Пояснювальна записка стосовно розроблення проєкту Галузевої рамки кваліфікацій української сфери інформаційної безпеки та кібербезпеки (ГРК КБ)

За своєю структурою ГРК КБ складається з 5 частин, а саме:

Частина 1. Функціональний розподіл та опис сфери інформаційної безпеки та кібербезпеки за видами трудової/професійної діяльності. Визначено та описано 7 видів трудової/професійної діяльності сфери інформаційної безпеки та кібербезпеки.

Частина 2. Розподіл видів трудової/професійної діяльності сфери інформаційної безпеки та кібербезпеки за сегментами трудової/професійної діяльності. Визначено та описано 33 таких сегментів.

Частина 3. Проєкт Галузевої рамки кваліфікацій української сфери інформаційної безпеки та кібербезпеки (ГРК КБ). Проєкт ГРК КБ побудовано відповідно до структури, норм та положень Національної рамки кваліфікацій з урахуванням окремих підходів, викладених у Галузевій рамці кваліфікацій в галузі знань «інформаційні технології». У проєкті ГРК КБ описано загальні вимоги до знань, умінь, комунікації, автономії та відповідальності тільки для тих 22 із 33 сегментів трудової/професійної діяльності, за якими в Україні передбачена/передбачається наявність повних та часткових професійних кваліфікацій відповідного спрямування. Остаточне заповнення у ГРК КБ для її кожного рівня необхідних знань та умінь є доцільним після розроблення та затвердження всіх професійних стандартів, які визначають повний перелік професійних кваліфікацій відповідного спрямування.

Частина 4. Розподіл професійних кваліфікацій сфери інформаційної безпеки та кібербезпеки за рівнями НРК та ГРК КБ

До цього розподілу ввійшло 60 повних, часткових та часткових додаткових професійних кваліфікацій сфери інформаційної безпеки та кібербезпеки.

За віднесенням до рівнів НРК вони розподілилися наступним чином:

- 5 рівень НРК: 2;
- 6 рівень НРК: 7:
- 7 рівень НРК: 48;
- 8 рівень НРК: 3.

За типом професійної кваліфікації розподіл має такий вигляд:

- Повні: 29;

- Часткові: 8;
- Часткові додаткові: 23.

Частина 5. Короткий опис (картки) професійних кваліфікацій ГРК КБ

Короткий опис професійних кваліфікацій частково проведено з урахуванням інформації, викладеної в проєкті ГРК КБ, у чинних професійних стандартах, у робочих версіях проєктів професійних стандартів, що розроблюються. Були також частково використані структура та окремі описи з Європейської рамки компетентностей із кібербезпеки.

Короткий опис (картки) професійних кваліфікацій ГРК КБ потребує подальшого доопрацювання та має за станом на 01.04.2023 року такий вигляд:

- Розроблено 14 карток за професійними кваліфікаціями, описаними у чинних 6 професійних стандартах (номери позицій у Частині 5): 6,19,20, 21, 22, 23, 28, 29, 34, 35, 36, 37, 44, 45;
- Розроблено 8 карток за професійними кваліфікаціями, описаними у проєктах 4 професійних стандартів, які розроблюються. Після їх розроблення та затвердження слід остаточно заповнити відповідні картки (номери позицій у Частині 5): 13,14, 15,16, 40, 41, 42, 43;
- Виписано орієнтовні переліки трудових функцій у 27 картках за професійними кваліфікаціями, які будуть описані у проєктах 11 професійних стандартів, які розроблюються. Після їх розроблення та затвердження слід остаточно заповнити відповідні картки (номери позицій у Частині 5): 1, 2, 3, 5, 7, 8, 9, 10, 11, 12, 17,18, 26, 27, 30, 31, 38, 39, 46, 47, 48, 49, 50, 51, 52, 53, 58;
- Не заповнено 8 карток на кваліфікації, які не пророблюються в рамках проєктної діяльності, але які входять до ГРК КБ (номери позицій у Частині 5): 4, 24, 25, 32, 33, 54, 55, 56, 57, 59, 60.

Проєкт

Галузева рамка кваліфікацій української сфери інформаційної безпеки та кібербезпеки (ГРК КБ)

Частина 1. Функціональний розподіл та опис сфери інформаційної безпеки та кібербезпеки за видами трудової/професійної діяльності

В основу функціонального розподілу сфери інформаційної безпеки та кібербезпеки покладений підхід та опис із Загальних принципів управління персоналом у сфері кібербезпеки (Національна освітня ініціатива у сфері кібербезпеки (NICE), а саме Таблиця 1 "Категорії персоналу в Загальних принципах NICE".

Функціональний розподіл та опис сфери інформаційної безпеки та кібербезпеки за видами трудової/професійної діяльності

Код	**Назва виду трудової/професійної діяльності**	**Стислий опис**
А	Забезпечення безпеки	Концептуалізація, розроблення, та/або створення безпечних системи інформаційних технологій (ІТ), з відповідальністю за аспекти розвитку системи та/або мережі
Б	Експлуатація та обслуговування систем, мереж та обладнання	Забезпечення підтримки, адміністрування та технічного обслуговування, необхідного для забезпечення ефективної та продуктивної роботи та безпеки системи/систем ІТ
В	Нагляд і корпоративне управління	Забезпечення керування, управління, спрямування або розвитку та захисту, направлених на те, щоб організація (установа, підприємство) могла ефективно проводити заходи з кібербезпеки
Г	Захист і охорона систем/мереж ІТ	Визначення, аналіз та пом'якшення загроз внутрішнім системам ІТ та/або мережам
Д	Аналіз профільної інформації	Проведення високо спеціалізованого перегляду та оцінки вхідної інформації про кібербезпеку, необхідних для визначення її корисності для розвідки тощо
Е	Збір і оброблення інформації	Забезпечення спеціалізованих операцій із заборони та дезінформації, збір інформації

		про кібербезпеку, яка може бути використана для розвитку розвідки/захисту
Є	Розслідування інциндентів	Розслідування подій кібербезпеки або злочинів, пов'язаних із системами ІТ, мережами та цифровими доказами

Частина 2. Розподіл видів трудової/професійної діяльності сфери інформаційної безпеки та кібербезпеки за сегментами трудової/професійної діяльності

В основу цього розподілу видів трудової/професійної діяльності сфери інформаційної безпеки та кібербезпеки покладена Таблиця 2 "Області спеціалізації в Загальних принципах NICE" із Загальних принципів управління персоналом у сфері кібербезпеки (Національна освітня ініціатива у сфері кібербезпеки (NICE).

Розподіл видів трудової/професійної діяльності сфери інформаційної безпеки та кібербезпеки за сегментами трудової/професійної діяльності

Вид трудової/ профе-сійної діяльнос-ті	**Сегменти трудової/професій-ної діяльності**	**Код ПП**	**Стислий опис**
А. Забез-печення безпеки	Управління ризиками	А1	Контролювати, оцінювати та підтримувати процеси документування, перевірки, оцінювання та авторизації, необхідні для забезпечення того, щоб існуючі та нові системи ІТ відповідали критеріям безпеки організації (установи, підприємства) та вимогам щодо ризиків
	Розроблення програмного забезпечення	А2	Розроблювати та створювати/програмувати нові (або модифікувати існуючі) комп’ютерні прикладні програми, програмне забезпечення або спеціальні програми-утиліти відповідно до кращих практик надання впевненості щодо програмного забезпечення.
	Розбудова архітектури систем	А3	Розроблювати концепції систем та працювати над фазами

			спроможностей життєвого циклу їх створення. Перетворювати технологію та умови зовнішнього середовища (законодавчі та нормативні акти тощо) в проєкти систем, засоби безпеки та робочі процеси
	Наукове та науково-технічне дослідження технологій	А4	Проводити оцінювання технології та процесів їх інтеграції на практиці. Забезпечувати і підтримувати спроможності прототипу та/або оцінювати його корисність
	Планування вимог до систем	А5	Консультуватися з клієнтами для збору та оцінки функціональних вимог та перетворювати їх в технічні рішення. Надавати клієнтам поради щодо застосування інформаційних систем для задоволення бізнес-потреб
	Тестування та оцінювання	А6	Розроблювати та проводити тестування систем для оцінювання відповідності специфікаціям та вимогам шляхом застосування принципів та методів економічно ефективного планування, оцінювання, перевірки та затвердження технічних, функціональних та експлуатаційних характеристик систем або елементів систем, що інтегрують ІТ
	Розроблення систем	А7	Реалізовувати етапи розроблення життєвого циклу створення систем
Б. Експлуа-тація та обслуго-вування систем, мереж та облад-нання	Управління профільними даними	Б1	Розроблювати та адмініструвати бази даних та/або системи управління даними, які дозволяють їх зберігати, запитувати, захищати та використовувати
	Управління доступом до інтелектуального капіталу та інформаційного контенту	Б2	Керувати та адмініструвати процеси та інструменти, які дозволяють організації (установі, підприємству) ідентифікувати, документувати та отримувати доступ до інтелектуального капіталу та інформаційного контенту

	Обслуговування клієнтів та технічна підтримка	Б3	Вирішувати технічні проблеми, встановлювати, налаштовувати, усувати несправності та забезпечувати технічне обслуговування та навчання у відповідності до вимог або запитів клієнтів (наприклад підтримку клієнтів на різних рівнях). Надавати початкову інформацію про інциденти профільному/відповідальному працівнику
	Обслуговування мереж	Б4	Встановлювати, налаштовувати, випробовувати, експлуатувати, обслуговувати та управляти мережами та їх брандмауерами, включаючи апаратне забезпечення (концентратори, мости, комутатори, мультиплексори, маршрутизатори, кабелі, проксі-сервери та захисні системи розподілу тощо) та програмне забезпечення, що дозволяє розповсюджувати та передавати інформації щодо усього спектру транзакцій для підтримки безпеки інформації та інформаційних систем
	Адміністрування систем	Б5	Встановлювати, налаштовувати, усувати несправності та підтримувати конфігурації серверів (апаратного та програмного забезпечення) для забезпечення їх конфіденційності, цілісності та доступності. Керувати обліковими записами, брандмауерами та патчами. Нести відповідальність за контроль доступу, паролі, а також створення та адміністрування облікового запису
	Аналіз систем	Б6	Досліджувати наявні комп’ютерні системи та процедури організації і розроблювати рішення для інформаційних систем, які допомагають організації (установі, підприємству) працювати більш безпечно, продуктивно та ефективно.

			Поєднувати інтереси бізнесу та IT, розуміючи їх потреби та обмеження
В. Нагляд і корпоративне управління	Юридичний супровід та захист	B1	Надавати юридично обґрунтовані поради та рекомендації керівництву та персоналу з різних актуальних тем у відповідній предметній сфері. Захищати правові та політичні зміни, вести справу від імені клієнта за допомогою широкого спектру письмової та усної діяльності, включаючи юридичні документи та судові розгляди
	Навчання та обізнаність у сфері інформаційної безпеки та кібербезпеки	B2	Проводити навчання персоналу у відповідній предметній області. Розроблювати, планувати, координувати, забезпечувати та/або оцінювати тренінгові програми, методи та методики
	Управління та нагляд за організацією кібербезпеки	B3	Здійснювати нагляд за програмою кібербезпеки інформаційної системи або мережі, включаючи управління наслідками інформаційної безпеки в рамках організації, спеціальну програму або іншу сферу відповідальності, включаючи стратегії, персонал, інфраструктуру, вимоги, політику, планування на випадок надзвичайних ситуацій, обізнаність про безпеку та інші ресурси
	Стратегічне планування та політика	B4	Розроблювати політики та плани та/або підтримувати зміни у політиці щодо організаційних ініціатив у галузі кіберпростору або необхідних змін/вдосконалення
	Управління працівниками з кібербезпеки	B5	Здійснювати нагляд, управляти та/або керувати роботою та працівниками, які виконують роботу з кібербезпеки, пов’язану з нею діяльність, або проводять/координують кібероперації
	Управління проєктами/програ-	B6	Застосовувати знання даних, інформації, процесів, взаємодії в

	мами та закупівля		організації (установі, підприємстві), навички та аналітичні знання, а також системи, мережі та спроможності інформаційного обміну для управління програмами закупівлі. Виконувати обов'язки корпоративного управління програмами придбання апаратного та програмного забезпечення, інформаційних систем та іншими політиками управління програмами. Забезпечувати пряму підтримку закупівлі систем, що використовують ІТ, застосовуючи профільні закони та політику. Здійснювати керівництво в галузі ІТ протягом усього життєвого циклу закупівлі.
Г. Захист і охорона систем/ мереж ІТ	Аналіз захисту кіберпростору	Г1	Проводити заходи захисту та використовувати інформацію, зібрану з різних джерел, для ідентифікації, аналізу та звітування про події, які виникають або можуть виникнути в мережі для захисту інформації, інформаційних систем та мереж від загроз
	Підтримка інфраструктури захисту кіберпростору	Г2	Тестувати, реалізовувати, використовувати, підтримувати, рецензувати та адмініструвати обладнання та програмне забезпечення інфраструктури, необхідної для ефективного управління мережею та ресурсами постачальників послуг комп'ютерної мережі. Здійснювати моніторинг мережі для активного усунення несанкціонованих дій
	Управління інцидентами	Г3	Реагувати на кризові або нагальні ситуації у відповідній області для зменшення негайних та потенційних загроз. Використовувати підходи, спрямовані на пом'якшення наслідків, підготовленість, реагування та відновлення, коли це потрібно, для виживання, збереження власності та

			інформаційної безпеки. Досліджувати та аналізувати всі необхідні заходи з реагування
	Оцінювання та управління вразливостями	Г4	Здійснювати оцінювання загроз та вразливостей. Визначати відхилення від прийнятних конфігурацій, корпоративної або локальної політики. Оцінювати рівень ризику та розроблювати/ рекомендувати відповідні контрзаходи щодо пом'якшення наслідків в операційних та неопераційних ситуаціях
Д. Аналіз профіль-ної інфор-мації	Аналіз загроз	Д1	Визначати та оцінювати спроможності та діяльність кримінальних злочинців у сфері кібербезпеки або іноземних розвідувальних служб. Готувати висновки, які допомагають ініціалізувати або підтримувати правоохоронні та контррозвідувальні розслідування чи заходи
	Аналіз вразливостей	Д2	Аналізувати зібрану інформацію для виявлення вразливостей та потенціалу для їх недопущення та успішної експлуатації інформаційних систем
	Аналіз даних з різних джерел	Д3	Аналізувати інформацію про загрози з різних джерел, напрямків та агентств у розвідувальному співтоваристві. Синтезувати та розглядати розвідувальну інформацію в контексті, з прогнозуванням можливих наслідків
	Аналіз інформації про оточуюче середовище	Д4	Застосовувати наявну інформацію про один або декілька регіонів, країни, недержавні організації та/або технології тощо, необхідну для успішного функціонування організації (установи, підприємства) сфери інформаційної безпеки та кібербезпеки
	Мовна, культурна та технічна експертиза профільної аналітичної	Д5	Здійснювати мовну, культурну та технічну експертизу для підтримки збору інформації, аналізу та іншої діяльності з кібербезпеки

	інформації		
Е. Збір і оброб-лення інформа-ції	Збір інформації	Е1	Збирати інформацію за допомогою відповідних стратегій та в межах пріоритетів, встановлених в процесі управління її збором
	Планування кібероперацій	Е2	Здійснювати поглиблене комплексне визначення цілей та планування системи захисту. Збирати інформацію та розроблювати детальні операційні плани та розпорядження за вимогою. Здійснювати стратегічне та операційне планування за всіма операціями для подальшої інтеграції інформації та операцій в кіберпросторі
	Проведення кібероперацій	Е3	Здійснювати заходи зі збору доказів щодо кримінальних та іноземних розвідувальних органів з метою пом'якшення можливих або реальних загроз, захисту від шпигунства чи інсайдерської загрози, іноземного саботажу, міжнародної терористичної діяльності або для підтримки іншої розвідувальної діяльності
Є. Розслідування інцин-дентів	Кіберрозслідування	Є1	Застосовувати тактики, методики та процедури повного спектру засобів і процесів розслідування, що включають в себе, але не обмежуються, методи інтерв'ю та допиту, розвідки, контррозвідки і виявлення спостереження, та належним чином збалансовувати переваги обвинувачення проти збору розвідувальних даних
	Цифрова криміналістика	Є2	Збирати, оброблювати, зберігати, аналізувати та надавати докази, пов'язані з комп'ютерною технікою, для підтримки зменшення вразливостей мережі та/або для кримінальних, шахрайських, контррозвідувальних або правоохоронних розслідувань

Частина 3. Проєкт Галузевої рамки кваліфікацій української сфери інформаційної безпеки та кібербезпеки (ГРК КБ)

Проєкт ГРК КБ побудовано відповідно до структури, норм та положень Національної рамки кваліфікацій з урахуванням окремих підходів, викладених у Галузевій рамці кваліфікацій в галузі знань «інформаційні технології» (Розробка та впровадження галузевої рамки кваліфікацій в галузі знань «Інформаційні технології» / В. А. Заславський, М. С. Нікітченко, Л. Л. Омельчук, О. М. Ямкова. – Київ: Київський національний університет, 2016. «Добродій» – 88 с. ISBN 978-966-97595-1-1.)

Заповнення у ГРК КБ для її кожного рівня необхідних знань та умінь є доцільним після розроблення та затвердження всіх професійних стандартів, які визначають повний перелік професійних кваліфікацій відповідного спрямування.

Проєкт

Галузева рамка кваліфікацій української сфери інформаційної безпеки та кібербезпеки (ГРК КБ)

<table>
<tr><th>Рівень НРК</th><th>Рівень ГРК КБ</th><th>Знання</th><th>Уміння</th><th>Комунікація</th><th>Автономність і відповідальність</th></tr>
<tr><td rowspan="2">5</td><td rowspan="2">5ЕЗ</td><td colspan="4">Здатність: здійснювати збір, обробку та/або геолокацію систем для експлуатації, пошуку та/або відстеження цілей, що представляють інтерес; виконувати мережеву навігацію, тактичний криміналістичний аналіз і, у випадку поставленого завдання, проводити операції в мережі</td></tr>
<tr><td></td><td></td><td>Взаємодія, співробітництво з широким колом осіб (колеги, керівники, клієнти) для провадження професійної діяльності</td><td>Здійснення обмежених управлінських функцій та прийняття рішень у звичних умовах з елементами не- передбачуваності. Покращення результатів власної професійної діяль-</td></tr>
</table>

					ності, результатів діяльності інших. Здатність до подальшого навчання з деяким рівнем автономності. Документування всіх видів діяльності під час та після її виконання
6	**6А6**	Здатність приймати участь у розробленні та проведенні тестування систем для оцінювання відповідності специфікаціям та вимогам шляхом застосування принципів та методів економічно ефективного планування, оцінювання, перевірки та затвердження технічних, функціональних та експлуатаційних характеристик систем або елементів систем, що інтегрують ІТ			
				Донесення до фахівців та іншої аудиторії інформації, ідей, проблем, рішень та власного досвіду в сфері професійної діяльності. Здатність ефективно фор-мувати	Управління комплексними діями або проєктами, відповідальність за прийняття рішень у непередбачуваних умовах. Відповідальність за професійний розвиток окремих осіб та/або груп осіб. Здатність до подальшого навчання
	6Б1	Здатність приймати участь у розробленні та адмініструванні баз даних та/або систем управління даними, які дозволяють їх зберігати, запитувати, захищати та використовувати			
	6Б3	Здатність вирішувати технічні проблеми, встановлювати, налаштовувати, усувати несправності та забезпечувати технічне обслуговування та навчання у відповідності до вимог або запитів клієнтів (наприклад підтримку клієнтів на різних рівнях). Надавати початкову інформацію про інциденти профільному/відповідальному працівнику			

	6Б5	Здатність встановлювати, налаштовувати, усувати несправності та підтримувати конфігурації серверів (апаратного та програмного забезпечення) для забезпечення їх конфіденційності, цілісності та доступності. Керувати обліковими записами, брандмауерами та патчами. Нести відповідальність за контроль доступу, паролі, а також створення та адміністрування облікового запису		комунікаційну стратегію. Здатність приймати участь у забезпеченні технічної підтримки і нав-	з високим рівнем автономності. Здатність обґрунтовано та самостійно обирати та освоювати інструментарій з розробки та
				чання	

			користувачів програмному забезпеченню, методам роботи з ІТ, мережею та системи кіберзахисту тощо. Здатність застосовувати методи керування економічними, людськими та технічними ресурсами в процесі виконання професійної діяльності. Здатність надавати пояснення і доносити проєктування/ розробки замовнику.	супроводження продуктів ІТ та систем/мереж кіберзахисту. Здатність самостійно оцінювати і враховувати економічні, соціальні, технологічні та екологічні чинники, що впливають на сферу професійної діяльності. Ініціювання заходів стосовно комплексного зв’язку із зацікавленими сторонами. Використання спеціальних знань для впливу на побудову рішення, забезпечення порад та рекомендацій. Забезпечення сумісності компонентів програмного

