Проєкт

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

ПРОФЕСІЙНИЙ СТАНДАРТ
«Аналітик з безпеки інформаційно-телекомунікаційних систем»

1. Загальні відомості

1.1. Основна мета професійної діяльності

Збирання, оброблення, аналізування та поширення результатів оцінювання кіберзагроз/сигналів попередження. Дослідження, аналізування 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 за КВЕД-2010 «Класифікація видів економічної діяльності»)

Секція	Назва секції	№ розділу	Назва розділу	№ групи (класу)	Назва групи (класу)
J	Інформація та телекомунікації	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	
		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 устаткованням
				Клас 62.09	Інша діяльність у сфері інформаційних технологій і комп'ютерних систем
		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
M	Професійна, наукова та технічна діяльність	74	Інша професійна, наукова та технічна діяльність	Група 74.9	Інша професійна, наукова та технічна діяльність, н.в.і.у
				Клас 74.90	

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

Розділ	**Підрозділ**	**Клас**	**Підклас**	**Група**
2	21	213	2139	2139.2
Професіонали	Професіонали в галузі фізичних, математичних та технічних наук	Професіонали в галузі обчислень (комп'ютеризації)	Професіонали в інших галузях обчислень (комп'ютеризації)	Професіонали в інших галузях обчислень

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)

Структурний підрозділ підприємства/організації, профільний структурний підрозділ підприємства/організації із захисту інформації та кіберзахисту.

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 аналітика з безпеки інформаційно-телекомунікаційних систем і провідного аналітика з безпеки інформаційно-телекомунікаційних систем – диплом магістра галузі знань 12 «Інформаційні технології» (7 рівень НРК) та 3 роки досвіду роботи за спеціальністю.

2. Навчання та професійний розвиток

2.1. Первинна професійна підготовка (назва кваліфікації)

Для аналітика з безпеки інформаційно-телекомунікаційних систем і провідного аналітика з безпеки інформаційно-телекомунікаційних систем підготовка на другому (магістерському) рівні вищої освіти 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);
- 124 «Системний аналіз» галузі знань 12 «Інформаційні технології» (7 рівень НРК);
- 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» (7 рівень НРК);
- 126 «Інформаційні системи та технології» галузі знань 12 «Інформаційні технології» (7 рівень НРК).

2.2. Підвищення кваліфікації без присвоєння нового рівня освіти

Підвищення кваліфікації аналітика 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

Закон України «Про інформацію»;

Закон України «Про державну таємницю»;

Закон України «Про доступ до публічної інформації»;

Закон України «Про захист персональних даних»;

Закон України «Про основні засади забезпечення кібербезпеки України»;

Закон України «Про критичну інфраструктуру»;

Закон України «Про захист прав споживачів";

Кодекс законів про працю України;

Постанова Кабінету Міністрів України від 29 березня 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 № 660 «Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»;

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

Наказ Адміністрації Держспецзв'язку від 06.10.2021 № 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 за № 132 «Про Порядок опрацювання і затвердження роботодавцем нормативних актів з охорони праці, що діють на підприємстві», зареєстрований у Міністерстві юстиції України 07.02.1994 за № 20/229.

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

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

Нормативні документи в галузі технічного захисту інформації (НД ТЗІ) щодо створення комплексних систем захисту інформації;

Державні стандарти України (ДСТУ) щодо впровадження систем керування інформаційною безпекою;

Галузеві стандарти в сфері інформаційної та кібербезпеки;

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

4. Загальні компетентності

ЗК.01	Здатність використовувати у професійній діяльності знання законів та підзаконних нормативно-правових актів України, нормативних і нормативно-технічних документів, галузевих стандартів в сфері інформаційної та кібербезпеки
ЗК.02	Здатність застосовувати у практичних ситуаціях знання та розуміння предметної області та розуміння професії
ЗК.03	Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово
ЗК.04	Здатність виявляти, ставити та вирішувати проблеми за професійним спрямуванням
ЗК.05	Здатність до пошуку, оброблення та аналізу інформації.
ЗК.06	Здатність оцінювати та забезпечувати якість виконуваних робіт.
ЗК.07	Здатність до адаптації та дії у новій ситуації
ЗК.08	Здатність до вибору стратегії спілкування, працювати в

	команді
ЗК.09	Здатність дотримуватися правил та норм з безпеки та охорони праці, зокрема щодо безпечної експлуатації електронного устаткування та електричного обладнання
ЗК.10	Здатність до абстрактного мислення, аналізу та синтезу, вчитися і бути сучасно навченим
ЗК.11	Здатність до аналізування шкідливого програмного забезпечення
ЗК.12	Здатність проводити сканування на вразливості і розпізнавати вразливості в системах безпеки інформації
ЗК.13	Здатність точно і повністю отримувати всі дані, що використовуються в роботі засобів розвідки, оцінювання та/або планування
ЗК.14	Здатність застосовувати принципи кібербезпеки та конфіденційності до організаційних вимог
ЗК.15	Здатність застосовувати методи виявлення вторгнень на базі хоста та мережі за допомогою технологій виявлення вторгнень
ЗК.16	Здатність інтерпретувати інформацію, зібрану інструментами моніторингу мережі

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

Умовні позначення	**Трудові функції**	**Професійні компетентності (за трудовою дією або групою трудових дій)**	**Умовні позначення**
А	Організація аналітичної діяльності з безпеки інформаційно-телекомунікаційних систем	Здатність застосовувати політику безпеки до програм, які взаємодіють одна з одною, перевіряти наявність мінімальних вимог безпеки до всього програмного забезпечення для досягнення цілей безпеки системи.	А 1
		Здатність здійснювати контроль за тим, що всі операції з безпеки та обслуговування системи (застосування виправлень безпеки тощо) належним чином задокументовані та оновлені і відповідають термінам, встановленим органом управління для передбачуваного операційного середовища	А 2
		Здатність застосовувати заходи безпеки для усунення вразливостей, здійснювати контроль за тим, що	А 3

		продукти з підтримкою функцій кібербезпеки або інші компенсаційні технології контролю безпеки знижують ідентифікований ризик до прийнятного рівня та рекомендувати зміни щодо безпеки.	
		Здатність інтегрувати автоматизовані можливості для оновлення або виправлення системного програмного забезпечення та розроблювати процеси і процедури для ручного оновлення та виправлення системного програмного забезпечення	А 4
		Здатність до вивчення топології мережі для усвідомлення потоків даних через мережу, забезпечувати інтеграцію та впровадження міждоменних рішень у безпечному середовищі	А 5
		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 та потенційний вплив для подальших дій відповідно до плану реагування на кіберінциденти організації (прийняти або обробити ризик).	А 6
		Здатність забезпечувати виконання аварійного відновлення та безперервність роботи, в тому числі розроблювати процедури та здійснювати тестування передачі операцій системи на альтернативний сайт на основі вимог доступності системи.	А 7
		Здатність впроваджувати заходи безпеки системи відповідно до встановлених процедур, визначених тактик, технік для наборів вторгнень, для забезпечення конфіденційності, цілісності, доступності, аутентифікації та невідмовності	А 8

Б	Аналізування заходів та ситуації з безпекою інформаційно-телекомуніка-ційних 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.	Б 1
		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.	Б 2
		Здатність виконувати аналізування тенденцій кіберзахисту та звітування про отримання мережевих сповіщеннь з різних джерел в організації, вказуючи можливі причини таких повідомлень	Б 3
		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).	Б 4
		Здатність перевіряти попередження системи виявлення вторгнень щодо мережевого трафіку за допомогою інструментів аналізування пакетів для локалізації та видалення шкідливого програмного забезпечення	Б 5
		Здатність відновлювати втрачені дані чи інформацію про зловмисну атаку або дію на основі інформації щодо мережевого трафіку	Б 6
		Здатність надавати допомогу в створенні сигнатур, які можна реалізувати в мережевих інструментах кіберзахисту у відповідь на нові або спостережувані загрози в мережевому середовищі	Б 7
В	Аналіз упереджу-вальних/	Здатність застосовувати принципи сервісно-орієнтованої архітектури безпеки, щоб відповідати вимогам	В 1

