) **Г4.31.** Різні класи атак (пасивні, активні, інсайдерські, суміжні, розподільні атаки) **Д1.31.** Процеси управління безпекою	послуг кіберзахисту у власній організації **Г7.У2.** Оцінювати засоби контролю безпеки на основі принципів кібербезпеки. (CIS CIS, NIST SP 800-53, Cybersecurity Framework)
		Д2. Здатність надавати керівникам рекомендації щодо кібербезпеки	**А1.33.** Принципи кібербезпеки та приватності/конфіденційності **А1.34.** Принципи та методи безпеки ІТ (брандмауери, демілітаризовані зони, шифрування) **А1.38.** Процеси управління ризиками (методи оцінювання та зменшення ризику) **А1.310.** Конкретні операційні впливи за недостатності заходів з кібербезпеки **А1.312.** Кіберзагрози та вразливості **А1.315.** Моделі безпеки (модель Белла-ЛаПадули, модель цілісності Біби, модель цілісності Кларка-Вілсона) **А1.322.** Закони, нормативні акти, політики та етика, які стосуються кібербезпеки та конфіденційності **А1.323.** Закони, статути (Укази Президента, керівні принципи виконавчої влади та/або	**Б7.У1.** Проєктувати, інтегрувати апаратні та програмні рішення **Г4.У1.** Оцінювати адекватність проєктів безпеки

	TCP/IP), системи управління контентом Web-сайтів (CMS), SCADA системи, списки контролю доступу, списки повноважень, обладнання апаратного забезпечення мереж, засоби безпеки на хостах, прикладні програми (Open Web Application Security Project Top 10 list)		адміністративних/ кримінальних правових інструкцій та процедур) **А3.32.** Загрози і вразливості безпеки системи та додатків (переповнення буфера, мобільний код, міжсайтові скрипти, мова процедур/структурована мова запитів [PL/SQL] та ін'єкції, умови протидії, прихований канал, повторення, атаки, орієнтовані на повернення, шкідливий код) **А8.31.** Методи аутентифікації, авторизації та контролю доступу **Г4.31.** Різні класи атак (пасивні, активні, інсайдерські, суміжні, розподільні атаки) **Д1.31.** Процеси управління безпекою	
		Д3. Здатність надавати керівникам рекомендації щодо кібербезпеки на основі інформації про значні загрози та вразливості	**А1.34.** Принципи та методи безпеки ІТ (брандмауери, демілітаризовані зони, шифрування) **А1.38.** Процеси управління ризиками (методи оцінювання та зменшення ризику) **А1.310.** Конкретні операційні впливи за недостатності заходів із кібербезпеки **А1.312.** Кіберзагрози та вразливості **А1.315.** Моделі безпеки (модель Белла-ЛаПадули, модель цілісності Біби, модель цілісності Кларка-Вілсона) **А1.322.** Закони, нормативні акти, політики та етика, які стосуються кібербезпеки та конфіденційності **А1.323.** Закони, статути (Укази Президента, керівні принципи виконавчої влади та/або адміністративних/ кримінальних правових інструкцій та процедур)	**Б2.У1.** Збирати дані з різноманітних ресурсів кіберзахисту **Б7.У1.** Проєктувати, інтегрувати апаратні та програмні рішення

			А8.31. Методи аутентифікації, авторизації та контролю доступу **Г4.31.** Різні класи атак (пасивні, активні, інсайдерські, суміжні, розподільні атаки)	
		Д4. Здатність працювати із заінтересованими сторонами для усунення інцидентів кібербезпеки та забезпечення захисту відповідно до вимог щодо усунення вразливостей	**А1.310.** Конкретні операційні впливи за недостатності заходів з кібербезпеки **А1.312.** Кіберзагрози та вразливості **А1.322.** Закони, нормативні акти, політики та етика, які стосуються кібербезпеки та конфіденційності	**Б2.У1.** Збирати дані з різноманітних ресурсів кіберзахисту **В2.У2.** Використовувати структуру та процеси звітності постачальника послуг кіберзахисту у власній організації
		Д5. Здатність надавати рекомендації до планів аварійного відновлення, непередбачених випадків та забезпечення безперервності операцій	**А1.38.** Процеси управління ризиками (методи оцінювання та зменшення ризику) **А1.310.** Конкретні операційні впливи за недостатності заходів з кібербезпеки **А1.312.** Кіберзагрози та вразливості **А1.322.** Закони, нормативні акти, політики та етика, які стосуються кібербезпеки та конфіденційності **Д1.31.** Процеси управління безпекою	**Б7.У1.** Проєктувати, інтегрувати апаратні та програмні рішення **Г4.У1.** Оцінювати адекватність проєктів безпеки

7. Дані щодо розроблення та затвердження професійного стандарту

7.1. Розробники проєкту професійного стандарту

Державна служба спеціального зв'язку та захисту інформації України.

Склад робочої групи:

Петрушкевич Олександр Володимирович, керівник робочої групи, заступник начальника Державного центру кіберзахисту Держспецзв'язку;

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

Гнатюк Сергій Леонідович, головний консультант відділу інформаційної безпеки та кібербезпеки Центру безпекових досліджень Національного інституту стратегічних досліджень;

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

Давидюк Андрій Вікторович, заступник начальника 1 відділу 4 управління Державного центру кіберзахисту Держспецзв'язку;

Жилін Артем Вікторович, начальник 6 управління Державного центру кіберзахисту Держспецзв'язку;

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

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

Лебеденко Кіра Сергіївна, директор ТОВ «СЕК'ЮРИТІ ЕКСПЕРТ ГРУП ЕКЕДЕМІ»;

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

Мазур Наталя Володимирівна, завідуюча відділом організаційно-правової роботи Профспілки працівників зв'язку України (за згодою);

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

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

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

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

Філіпова Ольга Валентинівна, комерційний директор компанії SAYCOM;

Чевардін Владислав Євгенійович, начальник кафедри кібербезпеки Військового інституту телекомунікацій та інформаційних імені героїв Крут;

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

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

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

7.2. Суб'єкт перевірки професійного стандарту

Національне агентство кваліфікацій.

7.3. Дата затвердження професійного стандарту

25 листопада 2022 року.

7.4. Рекомендована дата наступного перегляду професійного стандарту

25 листопада 2027 року.

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