			Донесення до відома зацікавлених в розробці програм і систем сторін інформації відносно прогнозів та аналітичних даних. Донесення до профільних фахівців інформації про властивості математичних моделей	забезпечення, мережі, системи тощо. Використання професійних знань для участі у створенні повної системи, яка буде задовольняти обмеженням системи і очікуванням клієнта. Використання спеціальних знань для дослідження наявних процесів і рішень в області захисту ІТ та кіберзахисту з метою визна- чення можливих нововведень. Розроблення рекомендацій, які базуються на обґрунтованій аргументації
7	**7А1**	Здатність контролювати, оцінювати та підтримувати процеси документування, перевірки, оцінювання та авторизації,	Зрозуміле і недвозначне	Прийняття рішень у складних і непе-

		необхідні для забезпечення того, щоб існуючі та нові системи ІТ відповідали критеріям безпеки організації (установи, підприємства) та вимогам щодо ризиків	донесення власних висновків, а також знань та пояснень, що їх обґрунтовують, до фахівців і інших осіб, зокрема до тих, що навчаються. Використання іноземних мов у професійній діяльності. Спілкування в діалоговому режимі з широкою науковою спільнотою та зацікавленими особами в розробці проєкту про проєктування продуктів кібербезпеки	редбачуваних умовах, що потребує застосування нових підходів та прогнозування. Відповідальність за розвиток про-фесійного знання, уміеь та навичок, оцінювання стратегічного розвитку команди. Здатність до подальшого навчання, яке значною мірою є автономним та самостійним. Здатність розвивати і реалізовувати нові конкурентоспроможні ідеї в сфері інформаційної безпеки та кібербезпеки. Прийняття рішень у складних і непе-
	7А3	Здатність розроблювати концепції систем та працювати над фазами спроможностей життєвого циклу їх створення. Перетворювати технологію та умови зовнішнього середовища (законодавчі та нормативні акти тощо) в проєкти систем, засоби безпеки та робочі процеси		
	7А4	Здатність проводити оцінювання технології та процесів їх інтеграції на практиці. Забезпечувати і підтримувати спроможності прототипу та/або оцінювати його корисність		
	7А6	Здатність розроблювати та проводити тестування систем для оцінювання відповідності специфікаціям та вимогам шляхом застосування принципів та методів економічно ефективного планування, оцінювання, перевірки та затвердження технічних, функціональних та експлуатаційних характеристик систем або елементів систем, що інтегрують ІТ		
	7А7	Здатність реалізовувати етапи розроблення життєвого циклу створення систем		
	7Б1	Здатність розроблювати та адмініструвати бази даних та/або системи управління даними, які дозволяють їх зберігати, запитувати, захищати та використовувати		

					редбачуваних умовах, що потребує застосування нових підходів до розробки математичних моделей предметних областей. Застосовування незалежного мислення і знання технологій для інтеграції розрізнених концепцій для створення унікальних проєктів/продуктів. Використання професійних знань для створення процесу, необхідного для цикла інтеграції, включаючи створення внутрішніх стандартів практики. Автономне призначення ресурсів для програм інтеграції.
	7Б3	Здатність вирішувати технічні проблеми, встановлювати, налаштовувати, усувати несправності та забезпечувати технічне обслуговування та навчання у відповідності до вимог або запитів клієнтів (наприклад підтримку клієнтів на різних рівнях). Надавати початкову інформацію про інциденти профільному/відповідальному працівнику			
	7Б5	Здатність встановлювати, налаштовувати, усувати несправності та підтримувати конфігурації серверів (апаратного та програмного забезпечення) для забезпечення їх конфіденційності, цілісності та доступності. Керувати обліковими записами, брандмауерами та патчами. Нести відповідальність за контроль доступу, паролі, а також створення та адміністрування облікового запису			
	7Б6	Здатність досліджувати наявні комп’ютерні системи та процедури організації і розроблювати рішення для інформаційних систем, які допомагають організації (установі, підприємству) працювати більш безпечно, продуктивно та ефективно. Поєднувати інтереси бізнесу та ІТ, розуміючи їх потреби та обмеження			
	7В1	Здатність надавати юридично обґрунтовані поради та рекомендації керівництву та персоналу з різних актуальних тем у відповідній предметній сфері. Захищати правові та			

		політичні зміни, вести справу від імені клієнта за допомогою широкого спектру письмової та усної діяльності, включаючи юридичні документи та судові розгляди		Здатність ефективно керувати економічними, людськими, технічними та іншими ресурсами.
	7В2	Здатність проводити навчання персоналу у відповідній предметній області		
	7В3	Здатність здійснювати нагляд за програмою кібербезпеки інформаційної системи або мережі, включаючи управління наслідками інформаційної безпеки в рамках організації, спеціальну програму або іншу сферу відповідальності, включаючи стратегії, персонал, інфраструктуру, вимоги, політику, планування на випадок надзвичайних ситуацій, обізнаність про безпеку та інші ресурси		
	7В4	Здатність розроблювати політики та плани та/або підтримувати зміни у політиці щодо організаційних ініціатив у галузі кіберпростору або необхідних змін/вдосконалення		
	7В6	Здатність застосовувати знання даних, інформації, процесів, взаємодії в організації (установі, підприємстві), навички та аналітичні знання, а також системи, мережі та спроможності інформаційного обміну для управління програмами закупівлі. Виконувати обов’язки корпоративного управління програмами придбання апаратного та програмного забезпечення, інформаційних систем та іншими політиками		

		управління програмами. Забезпечувати пряму підтримку закупівлі систем, що використовують ІТ, застосовуючи профільні закони та політику. Здійснювати керівництво в галузі ІТ протягом усього життєвого циклу закупівлі.		
	7Г1	Здатність проводити заходи захисту та використовувати інформацію, зібрану з різних джерел, для ідентифікації, аналізу та звітування про події, які виникають або можуть виникнути в мережі для захисту інформації, інформаційних систем та мереж від загроз		
	7Г2	Здатність тестувати, реалізовувати, використовувати, підтримувати, рецензувати та адмініструвати обладнання та програмне забезпечення інфраструктури, необхідної для ефективного управління мережею та ресурсами постачальників послуг комп'ютерної мережі. Здійснювати моніторинг мережі для активного усунення несанкціонованих дій		
	7Г3	Здатність реагувати на кризові або нагальні ситуації у відповідній області для зменшення негайних та потенційних загроз. Використовувати підходи, спрямовані на пом'якшення наслідків, підготовленість, реагування та відновлення, коли це потрібно, для виживання, збереження власності та інформаційної безпеки. Досліджувати та аналізувати всі необхідні заходи з реагування		

	7Г4	Здатність застосовувати наявну інформацію про один або декілька регіонів, країни, недержавні організації та/або технології тощо, необхідну для успішного функціонування організації (установи, підприємства) сфери інформаційної безпеки та кібербезпеки		
	7Д1	Здатність визначати та оцінювати спроможності та діяльність кримінальних злочинців у сфері кібербезпеки або іноземних розвідувальних служб. Готувати висновки, які допомагають ініціалізувати або підтримувати правоохоронні та контррозвідувальні розслідування чи заходи		
	7Є1	Здатність застосовувати тактики, методики та процедури повного спектру засобів і процесів розслідування, що включають в себе, але не обмежуються, методи інтерв'ю та допиту, розвідки, контррозвідки і виявлення спостереження, та належним чином збалансовувати переваги обвинувачення проти збору розвідувальних даних		
	7Є2	Здатність збирати, оброблювати, зберігати, аналізувати та надавати докази, пов'язані з комп'ютерною технікою, для підтримки зменшення вразливостей мережі та/або для кримінальних, шахрайських, контррозвідувальних або правоохоронних розслідувань		
8	**8В5**	Здатність здійснювати нагляд, управляти та/або керувати роботою та працівниками, які виконують роботу з	Лідерство, вільне компе-	Використання широких спеціальних

		кібербезпеки, пов’язану з нею діяльність, або проводять/координують кібероперації		тентне спілкування в діалоговому режимі з широким колом фахівців найвищої кваліфікації, та громадськістю в певній галузі наукової та/або професійної діяльності.	знань нових і інноваційних технологій, у поєднанні з глибоким розумінням бізнесу, передбачення майбутніх рішень. Забезпечення експертного керівництва і консультацій керівництва команди для підтримки прийняття стратегічних рішень. Ініціювання розробки інноваційних комплексних проєктів комп’ютерних систем, з керування інформацією та знаннями, лідерство та повна автономність під час їх реалізації. Глибоке усвідомлення та відповідальність за наукове обґрунтування

					стратегічних рішень, достовірність прогнозування розвитку профільної сфери. Безперервний саморозвиток і само-вдосконалення, відповідальність за розвиток підпорядкованих працівників. Прийняття стратегічних рішень, передбачення майбутніх рішень у сфері інформаційної безпеки та кібербезпеки для клієнто-орієнтованих процесів, нових бізнес-продуктів і послуг, управління та організація їх розбудови та експлуатації

Частина 4. Розподіл професійних кваліфікацій сфери інформаційної безпеки та кібербезпеки за рівнями НРК та ГРК КБ

До цього розподілу ввійшло 60 повних, часткових та часткових додаткових професійних кваліфікацій сфери інформаційної безпеки та кібербезпеки.

За віднесенням до рівнів НРК вони розподілилися наступним чином:

- 5 рівень НРК: 2;
- 6 рівень НРК: 7:
- 7 рівень НРК: 48;
- 8 рівень НРК: 3.

За типом професійної кваліфікації розподіл має такий вигляд:

- Повні: 29;
- Часткові: 8;
- Часткові додаткові: 23.

Розподіл професійних кваліфікацій сфери інформаційної безпеки та кібербезпеки за рівнями НРК та ГРК КБ

Номер з/п	**Рівень НРК**	**Рівень ГРК КБ**	**Назва професійної кваліфікації**	**Тип професійної кваліфікації**	**Код КП**	**Назва освітньої кваліфікації**
1	5	5Е3	Кібероператор	Повна	4113	Фаховий молодший бакалавр
2	5	5Е3	Старший кібероператор	Часткова додаткова	4113	Фаховий молодший бакалавр

3	6	6А6	Молодший фахівець з тестування систем захисту інформації	Часткова	2139.2	Бакалавр
4	6	6Б1	Молодший адміністратор бази даних *сфери інформаційної безпеки та кібербезпеки*	Часткова	2131.2	Бакалавр
5	6	6Б3	Молодший фахівець з технічного захисту інформації	Часткова	2139.2	Бакалавр
6	6	6Б5	Молодший адміністратор мереж і систем	Часткова	2139.2	Бакалавр
7	6	6В3	Молодший фахівець з криптографічного захисту інформації	Часткова	2139.2	Бакалавр
8	6	6Г2	Молодший фахівець з підтримки інфраструктури кіберзахисту	Часткова	2139.2	Бакалавр
9	6	6Г3	Молодший фахівець з реагування на інциденти кібербезпеки	Часткова	2139.2	Бакалавр
10	7	7А1	Уповноважений з авторизації безпеки інформації	Повна	2139.2	Магістр
11	7	7А1	Фахівець з оцінки заходів захисту інформації (кібербезпеки)	Повна	2139.2	Магістр
12	7	7А1	Провідний фахівець з оцінки заходів захисту інформації (кібербезпеки)	Часткова додаткова	2139.2	Магістр
13	7	7А3	Конструктор систем кібербезпеки	Повна	2132.2	Магістр
14	7	7А3	Провідний конструктор систем кібербезпеки	Часткова додаткова	2132.2	Магістр
15	7	7А4	Фахівець із кібердосліджень та розробок систем безпеки	Повна	2139.2	Магістр

16	7	7А4	Провідний фахівець із кібердосліджень та розробок систем безпеки	Часткова додаткова	2139.2	Магістр
17	7	7А6	Фахівець з тестування систем захисту інформації	Повна	2139.2	Магістр
18	7	7А6	Провідний фахівець з тестування систем захисту інформації	Часткова додаткова	2139.2	Магістр
19	7	7А7	Розробник систем захисту інформації	Повна	2132.2	Магістр
20	7	7А7	Провідний розробник систем захисту інформації	Часткова додаткова	2132.2	Магістр
21	7	7А7, 7Б3, 7Б6, 7Г2	Фахівець сфери захисту інформації	Повна	2139.2	Магістр
22	7	7А7, 7Б3, 7Б6, 7Г2	Провідний фахівець сфери захисту інформації	Часткова додаткова	2139.2	Магістр
23	7	7А7, 7Б3, 7Б6, 7Г2	Системний фахівець сфери захисту інформації	Часткова додаткова	2139.2	Магістр
24	7	7Б1	Адміністратор бази даних *сфери інформаційної безпеки та кібербезпеки*	Повна	2131.2	Магістр
25	7	7Б1	Провідний адміністратор бази даних *сфери інформаційної безпеки та кібербезпеки*	Часткова додаткова	2131.2	Магістр
26	7	7Б3	Фахівець з технічного захисту інформації	Повна	2139.2	Магістр
27	7	7Б3	Провідний фахівець з технічного захисту інформації	Часткова додаткова	2139.2	Магістр
28	7	7Б5	Адміністратор мереж і систем	Повна	2139.2	Магістр

29	7	7Б5	Провідний адміністратор мереж і систем	Часткова додаткова	2139.2	Магістр
30	7	7Б6	Аналітик систем захисту інформації	Повна	2139.2	Магістр
31	7	7Б6	Провідний аналітик систем захисту інформації	Часткова додаткова	2139.2	Магістр
32	7	7В1	Фахівець з юридичних консультацій та адвокації в сфері кібербезпеки	Повна	2139.2	Магістр
33	7	7В1	Провідний фахівець з юридичних консультацій та адвокації в сфері кібербезпеки	Часткова додаткова	2139.2	Магістр
34	7	7В2	Інструктор-методист з інформаційної безпеки та кібербезпеки	Повна	2139.2	Магістр
35	7	7В2	Провідний інструктор-методист з інформаційної безпеки та кібербезпеки	Часткова додаткова	2139.2	Магістр
36	7	7В3	Фахівець з питань безпеки (інформаційно-комунікаційні технології)	Повна	2139.2	Магістр
37	7	7В3	Провідний фахівець з питань безпеки (інформаційно-комунікаційні технології)	Часткова додаткова	2139.2	Магістр
38	7	7В3	Фахівець з криптографічного захисту інформації	Повна	2139.2	Магістр
39	7	7В3	Провідний фахівець з криптографічного захисту інформації	Часткова додаткова	2139.2	Магістр
40	7	7В4	Фахівець з планування політики та стратегії кібербезпеки	Повна	2139.2	Магістр

41	7	7В4	Провідний фахівець з планування політики та стратегії кібербезпеки	Часткова додаткова	2139.2	Магістр
42	7	7В6	Аудитор інформаційних технологій (з кібербезпеки)	Повна	2139.2	Магістр
43	7	7В6	Провідний аудитор інформаційних технологій (з кібербезпеки)	Часткова додаткова	2139.2	Магістр
44	7	7Г1	Аналітик з безпеки інформаційних систем	Повна	2139.2	Магістр
45	7	7Г1	Провідний аналітик з безпеки інформаційних систем	Часткова додаткова	2139.2	Магістр
46	7	7Г2	Фахівець з підтримки інфраструктури кіберзахисту	Повна	2139.2	Магістр
47	7	7Г2	Провідний фахівець з підтримки інфраструктури кіберзахисту	Часткова додаткова	2139.2	Магістр
48	7	7Г3	Фахівець з реагування на інциденти кібербезпеки	Повна	2139.2	Магістр
49	7	7Г3	Провідний фахівець з реагування на інциденти кібербезпеки	Часткова додаткова	2139.2	Магістр
50	7	7Г4	Аналітик з оцінки вразливостей	Повна	2139.2	Магістр
51	7	7Г4	Провідний налітик з оцінки вразливостей	Часткова додаткова	2139.2	Магістр
52	7	7Д1	Аналітик загроз безпеки	Повна	2139.2	Магістр
53	7	7Д1	Провідний аналітик загроз безпеки	Часткова додаткова	2139.2	Магістр
54	7	7Є1	Дізнавач (сфера кібербезпеки та захисту інформації)	Повна	2139.2	Магістр
55	7	7Є1	Слідчий з кіберзлочинів	Повна	2139.2	Магістр

56	7	7Є2	Експерт-криміналіст (сфера кібербезпеки та захисту інформації)	Повна	2139.2	Магістр
57	7	7Є2	Експерт-криміналіст судової експертизи (сфера кібербезпеки та захисту інформації)	Повна	2139.2	Магістр
58	8	8В5	Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту	Повна	1239	Доктор філософії
59	8	8В5	Керівник підприємства (установи, організації) (сфера захисту інформації)	Повна	1210.1	Доктор філософії
60	8	8В5	Заступник керівника підприємства (установи, організації) (сфера захисту інформації)	Часткова	1210.1	Доктор філософії

Частина 5. Короткий опис (картки) професійних кваліфікацій ГРК КБ

Короткий опис професійних кваліфікацій частково проведено з урахуванням інформації, викладеної в проєкті ГРК КБ, у чинних професійних стандартах, у робочих версіях проєктів професійних стандартів, що розроблюються. Були також частково використані структура та окремі описи з Європейської рамки компетентностей із кібербезпеки.

Короткий опис (картки) професійних кваліфікацій ГРК КБ потребує подальшого доопрацювання та має за станом на 01.04.2023 року такий вигляд:

- Розроблено 14 карток за професійними кваліфікаціями, описаними у чинних 6 професійних стандартах (номери позицій у Частині 5): 6,19,20, 21, 22, 23, 28, 29, 34, 35, 36, 37, 44, 45;
- Розроблено 8 карток за професійними кваліфікаціями, описаними у проєктах 4 професійних стандартів, які розроблюються. Після їх розроблення та затвердження слід остаточно заповнити відповідні картки (номери позицій у Частині 5): 13,14, 15,16, 40, 41, 42, 43;
- Виписано орієнтовні переліки трудових функцій у 27 картках за професійними кваліфікаціями, які будуть описані у проєктах 11 професійних стандартів, які розроблюються. Після їх розроблення та затвердження слід остаточно заповнити відповідні картки (номери позицій у Частині 5): 1, 2, 3, 5, 7, 8, 9, 10, 11, 12, 17,18, 26, 27, 30, 31, 38, 39, 46, 47, 48, 49, 50, 51, 52, 53, 58;
- Не заповнено 8 карток на кваліфікації, які не пророблюються в рамках проєктної роботи, але входять до ГРК КБ (номери позицій у Частині 5): 4, 24, 25, 32, 33, 54, 55, 56, 57, 59, 60.