	розвідувальних заходів з безпеки інформаційно-телекомуніка-ційних систем	організації до конфіденційності, цілісності та доступності	
		Здатність до впровадження конкретних контрзаходів з кіберзахисту (операцій та технічного обслуговування системи) для систем та/або програм, їх документування, та оновлення у разі потреби	В 2
		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.	В 3
		Здатність виконувати кореляцію подій, використовуючи інформацію, зібрану з різних джерел на підприємстві, щоб досягти усвідомлення ситуації та визначити ефективність спостережуваної атаки	В 4
		Здатність проводити тестування кібербезпеки розроблених додатків та/або систем, надавати вхідні дані для технологічних процесів системи управління ризиками	В 5
		Здатність перевіряти та оновлювати документацію з безпеки, яка відображає особливості проєктування безпеки програми/системи	В 6
		Здатність визначати програмне забезпечення та операційні системи мережевого пристрою на основі мережевого трафіку, визначати відображення мережі та дії операційної системи	В 7
		Здатність відстежувати зовнішні джерела даних, аналізувати та повідомляти про тенденції безпеки організації та її систем для підтримання актуальності стану системи з урахуванням загроз кіберзахисту та визначати, які проблеми безпеки можуть вплинути на організацію	В 8
Г	Проведення	Здатність розроблювати контент для	Г 1

	моніторингу та оцінювання діяльності із забезпечення безпеки інформаційно-телекомунікаційних систем	засобів кіберзахисту	
		Здатність надавати щоденні зведені звіти про мережеві події та діяльність, що стосуються практичних заходів кіберзахисту	Г 2
		Здатність використовувати інструменти кіберзахисту для постійного моніторингу та аналізування системної активності для виявлення зловмисної діяльності	Г 3
		Здатність оцінювати ефективність заходів з контролю безпеки	Г 4
		Здатність оцінювати всі процеси керування конфігурацією	Г 5
		Здатність оцінювати адекватні засоби контролю доступу на основі принципів найменших привілеїв і необхідності отримання відповідної інформації	Г 6
		Здатність оцінювати та контролювати процеси кібербезпеки, пов'язані з впровадженням системи та її тестування	Г 7
Д	Координація діяльності із забезпечення безпеки інформацій-но-телекомунікаційних систем	Здатність координувати роботу з персоналом із забезпечення кібербезпеки всієї організації для перевірки мережевих сповіщень	Д 1
		Здатність надавати керівництву рекомендації щодо кібербезпеки	Д 2
		Здатність надавати керівництву рекомендації щодо кібербезпеки на основі інформації про значні загрози і вразливості	Д 3
		Здатність працювати із заінтересованими сторонами для усунення інцидентів кібербезпеки та забезпечення захисту у відповідності до вимог щодо усунення вразливостей	Д 4
		Здатність надавати рекомендації до планів аварійного відновлення, непередбачених випадків та забезпечення безперервності операцій	Д 5

6. Опис трудових функцій

Трудові функції	Предмети і засоби праці (обладнання, устаткування, матеріали, продукти, інструменти)	Професійні компетентності	Знання	Уміння і навички
А. Організація аналітичної діяльності з безпеки інформаційно-телекомуніка-ційних систем	Нормативні акти, протоколи, стандарти та сертифікати відповідного спрямування; комп'ютерне, програмне та інше техніко-технологічне забезпечення; операційні та інші системи; інтерпретовані і компільовані комп'ютерні мови; комп'ютерні алгоритми, алгоритми шифрування; бази даних; фізичні та логічні	**А.1** Здатність застосовувати політику безпеки до програм, які взаємодіють одна з одною, перевіряти наявність мінімальних вимог безпеки до всього програмного забезпечення для досягнення цілей безпеки системи	**А1.З1** Концепції комп'ютерних мереж та протоколів, а також методології мережевої безпеки **А1.З2** Концепції архітектури мережевої безпеки, включаючи топологію, протоколи, компоненти та принципи (наприклад, застосування глибинного захисту) **А1.З3** Принципи кібербезпеки та конфіденційності, зокрема організаційних вимог (що стосуються конфіденційності, цілісності, доступності, аутентифікації, безвідмовності) **А1.З4** Принципи кібербезпеки та конфіденційності **А1.З5** Принципи та методи безпеки інформаційних технологій (IT) (наприклад, брандмауери, демілітаризовані зони, шифрування) **А1.З6** Принципи глибинного захисту та архітектури мережевої безпеки **А1.З7** Принципи, моделі, методи управління мережевими системами (наприклад, наскрізний моніторинг продуктивності систем) та інструментів	**А1.У1** Визначати, як має працювати система безпеки (включаючи її стійкість і надійність) і як зміни умов, операцій або середовища впливатимуть на ці результати **А1.У2** Проєктувати інтеграції апаратних та програмних рішень **А1.У3** Виявляти вторгнення на базі хоста та мережі за допомогою технологій виявлення вторгнень (наприклад, Snort)

	мережеві пристрої та інфраструктура, включаючи концентратори, комутатори, маршрутизатори, брандмауери тощо, 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 тощо), системи управління контентом Web-сайтів (CMS), SCADA системи, списки контролю доступу, списки		**А1.38** Принципи взаємодії людини з комп'ютером **А1.39** Процеси управління ризиками (наприклад, методи оцінювання та зменшення ризику) **А1.310** Як встановлювати, інтегровувати та оптимізовувати компоненти системи **А1.311** Конкретні операційні впливи за недостатності заходів з кібербезпеки **А1.312** Категорії кібер-зловмисників (наприклад, діти зі сценаріями, інсайдерські загрози, фінансовані іншою державою) **А1.313** Програму класифікації інформації в організації та процедуру компромісу інформації **А1.314** Кіберзагрози та вразливості. **А1.315** Операційні системи. **А1.316** Методи системного адміністрування, мережевих та операційних систем. **А1.317** Моделі безпеки (наприклад, модель Белла-ЛаПадули, модель цілісності Біби, модель цілісності Кларка-Вілсона). **А1.318** Різні типи комп'ютерних архітектур. **А1.319** Загальні вектори атак на мережевому рівні. **А1.320** Політики, процедури та правила кіберзахисту та інформаційної безпеки **А1.321** Політики, вимоги та процедури управління ризиками інформаційних технологій (IT). **А1.322** Стандарти безпеки персональних даних (PII) **А1.323** Стандарти безпеки даних індустрії платіжних карток (PCI) **А1.324** Стандарти безпеки даних персональної медичної інформації (PHI)	**А1.У4** Писати код мовою програмування, що підтримується (наприклад, Java, C++)

	повноважень, обладнання апаратного забезпечення мереж, засоби безпеки на хостах, прикладні програми (Open Web Application Security Project Top 10 list)		**A1.325** Закони, нормативні акти, політики та етика, які стосуються кібербезпеки та конфіденційності **A1.326** Закони, статути (наприклад, укази президента, керівні принципи виконавчої влади та/або адміністративних/кримінальних правових інструкцій та процедур тощо) **A1.327** Закони, правові повноваження, обмеження та правила, що стосуються діяльності з кіберзахисту **A1.328** Закони, політики, процедури або керівництва, що стосуються кібербезпеки критичної інфраструктури **A1.329** Алгоритми шифрування даних **A1.330** Криптографія та концепцій управління криптографічними ключами **A1.331** Комп'ютерні мови, що інтерпретуються та компілюються **A1.332** Процеси управління наборами, можливостей та обмежень **A1.333** Методології шифрування даних **A1.334** Ризики безпеки додатків (наприклад, Open Web Application Security Project Top 10 list)	
		A.2 Здатність здійснювати контроль за тим, що всі операції з безпеки та обслуговування системи (застосування виправлень безпеки тощо) належним чином задокументовані та	**A2.31** Закони, нормативні акти, політики та етика, які стосуються кібербезпеки та конфіденційності **A2.32** Встановлення, інтеграції та оптимізації компонентів системи **A2.33** Принципи кібербезпеки та конфіденційності, в тому числі організаційні вимоги (що стосуються конфіденційності, цілісності, доступності, аутентифікації, безвідмовності) **A2.34** Концепції в управлінні безпекою	**A2.У1** Розпізнавати та класифікувати типи вразливостей і пов'язаних з ними атак **A2.У2** Використовувати методику обробки інцидентів

		оновлені і відповідають термінам, встановленим органом управління для передбачуваного операційного середовища	(наприклад, Release Management, Patch Management) **А2.35** Результати дослідження внутрішніх загроз, звітності, інструментів дослідження та законів/норм **А2.36** Закони, статути (наприклад, укази президента, керівні принципи виконавчої влади та/або адміністративні/кримінальні правові інструкції та процедури **А2.37** Кіберзагрози та вразливості **А2.38** Нові інформаційні технології (IT) та технології кібербезпеки. **А2.39** Структури звітності постачальника послуг кіберзахисту та процесів у власній організації	
		А.3 Здатність застосовувати заходи безпеки для усунення вразливостей, здійснювати контроль за тим, що продукти з підтримкою функцій кібербезпеки або інші компенсаційні технології контролю безпеки знижують ідентифікований ризик до прийнятного рівня та рекомендувати зміни щодо безпеки	**А3.31** Процеси управління ризиками (наприклад, методи оцінювання та зменшення ризику) **А3.32** Кіберзагрози та вразливості **А3.33** Принципи кібербезпеки та конфіденційності, в тому числі організаційні вимоги (що стосуються конфіденційності, цілісності, доступності, аутентифікації, безвідмовності) (K0044) **А3.34** Концепції комп'ютерних мереж та протоколів, а також методології мережевої безпеки **А3.35** Принципи кібербезпеки та конфіденційності **А 3.36** Системи управління базами даних. **А3.37** Принципи взаємодії людини з комп'ютером **А3.38** Принципи та методи безпеки інформаційних технологій (IT) (наприклад, брандмауери, демілітаризовані зони, шифрування)	**А3.У1** Розпізнавати та класифікувати типи вразливостей та пов'язаних з ними атак **А3.У2** Проєктувати, здійснювати інтеграцію апаратних та програмних рішень **А3.У3** Виявляти вторгнення на базі хоста та мережі за допомогою технологій виявлення вторгнень (наприклад, Snort) **А3.У4** Застосовувати

			А3.39 Загрози і вразливості безпеки системи та додатків (наприклад, 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) **А3.310** Концепції в управлінні безпекою (наприклад, Release Management, Patch Management) **А 3.311** Процес розробки систем **А3.312** Політики, процедури та правила кіберзахисту та інформаційної безпеки	принципи кібербезпеки та конфіденційності до організаційних вимог (що стосується конфіденційності, цілісності, доступності, аутентифікації, безвідмовності)
		А.4 Здатність інтегрувати автоматизовані можливості для оновлення або виправлення системного програмного забезпечення та розроблювати процеси і процедури для ручного оновлення та виправлення системного програмного забезпечення	**А4.31** Принципи кібербезпеки та конфіденційності. **А4.32** Кіберзагрози та вразливості **А4.33** Встановлення, інтеграція та оптимізація компонентів системи **А4.34** Принципи та методи безпеки інформаційних технологій (IT) (наприклад, брандмауери, демілітаризовані зони, шифрування). **А4.35** Нові інформаційні технології (IT) та технології кібербезпеки **А4.36** Операційні системи **А4.37** Концепції паралельних та розподілених обчислень **А4.38** Інструменти, методи та прийоми проєктування систем безпеки **А4.39** Інструменти, методи та прийоми проєктування систем безпеки. **А4.310** Процеси розробки систе **А4.311** Розширення файлів (наприклад, .dll, .bat,	**А4.У1** Проєктувати, здійснювати інтеграцію апаратних та програмних рішень **А4.У2** Писати код мовою програмування, що підтримується (наприклад, Java, C++)

			.zip, .pcap, .gzip) **А4.312** Процеси проєктування мережі, включаючи розуміння цілей безпеки, операційних цілей та компромісів між ними **А4.313** Ризики безпеки додатків (наприклад, Open Web Application Security Project Top 10 list)	
		А5. Здатність до вивчення топології мережі для усвідомлення потоків даних через мережу, забезпечувати інтеграцію та впровадження міждоменних рішень у безпечному середовищі	**А.5.31** Концепції комп'ютерних мереж та протоколів, а також методології мережевої безпеки. **А5.32** Принципи кібербезпеки та конфіденційності. **А5.33** Принципи та методи безпеки інформаційних технологій (IT) (наприклад, брандмауери, демілітаризовані зони, шифрування) **А5.34** Інструменти, методи та прийоми проєктування систем безпеки **А5.35** Телекомунікаційні концепції (наприклад, канал зв'язку, наповнення системних каналів, спектральна ефективність, мультиплексування) **А5.36** Безпеку віртуальної приватної мережі (VPN) **А5.37** Мережеві інструменти (наприклад, ping, traceroute, nslookup) **А5.38** Типи мережевого зв'язку (наприклад, LAN, WAN, MAN, WLAN, WWAN) **А5.39** Вектори атак на мережевому рівні **А5.310** Методи системного адміністрування, мережевих та операційних систем **А5.311** Концепції архітектури мережевої безпеки, включаючи топологію, протоколи, компоненти та принципи (наприклад, застосування глибинного захисту)	**А5.У1** Використовувати аналізатори протоколів . **А5.У2** Проєктувати, здійснювати інтеграцію апаратних та програмних рішень **А5.У3** Розпізнавати та класифікувати типи вразливостей та пов'язаних з ними атак

			А5.312 Принципи, моделі, методи управління мережевими системами (наприклад, наскрізний моніторинг продуктивності систем) та інструментів **А5.313** Порти і служби Windows/Unix **А5.314** Концепції управління послугами для мереж та відповідних стандартів (наприклад, бібліотека інфраструктури інформаційних технологій, поточна версія [ITIL]) **А5.315** Модель OSI та базові мережеві протоколи (наприклад, TCP/IP) **А5.316** Принципи глибинного захисту та архітектури мережевої безпеки **А5.317** Мережеві протоколи, такі як TCP/IP, динамічної конфігурації хоста, системи доменних імен (DNS) і служби каталогів	
		А.6 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 та	**А6.31** Процеси управління ризиками (наприклад, методи оцінювання та зменшення ризику) **А6.32** Принципи кібербезпеки та конфіденційності **А6.33** Кіберзагрози та вразливості **А6.34** Операційні впливи за недостатності заходів з кібербезпеки **А6.35** Механізми контролю доступу хоста/мережі (наприклад, список контролю доступу, списки привілеїв) **А6.36** Встановлення, інтеграція та оптимізація компонентів системи **А6.37** Концепції в управлінні безпекою (наприклад, Release Management, Patch Management). **А6.38** Мережеві інструменти (наприклад, ping, traceroute, nslookup).	**А6.У1** Взначати, як має працювати система безпеки (включаючи її стійкість і надійність) і як зміни умов, операцій або середовища впливатимуть на ці результати **А6.У2** Використовувати методику обробки інцидентів **А6.У3** Розпізнавати та класифікувати типи

		потенційний вплив для подальших дій відповідно до плану реагування на кіберінциденти організації (прийняти або обробити ризик).	**А6.39** Політики, процедури та правила кіберзахисту та інформаційної безпеки. **А6.310** Вектори атак на мережевому рівні. **А6.311** Політики, вимоги та процедури управління ризиками інформаційних технологій (IT). **А6.312** Використання інструментів мережевого аналізування для виявлення вразливостей. **А6.313** Принципи, інструменти та методи тестування на проникнення. **А6.314** Концепції комп'ютерних мереж та протоколи, а також методології мережевої безпеки. **А6.315** Інструменти кіберзахисту та оцінювання вразливостей, їх можливостей. **А6.316** Принципи взаємодії людини з комп'ютером. **А6.317** Джерела поширення інформації про вразливості (наприклад, попередження, рекомендації, помилки та бюлетні). **А6.318** Методології реагування на інциденти та їх обробки.	вразливостей та пов'язаних з ними атак.
		А7. Здатність забезпечувати виконання аварійного відновлення та безперервність роботи, в тому числі розроблювати процедури та здійснювати тестування передачі операцій системи на	**А7.31** Закони, нормативні акти, політики та етика, які стосуються кібербезпеки та конфіденційності **А7.32** Принципи кібербезпеки та конфіденційності **А7.33** Операційні впливи за недостатності заходів з кібербезпеки **А7.34** Механізми контролю доступу хоста/мережі (наприклад, список контролю доступу, списки привілеїв) **А7.35** Принципи кібербезпеки та конфіденційності, в тому числі організаційні	**А7.У1** Проєктувати, здійснювати інтеграцію апаратних та програмних рішень **А7.У2** Читати та визначати приналежність електронних підписів **А7.У3** Розробляти та розгортати

		альтернативний сайт на основі вимог доступності системи.	вимоги (що стосуються конфіденційності, цілісності, доступності, аутентифікації, безвідмовності) **А7.36** Принципи та методи безпеки інформаційних технологій (IT) (наприклад, брандмауери, демілітаризовані зони, шифрування) **А7.37** Процеси розробки та застосування системи керування обліковими даними користувачів **А7.38** Процеси впровадження систем умовного депонування ключів підприємства для підтримки шифрування даних у стані спокою **А7.39** Методи тестування та оцінювання безпеки систем **А7.310** Концепції комп'ютерних мереж та протоколів, а також методології мережевої безпеки **А7.311** Системи управління базами даних **А7.312** Встановлення, інтеграція та оптимізація компонентів системи **А7.313** Операційні системи **А7.314** Телекомунікаційні концепції (наприклад, канал зв'язку, наповнення системних каналів, спектральна ефективність, мультиплексування).	інфраструктуру електронних підписів