1. **Кібероператор**

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	5
Рівень ГРК КБ	5Е3
Тип кваліфікації	Повна
Код КП	4113
Назва освітньої кваліфікації	Фаховий молодший бакалавр
Перелік трудових функцій та професійних компетентностей	А. Здійснення експлуатації та підтримки автоматизованих систем для отримання і здійснення доступу до цільових систем (Т0756) Б. Збір, оброблення та надання відповідних даних В. Проведення мережевої розвідки і аналізу вразливостей систем у мережі (Т0616) Г. Здійснення кібердіяльності з метою руйнування/видалення інформації, що міститься в комп’ютерах і обчислювальних мережах (Т0768)
Основні необхідні знання	
Основні необхідні уміння та навички	

2. Старший кібероператор

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	5
Рівень ГРК КБ	5Е3
Тип кваліфікації	Часткова додаткова
Код КП	4113
Назва освітньої кваліфікації	Фаховий молодший бакалавр
Перелік трудових функцій та професійних компетентностей	Трудові функції А, Б, В та Г, притаманні "Кібероператору", та додатково: Д. Аналіз внутрішньої операційної архітектури, інструментів та процедур для визначення способів підвищення продуктивності (T0566) Е. Розроблення нових методик для отримання і підтримки доступу до цільових систем (T0664)
Основні необхідні знання	
Основні необхідні уміння та навички	

3. Молодший фахівець з тестування систем захисту інформації

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	6
Рівень ГРК КБ	6А6
Тип кваліфікації	Часткова
Код КП	2139.2
Назва освітньої кваліфікації	Бакалавр
Перелік трудових функцій та професійних компетентностей	А. Проведення підготовчих робіт до тестування систем захисту інформації Б. Виконання тестування системи захисту інформації у процесі її розроблення (Т0511) В. Проведення тестування, оцінювання та перевірки програмного та/або апаратного забезпечення з метою визначення їх відповідності встановленим специфікаціям і вимогам (Т0539)
Основні необхідні знання	
Основні необхідні уміння та навички	

4. **Молодший адміністратор бази даних *сфери інформаційної безпеки та кібербезпеки***

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	6
Рівень ГРК КБ	6Б1
Тип кваліфікації	Часткова
Код КП	2131.2
Назва освітньої кваліфікації	Бакалавр
Перелік трудових функцій та професійних компетентностей	----------
Основні необхідні знання	----------
Основні необхідні уміння та навички	**----------**

5. Молодший фахівець з технічного захисту інформації

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	6
Рівень ГРК КБ	6Б3
Тип кваліфікації	Часткова
Код КП	2139.2
Назва освітньої кваліфікації	Бакалавр
Перелік трудових функцій та професійних компетентностей	А. Встановлення та підтримування програмного забезпечення операційної системи пристрою мережі інфраструктури (Т0125) Б. Діагностування та усунення системних інцидентів, проблем і подій, про які повідомили клієнти (Т0468) В. Аналіз даних про інциденти для виявлення тенденцій (Т0308) Г. Моніторинг і звітування про продуктивність комп'ютерної системи на рівні клієнта (Т0502)
Основні необхідні знання	
Основні необхідні уміння та навички	

6. Молодший адміністратор мереж і систем

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	6
Рівень ГРК КБ	6Б5
Тип кваліфікації	Часткова
Код КП	2139.2
Назва освітньої кваліфікації	Бакалавр
Перелік трудових функцій та професійних компетентностей	А. Підготовка до роботи систем і мереж щодо захисту інформації відповідно до політики підприємства/ організації А1. Здатність перевіряти придатність, функціональність, цілісність та ефективність апаратного забезпечення системи та мережі щодо захисту інформації А2. Здатність розробляти та документувати стандартні операційні процедури адміністрування систем щодо захисту інформації А3. Здатність контролювати процес встановлення, впровадження та налаштування компонентів системи щодо захисту інформації Б. Супроводження/ адміністрування діяльності систем і мереж щодо захисту інформації підприємства/ організації Б1. Здатність управляти системними/серверними ресурсами, включно з продуктивністю, ємністю, доступністю, ремонтопридатністю і здатністю відновлюватись Б2. Здатність дотримуватися стандартних операційних процедур адміністрування систем підприємства/організації

	Б3. Здатність впроваджувати та забезпечувати виконання політик і процедур використання локальної мережі В. Адміністрування баз даних В1. Здатність моніторити і підтримувати бази даних з метою забезпечення їхньої оптимальної продуктивності В2. Здатність виконувати резервне копіювання та відновлення баз даних для забезпечення цілісності даних В3. Здатність підтримувати програмне та інше забезпечення систем управління базами даних В4. Здатність впроваджувати стандарти управління даними, вимоги і специфікації Г. Обслуговування, встановлення та оновлення систем/серверів Г1. Здатність проводити періодичне обслуговування системи та мережі Г2. Здатність вирішувати проблеми з апаратним/програмним інтерфейсом та проблеми сумісності
Основні необхідні знання	Знати: -Концепції та протоколи комп'ютерних мереж, а також методології забезпечення мережевої безпеки - Інструменти та методики налаштування продуктивності компонентів системи - Теорії, концепції та методи адміністрування серверів і проєктування систем - Інструментальні утиліти для мережі - Засоби діагностики систем/серверів і методики визначення несправностей

	- Закони, нормативні акти, політики і етичні норми, як вони пов’язані з кібербезпекою та приватністю - Принципи кібербезпеки і приватності - Архітектуру інформаційних технологій підприємства/організації - Політику безпеки користувача організації, що використовує інформаційні технології (створення облікового запису, правила паролів, контроль доступу) - Методики адміністрування системи, мережі та захисту операційних систем - Операційні системи - Технології передання голосу через IP - Технології запису передаваних сигналів та методики «перешкод», які забезпечують передання небажаної інформації або не дозволяють інстальованим системам функціонувати коректно - Принципи і методи інтеграції системних компонентів - Принципи та концепції мережевих зв’язків на локальних і глобальних рівнях, включно з управлінням пропускною здатністю (трафіком) - Характеристики фізичних і віртуальних електронних засобів зберігання даних - Технології віртуалізації та розроблення й підтримки віртуальних машин - Теорію, концепції і методи системної інженерії систем - Методи, принципи та концепції комунікацій, які підтримують інфраструктуру мережі - Політику адміністрування даних і стандартизації даних

	- Засоби контролю доступу до баз даних, адаптивних до ризиків і заснованих на політиці підприємства/організації - Системи управління базами даних, мов побудови запитів, взаємозв'язків між таблицями, уявлення таблиць - Мови формування запитів, структуровану мову запитів (SQL) - Джерела, характеристики і принципи застосування активів даних підприємства/організації - Принципи організації та функціонування сучасних файлових систем, зберігання слабко- та сильноструктурованих даних та метаданих - Сучасні і перспективні функції безпеки відновлення даних в базах даних - Резервне копіювання та відновлення даних - Критерії або показники продуктивності та доступності систем - Теорію баз даних - Типи і періодичність планової підтримки апаратного забезпечення - Операційні системи сервера і клієнта - Спроможності прикладних програм управління мережевим обладнанням (маршрутизатори, комутатори, мости, сервери, засоби передання і відповідне технічне обладнання) - Управління мережевим доступом, ідентифікацією та доступом - Концепції архітектури безпеки мережі, включно з топологією, протоколами, компонентами і принципами
Основні необхідні уміння та навички	Уміти:

	- Користуватися загальнодоступними мережевими інструментами - Діагностувати несправні системні компоненти (сервери) - Встановлювати оновлення системи та компонентів (серверів, пристроїв, зокрема мережевих пристроїв) - Застосовувати принципи кібербезпеки та приватності при формуванні вимог організації (стосовно конфіденційності, цілісності, доступності, автентифікації та неспростовності) - Налаштовувати і використовувати програмні засоби захисту комп'ютерів (програмні фільтри, антивірусна програма й антишпигунське програмне забезпечення - Проводити планування, управління та обслуговування систем/серверів - Застосовувати принципи кібербезпеки і приватності при формуванні організаційних вимог (що стосуються конфіденційності, цілісності, доступності, автентифікації та неспростовності) - Проводити моніторинг та оптимізацію роботи системи/сервера - Здійснювати ідентифікацію та прогнозування системної/серверної роботи, доступності, можливостей або проблем з налаштуванням - Створювати схеми маршрутизації - Використовувати віртуальні машини - Експлуатувати мережеве обладнання, включно з концентраторами, маршрутизаторами, комутаторами, мостами, серверами, засобами передання та відповідним апаратним обладнанням - Підтримувати бази даних - Використовувати цілі та завдання підприємства / організації при розробленні та підтримці архітектури систем - Встановлювати, налаштовувати та усувати несправності в компонентах LAN та WAN, таких як маршрутизатори, концентратори та комутатори - Налаштовувати і оптимізувати ПЗ - Розробляти, оновлювати та/або підтримувати стандартні операційні процедури (SOP)

	- Визначати інциденти, проблеми та події в системі обробки звернень клієнтів - Адмініструвати операційні системи (ведення облікових записів, резервне копіювання даних, підтримання продуктивності системи, інсталяція і налаштування нового апаратного/програмного забезпечення) - Створювати запити та звіти відповідного спрямування - Розподіляти ємності сховища при проєктуванні систем управління даними - Робити запити і розробляти алгоритми для аналізу структур даних - Проводити моніторинг показників або індикаторів продуктивності та доступності системи - Виправляти фізичні та технічні проблеми, що впливають на роботу системи/сервера - Відновлювати системи/сервери після виявленого збою (програмне забезпечення для відновлення, відмовостійкі кластери, дублювання/«зеркалювання») - Встановлювати та підтримувати автоматизовані оцінки контролів безпеки

7. Молодший фахівець з криптографічного захисту інформації

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	6
Рівень ГРК КБ	6В3
Тип кваліфікації	Часткова
Код КП	2139.2
Назва освітньої кваліфікації	Бакалавр
Перелік трудових функцій та професійних компетентностей	А. Проведення підготовчих робіт із запровадження на підприємстві (в установі, організації) системи криптографічного захисту інформації Б. Забезпечення впровадження , оцінювання та затвердження заходів з криптографічного захисту інформації на підприємстві (в установі, організації) (Т0089) В. Підготовка та запровадження на практиці документації щодо розробки програми з криптографічного захисту інформації, а також формувати нові редакції, додаючи коментарі до закодованих інструкцій, щоб користувачі могли зрозуміти як функціонує програма (Т0026)
Основні необхідні знання	
Основні необхідні уміння та навички	

8. Молодший фахівець з підтримки інфраструктури кіберзахисту

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	6
Рівень ГРК КБ	6Г2
Тип кваліфікації	Часткова
Код КП	2139.2
Назва освітньої кваліфікації	Бакалавр
Перелік трудових функцій та професійних компетентностей	А. Створення, встановлення, налагодження та тестування спеціального технічного забезпечення для кіберзахисту (Т0335) Б. Здійснення системного адміністрування спеціалізованих прикладних програм кіберзахисту та систем, або пристроїв віртуальних приватних мереж, включаючи інсталяції, налаштування, обслуговування, резервне копіювання і відновлення (Т0180) В. Адміністрування тестових стендів та тестування/оцінювання апаратної інфраструктуруи правил/підписів, контролю доступу і конфігурації платформ, що обслуговуються провайдером послуг (Т0420)
Основні необхідні знання	
Основні необхідні уміння та навички	

9. Молодший фахівець з реагування на інциденти кібербезпеки

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	6
Рівень ГРК КБ	6ГЗ
Тип кваліфікації	Часткова
Код КП	2139.2
Назва освітньої кваліфікації	Бакалавр
Перелік трудових функцій та професійних компетентностей	А. Відстеження та документування інцидентів кібербезпеки з моменту їх виявлення до остаточного вирішення (Т0233) Б. Моніторинг зовнішніх джерел даних для підтримки поточного стану загроз кіберзахисту, та визначення того, які проблеми безпеки можуть вплинути на підприємство (установу, організацію) (Т0503) В. Аналіз тенденцій в області кіберзахисту, лог-файлів з різних джерел з метою визначення можливих загроз безпеці мережі, в масштабі реального часу аналіз кіберінцидентів метою підтримки створюваних груп реагування на інциденти (Т0161) Т0164, Т0175)
Основні необхідні знання	
Основні необхідні уміння та навички	

10. Уповноважений з авторизації безпеки інформації

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7А1
Тип кваліфікації	Повна
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	А. Керування підготовкою та супроводження при затвердженні пакетів документів з авторизації безпеки інформації (Т0145) Б. Керування підготовкою та супроводження при затвердженні пакетів документів з акредитації відповідної діяльності (Т0495) Г. Перегляд документів щодо авторизації та надання впевненості, щоб підтвердити, що рівень ризику знаходиться в допустимих межах для кожної прикладної програми, системи та мережі (Т0221) Д. Встановлення допустимих лімітів прикладного програмного забезпечення, мереж та систем (Т0371) Е. Проведення тренінгів для заінтересованих сторін з питань авторизації безпеки інформації
Основні необхідні знання	
Основні необхідні уміння та навички	

11. Фахівець з оцінки заходів захисту інформації (кібербезпеки)

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7А1
Тип кваліфікації	Повна
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	А. Оцінювання забезпечення впровадження та функціональності вимог безпеки та відповідних політик і процедур ІТ, визначення впливу впровадження нових систем або інтерфейсів між системами на стан захищеності діючої інфраструктури (Т0265, Т0268) Б. Аналіз системи безпеки, визначення пробілів в архітектурі безпеки та розроблення план управління ризиками, аналіз ризиків коли прикладна програма або система зазнають значних змін (Т0177, Т0181) В. Нагляд за виконанням планів заходів для усунення вразливостей, виявлених під час оцінювання ризиків, аудиторських та інспекторських перевірок (Т0364) Г. Оцінювання ефективності засобів контролю безпеки та процесів управління конфігурацією (Т0309, Т0344)
Основні необхідні знання	
Основні необхідні уміння та навички	

12. Провідний фахівець з оцінки заходів захисту інформації (кібербезпеки)

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7А1
Тип кваліфікації	Часткова додаткова
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	Трудові функції А, Б, В та Г, притаманні " Фахівцю з оцінки заходів захисту інформації (кібербезпеки)", та додатково: Д. Оцінювання дії з придбання, постачання, закупівлі та аутсорсингу відповідають вимогам з кібербезпеки (Т0277)
Основні необхідні знання	
Основні необхідні уміння та навички	

13. Конструктор систем кібербезпеки

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7А3
Тип кваліфікації	Повна
Код КП	2132.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	А. Проведення аналізу та технічних розрахунків під час роботи з документацією із проєктування/моделювання систем кіберзахисту А1. Здатність підбирати, систематизувати й аналізувати доступну конструкторську документацію, зокрема інших підприємств/організацій, з метою її використання в процесі проєктування та моделювання систем кіберзахисту А2. Здатність проводити технічні розрахунки в процесі проєктування/моделювання систем кіберзахисту, техніко-економічний і функціонально-вартісний аналіз їх ефективності А3. Здатність застосовувати на практиці загальні теоретично-методологічні знання відповідного спрямування Б. Розроблення технічних і робочих проєктів/моделей систем кіберзахисту та відповідної допоміжної документації Б1. Здатність розроблювати технічні і робочі проєкти/моделі систем кіберзахисту особливо складної, складної і середньої складності та відповідної допоміжної документації з використанням комп’ютерно-інтегрованих технологій

	Б2. Здатність застосовувати в конструкторській роботі засоби автоматизації проєктування/моделювання, передовий досвід розроблення/інтеграції конкурентоспроможних систем кіберзахисту Б3. Здатність забезпечувати в процесі проєктування/моделювання систем кіберзахисту відповідність розроблюваних моделей, схем та компонентів технічним завданням, стандартам, нормам охорони праці, вимогам найбільш економної технології виробництва та експлуатації Б4. Здатність застосовувати під час проєктування/моделювання систем кіберзахисту стандартизовані й уніфіковані програми, компоненти та операційні процедури Б5. Здатність погоджувати проєкти/моделі систем кіберзахисту, що розроблюються, з іншими структурними підрозділами організації, представниками замовника та/чи органів державного нагляду В. Проведення робіт з випробування, експлуатації, удосконалення, модернізації та уніфікації конструйованих моделей систем кіберзахисту В1. Здатність проводити розрахунки ризиків при розробленні нових моделей систем кіберзахисту В2. Здатність брати участь у роботах з уніфікації конструювання/моделювання систем кіберзахисту та їх компонентів
Основні необхідні знання	Знати: - Технології віртуалізації, формування віртуальних машин та їх технічної підтримки - Нові та ті, що розроблюються технології інформаційної та кібербезпеки

	- Зовнішні організації і наукові установи, діяльність яких спрямована на моделоювання систем кіберзахисту - Технологічні вимоги до документації відповідного спрямування - Технічні характеристики й економічні показники кращих вітчизняних і світових розробок із кіберзахисту - Передові світові технологічні тенденції виготовлення продукції у сфері кіберзахисту - Досвід передових вітчизняних і зарубіжних підприємств щодо конструювання/моделювання систем кіберзахисту - Класифікацію кіберзагроз та вразливостей - Операційні наслідки в результаті помилок кібербезпеки - Методи: автентифікації, авторизації та контролю доступу; аналізу спроможностей і вимог - Прикладні бізнес- процеси і функції в організації/підприємстві –замовнику - Вразливості прикладних приграм - Методи, принципи і концепції комунікацій, які підтримують інфраструктуру мережі - Спроможності та прикладні програми мережевого обладнання, включаючи маршрутизатори, комутатори, мости, сервери, засоби передачі і відповідне технічне обладнання - Класифікацію оцінок систем кіберзахисту і вразливостей, а також їх можливостей - Нові та виникаючі інформаційні технології та технології кібербезпеки - Основні концепції управління безпекою (управління версіями, патч-менеджмент тощо)

	- Стандарти й технічні умови, які використовуються під час проєктування/моделювання систем кіберзахисту - Експериментальні методології розроблення кіберпродуктів - Основні аспекти проєктування кіберпродукції - Методи та ризики, пов'язані з вибором компонентів кіберпродукції - Системи баз даних - Правила безперервності бізнесу та операційних планів відновлення безперервності після катастроф - Корпоративну архітектуру інформаційної безпеки організації/підприємства - Технологію побудови програмного забезпечення - Процедури інсталяції, інтеграції та оптимізації компонентів системи - Процес оцінки стану безпеки і процесу авторизації - Процес планування захисту програм - Концепції і моделі IT архітектури організації/підприємства - Порядок інтеграції цілей і завдань організації/підприємства в архітектуру - Порядок оформлення технічного завдання на роботи з проєктування та моделювання систем кіберзахисту - Процеси інтеграції технологій - Принципи, інструменти та методики тестування на проникнення - Концепції вдосконалення процесів організації та моделей зрілості процесів (Capability Maturity

	Model Integration (CMMI) for Development, CMMI for Services, and CMMI for Acquisitions тощо) - Технології виробництва, комунікації та розповсюдження медійних повідомлень, а також альтернативні способи інформування за допомогою текстових, мовних, візуальних повідомлень - Внутрішніх і зовнішніх замовників та партнерських організацій, включаючи їх інформаційні потреби, цілі, структури, можливості тощо
Основні необхідні уміння та навички	Уміти: - Освоювати досягнення у технологіях захисту інформації для забезпечення їх впровадження у відповідній організації - Аналізувати запропоновані архітектури, розподіляти послуги безпеки і обирати механізми безпеки - Збирати точні та повні дані з джерел, які використовуються при моделюванні систем кіберзахисту - Формувати й оновлювати базу знайдених матеріалів для подальшого її використання в роботі - Оцінювати і проєктувати функції управління безпекою, пов'язані з кіберпростором - Проводити оцінювання ефективності існуючих програм, процесів і вимог щодо архітектури систем кіберзахисту - Виконувати розрахунки технічних, техніко-економічних і функціонально-вартісних показників моделей систем кіберзахисту, що проєктуються про закупівлі - Аналізувати потреби та вимоги користувачів для планування архітектури - Застосовувати сучасні методи проєктування та моделювання систем кіберзахисту

	- Пояснювати особливості конструкції та основні аспекти робочих процесів у компонентах нових моделей систем кіберхахисту - Проєктувати архітектури та загальні принципи - Розроблювати: технічну документацію відповідного спрямування; компоненти архітектури або системних компонент підприємства, необхідних для задоволення потреб користувачів; багаторівневі рішення безпеки/міждоменних рішень - Розроблювати і застосовувати в моделюванні систем кіберзахисту технології, що стосуються кібербезпеки, математичні або статистичні моделі - Використовувати наукові підходи і методики при вирішенні проблем у моделюванні систем кіберзахисту - Застосовувати в практичній діяльності: процеси технічної розробки систем ; стандарти і процедури життєвого циклу програмного забезпечення і інженерії систем - Розроблювати/інтегрувати проєкти з кібербезпеки для систем та мереж із багаторівневими вимогами безпеки або вимогами для обробки кількох рівнів класифікації даних, що застосовуються головним чином до державних організацій - Застосовувати та інтегровувати інформаційні технології до запропонованих рішень - Визначати: необхідний рівень складності тесту для конкретної системи; як буде функціонувати система безпеки (включаючи її властивості відмовостійкості і надійності), та як зміни умов, операцій або середовища вплинуть на ці результати - Моделювати проєкти і побудову сценаріїв їх використання - Виступати основною сполучною ланкою між головним конструктором підприємства та інженером систем безпеки та співпрацювати з власниками систем, постачальниками загальних

	контролів та працівниками системи безпеки щодо розподілу контролів безпеки на системні, гібридні або загальні контролі - Консультувати посадових осіб, директорів інформаційних технологій, директорів із інформаційної безпеки та відповідальної посадової особи з управління ризиками/виконавчого ризику (функції) щодо питань безпеки - Розроблювати контрзаходи для виявлення ризиків безпеки - Визначати і документувати те, як впровадження нових систем або інтерфейсів між системами вплине на стан захищеності діючої інфраструктури

14. Провідний конструктор систем кібербезпеки

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7А3
Тип кваліфікації	Часткова додаткова
Код КП	2132.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	Трудові функції А, Б та В, притаманні "Конструктору систем кібербезпеки ", та додатково: Г. Проведення патентних досліджень, підготовка відгуків і висновків щодо проєктів профільних стандартів, раціоналізаторські пропозиції і винаходи, пов'язані з моделюванням систем кіберзахисту та наукомісткої продукції для підприємств/організацій, задіяних у забезпеченні кібербезпеки Г1. Здатність складати заявки на винаходи й промислові зразки моделей систем кіберзахисту Г2. Здатність готувати відгуки й висновки на проєкти стандартів, раціоналізаторські пропозиції й винаходи, які стосуються окремих компонентів нових моделей систем кіберзахисту Г3. Здатність проводити патентні дослідження у сфері конструювання, моделювання та експлуатації нових систем кіберзахисту Г4. Здатність визначати показники технічного рівня моделей систем кіберзахисту, які проєктуються/моделюються Д. Проведення робіт з адаптації процесів з моделювання систем кіберзахисту до існуючої в організації/на підприємстві системи

	менеджменту якості та підвищення загальної ефективності виробництва кіберпродукції та кіберпослуг Д1. Здатність здійснювати технічне керівництво профільними працівниками, задіяними в конструкторській діяльності Д2. Здатність взаємодіяти з керівництвом, профільними структурними підрозділами організації/підприємства, задіяного у забезпеченні кібербезпеки, стосовно питань відповідного спрямування
Основні необхідні знання	Основні необхідні знання, притаманні "Конструктору систем кібербезпеки", та додатково знати: - Стандарти й технічні умови, які використовуються під час складання заявок на винаходи й промислові зразки систем кіберзахисту - Основи: винахідництва щодо конструювання систем кіберзахисту; науково-технічної, винахідницької й раціоналізаторської діяльності в організаціях/ підприємствах з виробництва систем кіберзахисту - Стандарти й технічні умови, які використовуються під час запровадження на практиці результатів винахідницької й раціоналізаторської діяльності в організаціях/підприємствах з виробництва систем кіберзахисту - Нормативні документи і правила, що забезпечують захист авторських прав, патентування, винаходи - Новітні технології, інструменти, процедури, методи та процеси відповідного спрямування - Основи: патентознавства; - Основи реверс-інжинірингу