		А.8 Здатність впроваджувати заходи безпеки системи відповідно до встановлених процедур, визначених тактик, технік для наборів вторгнень, для забезпечення конфіденційності, цілісності, доступності, аутентифікації та невідмовності	**А.8.31** Методи аутентифікації, авторизації та контролю доступу **А8.32** Закони, нормативні акти, політики та етика, які стосуються кібербезпеки та конфіденційності **А8.33** Принципи кібербезпеки та конфіденційності **А8.34** Операційні впливи за недостатності заходів з кібербезпеки **А8.35** Методи аутентифікації, авторизації та контролю доступу **А 8.36** Механізми контролю доступу хоста/мережі (наприклад, список контролю доступу, списки привілеїв) **А8.37** Принципи та методи безпеки інформаційних технологій (IT) (наприклад, брандмауери, демілітаризовані зони, шифрування **А8.38** Механізми доступу до мережі, ідентифікації та управління доступом (наприклад, інфраструктура відкритих ключів, Oauth, OpenID, SAML, SPML) **А8.39** Концепції в управлінні безпекою (наприклад, Release Management, Patch Management) **А8.310** Політики, процедури та правила кіберзахисту та інформаційної безпеки **А8.311** Концепції комп'ютерних мереж та протоколів, а також методології мережевої безпеки **А8.312** Кіберзагрози та вразливості **А8.313** Інструменти кіберзахисту та оцінювання вразливостей, їх можливостей **А8.314** Принципи взаємодії людини з комп'ютером	**А8.У1** Розробляти та розгортати інфраструктуру електронних підписів **А8.У2** Проєктувати, здійснювати інтеграцію апаратних та програмних рішень **А8.У3** Визначати, як має працювати система безпеки (включаючи її стійкість і надійність) і як зміни умов, операцій або середовища впливатимуть на ці результати **А8.У4** Застосовувати принципи кібербезпеки та конфіденційності до організаційних вимог (що стосується конфіденційності, цілісності, доступності, аутентифікації, безвідмовності) **А8.У5** Розпізнавати та

			А8.315 Методології і прийоми виявлення вторгнень для виявлення вторгнень на базі хоста та мережі **А8.316** Мережеві атаки, зв'язок мережевої атаки із загрозами та вразливими місцями **А8.317** Принципи глибинного захисту та архітектури мережевої безпеки **А8.318** Вектори атаки на мережевому рівні **А8.319** Категорії кібер-зловмисників (наприклад, діти зі сценаріями, інсайдерські загрози, фінансовані іншою державою) **А8.320** Етапи кібератак (наприклад, розвідка, сканування, вибір вектору проникнення, отримання доступу, ескалація привілеїв, підтримка доступу, експлуатація мережі, приховування слідів)	класифікувати типи вразливостей та пов'язаних з ними атак
Б. Аналізування заходів та ситуації з безпекою інформаційно-телекомуніка-ційних систем	Нормативні акти, протоколи, стандарти та сертифікати відповідного спрямування; комп'ютерне, програмне та інше техніко-технологічне забезпечення; операційні та інші системи; інтерпретовані і компільовані комп'ютерні мови;	**Б1**. 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.З1** Концепції комп'ютерних мереж та протоколів, а також методологій мережевої безпеки **Б1.З2** Кіберзагрози та вразливості **Б1.З3** Методології і прийоми виявлення вторгнень для виявлення вторгнень на базі хоста та мережі **Б1.З4** Методи аналізування мережевого трафіку **Б1.З5** Загальні вектори атаки на мережевому рівні **Б1.З6** Принципи кібербезпеки та конфіденційності **Б 1.З7** Системи управління базами даних. **Б1.З8** Принципи та методи безпеки інформаційних технологій (ІТ) (наприклад, брандмауери, демілітаризовані зони, шифрування) **Б1.З9** Операційні системи	**Б1.У1** Виявляти вторгнення на базі хоста та мережі за допомогою технологій виявлення вторгнень (наприклад, Snort) **Б1.У2** Використовувати аналізатори протоколів **Б1.У3** Розпізнавати та класифікувати типи вразливостей та пов'язаних з ними

	комп’ютерні алгоритми, алгоритми шифрування; бази даних; фізичні та логічні мережеві пристрої та інфраструктура, включаючи концентратори, комутатори, маршрутизатори, брандмауери тощо, 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 тощо), системи		**Б1.3**10 Типикомп’ютерних архітектур **Б1.3**11 Мережеві інструменти (наприклад, ping, traceroute, nslookup) **Б1.3**12 Типи мережевого зв’язку (наприклад, LAN, WAN, MAN, WLAN, WWAN)	атак
		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.	**Б2.3**1 Концепції комп’ютерних мереж та протоколів, а також методології мережевої безпеки **Б2.3**2 Принципи кібербезпеки та конфіденційності **Б2.3**3 Кіберзагрози та вразливості **Б2.3**4 Конкретні операційні впливи за недостатності заходів з кібербезпеки **Б2.3**5 Інструменти кіберзахисту та оцінювання вразливостей та їх можливостей **Б2.3**6 Джерела поширення інформації про вразливості (наприклад, попередження, рекомендації, помилки та бюлетні) **Б2.3**7 Принципи кібербезпеки та конфіденційності, в тому числі організаційні вимоги (що стосуються конфіденційності, цілісності, доступності, аутентифікації, безвідмовності) **Б2.3**8 Принципи глибинного захисту та архітектури мережевої безпеки. **Б2.3**9 Політики, процедури та правила кіберзахисту та інформаційної безпеки **Б2.3**10 Загальні вектори атак на мережевому рівні **Б2.3**11 Категорії кібер-зловмисників (наприклад, діти зі сценаріями, інсайдерські загрози, фінансовані іншою державою) **Б2.3**12 Політики, вимоги та процедури управління ризиками інформаційних технологій	**Б2.У1** Збирати дані з різноманітних ресурсів кіберзахисту **Б2.У2** Розпізнавати та класифікувати типи вразливостей та пов’язаних з ними атак. **Б2.У3** Знаходити вразливості в системах безпеки. (наприклад, перевірка вразливостей та відповідності)

	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)		(IT) **Б2.313** Процеси управління ризиками (наприклад, методи оцінювання та зменшення ризику) **Б2.314** Механізми контролю доступу хоста/мережі (наприклад, список контролю доступу, списки привілеїв) **Б2.315** Засоби управління доступом, що ґрунтуються на політиках та ризиках	
		Б З Здатність виконувати аналізування тенденцій кіберзахисту та звітування про отримання мережевих сповіщенн з різних джерел в організації, вказуючи можливі причини таких повідомлень	Б З.З1 Закони, нормативні акти, політики та етика, які стосуються кібербезпеки та конфіденційності. Б З.З2 Принципи кібербезпеки та конфіденційності. Б З.З3 Кіберзагрози та вразливості. Б З.З4 Джерела поширення інформації про вразливості (наприклад, попередження, рекомендації, помилки та бюлетні). Б З.З5 Нові інформаційні технології (IT) та технології кібербезпеки. Б З.З6 Що є мережевою атакою, і зв'язок мережевої атаки із загрозами та вразливими місцями. Б З.З7 Концепції комп'ютерних мереж та протоколів, а також методології мережевої безпеки. Б З.З8 Методології реагування на інциденти та їх обробки. Б З.З9 Методології і прийоми виявлення вторгнень для виявлення вторгнень на базі хоста та мережі. Б З.З10 Методи аналізування мережевого трафіку . Б З.З11 Загрози і вразливості безпеки системи та додатків (наприклад, переповнення буфера,	Б З.У1 Збирати дані з різноманітних ресурсів кіберзахисту. Б З.У2 Проводити аналізування тенденцій. Б З.У3 Використовувати аналізатори протоколів.

			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). Б 3.312 Політики, процедури та правила кіберзахисту та інформаційної безпеки.	
		Б 4 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).	Б 4.31 Концепції комп'ютерних мереж та протоколів, а також методології мережевої безпеки. Б 4.32 Кіберзагрози та вразливості. Б 4.33 Методи аутентифікації, авторизації та контролю доступу. Б 4.34 Інструменти кіберзахисту та оцінювання вразливостей та їх можливостей. Б 4.35 Джерела поширення інформації про вразливості (наприклад, попередження, рекомендації, помилки та бюлетні). Б 4.36 Методології реагування на інциденти та їх обробки. Б 4.37 Методології і прийоми виявлення вторгнень для виявлення вторгнень на базі хоста та мережі. Б 4.38 Принципи та методи безпеки інформаційних технологій (IT) (наприклад, брандмауери, демілітаризовані зони, шифрування). Б 4.39 Методи аналізування мережевого трафіку. Б 4.310 Операційні системи. Б 4.311 Загрози і вразливості безпеки системи та додатків (наприклад, переповнення буфера, мобільний код, міжсайтові скрипти, мова процедур/структурована мова запитів [PL/SQL] та	Б 4.У1 Виявляти вторгнення на базі хоста та мережі за допомогою технологій виявлення вторгнень (наприклад, Snort). Б 4.У2 Використовувати методику обробки інцидентів. Б 4.У3 Розпізнавати та класифікувати типи вразливостей та пов'язаних з ними атак.

			ін'єкції, умови протидії, прихований канал, повторення, атаки, орієнтовані на повернення, шкідливий код). Б 4.312 Результати дослідження внутрішніх загроз, звітності, інструментів дослідження та законів/норм. Б 4.313 Тактики, прийоми і процедури протидії кіберінцидентам. Б 4.314 Загальні вектори атак на мережевому рівні. Б 4.315 Етапи кібератак (наприклад, розвідка, сканування, вибір вектору проникнення, отримання доступу, ескалація привілеїв, підтримка доступу, експлуатація мережі, приховування слідів). Б 4.316 Математика (наприклад, логарифми, тригонометрія, лінійна алгебра, числення, статистика та операційний аналіз).	
		Б 5 Здатність перевіряти попередження системи виявлення вторгнень щодо мережевого трафіку за допомогою інструментів аналізування пакетів для локалізації та видалення шкідливого програмного забезпечення	Б 5.31 Концепції комп'ютерних мереж та протоколів, а також методології мережевої безпеки. Б 5.32 Кіберзагрози та вразливості. Б 5.33 Методології і прийоми виявлення вторгнень для виявлення вторгнень на базі хоста та мережі. Б 5.34 Методи аналізування мережевого трафіку. Б 5.35 Порти і служби Windows/Unix. Б 5.36 Методи аналізування трафіку на рівні пакетів з використанням відповідних інструментів (наприклад, Wireshark, tcpdump). Б 5.37 Інструменти і програми системи виявлення вторгнень (IDS)/системи попередження вторгненнь (IPS).	Б 5.У1 Використовувати аналізатори протоколів. Б 5.У2 Виконувати аналізування трафіку на рівні пакетів. Б 5.У3 Використовувати методику обробки інцидентів. Б 5.У4 Писати код мовою

			Б 5.38 Принципи кібербезпеки та конфіденційності. Б 5.39 Інструменти кіберзахисту та оцінювання вразливостей та їх можливостей. Б 5.310 Комп'ютерні алгоритми. Б 5.311 Встановлення, інтеграція та оптимізація компонентів системи. Б 5.312 Методології реагування на інциденти та їх обробки. Б 5.313 Принципи та методи безпеки інформаційних технологій (IT) (наприклад, брандмауери, демілітаризовані зони, шифрування. Б 5.314 Операційні системи. Б 5.315 Загрози і вразливості безпеки системи та додатків (наприклад, 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). А 5.316 Програмна інженерія. А 5.317 Розширення файлів (наприклад, .dll, .bat, .zip, .pcap, .gzip). А 5.318 Вбудовані системи.	програмування, що підтримується (наприклад, Java, C++).
		Б 6 Здатність відновлювати втрачені дані чи інформацію про зловмисну атаку або дію на основі інформації щодо мережевого трафіку	Б 6.31 Концепції комп'ютерних мереж та протоколів, а також методології мережевої безпеки. Б 6.32 Кіберзагрози та вразливості. Б 6.33 Конкретні операційні впливи за недостатності заходів з кібербезпеки. Б 6.34 Інструменти кіберзахисту та оцінювання вразливостей та їх можливостей. Б 6.35 Методології реагування на інциденти та їх	Б 6.У1 Виявляти вторгнення на базі хоста та мережі за допомогою технологій виявлення вторгнень (наприклад, Snort). Б 6.У2 Розпізнавати

			обробки. Б 6.36 Що є мережевою атакою, і зв'язок мережевої атаки із загрозами та вразливими місцями. Б 6.37 Принципи глибинного захисту та архітектури мережевої безпеки. Б 6.38 Загальні вектори атаки на мережевому рівні. Б 6.39 Етапи кібератак (наприклад, розвідка, сканування, вибір вектору проникнення, отримання доступу, ескалація привілеїв, підтримка доступу, експлуатація мережі, приховування слідів).	та класифікувати типи вразливостей та пов'язаних з ними атак.
		Б 7 Здатність надавати допомогу в створенні сигнатур, які можна реалізувати в мережевих інструментах кіберзахисту у відповідь на нові або спостережувані загрози в мережевому середовищі	Б 7.31 Концепції комп'ютерних мереж та протоколів, а також методології мережевої безпеки. Б 7.32 Кіберзагрози та вразливості. Б 7.33 Комп'ютерні алгоритми. Б 7.34 Алгоритми шифрування даних. Б 7.35 Криптографія та концепції управління криптографічними ключами. Б 7.36 Джерела поширення інформації про вразливості (наприклад, попередження, рекомендації, помилки та бюлетні). Б 7.37 Методології і прийоми виявлення вторгнень для виявлення вторгнень на базі хоста та мережі. Б 7.38 Операційні системи. А 7.39 Структури звітності постачальника послуг кіберзахисту та процеси у власній організації. А 7.310 Етапів кібератак (наприклад, розвідка, сканування, вибір вектору проникнення, отримання доступу, ескалація привілеїв,	Б 7.У1 Писати код мовою програмування, що підтримується (наприклад, Java, C++). Б 7.У2 Проєктувти інтегрувати апаратні та програмні рішення..

			підтримка доступу, експлуатація мережі, приховування слідів). А 7.311 Методології шифрування даних. А 7.312 Вплив реалізації сигнатур для вірусів, шкідливих програм і атак.	
В Аналіз упереджу-вальних/ розвідувальних заходів з безпеки інформацій-но-телекомуніка-ційних систем	Нормативні акти, протоколи, стандарти та сертифікати відповідного спрямування; комп'ютерне, програмне та інше техніко-технологічне забезпечення; операційні та інші системи; інтерпретовані і компільовані комп'ютерні мови; комп'ютерні алгоритми, алгоритми шифрування; бази даних; фізичні та логічні мережеві пристрої та інфраструктура, включаючи концентратори,	В 1 Здатність застосовувати принципи сервісно-орієнтованої архітектури безпеки, щоб відповідати вимогам організації до конфіденційності, цілісності та доступності	В 1.31 Принципи кібербезпеки та конфіденційності. В 1.32 Кіберзагрози та вразливості. В 1.33 Методи аутентифікації, авторизації та контролю доступу. В 1.34 Системи управління базами даних. В 1.35 Механізми контролю доступу хоста/мережі (наприклад, список контролю доступу, списки привілеїв). В 1.36 Принципи кібербезпеки та конфіденційності, в тому числі організаційних вимог (що стосуються конфіденційності, цілісності, доступності, аутентифікації, безвідмовності). В 1.37 Нові інформаційні технології (IT) та технології кібербезпеки. В 1.38 Інструменти, методи та прийоми проєктування систем безпеки. В 1.39 Політики, процедури та правила кіберзахисту та інформаційної безпеки. В 1.310 Моделі безпеки (наприклад, модель Белла-ЛаПадули, модель цілісності Біби, модель цілісності Кларка-Вілсона). В 1.311 Стандарти безпеки персональних даних (PII). В 1.312 Стандарти безпеки даних індустрії платіжних карток (PCI). В 1.313 Стандарти безпеки даних персональної	В 1.У1 Розробляти та розгортати інфраструктуру електронних підписів. В 1.У2 Проєктувти інтегрувати апаратні та програмні рішення.

	комутатори, маршрутизатори, брандмауери тощо, 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 тощо), системи управління контентом Web-сайтів (CMS), SCADA системи, списки контролю доступу, списки повноважень, обладнання апаратного забезпечення мереж, засоби		медичної інформації (PHI). В 1.314 Каталоги послуг інформаційних технологій (IT). В 1.315 Процеси проєктування мережі, включаючи розуміння цілей безпеки, операційних цілей та компромісів між ними.	
		В 2 Здатність до впровадження конкретних контрзаходів з кіберзахисту (операцій та технічного обслуговування системи) для систем та/або програм, їх документування, та оновлення у разі потреби	В 2.31 Закони, нормативних актів, політики та етики, які стосуються кібербезпеки та конфіденційності. В 2.32 Принципи кібербезпеки та конфіденційності. В 2.33 Кіберзагрози та вразливості. Б 2.34 Конкретні операційні впливи за недостатності заходів з кібербезпеки. В 2.35 Методи аутентифікації, авторизації та контролю доступу. В 2.36 Інструменти кіберзахисту та оцінювання вразливостей та їх можливостей. В 2.37 Встановлення, інтеграція та оптимізація компонентів системи. В 2.38 Принципи кібербезпеки та конфіденційності, в тому числі організаційних вимог (що стосуються конфіденційності, цілісності, доступності, аутентифікації, безвідмовності). В 2.39 Механізми доступу до мережі, ідентифікації та управління доступом (наприклад, інфраструктура відкритих ключів, Oauth, OpenID, SAML, SPML). В 2.310 Операційні системи. В 2.311 Загрози і вразливості безпеки системи та додатків (наприклад, переповнення буфера,	В 2.У1 Розробляти та розгортати інфраструктуру електронних підписів. В 2.У2 Проєктувти інтегрувати апаратні та програмні рішення . В 2.У3 Визначати, як має працювати система безпеки (включаючи її стійкість і надійність) і як зміни умов, операцій або середовища впливатимуть на ці результати. В 2.У4 Розробляти та застосувати засоби контролю доступу до системи безпеки. В 2.У5 Застосовувати