	- Характеристики сучасного технологічного обладнання, яке використовується під час створення систем кіберзахисту та їх компонентів - Технологію створення систем кіберзахисту та їх компонентів - Технологічні характеристики сучасного технологічного оснащення, яке використовується при створенні систем кіберзахисту та їх компонентів - Моделі та симуляції, які застосовуються для аналізу або прогнозування продуктивності системи за різних умов експлуатації - Чинні вітчизняні, зарубіжні та міжнародні стратегії мінімізації ризиків для зменшення витрат, графіку, продуктивності і ризиків безпеки - Порядок побудови, тестування та модифікації прототипів кіберпродуктів - Підходи до визначення, оцінювання та рекомендування продуктів системи кібербезпеки або продуктів, що сприяють кібербезпеці - Загальні принципи управління ризиками та відповідну документацію (плани забезпечення життєвого циклу системи, концепція операцій, операційні процедури і навчальні матеріали з технічного обслуговування тощо)
Основні необхідні уміння та навички	Основні необхідні уміння та навички, притаманні "Конструктору систем кібербезпеки", та додатково уміти: - Брати участь у розробленні профільних патентних і ліцензійних паспортів - Готувати замовлення на нове устаткування й заявки на винаходи й промислові зразки відповідного спрямування - Обґрунтовувати й оцінювати інноваційні проєкти у виробництві систем кіберзахисту - Використовувати сучасні методи виконання винахідницьких завдань, захисту інтелектуальної

	власності на технічні рішення, створені в процесі профільної професійної діяльності - Брати участь у підготовці висновків про доцільність використання підприємством раціоналізаторських пропозицій щодо вдосконалення технології виробництва систем кіберзахисту - Проводити: патентні дослідження відповідного спрямування; розрахунки показників технічного рівня проєктованих об'єктів техніки й технології виробництва нових систем кіберзахисту - Брати участь у розробленні профільних патентних і ліцензійних паспортів, замовлень на нове устаткування, заявок на винаходи й промислові зразки нових систем кіберзахисту - Розроблювати: архітектури або компоненти системи відповідно до технічних умов; стандарти даних, політики та процедури - Надавати консультації щодо витрат на проєкт, концепцій проєктування або змін в проєкті - Складати: технічні вимоги до технологічного обладнання й оснащення, задіяного під час створення систем кіберзахисту та їх компонентів; заявки щодо внесення до плану закупівлі структурним підрозділом технологічного обладнання й оснащення, необхідного для створення систем кіберзахисту та їх компонентів - Розроблювати техніко-економічне обґрунтування на придбання/отримання технологічного обладнання й оснащення, задіяного під час створення систем кіберзахисту та їх компонентів - Забезпечувати заходи щодо тестування та оцінки систем кіберзахисту та сертифікації - Використовувати: спеціалізоване обладнання та методики каталогізації, документування, вилучення, збирання, упаковки та зберігання цифрових доказів; моделі та симуляції для аналізу або прогнозування продуктивності системи кіберзахисту за різних умов експлуатації

	- Розроблювати стратегії мінімізації ризиків для зменшення витрат, графіку, продуктивності і ризиків безпеки - Будувати, тестувати та модифікувати прототипи продуктів за допомогою робочих моделей або теоретичних моделей - Визначати, оцінювати та рекомендувати продукти системи кібербезпеки або продукти, що сприяють кібербезпеці, для використання в системі, і гарантувати, що рекомендовані продукти відповідають організаційним вимогам щодо їхньої оцінки та затвердження - Надавати вхідні дані для діяльності процесу загальних принципів управління ризиками та відповідну документацію - Зберігати, відновлювати та обробляти дані для аналізу можливостей системи та вимог

15. Фахівець із кібердосліджень та розробок систем безпеки

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7А4
Тип кваліфікації	Повна
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	А. Проведення кібердосліджень А1. Здатність досліджувати сучасні технології щоб зрозуміти можливості необхідної системи або мережі А2. Здатність переглядати та затверджувати програми, процеси і вимоги щодо збору та зберігання даних А3. Здатність визначати стратегії кіберможливостей для розробки програмно-апаратних комплексів А4. Здатність оцінювати вразливості мережевої інфраструктури, щоб поширити можливості, які розробляються Б. Проєктування і розроблення нових інструментів/технологій, що стосуються кібербезпеки Б1. Здатність співпрацювати із зацікавленими сторонами для визначення та розроблення відповідної технології рішень Б2. Здатність дотримуватися стандартів і процедур життєвого циклу програмного забезпечення і інженерії систем Б3. Здатність розроблювати засоби зворотної інженерії для підвищення спроможностей і виявлення вразливостей

	Б4. Здатність розроблювати нові можливості управління даними для забезпечення підтримки мобільного персоналу В. Розроблення засобів та методів усунення проблем при проєктуванні та усунення вразливостей при експлуатації систем безпеки В1. Здатність усувати проблеми, що виникають в процесі проєктування прототипів, а також на етапах проектування, розробки і перед запуском продукту В2. Здатність визначати функціональні властивості і властивості, пов'язані із забезпеченням безпеки, з метою пошуку сприятливих можливостей для експлуатації або усунення вразливостей Г. Проєктування та розроблення систем безпеки Г1. Здатність розроблювати детальну проєктну документацію з безпеки для специфікацій компонентів та інтерфейсів з метою підтримки проєкту та розроблення системи безпеки Г2. Здатність проводити аналіз ризиків, коли прикладна програма або система зазнають суттєвих змін Г3. Здатність проводити аналіз ризиків, коли прикладна програма або система зазнають суттєвих змін Д. Впровадження та супроводження систем безпеки Д1. Здатність супроводжувати розроблені системи безпеки Д2. Здатність забезпечувати вхідні дані для планів впровадження і стандартні операційні процедури, які стосуються безпеки інформаційних систем
Основні необхідні знання	Знати:

	- Нові та ті, що розроблюються технології інформаційної та кібербезпеки - Зовнішні організації і наукові установи, діяльність яких спрямована на дослідження кіберпростору - Технологічні вимоги до науково-технічної та іншої дослідницької документації відповідного спрямування - Технічні характеристики й економічні показники кращих вітчизняних і світових розробок із кіберзахисту - Передові світові технологічні тенденції виготовлення продукції у сфері кіберзахисту - Досвід передових вітчизняних і зарубіжних підприємств щодо конструювання кіберпродукції й застосування нових технологій її виробництва - Експериментальні методології розроблення кіберпродуктів - Основні аспекти проєктування кіберпродукції - Методи та ризики, пов'язані з вибором компонентів кіберпродукції - Інструменти аналізу мереж для виявлення вразливостей у програмному забезпеченні, яке здійснює комунікацію - Основні бізнес-процеси і місію організації - Стандарти розробки контрзаходів для виявлених ризиків - Підходи щодо планування мережі і відтворення мереж - Порядок оформлення технічного завдання на дослідницькі роботи з проєктування кіберпродукції - Сучасні та новітні технології проєктування прототипів - Порядок застосування в роботі оригінальних форматів відображення інформації

	- Концепції, процедури, програмне забезпечення, обладнання та/або технологічні прикладні програми, необхідні для визначення функціональних властивостей і властивостей, пов'язаних із забезпеченням безпеки - Підходи до проєктування, розроблення, інтегрування і оновлення показників захищеності системи, які забезпечують конфіденційність, цілісність, доступність, автентифікацію і безвідмовність - Засоби/заходи, що використовують алгоритми побудовані на основі штучного інтелекту для аналізу втручання в роботу інформаційних систем - Нормативні документи і правила, що забезпечують захист авторських прав, патентування, винаходи - Новітні технології, інструменти, процедури, методи та процеси відповідного спрямування - Класифікацію технічних та процедурних процесів для безпечного резервного копіювання системи та захищеного зберігання резервних даних - Наявні плани аварійного відновлення та безперервності операцій для систем, що розробляються - Процедура тестування систем до їхнього вводу у продуктивне середовище - Методологію тестування та оцінки систем безпеки та сертифікації - Номенклатуру спеціалізованого обладнання та методики каталогізації, документування, вилучення, збирання, упаковки та зберігання цифрових доказів - Моделі та симуляції, які застосовуються для аналізу або прогнозування продуктивності системи за різних умов експлуатації - Чинні вітчизняні, зарубіжні та міжнародні стратегії мінімізації ризиків для зменшення витрат, графіку, продуктивності і ризиків безпеки

	- Методику оцінки ризиків інформаційної безпеки
Основні необхідні уміння та навички	Уміти: - Освоювати досягнення у технологіях захисту інформації для забезпечення їх впровадження у відповідній організації - Адаптувати технічну інформацію щодо кібердосліджень та їх результатів до рівня розуміння користувача/споживача/ замовника - Збирати точні та повні дані з джерел, які використовуються при кібердослідженнях - Здійснювати моніторинг змін у нормативно-правових документах відповідного спрямування - Формувати й оновлювати базу знайдених матеріалів для подальшого її використання в роботі - Проводити оцінювання ефективності існуючих програм, процесів і вимог щодо збору та зберігання даних - Здійснювати комплексний аналіз відповідності змісту програм, процесів і вимог щодо збору та зберігання даних встановленим стандартам та регламентам - Читати й аналізувати схеми й креслення, конструкторську, технологічну та іншу документацію відповідного спрямування - Працювати з електронними архівами стандартів і технічних умов, які використовуються під час проєктування кіберпродукції - Надавати визначення та здійснювати опис експериментальних методів дослідження структурних, фізико-механічних і технологічних властивостей матеріалів та компонентів кіберпродукції - Визначати стратегії кіберможливостей для розробки програмно-апаратних комплексів для замовника, ґрунтуючись на вимогах місії

	- Оцінювати вразливості мережевої інфраструктури - Ураховувати у дослідницькій та проєктній діяльності виявлені вразливості мережевої інфраструктури - Проводити моніторинг зауважень, скарг, прокламацій та пропозицій партнерів та користувачів нової кіберпродукції щодо оцінювання наявних вразливості мережевої інфраструктури - Досліджувати і оцінювати наявні технології і стандарти розроблення нової кіберпродукції - Розроблювати настанови стосовно впровадження розроблених систем клієнтам або командам впровадження - Здійснювати зворотній зв'язок з партнерами, підрядниками проєктних та науково-дослідних робіт з розроблення нової кіберпродукції - Розроблювати і застосовувати в проєктуванні нових інструментів/ технологій, що стосуються кібербезпеки, математичні або статистичні моделі - Використовувати наукові підходи і методики при вирішенні проблем у проєктуванні та розробленні нових інструментів/ технологій, що стосуються кібербезпеки - Застосовувати процеси технічної розробки систем -Застосовувати у практичній діяльності стандарти і процедури життєвого циклу програмного забезпечення і інженерії систем - Проєктувати інтеграцію технологічних процесів і рішень, включаючи застарілі системи і сучасні мови програмування - Налаштовувати і використовувати у процесі проєктування прототипів

	- Конфігурувати і використовувати у процесі проєктування прототипів компоненти системи мережевої безпеки - Використовувати сучасні та новітні технології у процесі проєктування прототипів - Проєктувати апаратне забезпечення, операційні системи та прикладне програмне забезпечення для належного дотримання вимог кібербезпеки - Розроблювати та направляти на розгляд процедури тестування та затвердження системи і документацію - Розроблювати та документувати вимоги, властивості та обмеження для процедур проєктування та процесів - Розроблювати та документувати стандартні операційні процедури адміністрування систем - Аналізувати потреби та вимоги користувачів з метою планування і проведення розробки системи безпеки - Проєктувати, розробляти, інтегрувати і оновлювати показники захищеності системи, які забезпечують конфіденційність, цілісність, доступність, автентифікацію і безвідмовність - Розроблювати або інтегровувати відповідні резервні спроможності у загальні проєкти системи та забезпечувати відповідні технічні та процедурні процеси для безпечного резервного копіювання системи та захищеного зберігання резервних даних - Розроблювати та впроваджувати процедури резервного копіювання та відновлення мережі - Розроблювати та підтримувати стратегічні плани - Розроблювати архітектури або компоненти системи відповідно до технічних умов - Розроблювати стандарти даних, політики та процедури - Включати рішення щодо вразливості системи у проєкти систем

	- Розроблювати вимоги безпеки для забезпечення виконання вимог для всіх систем або прикладних програм - Розроблювати спеціальні контрзаходи з кібербезпеки та стратегії пом'якшення ризиків для систем та/або прикладних програм - Визначати компоненти чи елементи, розподіляти функції безпеки для цих елементів і описувати взаємозв'язок між елементами - Розроблювати детальну проєктну документацію з безпеки для специфікацій компонентів та інтерфейсів з метою підтримки проєкту та розроблення системи безпеки - Розроблювати стратегії мінімізації ризиків для зменшення витрат, графіку, продуктивності і ризиків безпеки - Виконувати оцінку ризиків інформаційної безпеки - Визначати, оцінювати та рекомендувати продукти системи кібербезпеки або продукти, що сприяють кібербезпеці, для використання в системі, і гарантувати, що рекомендовані продукти відповідають організаційним вимогам щодо їхньої оцінки та затвердження

16. Провідний фахівець із кібердосліджень та розробок систем безпеки

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7А4
Тип кваліфікації	Часткова додаткова
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	Трудові функції А, Б, В, Г та Д притаманні "Фахівцю з кібердосліджень та розробок систем безпеки", та додатково: Е. Консультування, популяризація та оцінювання її результатів стосовно застосування на практиці результатів кібердосліджень Е1. Здатність застосовувати принципи навчання дорослих Е2. Здатність розроблювати обґрунтовані і надійні оцінки результатів кібердосліджень та результатів навчання відповідного спрямування
Основні необхідні знання	Основні необхідні знання, притаманні "Фахівцю з кібердосліджень та розробок систем безпеки ", та додатково знати: - Методи соціальної інженерії - Вимоги і правила дотримання академічної доброчесності - Методи і технології підготовки доповідей та презентацій - Порядок та методи оцінювання результатів навчання - Класифікацію методів оцінювання та процедуру їх застосування на практиці

	- Методики оцінювання результатів навчання (рубрики, плани оцінювання, тестування, вікторини) - Методи та процеси тестування і оцінювання слухачів
Основні необхідні уміння та навички	Основні необхідні уміння та навички, притаманні "Фахівцю з кібердосліджень та розробок систем безпеки", та додатково уміти: - Використовувати методи соціальної інженерії - Готувати та проводити брифінги з питань проведення кібердосліджень та їх результатів - Ознайомлювати працівників та керівництво з новітніми корпоративними, вітчизняними, зарубіжними та міжнародними напрацюваннями у сфері кіберзахисту - Брати участь у розробленні внутрішніх регламентів з присвоєння/присудження кваліфікацій слухачам - Приймати участь в оцінюванні в організації результатів кібердосліджень - Готувати керівництву пропозиції щодо поліпшення в організації роботи з проведення кібердосліджень, підвищення їх ефективності та результативності

17. Фахівець з тестування систем захисту інформації

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7А6
Тип кваліфікації	Повна
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	Трудові функції А, Б та В, притаманні " Молодшому фахівцю з тестування систем захисту інформації ", та додатково: Г. Аналіз результатів тестування програмного, апаратного забезпечення або сумісності (Т0426) Д. Розроблення рекомендацій на основі результатів тестування (Т0143)
Основні необхідні знання	
Основні необхідні уміння та навички	

18. Провідний фахівець з тестування систем захисту інформації

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7А6
Тип кваліфікації	Часткова додаткова
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	Трудові функції А, Б, В, Г та Д, притаманні "Фахівцю з тестування систем захисту інформації ", та додатково: Е. Координація робіт з тестування систем захисту інформації
Основні необхідні знання	
Основні необхідні уміння та навички	

19. Розробник систем захисту інформації

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7А7
Тип кваліфікації	Повна
Код КП	2132.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	А. Проєктування систем захисту інформації А1. Здатність аналізувати проєктні обмеження, аналізувати компроміси та детальний проєкт системи та безпеки, а також розглядати підтримку життєвого циклу ЗА2. Здатність проєктувати апаратне забезпечення, операційні системи та прикладне програмне забезпечення для належного дотримання вимог кібербезпеки Б. Розроблення компонентів систем захисту інформації Б1. Здатність розроблювати вимоги до безпеки та її урахування у всіх системах захисту інформації або прикладних програмах Б2. Здатність розроблювати стратегії зменшення ризиків для усунення вразливостей з ураховуванням рекомендацій щодо зміни заходів безпеки у системі або системних компонентах Б3. Здатність забезпечувати, щоб діяльність з проєктування та розвитку кібербезпеки (з наданням функціонального опису впровадження безпеки) була належним чином задокументована і оновлювалася за необхідності В. Оцінювання та впровадження систем захисту інформації та їх компонентів

	B1. Здатність оцінювати системи кібербезпеки або продукти, що сприяють кібербезпеці B2. Здатність забезпечувати заходи щодо тестування та оцінки систем безпеки та сертифікації B3. Здатність впроваджувати проєкти системи безпеки для нових або існуючих систем захисту інформації
Основні необхідні знання	Знати: -Концепції і протоколи комп'ютерних мереж, методології забезпечення мережевої безпеки - Принципи кібербезпеки і приватності - Класифікацію кіберзагроз та вразливостей - Класифікацію операційних наслідків в результаті помилок кібербезпеки - Політики, вимоги і процедури безпеки ланцюжка постачання інформаційних технологій та управління ризиками ланцюжка постачання - Принципи і методи структурного аналізу - Технологічні процеси систем - Моделі системи безпеки - Типи, зміст та структуру систем баз даних - Електротехніку, яка застосовується в архітектурі комп'ютера - Принципи і концепції мережевих зв'язків на локальних і глобальних рівнях, включаючи управління пропускної здатністю (трафіком) - Концепції архітектури безпеки мережі, включаючи топологію, протоколи, компоненти і принципи - Криптологію та криптоаналіз - Концепції паралельних і розподілених обчислень - Засоби контролю доступу, адаптивні до ризиків і заснованих на політиці кібербезпеки

	- Інструменти, методи і методики проєктування систем, включаючи автоматизовані системи аналізу і інструменти проєктування - Інженерні концепції розробки процесів і процедур захисту інформації - Принципи управління життєвим циклом системи, включаючи забезпечення безпеки та експлуатаційної придатності програмного забезпечення - Концепції телекомунікацій - Методи автентифікації доступу - Типи, будову та інші характеристики мікропроцесорів - Порядок, принципи та правила управління мережевим доступом, ідентифікацією, та доступом -Типи, будову та інші характеристики операційних систем - Теорію управління потоками в мережах - Моделі розробки програмного забезпечення - Технологію побудови програмного забезпечення - Методики управління ризиками в ланцюжку постачання - Системи управління безпекою інформації - Класифікацію контрзаходів для виявлених ризиків безпеки - Мережеві протоколи - Принципи і методи забезпечення безпеки інформаційних технологій (наприклад, мережеві екрани, ДМЗ, шифрування) - Програму класифікації інформації і процедури її розкриття, які використовуються на підприємстві/ в організації - Класифікацію та характеристики вбудованих систем - Способи управління безпечною конфігурацією - Основи корпоративної архітектури безпеки інформації організації - Порядок оцінювання впливу кіберзагроз на приватність - Системи критичної інфраструктури з ІТ, які були розроблені без розгляду безпеки системи

	- Вимоги до процедур оцінки і валідації систем захисту інформації та персоналу, прийнятих на підприємстві/в організації - Стандарти безпеки персональних ідентифікаційних даних - Стандарти безпеки даних індустрії платіжних карт - Стандарти безпеки медичних персональних даних - Методи тестування систем захисту інформації - Концепції управління послугами для мереж і відповідних стандартів
Основні необхідні уміння та навички	Уміти: - Використовувати моделі та симуляції для аналізу або прогнозування продуктивності системи за різних умов експлуатації - Визначати та пріоритезувати основні системні функції або підсистеми - Аналізувати потреби та вимоги користувачів з метою планування і проведення розробки систем захисту інформації - Застосовувати принципи кібербезпеки при формуванні вимог підприємства/організації (стосовно конфіденційності, цілісності, доступності, автентифікації і неспростовності) - Відстежувати системні вимоги з метою проєктування компонентів та виконувати аналіз недоліків розробки - Застосовувати процеси управління ризиками - Застосовувати інтерпретовані і компільовані комп'ютерні мови - Застосовувати процеси проєктування мереж, включаючи розуміння цілей системи безпеки, операційних цілей та компромісів - Використовувати проєктне моделювання - Застосовувати принципи і методи кібербезпеки, а також організаційні вимоги (щодо забезпечення конфіденційності, цілісності, доступності, автентифікації і неспростовності) - Застосовувати принципи, моделі, інструменти та методи управління мережевими системами