	безпеки на хостах, прикладні програми (Open Web Application Security Project Top 10 list)		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). В 2.312 Що є мережевою атакою, і зв'язок мережевої атаки із загрозами та вразливими місцями. В 2.313 Розширення файлів (наприклад, .dll, .bat, .zip, .pcap, .gzip). В 2.314 Етапи кібератак (наприклад, розвідка, сканування, вибір вектору проникнення, отримання доступу, ескалація привілеїв, підтримка доступу, експлуатація мережі, приховування слідів). В 2.315 Процеси розробки контрзаходів для виявлених ризиків безпеки.	принципи кібербезпеки та конфіденційності до організаційних вимог (що стосується конфіденційності, цілісності, доступності, аутентифікації, безвідмовності). В 2.У6 Використовувати структуру та процеси звітності постачальника послуг кіберзахисту у власній організації.
		В 3 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	В 3.31 Процеси управління ризиками (наприклад, методи оцінювання та зменшення ризику). В 3.32 Закони, нормативні акти, політики та етика, які стосуються кібербезпеки та конфіденційності. В 3.33 Кіберзагрози та вразливості. В 3.34 Методології реагування на інциденти та їх обробки. В 3.35 Закони, статути (наприклад, укази президента, керівні принципи виконавчої влади та/або адміністративні/кримінальні правові інструкції та процедури. В 3.36 Принципи кібербезпеки та конфіденційності. В 3.37 Конкретні операційні впливи за	В 3.У1 Розпізнавати та класифікувати типи вразливостей та пов'язаних з ними атак. В 3.У2 Використовувати структуру та процеси звітності постачальника послуг кіберзахисту у власній організації. В 3.У3 Проєктувти інтегрувати апаратні

		оцінювання наявних заходів та/або поведінки системного середовища.	недостатності заходів з кібербезпеки. В 3.38 Джерела поширення інформації про вразливості (наприклад, попередження, рекомендації, помилки та бюлетні). В 3.39 Принципи глибинного захисту та архітектури мережевої безпеки. В 3.310 Політики, процедури та правила кіберзахисту та інформаційної безпеки.	та програмні рішення. В 3.У4 Визначати, як має працювати система безпеки (включаючи її стійкість і надійність) і як зміни умов, операцій або середовища впливатимуть на ці результати.
		В 4 Здатність виконувати кореляцію подій, використовуючи інформацію, зібрану з різних джерел на підприємстві, щоб досягти усвідомлення ситуації та визначити ефективність спостережуваної атаки	В 4.31 Процеси управління ризиками (наприклад, методи оцінювання та зменшення ризику). В 4.32 Методології і прийоми виявлення вторгнень для виявлення вторгнень на базі хоста та мережі. В 4.33 Принципи та методи безпеки інформаційних технологій (IT) (наприклад, брандмауери, демілітаризовані зони, шифрування). В 4.34 Математика (наприклад, логарифми, тригонометрія, лінійна алгебра, числення, статистика та операційний аналіз). В 4.35 Структури звітності постачальника послуг кіберзахисту та процесів у власній організації.	В 4.У1 Збирати дані з різноманітних ресурсів кіберзахисту. В 4.У2 Вміння виконувати аналізування трафіку на рівні пакетів.
		В 5 Здатність проводити тестування кібербезпеки розроблених додатків та/або систем, надавати вхідні дані	В 5.31 Принципи кібербезпеки та конфіденційності. В 5.32 Кіберзагрози та вразливості. В 5.33 Конкретні операційні впливи за недостатності заходів з кібербезпеки.	В 5.У1 Виявляти вторгнення на базі хоста та мережі за допомогою технологій виявлення вторгнень (наприклад,

		для технологічних процесів системи управління ризиками	В 5.34 Інструменти кіберзахисту та оцінювання вразливостей та їх можливостей. В 5.35 Комп'ютерні алгоритми. В 5.36 Системи управління базами даних. В 5.37 Механізми контролю доступу хоста/мережі (наприклад, список контролю доступу, списки привілеїв). В 5.38 Операційні системи. В 5.39 Загрози і вразливості безпеки системи та додатків (наприклад, 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). В 5.310 Програмна інженерія. В 5.311 Що є мережевою атакою, і зв'язок мережевої атаки із загрозами та вразливими місцями. В 5.312 Принципи глибинного захисту та архітектури мережевої безпеки. В 5.313 Комп'ютерні мови, що інтерпретуються та компілюються. В 5.314 Політики, процедур та правил кіберзахисту та інформаційної безпеки. В 5.315 Процеси управління ризиками (наприклад, методи оцінювання та зменшення ризику). В 5.316 Джерела поширення інформації про вразливості (наприклад, попередження, рекомендації, помилки та бюлетні). В 5.317 Структури звітності постачальника послуг кіберзахисту та процесів у власній організації.	Snort). В 5.У2 Писати код мовою програмування, що підтримується (наприклад, Java, C++). В 5.У3 Збирати дані з різноманітних ресурсів кіберзахисту.

		В 6 Здатність перевіряти та оновлювати документацію з безпеки, яка відображає особливості проєктування безпеки програми/системи	В 6.31 Закони, нормативні акти, політики та етика, які стосуються кібербезпеки та конфіденційності. В 6.32 Принципи кібербезпеки та конфіденційності. В 6.33 Інструменти, методи та прийоми проєктування систем безпеки.	В 6.У1 Використовувати структуру та процеси звітності постачальника послуг кіберзахисту у власній організації. В 6.У2 Визначати, як має працювати система безпеки (включаючи її стійкість і надійність) і як зміни умов, операцій або середовища впливатимуть на ці результати.
		В 7 Здатність визначати програмне забезпечення та операційні системи мережевого пристрою на основі мережевого трафіку, визначати відображення мережі та дії операційної системи	В 7.31 Концепції комп'ютерних мереж та протоколів, а також методології мережевої безпеки. В 7.32 Нові інформаційні технології (IT) та технології кібербезпеки. В 7.33 Методології і прийоми виявлення вторгнень для виявлення вторгнень на базі хоста та мережі. В 7.34 Принципи та методи безпеки інформаційних технологій (IT) (наприклад, брандмауери, демілітаризовані зони, шифрування. В 7.35 Методи формалізації відображення мережі та відтворення мережевих топологій (K0300). В 7.36 Інструменти командного рядка операційної системи.	В 7.У1 Використовувати аналізатори протоколів. В 7.У2 Виконувати аналізування трафіку на рівні пакетів.
		В 8 Відстежує зовнішні джерела даних (наприклад,	В 8.31 Процеси управління ризиками (наприклад, методи оцінювання та зменшення ризику). В 8.32 Кіберзагрози та вразливості.	В 8.У1 Збирати дані з різноманітних ресурсів кіберзахисту.

		сайти постачальників послуг кіберзахисту, команди реагування на комп'ютерні надзвичайні події, фокус безпеки), для підтримання актуальності стану системи з урахуванням загроз кіберзахисту та визначає, які проблеми безпеки можуть вплинути на організацію (Т0503).	В 8.33 Інструменти кіберзахисту та оцінювання вразливостей та їх можливостей. В 8.34 Джерела поширення інформації про вразливості (наприклад, попередження, рекомендації, помилки та бюлетні). В 8.35 Структури звітності постачальника послуг кіберзахисту та процесів у власній організації. В 8.36 Зовнішні системи збору даних, включаючи збір, фільтрацію та вибір трафіку. В 8.37 Концепції комп'ютерних мереж та протоколів, а також методології мережевої безпеки. В 8.38 Принципи кібербезпеки та конфіденційності. В 8.39 Конкретні операційні впливи за недостатності заходів з кібербезпеки.	В 8.У2 Визначати, як має працювати система безпеки (включаючи її стійкість і надійність) і як зміни умов, операцій або середовища впливатимуть на ці результати. Б 8.У3 Проводити аналізування тенденцій.
Г Проведення моніторингу та оцінювання діяльності із забезпечення безпеки інформаційно-телекомуніка-ційних систем	Нормативні акти, протоколи, стандарти та сертифікати відповідного спрямування; комп'ютерне, програмне та інше техніко-технологічне забезпечення; операційні та інші системи; інтерпретовані і компільовані комп'ютерні мови;	Г 1 Здатність розроблювати контент для засобів кіберзахисту	Г 1.З1 Принципи кібербезпеки та конфіденційності. Г 1.З2 Кіберзагрози та вразливості. Г 1.З3 Конкретні операційні впливи за недостатності заходів з кібербезпеки. Г 1.З4 Інструменти кіберзахисту та оцінювання вразливостей та їх можливостей. Г 1.З5 Комп'ютерні алгоритми. Г 1.З6 Системи управління базами даних. Г 1.З7 Джерела поширення інформації про вразливості (наприклад, попередження, рекомендації, помилки та бюлетні). Г 1.З8 Програмна інженерія. Г 1.З9 Результати дослідження внутрішніх загроз, звітності, інструментів дослідження та законів/норм. Г 1.З10 Принципи глибинного захисту та	Г 1.У1 Використовувати аналізатори протоколів. Г 1.У2 Застосовувати принципи кібербезпеки та конфіденційності до організаційних вимог (що стосується конфіденційності, цілісності, доступності, аутентифікації, безвідмовності).

	комп’ютерні алгоритми, алгоритми шифрування; бази даних; фізичні та логічні мережеві пристрої та інфраструктура, включаючи концентратори, комутатори, маршрутизатори, брандмауери тощо, 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 тощо), системи		архітектури мережевої безпеки. Г 1.311 Зовнішні системи збору даних, включаючи збір, фільтрацію та вибір трафіку. Г 1.312 Загальні вектори атак на мережевому рівні.	
		Г 2 Здатність надавати щоденні зведені звіти про мережеві події та діяльність, що стосуються практичних заходів кіберзахисту	Г 2.31 Концепції комп’ютерних мереж та протоколів, а також методології мережевої безпеки. Г 2.32 Принципи кібербезпеки та конфіденційності, в тому числі організаційні вимоги (що стосуються конфіденційності, цілісності, доступності, аутентифікації, безвідмовності). Г 2.33 Методології і прийоми виявлення вторгнень для виявлення вторгнень на базі хоста та мережі. Г 2.34 Політики, процедури та правила кіберзахисту та інформаційної безпеки.	Г 2.У1 Збирати дані з різноманітних ресурсів кіберзахисту. Г 2.У2 Вміння виконувати аналізування трафіку на рівні пакетів. Г 2.У3 Використовувати аналізатори протоколів.
		Г 3 Здатність використовувати інструменти кіберзахисту для постійного моніторингу та аналізування системної активності для виявлення зловмисної діяльності	Г 3.31 Концепціх комп’ютерних мереж та протоколів, а також методології мережевої безпеки. Г 3.32 Принципи кібербезпеки та конфіденційності. Г 3.33 Інструменти кіберзахисту та оцінювання вразливостей та їх можливостей. Г 3.34 Методології і прийоми виявлення вторгнень для виявлення вторгнень на базі хоста та мережі. Г 3.35 Принципи та методи безпеки інформаційних технологій (IT) (наприклад, брандмауери, демілітаризовані зони, шифрування). Г 3.36 Операційні системи.	Г 3.У1 Розробляти та застосовувати засоби контролю доступу до системи безпеки. Г 3.У2 Використовувати аналізатори протоколів.

	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)		Г 3.37 Засоби управління доступом, що ґрунтуються на політиках та ризиках. Г 3.38 Загальні вектори атаки на мережевому рівні. Г 3.39 Етапи кібератак (наприклад, розвідка, сканування, вибір вектору проникнення, отримання доступу, ескалація привілеїв, підтримка доступу, експлуатація мережі, приховування слідів). Г 3.310 Використання інструментів моніторингу в рамках підмережі.	
		Г 4 Здатність оцінювати ефективність заходів з контролю безпеки	Г 4.31 Процеси управління ризиками (наприклад, методи оцінювання та зменшення ризику). Г 4.32 Принципи кібербезпеки та конфіденційності. Г 4.33 Кіберзагрози та вразливості. Г 4.34 Конкретні операційні впливи за недостатності заходів з кібербезпеки. Г 4.35 Методи аутентифікації, авторизації та контролю доступу. Г 4.36 Інструменти кіберзахисту та оцінювання вразливостей та їх можливостей. Г 4.37 Механізми контролю доступу хоста/мережі (наприклад, список контролю доступу, списки привілеїв). Г 4.38 Встановлення, інтеграція та оптимізація компонентів системи. Г 4.39 Принципи взаємодії людини з комп’ютером. Г 4.310 Принципи кібербезпеки та конфіденційності, в тому числі організаційні вимоги (що стосуються конфіденційності, цілісності, доступності, аутентифікації,	Г 4.У1 Оцінювати адекватність проєктів безпеки. Г 4.У2 Оцінювати проєкти систем безпеки. Г 4.У3 Оцінювати засоби контролю безпеки на основі принципів кібербезпеки. (наприклад, CIS CIS, NIST SP 800-53, Cybersecurity Framework тощо).

			безвідмовності). Г 4.311 Політики, процедури та правила кіберзахисту та інформаційної безпеки. Г 4.312 Різні класи атак (наприклад, пасивні, активні, інсайдерські, суміжні, розподільні атаки). Г 4.313 Методи тестування та оцінювання безпеки систем. Г 4.314 Як використовувати інструменти мережевого аналізування для виявлення вразливостей. Г 4.315 Принципи, інструменти та методи тестування на проникнення.	
		Г 5 Здатність оцінювати всі процеси керування конфігурацією	Г 5.31 Процеси управління ризиками (наприклад, методи оцінювання та зменшення ризику). Г 5.32 Принципи кібербезпеки та конфіденційності. Г 5.33 Кіберзагрози та вразливості. Г 5.34 Комп'ютерні алгоритми. Г 5.35 Принципи кібербезпеки та конфіденційності, в тому числі організаційні вимоги (що стосуються конфіденційності, цілісності, доступності, аутентифікації, безвідмовності). Г 5.36 Нові інформаційні технології (IT) та технологій кібербезпеки. Г 5.37 Операційні системи. Г 5.38 Ключові концепції в управлінні безпекою (наприклад, Release Management, Patch Management). Г 5.39 Техніки управління конфігурацією.	Г 5.У1 Оцінювати адекватність проєктів безпеки. Г 5.У2 Оцінювати проєкти систем безпеки. Г 5.У3 Оцінювати засоби контролю безпеки на основі принципів кібербезпеки. (наприклад, CIS CIS, NIST SP 800-53, Cybersecurity Framework тощо).
		Г 6 Здатність оцінювати адекватні засоби контролю	Г 6.31 Процеси управління ризиками (наприклад, методи оцінювання та зменшення ризику). Г 6.32 Принципи кібербезпеки та	Г 6.У1 Оцінювати адекватність проєктів безпеки.

		доступу на основі принципів найменших привілеїв і необхідності отримання відповідної інформації	конфіденційності. Г 6.33 Методи аутентифікації, авторизації та контролю доступу. Г 6.34 Інструменти кіберзахисту та оцінювання вразливостей та їх можливостей. Г 6.35 Алгоритми шифрування даних. Г 6.36 Криптографія та концепції управління криптографічними ключами. Г 6.37 Системи управління базами даних. Г 6.38 Різні класи атак (наприклад, пасивні, активні, інсайдерські, суміжні, розподільні атаки). Г 6.39 Моделі безпеки (наприклад, модель Белла-ЛаПадули, модель цілісності Біби, модель цілісності Кларка-Вілсона).	Г 6.У2 Оцінювати проєкти систем безпеки. Г 6.У3 Оцінювати засоби контролю безпеки на основі принципів кібербезпеки. (наприклад, CIS CIS, NIST SP 800-53, Cybersecurity Framework тощо).
		Г 7 Здатність оцінювати та контролювати процеси кібербезпеки, пов’язані з впровадженням системи та її тестування	Г 7.31 Процеси управління ризиками (наприклад, методи оцінювання та зменшення ризику). Г 7.32 Закони, нормативні акти, політики та етика, які стосуються кібербезпеки та конфіденційності. Г 7.33 Принципи кібербезпеки та конфіденційності. Г 7.34 Кіберзагрози та вразливості. Г 7.35 Конкретні операційні впливи за недостатності заходів з кібербезпеки. Г 7.36 Інструменти кіберзахисту та оцінювання вразливостей та їх можливостей. Г 7.37 Встановлення, інтеграція та оптимізація компонентів системи. Г 7.38 Як оцінити надійність постачальника та/або продукту. Г 7.39 Методи тестування та оцінювання безпеки систем. Г 7.38 Принципи, інструменти та методи тестування на проникнення .	Г 7.У1 Оцінювати адекватність проєктів безпеки. Г 7.У2 Оцінювати проєкти систем безпеки. Г 7.У3 Оцінювати засоби контролю безпеки на основі принципів кібербезпеки. (наприклад, CIS CIS, NIST SP 800-53, Cybersecurity Framework тощо).