	- Застосовувати інструменти, методи і техніки проєктування систем, включаючи інструменти автоматизованого аналізу та проєктування систем - Проєктувати інтеграцію апаратних і програмних рішень - Розроблювати контролі безпеки на основі принципів і доктрин кібербезпеки - Розроблювати і застосувати засоби контролю доступу в системах захисту інформації - Впроваджувати та інтегрувати методології життєвого циклу розробки систем (SDLC) - Розроблювати та модифіковувати системи захисту інформації, їх прототипи за допомогою робочих моделей або теоретичних моделей - Розроблювати функції управління криптографічними ключами - Зберігати, відновлювати та обробляти дані для аналізу можливостей системи та вимог - Розроблювати, інтегрувати і оновлювати показники захищеності системи, які забезпечують конфіденційність, цілісність, доступність, автентифікацію і неспростовність - Розроблювати контрзаходи для виявлення ризиків безпеки - Розроблювати спеціальні контрзаходи з кібербезпеки та стратегії пом'якшення ризиків для систем та/або прикладних програм - Розроблювати плани аварійного відновлення та безперервності операцій для систем, що розробляються, та забезпечувати тестування систем до їхнього вводу у продуктивне середовище - Розроблювати стратегії мінімізації ризиків для зменшення витрат, графіку, продуктивності і ризиків безпеки - Виконувати оцінку ризиків інформаційної безпеки - Розроблювати детальну проєктну документацію з безпеки для специфікацій компонентів та інтерфейсів з метою підтримки проєкту та розробки системи - Розроблювати та надавати вхідні дані для діяльності процесу загальних принципів управління ризиками та відповідну документацію

	- Підтверджувати стабільність, сумісність, портативність і/або масштабованість архітектури системи - Виявляти системи критичної інфраструктури з інформаційно-телекомунікаційними технологіями, які були спроєктовані без врахування безпеки системи - Оцінювати адекватність проєктів систем захисту інформації - Проводити процедури сканування вразливостей і розпізнавання вразливостей в системах захисту інформації - Оцінювати ефективність заходів з кібербезпеки, які використовуються системою (системами) - Оцінювати загрози та вразливості комп'ютерної системи (систем) для розробки профілю ризику безпеки - Тестувати і оцінювати захищені інтерфейси між інформаційними системами, фізичними системами і/або вбудованими технологіями - Виконувати аналіз ризиків щоразу, коли прикладна програма або система зазнають значних змін - Здійснювати огляди безпеки та виявляти пробіли в архітектурі безпеки - Виявляти системні проблеми безпеки на основі аналізу даних вразливостей та конфігурації - Впроваджувати захищені інтерфейси між інформаційними системами, фізичними системами і/або вбудованими технологіями - Розробляти/приймати участь настанови стосовно впровадження розроблених систем клієнтам або командам впровадження - Забезпечувати вимоги до безпеки профільних предметів та засобів праці протягом усього процесу закупівель - Забезпечувати вхідні дані для планів впровадження і стандартні операційні процедури, які стосуються систем захисту інформації

20. Провідний розробник систем захисту інформації

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7А7
Тип кваліфікації	Часткова додаткова
Код КП	2132.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	Трудові функції А, Б та В, притаманні "Розробнику систем захисту інформації", та додатково: Г. Координація діяльності з розроблення систем захисту інформації Г1. Здатність здійснювати технічне керівництво профільними розробниками систем захисту інформації Г2. Здатність взаємодіяти з керівництвом, технологічними та іншими підрозділами підприємства/ організації стосовно технологічних питань відповідного спрямування Г3. Здатність взаємодіяти із зовнішніми партнерами в межах визначених повноважень
Основні необхідні знання	Основні необхідні знання, притаманні "Розробнику систем захисту інформації", та додатково знати: - Керівництва/настанови, інструкції та/чи інші нормативні акти роботодавця, які застосовуються для організації та координації діяльності з розроблення систем захисту інформації - Посадові інструкції на посади розробників систем захисту інформації - Основи управління персоналом

	- Структуру, розподіл функцій між керівниками, підпорядкованість підрозділів тощо підприємства/організації - Положення про структурні підрозділи підприємства**/**організації, задіяні в спільному виконанні технологічних та інших функціональних завдань - Нормативні акти роботодавця з питань взаємодії з керівництвом, технологічними та іншими підрозділами підприємства/організації - Основи комунікаційного менеджменту - Основи ділової етики - Порядок і типові вимоги до проведення ділових/комерційних перемовин - Порядок розроблення та виконання договірних робіт для зовнішніх партнерів
Основні необхідні уміння та навички	Основні необхідні уміння та навички, притаманні "Розробнику систем захисту інформації", та додатково уміти: - Приймати участь у координації комплексу робіт із своєчасної та якісної підготовки розроблення систем захисту інформації - Готувати службові записки та іншу документацію, необхідну для навчання/підвищення кваліфікації підпорядкованих розробників систем захисту інформації відповідного структурного підрозділу підприємства/організації - Узгоджувати повідомлення із заінтересованими структурними підрозділами та відповідальними посадовими особами щодо змін проєктної документації з розроблення систем захисту інформації - Готувати, обґрунтовувати та оприлюднювати пропозиції щодо покращення в структурному підрозділі/на підприємстві/в організації розроблення систем захисту інформації

	- Готувати іншу документацію, необхідну для забезпечення безперебійної роботи закріпленого структурного підрозділу/групи/дільниці - Проводити спілкування із зовнішніми партнерами стосовно питань розроблення систем захисту інформації доступними засобами комунікації - Приймати участь в ділових/комерційних перемовинах із зовнішніми партнерами ГЗ.УЗ. Супроводжувати договірні роботи із зовнішніми партнерами

21. Фахівець сфери захисту інформації

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7А7, 7Б3, 7Б6, 7Г2
Тип кваліфікації	Повна
Код КП	2132.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	А. Впровадження систем та комплексів захисту інформації А1. Здатність аналізувати потреби та вимоги користувачів (замовників) щодо захисту інформації та кіберзахисту з метою впровадження систем та комплексів захисту інформації А2. Здатність виявляти, досліджувати (оцінювати), системно аналізувати загрози для інформації, аналізувати ризики безпеки інформації та кібербезпеки у разі реалізації загроз А3. Здатність формувати стратегію і політики безпеки інформації в інформаційно-комунікаційних системах (бере участь як член команди) А4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою (підприємства/організації) (бере участь як член команди) А5. Здатність виконувати передпроєктні роботи щодо систем та комплексів захисту інформації А6. Здатність проводити спеціальні дослідження засобів обробки інформації та технічних засобів та об’єктів інформаційної діяльності А7. Здатність впроваджувати (активізувати) програмні та апаратні засоби захисту інформації в системах та на об’єктах

	А8. Здатність адмініструвати системи, мережі та системи безпеки інформації (бере участь як член команди) А9. Здатність розробляти, впроваджувати та аналізувати технічні документи, положення, інструкції щодо систем та комплексів захисту інформації Б. Оцінювання відповідності систем, комплексів та засобів захисту інформації Б1. Здатність проводити оцінку відповідності (атестацію) комплексів технічного захисту інформації (бере участь як член команди) Б2. Здатність проводити оцінку відповідності (державну експертизу) комплексних систем захисту інформації (бере участь як член команди) Б3. Здатність проводити оцінку відповідності систем управління інформаційною безпекою В. Експлуатація та обслуговування систем і комплексів захисту інформації, моніторинг та аудит загроз для інформації В1. Здатність підтримувати системи та комплекси захисту інформації у робочому стані, оцінювати їх надійність та здійснювати контроль їх працездатності та виявлення місць відмов В2. Здатність проводити періодичне обслуговування інформаційних систем та мереж, комплексних систем захисту інформації та комплексів технічного захисту інформації В3. Здатність виконувати попередній нескладний ремонт несправного апаратного забезпечення системи/сервера В4. Здатність здійснювати контроль за станом технічного та криптографічного захисту інформації (бере участь як член команди) В5. Здатність здійснювати постійний моніторинг (аудит) загроз для інформації та відповідну модернізацію (доробку) систем та комплексів захисту інформації

	В6. Здатність проводити процедури сканування вразливостей і розпізнавання вразливостей в системах безпеки Г. Оцінювання відповідності програмних та апаратних засобів технічного та криптографічного захисту інформації Г1. Здатність проводити оцінку відповідності (державну експертизу) програмних засобів технічного та криптографічного захисту інформації Г2. Здатність проводити оцінку відповідності (державну експертизу, сертифікацію) апаратних засобів технічного та криптографічного захисту інформації
Основні необхідні знання	Знати: - Поняття та класифікація інформації з обмеженим доступом, державні інформаційні ресурси, поняття технічного та криптографічного захисту інформації - Концепції і протоколи комп'ютерних мереж, методології забезпечення мережевої безпеки та захисту інформації в автоматизованих (інформаційних) системах та на об'єктах інформаційної діяльності - Методи та процеси управління ризиками (методи оцінки та зниження ризиків) - Закони, нормативні акти, нормативні документи, що визначають вимоги із захисту інформації та кіберзахисту - Політики і етичні норми приватності стосовно безпеки інформації та кібербезпеки - Класифікація операційних наслідків в результаті помилок із захисту інформації та кібербезпеки - Політики, вимоги і процедури безпеки ланцюжка постачання інформаційних технологій та управління ризиками ланцюжка постачання

	- Поняття комплексних систем захисту інформації та комплексів технічного захисту інформації, їх склад та призначення - Моделі та симуляції інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, призначених для аналізу вразливості та прогнозування продуктивності таких систем за різних умов експлуатації - Класифікацію загроз для інформації та кіберзагроз - Методи (способи) і методики виявлення, дослідження та системного аналізу загроз для інформації та кіберзагроз - Форми і зміст моделей загроз для інформації, моделі порушника інформації; порядок їх розробки - Поняття ризиків безпеки інформації та кібербезпеки - Підходи, методи (способи) оцінки та аналізу ризиків безпеки інформації та кібербезпеки - Класифікацію операційних наслідків, спричинених помилками в системі кібербезпеки - Поняття спеціальних впливів на засоби обробки інформації з метою знищення (спотворення) , блокування інформації - Поняття системи управління інформаційною безпекою підприємства/організації - Принципи створення систем управління інформаційною безпекою - Загальний порядок створення комплексних систем захисту інформації та комплексів технічного захисту інформації - Порядки категоріювання об’єктів, обстеження середових функціонування автоматизованих систем та об’єктів інформаційної діяльності, розробки моделей загроз для інформації, розробки та зміст технічних завдань на створення

	комплексних систем захисту інформації та комплексів технічного захисту інформації - Методи, методики та теорії: вимірювання фізичних величин та принципи роботи сучасних засобів вимірювальної техніки, спеціальних досліджень засобів обробки інформації і об'єктів інформаційної діяльності, електромагнітного поля (в частині, необхідній для виконання професійних функцій), акустики (в частині, необхідній для виконання професійних функцій) - Пристрої електротехніки (в частині, що складають архітектуру комп'ютера: друковані плати, мікросхеми, процесори, елементи пам'яті) - Спектри сигналів та методи спектрального аналізу - Загальні положення теорії інформації та методи кодування, теорії ймовірностей та нечітких множин - Статистичну радіотехніку - Методологічні та математичні основи комп'ютерного проектування та моделювання систем - Мови програмування мікроконтролерів та контролерів відповідно до норм IEC 61131-3 -Порядок розробки та зміст технічних проектів комплексних систем захисту інформації та комплексів технічного захисту інформації - Методи техніко-економічного аналізу та обґрунтування проектних рішень - Процедури активізації (настроювання) програмних механізмів захисту інформації в інформаційних системах, підключення до локальної мережі підприємства (організації) та до глобальних мереж. Процедури активізації (настроювання) програмних мережевих механізмів захисту інформації - Концепції управління послугами для мереж і відповідних стандартів (бібліотека

	інфраструктури інформаційних технологій, адміністрування систем, мереж та систем безпеки інформації - Методики адміністрування систем, мереж та систем безпеки інформації - Політики адміністрування даних - Принципи, концепції і методи адміністрування серверів - Систему технічних документів щодо систем та комплексів захисту інформації - Вимоги до структури та змісту технічних документів щодо систем та комплексів захисту інформації, до розроблення технічних документів положень, інструкцій, методичних матеріалів щодо систем та комплексів захисту інформації - Сучасні підходи до формування вимог до захисту інформації в інформаційно-комунікаційних системах та на об’єктах інформаційної діяльності - Інструменти, методи і техніки проєктування систем, включаючи інструменти автоматизованого аналізу та проєктування систем - Поняття атестації комплексів технічного захисту інформації, поняття та загальний зміст програми та методики проведення атестації комплексів технічного захисту інформації - Порядок, умови та організація проведення атестації комплексів технічного захисту інформації - Техніко-технологічне, комп’ютерне, програмне та інше забезпечення атестації комплексів технічного захисту інформації - Засоби вимірювальної техніки та методики вимірювань оцінюваних показників комплексів технічного захисту інформації

	- Поняття оцінки відповідності систем управління інформаційною безпекою - Порядок, умови та організація проведення оцінки відповідності систем управління інформаційною безпекою - Документи, що оформлюються за результатами оцінки відповідності систем управління інформаційною безпекою - Поняття та порядок проведення державної експертизи в сфері криптографічного захисту інформації - Умови та організація проведення державної експертизи в сфері криптографічного захисту інформації - Поняття та загальний зміст програми та методики проведення експертних досліджень при проведенні державної експертизи в сфері криптографічного захисту інформації - Документи, що оформлюються за результатами державної експертизи в сфері криптографічного захисту інформації - Загальні положення криптології, криптографії та криптографічного аналізу - Принципи взаємодії «людина-комп’ютер», стійкості і надмірності в комп’ютерних системах та комплексах захисту інформації - Загальні положення теорії надійності, методи діагностики працездатності та виявлення місця відмов в комп'ютерних системах, системах та комплексах захисту інформації - Типи і періодичність планової підтримки апаратного забезпечення, періодичність підтримки та оновлення програмного забезпечення - Підходи щодо забезпечення безпеки віртуальних приватних мереж (VPN) - Інструменти діагностики систем і методик визначення несправностей

	- Засоби та діагностики систем/серверів, методики визначення несправностей - Технічні регламенти та специфікації відповідного ремонту - Методи контролю за станом технічного та криптографічного захисту інформації - Організація та порядок здійснення контролю за станом технічного та криптографічного захисту інформації - Інструментарій контролю за станом технічного та криптографічного захисту інформації - Методи та технології моніторингу (аудиту) загроз для конфіденційності, цілісності та доступності інформації - Методи, засоби та інформаційні технології виявлення несанкціонованого доступу до інформації на різних ієрархічних рівнях інформаційно-комунікаційної системи - Класифікація контрзаходів для виявлених ризиків безпеки інформації - Способи модернізації (доробки) систем та комплексів захисту інформації відповідно до виявлених актуальних загроз для інформації - Загальні способи оцінювання відповідності програмних засобів технічного захисту інформації - Поняття державної експертизи програмних засобів технічного захисту інформації - Порядок та організація проведення державної експертизи програмних засобів технічного захисту інформації - Документи, що оформлюються за результатами державної експертизи програмних засобів технічного захисту інформації - Техніко-технологічне, комп’ютерне, програмне та інше забезпечення оцінювання відповідності апаратних засобів технічного та криптографічного захисту інформації

	- Засоби вимірювальної техніки та методики вимірювань оцінюваних показників апаратних засобів технічного та криптографічного захисту інформації
Основні необхідні уміння та навички	Уміти: - Визначати (формулювати) потреби: щодо захисту інформації, що обробляється в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах користувачів (замовників); захисту інформації, що озвучується на об'єктах інформаційної діяльності підприємства (організації); кібербезпеки в електронних комунікаційних та інформаційно-комунікаційних системах користувачів (замовників) ; захисту інформації та кіберзахисту в інформаційно-комунікаційних системах та на об'єктах інформаційної діяльності підприємства (організації) - Аналізувати потреби та вимоги користувачів з метою планування і проведення розробки системи безпеки - Використовувати моделі та симуляції інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем для аналізу вразливості та прогнозування продуктивності таких систем за різних умов експлуатації - Виявляти загрози для інформації та кіберзагрози в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, для інформації, що озвучується на об'єктах інформаційної діяльності (обґрунтовувати можливість створення певних технічних каналів витоку інформації, що озвучується на конкретному об'єкті інформаційної діяльності) - Розробляти модель загроз для інформації: від несанкціонованих дій та модель порушника інформації; від витоку технічними каналами; від спеціальних впливів на засоби обробки інформації - Ураховувати методи управління: мережевими системами при обґрунтуванні концепції безпеки

	інформації; ризиками при обґрунтуванні концепції безпеки інформації - Розробляти групові політики та переліки контролю доступу для забезпечення відповідності стандартам організації, бізнес-правилам та потребам - Застосовувати політики безпеки інформації в інформаційно-комунікаційних системах для досягнення цілей безпеки системи - Здійснювати обстеження: середовищ функціонування автоматизованих систем; об’єктів інформаційної діяльності - Розробляти: моделі загроз для інформації; технічні завдання на створення комплексних систем захисту інформації; технічні завдання на створення комплексів технічного захисту інформації; проєкти комплексних систем захисту інформації та комплексів технічного захисту інформації багаторівневими вимогами безпеки або вимогами для обробки кількох рівнів класифікації даних - Використовувати методи комп’ютерного проектування та моделювання систем для розробки технічних проектів комплексних систем захисту інформації та комплексів технічного захисту інформації - Визначати та групувати за пріоритетами основні системні функції або підсистеми, необхідні для підтримки основних можливостей або бізнес-функцій з метою відновлення або поновлення після відмови системи або під час відновлення системи на основі загальних системних вимог щодо безперервності та доступності - Аналізувати проєктні обмеження та можливі компроміси системи безпеки інформації (комплексної системи захисту інформації) - Проєктувати, розробляти та модифікувати програмні системи, використовуючи науковий аналіз та математичні моделі для прогнозування та вимірювання результатів та наслідків проекту - Активізувати (налаштовувати) програмні механізми захисту інформації в інформаційних системах, електронних комунікаційних та інформаційно-комунікаційних системах (

	програмні фільтри, антивірусні програми, антишпигунське програмне забезпечення) - Впроваджувати (налаштовувати) програмно-апаратні засоби захисту інформації в інформаційних системах, електронних комунікаційних та інформаційно-комунікаційних системах - Розробляти та документувати стандартні операційні процедури адміністрування систем, мереж та систем безпеки інформації - Координувати свої дії з аналітиками системи захисту кіберпростору для управління та адміністрування оновлень правил та сигнатур для спеціалізованих прикладних програм у сфері кіберзахисту та захисту інформації - Здійснювати системне адміністрування операційних систем та спеціалізованих прикладних програм кіберзахисту та захисту інформації, систем - Здійснювати адміністрування серверів - Дотримуватись стандартних операційних процедур адміністрування систем організації - Управляти системними/серверними ресурсами, включаючи продуктивність, ємність, доступність, ремонтопридатність і здатність відновлюватись - Складати програму та методику проведення державної експертизи комплексних систем захисту інформації - Проводити попереднє ознайомлення з об’єктом експертизи та поглиблене обстеження об’єкта експертизи - Проводити експертні випробування та дослідження комплексних систем захисту інформації - Оформлювати протоколи експертних випробувань та атестати відповідності комплексних систем захисту інформації - Здійснювати експертизу комплексних систем захисту інформації шляхом декларування, оформлювати декларації відповідності комплексних систем захисту інформації та організовувати їх затвердження і реєстрацію - Здійснювати експертизу засобів технічного захисту інформації, оформлювати протоколи

	експертних випробувань засобів технічного захисту інформації та експертні висновки на засоби ТЗІ, організовувати затвердження і реєстрацію експертних висновків - Здійснювати контроль працездатності комп'ютерних систем, систем та комплексів захисту інформації - Діагностувати несправне апаратне забезпечення системи/сервера - Застосовувати засоби контролю працездатності та виявлення місця відмов - Виявляти місця відмов в комп'ютерних системах, системах та комплексах захисту інформації - Організовувати (проводити) ремонт апаратних засобів захисту інформації зі складу комплексних систем захисту інформації та комплексів технічного захисту інформації - Встановлювати оновлення системи та компонентів (серверів, пристроїв, мережевих пристроїв) - Моніторити та оптимізувати роботу системи/сервера - Відновлювати системи/сервери після виявленого збою (програмне забезпечення для відновлення, відмовостійкі кластери, дублювання/ «зеркалювання») - Здійснювати оновлення баз даних антивірусних програм, програмних механізмів захисту інформації - Організовувати (приймати участь в організації) контроль за станом технічного та криптографічного захисту інформації - Перевіряти виконання вимог нормативно-правових актів та нормативних документів з технічного та криптографічного захисту інформації на підприємстві/ в організації - Застосовувати засоби контролю захищеності інформації - Користуватися інструментарієм контролю за станом технічного та криптографічного захисту інформації - Визначати стан технічного та криптографічного захисту інформації на підприємстві/ в організації

	- Оформлювати документи за результатами контролю стану технічного та криптографічного захисту інформації на підприємстві/ в організації - Здійснювати моніторинг та аудит загроз для інформації в інформаційних системах та мережах та оцінку ризиків безпеки інформації - Проводити аудити/огляди систем та комплексів захисту інформації (систем безпеки інформації) та інформаційно-комунікаційних систем - Складати програму та методику проведення державної експертизи програмних засобів технічного захисту інформації - Проводити експертні випробування та дослідження програмних засобів технічного захисту інформації (оцінювати функціональні послуги безпеки, оцінювати рівні гарантій коректності реалізації функціональних послуг безпеки) - Оцінювати відповідність програмних засобів технічного захисту інформації задекларованим характеристикам та вимогам нормативних документів системи технічного захисту інформації - Складати програму та методику проведення державної експертизи апаратних засобів технічного захисту інформації - Проводити експертні випробування та дослідження апаратних засобів технічного захисту інформації (склади схеми вимірювань характеристик засобів, вимірювати (визначати) функціональні характеристики засобів) - Оцінювати відповідність апаратних засобів технічного захисту інформації задекларованим характеристикам та вимогам нормативних документів системи технічного захисту інформації - Оформлювати протоколи експертних випробувань та експертні висновки за результатами державної експертизи та організовувати їх затвердження і реєстрацію

22. Провідний фахівець сфери захисту інформації

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7А7, 7Б3, 7Б6, 7Г2
Тип кваліфікації	Часткова додаткова
Код КП	2132.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	Трудові функції А, Б,В та Г притаманні "Фахівцю сфери захисту інформації", та додатково: А. Впровадження систем та комплексів захисту інформації А10. Здатність виявляти закладні пристрої на об’єктах інформаційної діяльності (бере участь як член команди) Б. Оцінювання відповідності систем, комплексів та засобів захисту інформації Б4. Здатність проводити оцінку відповідності (державну експертизу) засобів криптографічного захисту інформації Д. Унормування системи технічного та криптографічного захисту інформації Д1. Здатність аналізувати, інтегрувати і використовувати кращі світові практики, стандарти при розробці нормативних документів системи технічного та криптографічного захисту інформації (бере участь як член команди) Д2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування щодо системи технічного та криптографічного захисту інформації (бере участь як член команди)

Основні необхідні знання	Основні необхідні знання, притаманні "Фахівцю сфери захисту інформації", та додатково знати: - Організаційно-технічну **с**истему захисту інформації та кіберзахисту України **-** Систему нормативних документів (нормативна база) системи технічного та криптографічного захисту інформації України **-**Кращі світові практики, стандарти із захисту інформації **-** Загальні поняття та способи (методи) системного та експертного аналізу стосовно кращих світових практик, стандартів із захисту інформації - Порядок розробки та впровадження нормативних документів системи технічного та криптографічного захисту інформації **-** Порядок актуалізації нормативних документів системи технічного та криптографічного захисту інформації
Основні необхідні уміння та навички	Основні необхідні уміння та навички, притаманні "Фахівцю захисту інформації", та додатково уміти: - Аналізувати систему нормативних документів (нормативну базу) системи технічного та криптографічного захисту інформації України **-** Виявляти, ставити та вирішувати проблемні питання щодо системи нормативних документів (нормативної бази) системи технічного та криптографічного захисту інформації України **-** Проводити системний аналіз світових практик, стандартів із захисту інформації **-** Організовувати проведення експертного аналізу кращих світових практик, стандартів із захисту інформації **-** Брати участь в експертному аналізі кращих світових практик, стандартів із захисту інформації

	- Розробляти (брати участь у розробці) нормативні документи системи технічного та криптографічного захисту інформації - Писати та публікувати методики та настанови з кіберзахисту та інструктивні матеріали - Впроваджувати нормативні документи системи технічного та криптографічного захисту інформації - Здійснювати актуалізацію нормативних документів системи технічного та криптографічного захисту інформації - Використовувати результати аналізу кращих світових практик, стандартів при розробці нормативних документів системи технічного та криптографічного захисту інформації

23. Системний фахівець сфери захисту інформації

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7А7, 7Б3, 7Б6, 7Г2
Тип кваліфікації	Часткова додаткова
Код КП	2132.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	Трудові функції А, Б,В, Г та Д, притаманні "Провідному фахівцю сфери захисту інформації", та додатково: Е. Координація діяльності з технічного та криптографічного захисту інформації Е1. Здатність здійснювати технічне керівництво фахівцями структурних підрозділів підприємства (організації), до функцій яких входять питання захисту інформації та кібербезпеки Е2. Здатність взаємодіяти з керівництвом та фахівцями технологічних та інших підрозділів підприємства/ організації з технологічних та інших питань, пов’язаних із забезпеченням захисту інформації та кіберзахисту Е3. Здатність взаємодіяти із зовнішніми партнерами в межах визначених повноважень Е4. Здатність надавати консультативні послуги та технічну допомогу з питань технічного та криптографічного захисту інформації та кіберзахисту
Основні необхідні знання	Основні необхідні знання, притаманні "Провідному фахівцю сфери захисту інформації", та додатково знати:

	- Керівництва (настанови, інструкції) нормативні акти роботодавця з організації, координації діяльності та взаємодії структурних підрозділів підприємства**/** організації **-** Посадові інструкції фахівців структурних підрозділів підприємства**/**організації, до функцій яких входять питання захисту інформації та кібербезпеки **-** Основи управління персоналом **-** Архітектура ІТ підприємства - Структура підприємства (організації), функції структурних підрозділів, розподіл функцій між керівниками підприємства (організації), підпорядкованість підрозділів - Положення про структурні підрозділи підприємства (організації), що задіяні в спільному виконанні технологічних та функціональних завдань **-** Нормативні документи підприємства (організації) з питань організації його діяльності - Основи комунікаційного менеджменту **-** Основи ділової етики **-** Порядок і типові вимоги до проведення ділових/комерційних перемовин **-** Порядок розроблення та виконання договірних робіт для зовнішніх партнерів - Порядок і типові вимоги з надання консультативних послуг з питань технічного та криптографічного захисту **-** Предметну область консультативних послуг з питань технічного та криптографічного захисту інформації та кіберзахисту
Основні необхідні уміння та навички	Основні необхідні уміння та навички, притаманні "Провідному фахівцю захисту інформації", та додатково уміти:

	-Здійснювати методичне та технічне керівництво фахівцями структурних підрозділів підприємства (організації), до функцій яких входять питання захисту інформації та кібербезпеки - Координувати роботи (брати участь у координації робіт) із захисту інформації та кібербезпеки в структурних підрозділах підприємства/організації - Координувати та надавати експертну технічну підтримку технічним спеціалістам з кіберзахисту в масштабах усієї організації для управління інцидентами у сфері кіберзахисту - Виконувати обов'язки внутрішнього консультанта і радника в своїй експертній області. Надавати консультативно-методичну допомогу працівникам структурних підрозділів підприємства (організації), до функцій яких входять питання захисту інформації та кібербезпеки, з відповідних питань - Приймати участь в організації та навчанні (підвищенні кваліфікації) працівників структурних підрозділів підприємства (організації), до функцій яких входять питання захисту інформації та кібербезпеки, з відповідних питань - Взаємодіяти з керівництвом та працівниками технологічних та інших підрозділів підприємства (організації) з технологічних та інших питань, пов'язаних із забезпеченням захисту інформації та кіберзахисту - Готувати звернення (листи), заяви, звітно-аналітичні та документи щодо організації та здійснення захисту інформації та кіберзахисту у профільному та інших структурних підрозділах підприємства (організації) - Співпрацювати із зовнішніми партнерами доступними засобами комунікації стосовно питань захисту інформації і кіберзахисту - Приймати участь в ділових/комерційних перемовинах із зовнішніми партнерами - Супроводжувати договірні роботи із зовнішніми партнерами - Взаємодіяти з регуляторними органами та органами з акредитації

	- Надавати консультативні послуги з питань технічного та криптографічного захисту інформації та кіберзахисту - Консультувати керівництво (директора з інформаційних технологій) або уповноважених представників щодо рівня ризику та стану безпеки - Консультувати керівництво або уповноважених представників щодо аналізу витрат/вигоди програм, політик, процесів, систем та елементів інформаційної безпеки - Консультувати керівництво або уповноважених представників щодо змін, які впливають на стан кібербезпеки в організації - Аналізувати питання, пов’язані з предметною областю - Аналізувати запити на отримання інформації з метою визначення наявності необхідної інформації для відповіді - Здійснювати управління відносинами з клієнтами, включаючи визначення потреб/вимог клієнтів, управління очікуваннями клієнта та демонстрацію відданості досягненню якісних результатів - Інтерпретувати закони, нормативні акти, політики, стандарти чи процедури в області технічного та криптографічного захисту інформації та кіберзахисту щодо конкретних питань - Проводити інтерактивні тренінгові вправи для створення ефективного навчального середовища

24. Адміністратор бази даних *сфери інформаційної безпеки та кібербезпеки*

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7Б1
Тип кваліфікації	Повна
Код КП	2131.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	-------
Основні необхідні знання	-------
Основні необхідні уміння та навички	**------**

25. Провідний адміністратор бази даних *сфери інформаційної безпеки та кібербезпеки*

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7Б1
Тип кваліфікації	Часткова додаткова
Код КП	2131.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	---------
Основні необхідні знання	--------
Основні необхідні уміння та навички	**---------**

26.Фахівець з технічного захисту інформації

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7Б3
Тип кваліфікації	Повна
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	Трудові функції А, Б,В та Г, притаманні " Молодшому фахівцю з технічного захисту інформації", та додатково: Д. Управління активами/проведення інвентаризації активів, що належать до ресурсів ІТ (Т0496) Е. Розроблення рекомендацій на основі аналізу тенденцій щодо удосконалення програмних та апаратних рішень для підвищення якості обслуговування клієнтів (Т0482)
Основні необхідні знання	
Основні необхідні уміння та навички	

27. Провідний фахівець з технічного захисту інформації

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7Б3
Тип кваліфікації	Часткова додаткова
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	Трудові функції А, Б,В, Г, Д та Е, притаманні "Фахівцю з технічного захисту інформації", та додатково: Є. Розроблення і проведення технічних тренінгів для навчання інших або задоволення потреб клієнтів (Т0315)
Основні необхідні знання	
Основні необхідні уміння та навички	

28. Адміністратор мереж і систем

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7Б5
Тип кваліфікації	Повна
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	Трудові функції А, Б, В та Г, притаманні "Молодшому адміністратору мереж і систем", та додатково: Д. Діагностування несправного апаратного забезпечення системи/сервера Д1. Здатність діагностувати несправне апаратне забезпечення системи/сервера
Основні необхідні знання	Основні необхідні знання, притаманні "Молодшому адміністратору мереж і систем", та додатково знати: - Інструменти командного рядка операційної системи
Основні необхідні уміння та навички	Основні необхідні уміння та навички, притаманні "Молодшому адміністратору мереж і систем", та додатково уміти: -Використовувати командний рядок операційних систем - Інтерпретувати інформацію, зібрану мережевими інструментами

29. Провідний адміністратор мереж і систем

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7Б5
Тип кваліфікації	Часткова додаткова
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	Трудові функції А, Б, В, Г та Д, притаманні "Адміністратору мереж і систем", та додатково: Е. Координація діяльності з адміністрування мереж і систем Е1. Здатність налаштовувати та оптимізовувати мережеві концентратори, маршрутизатори та комутатори Е2. Здатність діагностувати проблеми підключення до мережі Е3. Здатність тестувати та підтримувати мережеву інфраструктуру, включно з програмним та апаратним забезпеченням Е4. Здатність надавати рекомендації з кібербезпеки керівництву на основі значних загроз і вразливостей
Основні необхідні знання	Основні необхідні знання, притаманні "Адміністратору мереж і систем", та додатково знати: - Безпеку віртуальних приватних мереж - Різні типи мереж зв’язку - Мережеві протоколи, такі як TCP/IP, динамічне конфігурування вузлів, системи доменних імен (DNS) та інші профільні послуги

	- Кіберзагрози та вразливості - Конкретні операційні наслідки у результаті помилок кібербезпеки
Основні необхідні уміння та навички	Основні необхідні уміння та навички, притаманні "Адміністратору мереж і систем", та додатково уміти: - Налаштовувати маршрути локальної мережі/глобальної мережі організації - Проводити моніторинг потоків трафіку, що проходять крізь мережу - Діагностувати проблеми з підключенням - Проводити процедури сканування вразливостей і їх розпізнавання у системах безпеки - Розробляти і застосовувати засоби контролю доступу в системах безпеки - Оцінки засобів контролю безпеки на основі принципів і доктрин кібербезпеки - Виявляти вразливості в захищених системах (сканування вразливостей і перевірка відповідності)

30. Аналітик систем захисту інформації

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7Б6
Тип кваліфікації	Повна
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	А. Аналіз системи безпеки, визначення пробілів в архітектурі безпеки і розроблення план управління ризиками (Т0177) Б. Аналіз і моніторинг кібербезпеки, пов’язаної з практиками впровадження і тестування системи (Т0504) В. Оцінювання ефективності засобів контролю безпеки (Т0309) Г. Впровадження заходів безпеки для усунення вразливостей, зниження ризиків, підготовка рекомендацій щодо змін в систему або її компоненти (Т0485)
Основні необхідні знання	
Основні необхідні уміння та навички	

31. Провідний аналітик систем захисту інформації

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7Б6
Тип кваліфікації	Часткова додаткова
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	Трудові функції А, Б, В та Г , притаманні " Аналітику систем захисту інформації", та додатково: Д. Планування аналітичної діяльності щодо безпеки систем та розроблення рекомендацій щодо коригування політики підприємства (установи, організації) для мінімізації ризиків у кіберсередовищі (Т0187)
Основні необхідні знання	
Основні необхідні уміння та навички	

32. Фахівець з юридичних консультацій та адвокації в сфері кібербезпеки

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7В1
Тип кваліфікації	Повна
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	----------
Основні необхідні знання	----------
Основні необхідні уміння та навички	**----------**

33. Провідний фахівець з юридичних консультацій та адвокації в сфері кібербезпеки

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7В1
Тип кваліфікації	Часткова додаткова
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	--------
Основні необхідні знання	--------
Основні необхідні уміння та навички	**--------**

34. Інструктор-методист з інформаційної безпеки та кібербезпеки

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7В2
Тип кваліфікації	Повна
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	А. Планування консультативно-методичної та навчальної роботи в організації/ структурному підрозділі сфери інформаційної та кібербезпеки А1. Здатність планувати і координувати реалізацію методик та форматів проведення аудиторних занять з метою створення найбільш ефективного навчального середовища А2. Здатність оцінювати ефективність та комплексність наявних програм навчання та тренінгів, потреб у навчанні та вимог до слухачів Б. Підготовка профільних навчально-методичних матеріалів Б1. Здатність розроблювати нові або визначати наявні матеріали для обізнаності та тренінгів, що підходять для цільових аудиторій Б2. Здатність розроблювати або брати участь у розробці методичних матеріалів або програм для тренінгів на робочому місці Б3. Здатність розроблювати рекомендації щодо переглядів навчальних планів і програм на основі відгуків про попередні навчальні заняття В. Проведення навчання та тренінгів для працівників сфери інформаційної та кібербезпеки

	В1. Здатність здійснювати технічне та методологічне супроводження занять/ тренінгів В2. Здатність проводити навчання та тренінги з урахуванням аудиторії та фізичних/віртуальних середовищ Г. Проведення оцінювання результатів навчання слухачів сфери інформаційної та кібербезпеки Г1. Здатність розроблювати або брати участь у розробці стандартів оцінювання та присвоєння/присудження кваліфікацій слухачам Г2. Здатність проводити оцінювання та присвоєння/присудження кваліфікацій слухачам
Основні необхідні знання	Знати: - Технологічні задачі і завдання управління та лідерства пов'язані з організаційними процесами, механізми вирішення проблем - Концепції і протоколи комп'ютерних мереж, а також методологію забезпечення безпеки мереж - Методики управління ризиками - Закони, нормативні акти, політики і етичні норми, та як вони пов'язані з конфіденційністю персональних даних та кібербезпекою - Принципи забезпечення конфіденційності персональних даних та кібербезпеки - Кіберзагрози та вразливості - Нові та ті, що розроблюються технології інформаційної та кібербезпеки - Політику навчання в організації - Системи управління навчанням та практику їх використання - Види доведення інформації - Способи навчання - Принципи (специфіку) роботи з аудиторією післядипломної освіти

	- Методи визначення вимог до інфраструктури тестування та оцінювання - Принципи і процеси проведення тренінгів та оцінки потреби у навчанні - Відповідні концепції, процедури, програмне забезпечення, обладнання і прикладні технологічні програми які застосовуються для навчання - Вимоги: до структури та змісту навчальної програми; до розроблення навчальних та методичних матеріалів; до формування навчальних програм - Організацію кіберзмагань, як засіб розвитку навичок шляхом надання практичного досвіду в симульованих та реальних ситуаціях - Порядок, процедура та форми підготовки кадрів на робочому місці, зміст навчальної програми для тренінгів на робочому місці - Принципи і методи навчання та виховання для розробки навчальних програм, навчання та інструктажів для окремих осіб та груп, а також вимірювання підготовки та освітні ефекти - Методи та підходи щодо переглядів та/чи вдосконалення навчальних планів і програм - Вимоги системи забезпечення якості - Зміст навчальної програми відповідного спрямування - Особливості організації навчального процесу для різних форм набуття компетентності -Форми організації навчального процесу - Сучасні методи, засоби та технології викладання - Методи і способи організації індивідуальної та групової роботи слухачів під час навчання - Основи вікової психології, педагогіки та андрагогіки - Методи і способи ефективної комунікації

	- Освітні комп’ютерні послуги і послуги дистанційної освіти - Принципи і методи тренінгів та занять для розробки навчально-методичних матеріалів індивідуального та групового навчання, освіти а також вимірювання їх результатів - Методи здійснення індивідуального супроводу, наставництва/менторства - Методики оцінювання результатів навчання (рубрики, плани оцінювання, тестування, вікторини) - Методи та процеси тестування і оцінювання слухачів - Порядок та методи оцінювання результатів навчання - Порядок присвоєння/ присудження часткової професійної/ освітньої кваліфікації - Методи соціальної інженерії - Вимоги і правила дотримання академічної доброчесності - Порядок та методи оцінювання результатів навчання - Порядок присвоєння/присудження професійної/ освітньої кваліфікації
Основні необхідні уміння та навички	Уміти: - Планувати і координувати методики та формати проведення лекцій, демонстрацій, інтерактивних занять, мультимедійних презентації тощо - Адаптувати технічну інформацію для планування до рівня розуміння користувача/споживача/ замовника - Збирати точні та повні дані з джерел, які використовуються для розвідки, оцінювання та/або планування - Планувати позааудиторні освітні заходи

	- Формувати цілі та завдання для освітніх програм з інформаційної та кібербезпеки - Проводити оцінювання ефективності існуючих програм навчання та тренінгів - Здійснювати комплексний аналіз відповідності змісту навчальних програм встановленим стандартам якості навчання - Проводити соціологічні анонімні опитування слухачів, інтерв'ювання інших заінтересованих осіб стосовно покращення методів навчання та змісту навчальних програм - Оцінювати конкретні результати роботи щодо підготовки, перепідготовки та підвищення кваліфікації працівників - Розроблювати або брати участь у розробці: політик та протоколів для кібертренінгів; індивідуальних/колективних планів розвитку, навчання та/або вдосконалення результатів навчання; чітких вказівок і навчальних матеріалів - Обґрунтувати зв'язок навчальної програми для тренінгів на робочому місці зі стратегією розвитку організації у сфері інформаційної та кібербезпеки - Редагувати зміст навчальної програми для тренінгів на робочому місці відповідно до їх оновлення та встановлених часових вимог - Адаптувати навчальну програму для тренінгу на робочому місці відповідно до його оновлення та встановлених часових вимог - Інтегрувати нові наукові ідеї та підходи у зміст навчальних програм в необхідних обсягах і формах - Аналізувати вимоги та очікування слухачів, їх роботодавців та інших заінтересованих осіб щодо навчальної програми/тренінгу чи курсу - Ураховувати в обґрунтованому обсязі вимоги керівництва організації під час періодичного перегляду та вдосконалення навчальних планів, програм - Конфігурувати і використовувати у навчальному процесі компоненти системи мережевої безпеки

	- Використовувати сучасні та новітні технології у навчальних цілях, відображати дані в оригінальних форматах - Забезпечувати розробку та виконання сценаріїв тренінгів - Застосовувати концепції, процедури, програмне забезпечення, обладнання та/або технологічні прикладні програми під час навчання студентів/слухачів - Готувати та проводити навчальні заняття та брифінги з обізнаності, дотримання політик і процедур безпеки користувачами систем, мереж і даних - Сприяти дискусіям у невеликих групах - Проводити разом із слухачами електронну криміналістичну експертизу в кількох середовищах операційних систем - Розроблювати (брати участь) письмові тести для визначення рівня професійної придатності та оцінювання кваліфікації слухачів; критерії оцінювання результатів навчання; правила оцінювання результатів навчання; внутрішніх регламентів з присвоєння/присудження кваліфікацій слухачам - Використовувати інструменти та методики тестування на проникнення; методи соціальної інженерії - Приймати участь в оцінюванні результатів навчання та присвоєнні/присудженні професійних/освітніх кваліфікацій слухачам