Д Координація діяльності із забезпечення безпеки інформацій-но-телекомуніка-ційних систем	Нормативні акти, протоколи, стандарти та сертифікати відповідного спрямування; комп'ютерне, програмне та інше техніко-технологічне забезпечення; операційні та інші системи; інтерпретовані і компільовані комп'ютерні мови; комп'ютерні алгоритми, алгоритми шифрування; бази даних; фізичні та логічні мережеві пристрої та інфраструктура, включаючи концентратори, комутатори, маршрутизатори, брандмауери тощо, бездротові технології та	Д 1 Здатність координувати роботу з персоналом із забезпечення кібербезпеки всієї організації для перевірки мережевих сповіщень	Д 1.31 Закони, нормативні акти, політики та етика, які стосуються кібербезпеки та конфіденційності. Д 1.32 Принципи кібербезпеки та конфіденційності. Д 1.35 Конкретні операційні впливи за недостатності заходів з кібербезпеки. Д 1.36 Різні класи атак (наприклад, пасивні, активні, інсайдерські, суміжні, розподільні атаки). Д 1.37 Закони, статути (наприклад, укази президента, керівні принципи виконавчої влади та/або адміністративні/кримінальні правові інструкції та процедури. Д 1.38 Моделі безпеки (наприклад, модель Белла-ЛаПадули, модель цілісності Біби, модель цілісності Кларка-Вілсона). Д 1.39 Процеси управління безпекою.	В 7.У1 Використовувати структуру та процеси звітності постачальника послуг кіберзахисту у власній організації. В 7.У2 Оцінювати засоби контролю безпеки на основі принципів кібербезпеки. (наприклад, CIS CIS, NIST SP 800-53, Cybersecurity Framework тощо).
		Д 2 Здатність надавати керівництву рекомендації щодо кібербезпеки	Д 2.31 Процеси управління ризиками (наприклад, методи оцінювання та зменшення ризику). Д 2.32 Закони, нормативни акти, політики та етика, які стосуються кібербезпеки та конфіденційності. Д 2.33 Принципи кібербезпеки та конфіденційності. Д 2.34 Кіберзагрози та вразливості. Д 2.35 Конкретні операційні впливи за недостатності заходів з кібербезпеки. Д 2.36 Методи аутентифікації, авторизації та контролю доступу. Д 2.37 Принципи кібербезпеки та конфіденційності, в тому числі організаційні вимоги (що стосуються конфіденційності, цілісності, доступності, аутентифікації,	Д 2.У1 Проєктувати інтегрувати апаратні та програмні рішення. Д 2.У2 Оцінювати адекватність проєктів безпеки.

	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 тощо), 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		безвідмовності). Д 2.38 Принципи та методи безпеки інформаційних технологій (IT) (наприклад, брандмауери, демілітаризовані зони, шифрування. Д 2.39 Загрози і вразливості безпеки системи та додатків (наприклад, 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). Д 2.310 Різні класи атак (наприклад, пасивні, активні, інсайдерські, суміжні, розподільні атаки). Д 2.311 Закони, статути (наприклад, укази президента, керівні принципи виконавчої влади та/або адміністративні/кримінальні правові інструкції та процедури. Д 2.312 Моделі безпеки (наприклад, модель Белла-ЛаПадули, модель цілісності Біби, модель цілісності Кларка-Вілсона). Д 2.313 Процеси управління безпекою.	
		Д 3 Здатність надавати керівництву рекомендації щодо кібербезпеки на основі інформації про значні загрози і вразливості	Д 3.31 Процеси управління ризиками (наприклад, методи оцінювання та зменшення ризику). Д 3.32 Закони, нормативні акти, політики та етика, які стосуються кібербезпеки та конфіденційності. Д 3.33 Принципи кібербезпеки та конфіденційності. Д 3.34 Кіберзагрози та вразливості. Д 3.35 Конкретні операційні впливи за недостатності заходів з кібербезпеки. Д 3.36 Методи аутентифікації, авторизації та контролю доступу.	Д 3.У1 Проєктувати інтегрувати апаратні та програмні рішення. Д 3.У2 Збирати дані з різноманітних ресурсів кіберзахисту.

	Security Project Top 10 list)		Д 3.37 Принципи кібербезпеки та конфіденційності, в тому числі організаційні вимоги (що стосуються конфіденційності, цілісності, доступності, аутентифікації, безвідмовності). Д 3.38 Принципи та методи безпеки інформаційних технологій (IT) (наприклад, брандмауери, демілітаризовані зони, шифрування. Д 3.39 Результати дослідження внутрішніх загроз, звітності, інструментів дослідження та законів/норм. Д 3.310 Різні класи атак (наприклад, пасивні, активні, інсайдерські, суміжні, розподільні атаки). Д 3.311 Закони, статути (наприклад, укази президента, керівні принципи виконавчої влади та/або адміністративних/кримінальних правових інструкцій та процедур. Д 3.312 Моделі безпеки (наприклад, модель Белла-ЛаПадули, модель цілісності Біби, модель цілісності Кларка-Вілсона).	
		Д 4 Здатність працювати із заінтересованими сторонами для усунення інцидентів кібербезпеки та забезпечення захисту у відповідності до вимог щодо усунення вразливостей	Д 4.31 Закони, нормативні акти, політики та етика, які стосуються кібербезпеки та конфіденційності. Д 4.32 Принципи кібербезпеки та конфіденційності. Д 4.33 Кіберзагрози та вразливості. Д 4.34 Конкретні операційні впливи за недостатності заходів з кібербезпеки. Д 4.35 Програми класифікації інформації організації та процедур компромісу інформації.	Д 4.У1 Збирати дані з різноманітних ресурсів кіберзахисту. Д 4.У2 Використовувати структуру та процеси звітності постачальника послуг кіберзахисту у власній організації.
		Д 5 Здатність надавати рекомендації до планів	Д 5.31 Процеси управління ризиками (наприклад, методи оцінювання та зменшення ризику).	Д 5.У1 Проєктувати інтегрувати апаратні

		аварійного відновлення, непередбачених випадків та забезпечення безперервності операцій	Д 5.З2 Закони, нормативні акти, політики та етика, які стосуються кібербезпеки та конфіденційності. Д 5.З3 Принципи кібербезпеки та конфіденційності. Д 5.З4 Кіберзагрози та вразливості. Д 5.З5 Конкретні операційні впливи за недостатності заходів з кібербезпеки. Д 5.З6 Процеси управління безпекою.	та програмні рішення. Д 5.У2 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.

Колектив розробників професійного стандарту:

Безштанько Віталій, головний спеціаліст 1 відділу Департаменту кіберзахисту Державної служби спеціального зв'язку та захисту інформації України; Петрушкевич Олександр, перший заступник начальника Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України; Жилін Артем, заступник начальника Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України; Давидюк Андрій, заступник начальника відділу Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України; Юдін Олексій, заступник директора Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації Державної служби спеціального зв'язку та захисту інформації України; Юдін Олександр, професор кафедри кібербезпеки Науково-навчального інституту інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України; Супрун Ольга, професор кафедри кібербезпеки Науково-навчального інституту інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України; Чевардін Владислав, начальник кафедри кібербезпеки Військового інституту телекомунікацій та інформатизації імені героїв Крут; Давиденко Анатолій, провідний науковий співробітник Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України; Гнатюк Сергій, головний консультант відділу інформаційної безпеки та кібербезпеки Центру безпекових досліджень Національного інституту стратегічних досліджень; Корченко Олександр, президент Громадської організації "Асоціація спеціалістів кібербезпеки", заступник голови профспілкової організації кафедри безпеки інформаційних технологій Національного авіаційного університету; Іванченко Ігор, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету; Мазур Наталія, заступник Голови Профспілки працівників зв'язку України; Олексюк Лілія, голова Громадської організації «Всеукраїнська асоціація «Інформаційна безпека та інформаційні технології»; Пазюк Андрій, віце-президент Громадської організації «Українська академія кібербезпеки»; Філіпова Ольга, комерційний директор компанії SAYCOM; Лебеденко Кіра, директор ТОВ «СЕК'ЮРИТІ ЕКСПЕРТ ГРУП ЕКЕДЕМІ».

7.2. Суб'єкт перевірки професійного стандарту

Національне агентство кваліфікацій

7.3. Дата затвердження професійного стандарту

7.4. Дата внесення професійного стандарту до Реєстру професійних стандартів

7.5. Рекомендована дата наступного перегляду професійного стандарту

Вересень 2027 року.