35. Провідний інструктор-методист з інформаційної безпеки та кібербезпеки

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7В2
Тип кваліфікації	Часткова додаткова
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	Трудові функції А, Б, В та Г, притаманні " Інструктору-методисту з інформаційної безпеки та кібербезпеки", та додатково: Д. Участь у проведенні консультаційної та/чи виконанні дослідно-експериментальної роботи відповідного спрямування Д1. Здатність виконувати обов’язки внутрішнього консультанта і радника у своїй експертній області Д2. Здатність проводити дослідно-експериментальну роботу стосовно процедури сканування та розпізнавання вразливостей в системах інформаційної та кібербезпеки Д3. Здатність розроблювати або допомагати в розробці навчальних матеріалів для тренінгів для покращення розуміння співробітниками політики конфіденційності персональних даних та кібербезпеки
Основні необхідні знання	Основні необхідні знання, притаманні " Інструктору-методисту з інформаційної безпеки та кібербезпеки ", та додатково знати: - Основні бізнес-процеси і місію організації

	- Прийняті в організації правила класифікації інформації щодо рівнів захисту і процедур доступу до неї - Посадові завдання та обов'язки внутрішнього консультанта/радника за профільними спеціалізаціями - Джерела і методи збору інформації, її узагальнення, структурування, систематизацію - Методи і технології підготовки доповідей та презентацій - Основні небезпеки, ризики і вразливості - Процедури сканування (пошуку) вразливостей в системах безпеки - Порядок розпізнавання вразливостей в системах безпеки - Зовнішні організації і академічні установи, діяльність яких спрямована на дослідження кіберпростору - Нормативні документи і правила, що забезпечують захист авторських прав, патентування, винаходи тощо - Новітні технології, інструменти, процедури, методи та процеси відповідного спрямування
Основні необхідні уміння та навички	Основні необхідні уміння та навички, притаманні "Інструктору-методисту з інформаційної безпеки та кібербезпеки ", та додатково уміти: - Виконувати обов’язки внутрішнього консультанта/радника в технічній сфері та галузі авторського права щодо електронних носіїв інформації тощо - Готувати та проводити брифінги відповідного спрямування - Комунікувати з керівниками різних рівнів (міжособистісне спілкування, доступність, уміння ефективно сприймати мову виступаючих,

	відповідно до аудиторії коректувати стиль і мову виступу тощо) - Аналізувати пропускну здатність, характеристики та продуктивність комунікаційної системи - Приймати участь у проведенні сканування та розпізнавання вразливостей в системах безпеки - Розроблювати або допомагати в розробці навчальних матеріалів для покращення розуміння співробітниками політики конфіденційності компанії, практики та процедур обробки даних, юридичних зобов'язань - Освоювати досягнення у технологіях захисту інформації для забезпечення їх впровадження у відповідній організації - Використовувати інструменти управління мережею для аналізу структури мережевого трафіку - Застосовувати навики реверс-інжинірингу для визначення функцій і належності інструментів віддаленого доступу

36.Фахівець з питань безпеки (інформаційні технології)

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7В3
Тип кваліфікації	Повна
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	A. Організація та практична реалізація заходів з питань безпеки ІТ A1. Здатність визначати та/або впроваджувати політики і процедури для забезпечення належного захисту критичної інфраструктури та ІКТ A2. Здатність керувати аналізом загроз або цільовим аналізом інформації про кіберзахист, а також отриманням даних про загрози в межах підприємства (установи, організації) A3. Здатність визначати специфічні вимоги безпеки до системи інформаційно-комунікаційних технологій на всіх етапах її життєвого циклу A4. Здатність забезпечувати успішне впровадження та функціональність вимог безпеки та відповідних політик і процедур ІТ, які узгоджені з цілями та місією підприємства (установи, організації) A5. Здатність визначати наслідки застосування нових технологій або оновлень у програмах захисту ІТ A6. Здатність визначати проблеми безпеки у процесі стабільної роботи та управління програмним забезпеченням та вживати заходів безпеки, коли життєвий цикл продукту закінчується

	Б. Забезпечення фінансово-матеріальної, інституціональної, методологічної та іншої підтримки IT Б1. Здатність забезпечувати фінансово-матеріальну підтримку безпеки IT на підприємстві (в установі, організації) Б2. Здатність забезпечувати методологічну підтримку безпеки IT на підприємстві (в установі, організації) Б3. Здатність забезпечувати інституціональну та іншу підтримку безпеки IT на підприємстві (в установі, організації) В. Моніторинг та оцінювання діяльності з питань безпеки IT В1. Здатність брати участь в оцінюванні ризику інформаційній безпеці під час проведення процедури оцінки В2. Здатність керувати моніторингом джерел даних, що стосуються забезпечення захисту інформації, з метою забезпечення обізнаності підприємства (установи, організації) про ситуацію В3. Здатність моніторити та оцінювати ефективність засобів кібербезпеки підприємства (установи, організації) з метою гарантованого підтвердження того, що вони забезпечують необхідний рівень захисту Г. Контроль / нагляд за діяльністю з питань безпеки IT Г1. Здатність відслідковувати результати аудиту та розробляти рекомендації, щоб забезпечити вжиття відповідних заходів щодо зменшення негативних наслідків Г2. Здатність наглядати за захисними чи коректувальними заходами при виявленні кіберінциденту або вразливості
Основні необхідні знання	Знати: -Концепції і протоколи комп'ютерних мереж, а також методології забезпечення мережевої безпеки - Процеси управління ризиками (методи оцінки та зниження ризиків)

	- Закони, нормативні акти, політики і етичні норми, та як вони пов’язані з кібербезпекою і конфіденційністю - Принципи кібербезпеки і конфіденційності - Класифікацію кіберзагроз та вразливостей - Конкретні операційні наслідки в результаті помилок кібербезпеки - Корпоративні цілі та завдання, пов’язані з використанням ІТ на підприємстві (в установі, організації) - Політики, вимоги і процедури безпеки ланцюжка постачання ІТ та управління ризиками ланцюжка постачання - Системи критичної інфраструктури з інформаційно-комунікаційними технологіями, які були розроблені без розгляду безпеки системи - Джерела поширення інформації про вразливість (попередження, рекомендації, списки помилок і бюлетені) - Методологію реагування на інциденти і обробки даних інцидентів - Методи аналізу мережевого трафіку - Теорію управління потоками в мережах - Методики адміністрування системи, мережі та захисту операційних систем - Алгоритми шифрування - Особливості резервного копіювання та відновлення даних - Механізми контролю доступу до хостів / мереж (списки контролю доступу, списки повноважень) -Теорію, концепції і методи адміністрування серверів і проєктування систем - Операційні системи сервера і клієнта - Підхід підприємства (установи, організації) до прийняття ризиків та/або управління ризиками - Програми, робочі ролі та відповідальність при управлінні інцидентами в організації

	- Поточні та ймовірні загрози / вектори загроз - Способи впровадження систем депонування ключів з метою забезпечення локального шифрування даних - Загрози і вразливості безпеки систем і прикладного програмного забезпечення - Класифікацію мережевих атак, наявний зв'язок між мережевими атаками і загрозами та вразливостями - Використовувану програму класифікації інформації і процедур розкриття - Прикладні бізнес процеси і функції в організації-замовнику - Принципи безперервності бізнесу та операційних планів відновлення безперервності після катастроф - Методики управління ризиками в ланцюжку постачання - Вимоги до закупівлі критичних ІТ - Стандарти, політики і авторизовані підходи до проєктування програмного забезпечення, прийняті на підприємстві (в установі, організації) - Принципи управління життєвим циклом системи, включаючи забезпечення безпеки та експлуатаційної придатності програмного забезпечення - Процеси інтеграції технологій - Принципи управління життєвим циклом системи, включаючи забезпечення безпеки та експлуатаційної придатності програмного забезпечення - Процеси інтеграції технологій - Критерії або показники продуктивності і доступності систем - Сучасні галузеві методи оцінки, впровадження та розповсюдження інструментів та процедур оцінки безпеки інформаційно-комунікаційних технологій, моніторингу, виявлення та усунення

	несправностей, які використовують концепції та можливості на основі стандартів - Стандарти: безпеки персональних ідентифікаційних даних (PII), безпеки даних в сфері платіжних карт (PCI), безпеки медичних персональних даних (PHI) - Принципи, інструменти та методики тестування на проникнення - Порядок проведення моніторингу ефективності засобів кібербезпеки підприємства / організації; проведення оцінювання ефективності засобів кібербезпеки підприємства / організації; підтвердження спроможності засобів кібербезпеки забезпечувати необхідний рівень захисту - Засоби контролю, пов'язані з використанням, обробкою, зберіганням та переданням даних - Порядок розроблення заходів, спрямованих на виконання зауважень та рекомендацій, визначених за результатами аудиту - Порядки: контролю за виконанням заходів, спрямованих на виконання зауважень та рекомендацій, визначених за результатами аудиту; нагляду за захисними чи коригувальними заходами при виявленні кіберінциденту або вразливості - Класифікацію мережевих атак, наявний зв'язок між мережевими атаками і загрозами та вразливостями
Основні необхідні уміння та навички	Уміти: - Збирати та підтримувати дані, необхідні для забезпечення звітності про стан системи кібербезпеки - Переглядати стандарти політики та стратегії її впровадження, щоб забезпечити відповідність процедур та настанов політикам кібербезпеки - Рекомендувати політику та координувати її перегляд та затвердження - Керувати захисними чи коректувальними заходами при виявленні кіберінциденту або вразливості

	- Розпізнавати можливе порушення безпеки і вживати відповідних заходів, щоб повідомити про інцидент, якщо необхідно - Інтерпретувати випадки невідповідності для визначення їхнього впливу на рівень ризику та/або загальну ефективність програми кібербезпеки підприємства (установи, організації) - Визначати, як буде функціонувати система безпеки (включаючи її властивості відмовостійкості і надійності), та як зміни умов, операцій або середовища вплинуть на ці результати - Використовувати офіційні документи та специфічні документи підприємства / організації для управління їхніми системами обчислювального середовища - Надавати системні вихідні дані для формування вимог кібербезпеки, які повинні бути включені в операційні інструкції та відповідні документи, що стосуються системи постачання - Використовувати пристрої віртуальних приватних мереж (VPN) і шифрування, шифрування інфраструктури відкритих ключів (PKI) та можливостей цифрового підпису в програмних додатках - Готувати, розповсюджувати та підтримувати плани, інструкції, настанови та стандартні функціональні процедури стосовно безпеки функціонування мережевих систем(-и) - Брати участь у процесах розроблення або модифікації планів і вимог програм кібербезпеки комп'ютерного середовища - Виявляти системи критичної інфраструктури з інформаційно-телекомунікаційними технологіями, які були спроєктовані без урахування безпеки системи

	- Інтерпретувати та/або затверджувати вимоги щодо безпеки спроможностей нових інформаційних технологій - Проводити процедури тестування і перевірки автентичності програмного забезпечення. - Визначати і документувати програмні коригування або версії програми, які залишають вразливості. - Здійснювати пробні запуски програм і прикладного програмного забезпечення - Виявляти системи критичної інфраструктури з ІТ, які були спроєктовані без урахування безпеки системи - Повідомляти вартість створення системи безпеки ІТ зацікавленим сторонам на всіх рівнях - Прогнозувати поточні потреби у послугах та забезпечувати перегляд припущень щодо безпеки за необхідності - Контролювати, щоб усі дії з придбання, постачання, закупівлі та аутсорсингу відповідали вимогам кібербезпеки, які відповідають цілям підприємства (установи, організації) - Брати участь, за необхідності, у процесі закупівлі, дотримуючись відповідних практик управління ризиків в ланцюжку постачання - Оцінювати ефективність функції закупівель з точки зору задоволення вимог інформаційної безпеки і ризиків у ланцюжку постачання через закупівельну діяльність та рекомендувати вдосконалення - Керувати та контролювати бюджет інформаційної безпеки та укладання контрактів - Оцінювати надійність постачальника та/або продукту - Впроваджувати вимоги до захисту інформації у процеси закупівель

	- Організовувати публікацію настанов із захисту комп'ютерної мережі (TCNO, концепції операцій, звіти мережевих аналітиків, NTSM, MTO) для зацікавлених сторін підприємства (установи, організації) - Розробляти методологію кібербезпеки підприємства та управління ризиком ланцюжка постачання для розробки безперервності операційних планів - Брати участь в оцінці ризику безпеки інформації під час проведення процедури оцінки і авторизації - Оцінювати та затверджувати програми розвитку для забезпечення належного встановлення базових засобів безпеки; витрати-вигоду, економічний аналіз та аналіз ризиків у процесі ухвалення рішень - Моніторити ефективність засобів кібербезпеки підприємства / організації - Оцінювати ефективність засобів кібербезпеки підприємства / організації - Підтверджувати спроможність засобів кібербезпеки забезпечувати необхідний рівень захисту - Відслідковувати виконання заходів, спрямованих на виконання зауважень та рекомендацій, визначених за результатами аудиту - Наглядати за захисними чи коригувальними заходами при виявленні кіберінциденту або вразливості - Брати участь у розробленні відповідних заходів та профілактичних робіт відповідного спрямування

37.Провідний фахівець з питань безпеки (інформаційні технології)

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7В3
Тип кваліфікації	Часткова додаткова
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	Трудові функції А, Б, В та Г, притаманні "Фахівцю з питань безпеки (інформаційні технології)", та додатково: Д. Координація та участь в управлінні діяльністю із забезпечення безпеки ІТ Д1. Здатність здійснювати керівництво профільними працівниками з безпеки ІТ Д2. Здатність взаємодіяти з керівництвом, технологічними та іншими підрозділами підприємства (установи, організації) стосовно технологічних питань відповідного спрямування Д3. Здатність взаємодіяти із зовнішніми партнерами в межах визначених повноважень
Основні необхідні знання	Основні необхідні знання, притаманні " Фахівцю з питань безпеки (інформаційні технології)", та додатково знати: - Керівництва (настанови, інструкції) інші нормативні акти роботодавця з організації, координації діяльності та взаємодії структурних підрозділів підприємства (установи, організації) - Посадові інструкції фахівців структурних підрозділів підприємства (установи, організації), до функцій яких входять питання безпеки ІТ - Основи управління персоналом - Порядок розроблення та підписання трудових договорів та контрактів - Основи трудового законодавства

	- Процедуру розроблення програм та проведення тренінгів персоналу з питань безпеки ІТ - Структуру підприємства (установи, організації), функції структурних підрозділів, розподіл функцій між керівниками, підпорядкованість підрозділів - Положення про структурні підрозділи підприємства (установи, організації), що задіяні в спільному виконанні технологічних та інших функціональних завдань - Нормативні документи підприємства (установи, організації) з питань організації його діяльності - Підходи щодо розбудови загальної архітектури захисту інформації підприємства (установи, організації) (EISA) з урахуванням вимог загальної стратегії безпеки організації - Регламент управління ризиками як засобу забезпечення зменшення ризиків безпеки, і введення даних щодо інших технічних ризиків - Основи менеджменту, зокрема комунікаційного - Основи маркетингу - Основи ділової етики - Порядок і типові вимоги до проведення ділових / комерційних перемовин; розроблення та виконання договірних робіт для зовнішніх партнерів
Основні необхідні уміння та навички	Основні необхідні уміння та навички, притаманні "Фахівцю з питань безпеки (інформаційні технології)", та додатково уміти: -Забезпечувати керівництво та управління персоналом у сфері ІТ матеріалами та інструментаріями, необхідними для того, щоб обізнаність в кібербезпеці, базові знання, грамотність та тренінги операційного персоналу відповідали їх функціональним обов'язкам - Наглядати за виконанням програм тренінгів з інформаційної безпеки та обізнаності - Консультувати вище керівництво щодо рівня ризику та стану безпеки - Консультувати керівників вищої ланки щодо аналізу витрат / вигоди програм, політик, процесів, систем та елементів інформаційної безпеки

	- Консультувати профільних керівників вищої ланки або уповноважених представників щодо змін, які впливають на стан кібербезпеки на підприємстві підприємства (в установі, організації) - Керувати, контролювати персонал та укладання з ним контрактів - Визначати ролі і обов'язки для призначеного персоналу безпеки комунікацій - Брати участь в корпоративному процесі управління ризиками, щоб забезпечити зменшення ризиків безпеки, вводити данні щодо інших технічних ризиків - Надавати технічну документацію, звіти про інциденти, результати комп'ютерних перевірок, висновки та іншу інформацію про ситуацію для головних організацій - Створювати загальну архітектуру захисту інформації підприємства (установи, організації) (EISA) з урахуванням вимог загальної стратегії безпеки організації - Визначати альтернативні стратегії захисту інформації для дотримання цілей організаційної безпеки - Знаходити необхідні ресурси, включно з фінансовими, для забезпечення безперервності функціонування операційних програм підприємства (установи, організації) - Сприяти підвищенню обізнаності керівництва щодо ситуацій безпеки та забезпечувати належні принципи безпеки в баченні та цілях підприємства (установи, організації) - Взаємодіяти із зовнішніми організаціями (службою зі зв'язків із громадськістю, правоохоронними органами) для забезпечення належного та точного розповсюдження фактів про інциденти та інших відомостей про захист комп'ютерної мережі - Співпрацювати із зацікавленими сторонами з метою забезпечення безперервної діяльності організації в межах програми, стратегії та виконання завдань - Супроводжувати договірні роботи із зовнішніми партнерами

38. Фахівець з криптографічного захисту інформації

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7В3
Тип кваліфікації	Повна
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	Трудові функції А, Б та В, притаманні " Молодшому фахівцю з криптографічного захисту інформації ", та додатково: Г. Взаємодія із зацікавленими сторонами з метою забезпечення безперервної діяльності підприємства (установи, організації) у сфері криптографічного захисту інформації (Т0044)
Основні необхідні знання	
Основні необхідні уміння та навички	

39. Провідний фахівець з криптографічного захисту інформації

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7В3
Тип кваліфікації	Часткова додаткова
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	Трудові функції А, Б, В та Г, притаманні " Фахівцю з криптографічного захисту інформації ", та додатково: Д. Консультування вищого керівництва щодо рівня ризику та стану криптографічного захисту інформації на підприємстві (в установі, організації) (Т0003)
Основні необхідні знання	
Основні необхідні уміння та навички	

40. Фахівець з планування політики та стратегії кібербезпеки

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7В4
Тип кваліфікації	Повна
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	А. Виконання підготовчих робіт у сфері планування політики та стратегії розвитку інформаційної безпеки та кібербезпеки А1. Здатність інтерпретувати і застосовувати чинні закони та нормативні документи відповідного спрямування та інтегрувати їх в політику організації А2. Здатність застосовувати у практичній діяльності вітчизняні, міжнародні та зарубіжні чинні та перспективні політики та стратегії розвитку кібербезпеки А3. Здатність аналізувати політику організації у сфері кібербезпеки Б. Планування політики, стратегії, програм та настанов для подальшого впровадження заходів з кібербезбеки Б1. Здатність сприяти обізнаності керівництва стосовно кіберполітики і кіберстратегій Б2. Здатність визначати та інтегрувати середовища для поточної та майбутньої місій кіберстратегії Б3. Здатність розроблювати/інтегровувати кіберстратегію, узгоджену зі стратегічним планом організації

	Б4. Здатність підтримувати керівника з інформаційних технологій у формуванні політик та стратегій, які стосуються кібербезпеки В. Надання консультаційних послуг із методологічного забезпечення планування політики, стратегії, програм та настанов з кібербезбеки В1. Здатність розроблювати проєкти з розвитку кібербезпеки, ознайомлювати персонал і публікувати політику кібербезпеки В2. Здатність надавати керівництву, персоналу і користувачам консультації із застосування на практиці методології щодо політики кібербезпеки Г. Проведення моніторингу виконання політики, принципів і практик надання послуг з планування та управління політикою кібербезпеки Г1. Здатність моніторити виконання політик, принципів і практик при наданні послуг з планування та управління політикою кібербезпеки Г2. Здатність брати участь в аудитах кіберпрограм і кіберпроектів
Основні необхідні знання	Знати: - Галузеві показники, корисні для визначення тенденцій розвитку технологій - Сучасні і перспективні кібертехнології - Сервіс-орієнтовані принципи архітектури безпеки - Стратегії кіберможливостей для розробки програмно-апаратних комплексів - Стандарти політики та стратегії кібербезпеки - Форму запиту на профільну інформацію - Сучасні галузеві методи оцінки, впровадження та розповсюдження інструментів та процедур

	оцінки безпеки інформаційних технологій, моніторингу, виявлення та усунення несправностей, що використовують концепції та можливості на основі стандартів - Порядок аналізу: політики організації у сфері кібербезпеки; потреби та вимог користувачів для планування архітектури; потреби безпеки і вимог до програмного забезпечення - Фундаментальні кіберконцепції, принципів, обмеження і ефекти - Рекомендації щодо оптимізації та вирішення в організації проблем відповідно до розвитку інформаційних технологій - Нові/існуючі заходи безпеки, стійкості та надійності організації - Рекомендації щодо аналізу кризових ситуацій з метою забезпечення суспільної та персональної безпеки, захисту кіберресурсів - Концепцію планування в організації - Положення про ініціювання планування діяльності організації - Зміст та порядок адаптивного планування, планування в кризових умовах та планування з урахуванням обмеженого часу - Відповідні концепції, процедури, програмне забезпечення, обладнання і прикладні технологічні програми які застосовуються для планування - Вимоги до структури та змісту стратегій, програм та політик з розвитку кібербезпеки - Порядок розроблення профільних, зокрема стратегічних, планів - Проєктну документацію з безпеки для специфікацій компонентів та інтерфейсів - Порядок розроблення планів аварійного відновлення та безперервності операцій для систем, що розробляються, та тестування систем до їхнього вводу у продуктивне середовище

	- Стратегії зменшення ризиків для усунення кібервразливостей - Плани запобіжних і/або антикризових заходів відповідного спрямування - Процедури планування кризових дій та в умовах обмеженого часу - Процедури планування кібероперацій в кризових ситуаціях - Методики оцінювання працівників щодо реалізації заходів стратегій, політик та програм з розвитку кіберзахисту - Методи та процеси тестування і оцінювання працівників щодо реалізації заходів стратегій, політик та програм з розвитку кіберзахисту - Підходи та методи до розроблення і верифікації критеріїв оцінювання працівників щодо реалізації заходів стратегій, політик та програм з розвитку кіберзахисту
Основні необхідні уміння та навички	Уміти: - Планувати і координувати методики та формати інтеграції чинних законів, нормативних актів, міжнародних та зарубіжних практик в політику кіберзахисту в політику організації - Адаптувати технічну інформацію для планування до рівня розуміння користувача/споживача/ замовника - Збирати точні та повні дані з джерел, які використовуються для розвідки, оцінювання та/або планування - Інтерпретувати та застосовувати закони, нормативні акти, політики, стандарти чи процедури до конкретних питань - Приймати участь в аналізі потреби та вимог користувачів для планування архітектури - Приймати участь в аналізі потреби безпеки і вимог до програмного забезпечення з метою визначення доцільності проєкту з урахуванням часових і цінових обмежень, а також мандатів безпеки

	- Готувати пропозиції щодо пошуку та управління необхідними ресурсами, включаючи фінансові, для забезпечення безперервності дії політик та стратегій, програм з розвитку кібербезпеки, функціонування операційних програм підприємства - Розроблювати або брати участь у розробленні стратегій, програм та політик з розвитку кібербезпеки - Розроблювати вказівки і настанови для працівників, залучених до розроблення стратегій, програм та політик з розвитку кібербезпеки - Приймати участь в організації процесів планування, включаючи підготовку функціональних і спеціальних планів підтримки, підготовки і забезпечення ділового листування, а також процесів кадрового забезпечення - Розроблювати профільні плани та готувати відповідну кореспонденцію - Аналізувати інформацію з метою визначення, рекомендацій та планування розробки нової прикладної програми або модифікації існуючої прикладної програми - Планувати розроблення та приймати участь у розробленні та підтримці/супроводженні стратегічних планів організації з кібербезпеки - Планувати розроблення детальної проєктної документації з безпеки для специфікацій компонентів та інтерфейсів з метою підтримки проєкту та розроблення системи - Планувати розроблення планів аварійного відновлення та безперервності операцій для систем, що розробляються, та забезпечення тестування систем до їхнього вводу у продуктивне середовище - Інтегрувати нові наукові ідеї та підходи у зміст стратегій, програм та політик з розвитку кібербезпеки в необхідних обсягах і формах

	- Розроблювати групові політики та переліки контролю доступу для забезпечення відповідності стандартам організації, бізнес-правилам та потребам - Розроблювати стратегії зменшення ризиків для усунення вразливостей та рекомендувати, у випадку необхідності, зміни заходів безпеки у системі або системних компонентах - Планувати та розроблювати рекомендації щодо змін або коригувань на основі результатів застосування або системного середовища - Розроблювати і підтримувати плани запобіжних і/або антикризових заходів - Планувати проєктування та розроблення продуктів кібербезпеки та продуктів, які сприяють кібербезпеці - Розробляти методи моніторингу та оцінки ризиків, відповідності та зусиль щодо надання впевненості у результативності заходів стратегій, політик, програм та планів - Оцінювати витрати-вигоду, економічний аналіз та аналіз ризиків у процесі прийняття рішень - Оцінювати ефективність законів, правил, політик, стандартів чи процедур відповідного спрямування - Відслідковувати результати аудиту та розробляти рекомендації, щоб забезпечити вжиття відповідних заходів щодо зменшення негативних наслідків - Підтримувати та сприяти безперервному моніторингу в організації стосовно планування стратегій, політик, програм та планів з розвитку кіберзахисту

41. Провідний фахівець з планування політики та стратегії кібербезпеки

Характеристики професійної кваліфікації	Значення та опис
Рівень НРК	7
Рівень ГРК КБ	7В4
Тип кваліфікації	Часткова додаткова
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	Трудові функції А, Б, В та Г, притаманні " Фахівцю з планування політики та стратегії кібербезпеки ", та додатково: Д. Підтримання комунікації із стейкголдерами в сфері планування політики та стратегії розвитку кібербезпеки Д1. Здатність брати участь у роботі відомчих і міжвідомчих рад з питань політики та стратегії розвитку кібербезпеки Д2. Здатність оцінювати потреби в політиці та співпрацювати з зацікавленими сторонами з метою розроблення політик корпоративного управління діяльністю в сфері кібербезпеки Д3. Здатність знаходити консенсус із зацікавленими сторонами щодо запропонованих змін кіберполітики Е. Надання консультаційних послуг з питань планування політики та стратегії розвитку кібербезпеки та процесів управління кіберперсоналом Е1. Здатність готувати керівництву рекомендації щодо планування підтримки адекватного фінансування освітніх ресурсів у кіберсфері Е2. Здатність забезпечувати планування політики і процесів управління кіберперсоналом

	Е3. Здатність планувати перегляд/оцінювання ефективності кіберперсоналу для коригування вимог до навичок та/або стандартів кваліфікації
Основні необхідні знання	Основні необхідні знання, притаманні "Фахівцю з планування політики та стратегії кібербезпеки ", та додатково знати: -Основні бізнес-процеси і місію організації - Прийняті в організації правила класифікації інформації щодо рівнів захисту і процедур доступу до неї - Посадові завдання та обов'язки внутрішнього консультанта/радника за профільними спеціалізаціями - Джерела і методи збору інформації, її узагальнення, структурування, систематизацію - Методи і технології підготовки доповідей та презентацій - Основні небезпеки, ризики і кібервразливості - Методи та процедура прогнозування потреб у послугах з кібербезпеки - Принципи забезпечення безпеки інформації - Можливості і обмеження внутрішніх і зовнішніх організацій-партнерів - Звітність внутрішніх і зовнішніх організацій-партнерів - Внутрішню та зовнішню тактику прогнозування і/або моделювання спроможностей та дій загроз - Політику організації і концепції планування її співпраці з внутрішніми і/або зовнішніми організаціями - Зовнішні організації і установи, діяльність яких спрямована на розвиток, захист та дослідження кіберпростору - Нормативні документи і правила, що забезпечують планування, проєктування,

	розроблення та моніторинг політик, стратегій та програм із кіберзахисту організації - Новітні технології, інструменти, процедури, методи та процеси відповідного спрямування - Інструменти управління мережею для аналізу структури мережевого трафіку - Аналізатори протоколів - Повноваження організації і організації-партнера, відповідальність та внески у досягнення поставлених цілей - Політику, засоби, спроможності і процедури організації та організації-партнера - Прикладні бізнес процеси і функції в організації-замовнику - Принципи безперервності бізнесу та операційних планів відновлення безперервності після катастроф - Методики управління ризиками в ланцюжку постачання - Вимоги до закупівлі критичних інформаційних технологій - Методи прогнозування в освітніх послугах для організації - Порядок планування закупівлі освітніх послуг - Керівництва/настанови, інструкції та/або інші нормативні акти роботодавця, які застосовуються для організації та координації діяльності з планування політики і процесів управління кіберперсоналом - Посадові інструкції/професійні стандарти на посади кіберперсоналу - Основи управління персоналом - Структуру організації, функції структурних підрозділів, розподіл функцій між керівниками організації, підпорядкованість підрозділів

Основні необхідні уміння та навички	Основні необхідні уміння та навички, притаманні "Фахівцю з планування політики та стратегії кібербезпеки", та додатково уміти: - Виконувати обов’язки внутрішнього консультанта/радника в сфері планування заходів з розвитку кібербезпеки в організації - Комунікувати з керівниками різних рівнів (міжособистісне спілкування, доступність, уміння ефективно сприймати мову виступаючих, відповідно до аудиторії коректувати стиль і мову виступу) - Переглядати існуючі та перспективні політики із зацікавленими сторонами - Оцінювати потреби в політиці та співпрацювати з зацікавленими сторонами з метою розробки політик корпоративного управління діяльністю в сфері кібербезпеки - Прогнозувати спільно із стейкголдерами поточні потреби у послугах та забезпечувати, що припущення щодо безпеки переглядаються за необхідності - Визначати спільно із стейкголдерами та/або впроваджувати політики і процедури, щоб забезпечити належний захист критичної інфраструктури - Співпрацювати із зацікавленими сторонами, щоб визначити та/або розробити відповідні технології прийняття рішень - Інтегрувати процеси планування /визначення цілій з іншими організаціями - Проводити заходи з довгострокового стратегічного планування за участю внутрішніх і зовнішніх партнерів з кібердіяльності - Аналізувати та звітувати перед керівництвом про користування активами і ресурсами управління знаннями - Повідомляти вартість запланованих освітніх ресурсів у кіберсфері зацікавленим сторонам організації на всіх рівнях

	- Прогнозувати поточні потреби у освітніх послугах та забезпечувати перегляд припущень щодо безпеки за необхідності - Контролювати ситуацію, щоб усі дії з планування придбання, постачання, закупівлі та аутсорсингу освітніх послуг у кіберсфері відповідали вимогам кібербезпеки, які відповідають цілям організації - Приймати участь у плануванні в організації контролю за використанням бюджету на персонал та укладанням контрактів - Приймати участь у плануванні політики і процесів управління кіберперсоналом - Визначати альтернативні стратегії розвитку кіберперсоналу для дотримання цілей організаційної безпеки - Планувати найбільш оптимальну структуру організації та розподіл її кіберперсоналу відповідно до цілей та завдань стратегічного та оперативного планів - Готувати пропозиції керівництву щодо оновлення нормативних актів роботодавця у сфері соціально-трудових відносин в організації

42. Аудитор інформаційних технологій (з кібербезпеки)

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7В6
Тип кваліфікації	Повна
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	А. Підготовка до проведення аудиту програм та проєктів з ІТ у сфері кібербезпеки А1. Здатність планувати проведення аудиту програм та проєктів з інформаційних технологій у сфері кібербезпеки А2. Здатність виконувати підготовчі заходи для проведення аудиту програм та проєктів з інформаційних технологій у сфері кібербезпеки Б. Проведення аудиту програм та проєктів з ІТ у сфері кібербезпеки Б1. Здатність переглядати та/чи здійснювати аудит програм та проєктів з інформаційних технологій у сфері кібербезпеки Б2. Здатність здійснювати аналіз імпортних/експортних операцій з придбання інформаційних систем і програмного забезпечення у сфері кібербезпеки, оцінювати ефективність функції закупівель з точки зору задоволення вимог інформаційної безпеки і ризиків у ланцюжку постачання через закупівельну діяльність та рекомендувати вдосконалення Б3. Здатність забезпечувати включення до положень контракту вимог до ланцюжка

	постачання, інформаційних систем, мережі, продуктивності та кібербезпеки Б4. Здійснювати аудит про ефективність послуг, де вказані усі будь-які значні проблеми і відхилення, ініціюючи, у разі необхідності, коригувальні дії та гарантуючи, що усі невирішені питання будуть відстежені В. Підготовка пропозицій щодо покращення аудиту програм та проєктів з ІТ у сфері кібербезпеки В1. Здатність розроблювати методи моніторингу та оцінки ризиків, відповідності та зусиль щодо надання стійкості ІТ у сфері кібербезпеки В2. Здатність готувати рекомендації щодо можливих удосконалень і оновлень аудиторської діяльності програм та проєктів з інформаційних технологій у сфері кібербезпеки в сфері В3. Здатність забезпечувати постійну оптимізацію процесів аудиту та вирішення проблем його проведення
Основні необхідні знання	Знати: - Технологічні задачі і завдання управління та лідерства, пов’язані з організаційними процесами, механізми вирішення проблем - Концепції і протоколи комп’ютерних мереж, а також методологію забезпечення безпеки мереж - Методики управління ризиками (методи оцінювання та оброблення ризиків) - Закони, нормативні акти, політики і етичні норми, та як вони пов’язані з конфіденційністю персональних даних та кібербезпекою - Принципи забезпечення конфіденційності персональних даних та кібербезпеки - Кіберзагрози та вразливості - Основні операційні наслідки інцидентів кібербезпеки

	- Методи автентифікації, авторизації та контролю доступу - Технології віртуалізації, формування віртуальних машин їх технічна підтримка - Нові та ті, що розроблюються технології інформаційної та кібербезпеки - Системи управління аудитом програм та проєктів з інформаційних технологій у сфері кібербезпеки та практику їх використання - Класифікацію програм та проєктів з інформаційних технологій у сфері кібербезпеки - Принципи і методи аналізу прийнятих в галузевих стандартах або в організації/на підприємстві - Архітектурні концепції та загальні принципи інформаційних технологій - Вимоги в рамках Загальних принципів управління ризиками (RMF) - Принципи і способи управління ресурсами - Порядок проведення аудиту, технічного огляду, моніторингу придбання та застосування на підприємстві систем інформаційного та кіберзахисту - Порядок інструктажу підпорядкованих працівників щодо змісту та термінів проведення аудиту, технічного огляду, моніторингу придбання та застосування на підприємстві систем інформаційного та кіберзахисту тощо - Форми звітності та процедура розповсюдження результатів аудиту серед заінтересованих осіб - Технологічні задачі і завдання управління та лідерства, пов'язані з організаційними процесами, механізми вирішення проблем - Вимоги до структури та змісту проведення профільного аудиту

	- Вимоги та підходи до розроблення проєктів та програм у сфері інформаційного та кіберзахисту - Сучасні підходи до оцінювання програм та проєктів з інформаційних технологій у сфері кібербезпеки - Основи проєктного менеджменту - Методи оцінки ризиків/загроз - Принципи управління життєвим циклом системи, включаючи забезпечення безпеки та експлуатаційної придатності програмного забезпечення - Методики управління ризиками в ланцюжку постачання - Нормативні акти експортно-імпортного контролю та відповідальні установи, з метою зниження ризиків ланцюжка постачання - Стандарти, процеси і практики управління ризиками в ланцюжку постачання - Політики, вимоги і процедур безпеки ланцюжка постачання інформаційних технологій та управління ризиками ланцюжка постачання - Концепції вдосконалення процесів організації та моделей зрілості процесів, зокрема Capability Maturity Model Integration (CMMI) for Development, CMMI for Services, and CMMI for Acquisitions (K0198) - Концепції управління послугами для інформаційних мереж - Технічну документацію відповідного спрямування - Методи та підходи щодо переглядів та/чи вдосконалення положень контракту - Вимоги системи забезпечення якості - Класифікацію послуг, за якими проводиться аудит/технічний огляд чи моніторинг - Правила підготовки звітів про надані послуги відповідного спрямування

	- Технологію коригувальних дій стосовно усунення недоліків, направлених на підвищення якості та ефективності послуг відповідного спрямування - Порядок відстеження недоліків та невирішених питань при наданні профільних послуг - Методи моніторингу ризиків, відповідності та зусиль щодо надання стійкості ІТ у сфері кібербезпеки - Основи методології моніторингових досліджень - Критерії оцінювання ризиків та загроз - Порядок проведення моніторингу програм та проєктів відповідного спрямування - Програмне забезпечення відповідного спрямування - Класифікацію оптимізаційних моделей - Порядок оцінювання результатів профільного аудиту - Методи та засоби оцінювання результатів аудиту - Вітчизняний, зарубіжний та міжнародний досвід оцінювання аудиторської діяльності відповідного спрямування
Основні необхідні уміння та навички	Уміти: - Планувати на рік, квартал, місяць тиждень проведення аудиту програм та проєктів з ІТ у сфері кібербезпеки - Адаптувати технічну інформацію для планування аудиту програм та проєктів ІТ у сфері кібербезпеки - Збирати точні та повні дані з джерел, які використовуються для оцінювання та планування аудиту програм та проєктів ІТ у сфері кібербезпеки - Планувати підготовчі заходи для проведення аудиту програм та проєктів з ІТ у сфері кібербезпеки

	- Формувати цілі та завдання аудиту програм та проєктів з ІТ у сфері кібербезпеки - Розроблювати або брати участь у розробці індивідуальних/колективних планів з проведення відповідного аудиту - Проводити інструктаж підпорядкованих працівників щодо змісту та термінів проведення аудиту, технічного огляду, моніторингу придбання та застосування на підприємстві систем інформаційного та кіберзахисту тощо - Вивчати необхідну документацію, дані, інформацію, нормативну базу, фінансові та інші матеріали, необхідні для якісного проведення аудиту - Забезпечувати доступ та попереднє ознайомлення заінтересованих сторін із заходами плану підготовчих робіт та планом проведення аудиту інструктажу підпорядкованих працівників щодо змісту та термінів проведення аудиту, технічного огляду, моніторингу придбання та застосування на підприємстві систем інформаційного та кіберзахисту тощо - Використовувати передові методи аудиторської діяльності стосовно оцінювання проєктів та програм з розвитку інформаційного та кіберзахисту - Застосовувати чіткі вказівки стосовно проведення аудиту, програмне забезпечення відповідного спрямування - Проводити постійний моніторинг застосування та реалізації на практиці проєктів та програм з розвитку інформаційного та кіберзахисту - Визначати у межах своїх повноважень показники або індикатори продуктивності системи та дій, спрямовані на підвищення або виправлення продуктивності, виходячи з призначення системи - Проводити аудит та/чи технічний огляд інформаційних систем - Відстежувати і пріоритезувати потреби в інформації і вимоги до збору даних розвідки серед розширеної організації - Оцінювати ефективність функції закупівель з точки зору задоволення вимог інформаційної

	безпеки і ризиків у ланцюжку постачання через закупівельну діяльність - Рекомендувати заходи щодо вдосконалення системи закупівель відповідного обладнання та програмного забезпечення - Готувати та редагувати звіт про результати аналізу імпортних/експортних операцій з придбання інформаційних систем і програмного забезпечення у сфері кібербезпеки - Визначати рівень ефективності послуг, що надаються - Аналізувати хід надання послуг відповідного спрямування, відстежувати наявні недоліки та невирішені питання - Готувати пропозиції заінтересованим сторонам стосовно недопущення у подальшому виявлених недоліків та невирішених питань при наданні профільних послуг коригувальних дій стосовно усунення недоліків, направлених на підвищення якості та ефективності послуг відповідного спрямування - Розроблювати методи моніторингу та оцінювання ризиків, відповідності та зусиль щодо надання стійкості ІТ у сфері кібербезпеки - Проводити постійну оптимізацію процесів профільного аудиту - Готувати пропозиції керівництву щодо вирішення проблем проведення аудиту програм та проєктів з ІТ у сфері кібербезпеки

43. Провідний аудитор інформаційних технологій (з кібербезпеки)

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7В6
Тип кваліфікації	Часткова додаткова
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	Трудові функції А, Б та В, притаманні аналітику з безпеки інформаційних систем, та додатково: Г. Проведення навчання та тренінгів для працівників, зайнятих в аудиті програм та проєктів з ІТ у сфері кібербезпеки Г1. Здатність готувати засоби та методи короткотермінового навчання/тренінгів працівників, зайнятих в аудиті програм та проєктів з ІТ у сфері кібербезпеки Г2. Здатність проводити навчання та тренінги відповідного спрямування
Основні необхідні знання	Основні необхідні знання, притаманні аудитору інформаційних технологій (з кібербезпеки), та додатково знати: - Вимоги до структури та змісту навчальної програми, до розроблення навчальних та методичних матеріалів - Сучасні підходи до формування навчальних програм - Зміст навчальної програми відповідного спрямування - Особливості організації навчального процесу для різних форм набуття компетентності - Форми організації навчального процесу - Види навчальних занять - Сучасні методи, засоби та технології викладання - Методи і способи організації індивідуальної та групової роботи слухачів під час навчання

	- Основи вікової психології, педагогіки та андрагогіки - Методи і способи ефективної комунікації, соціальної інженерії
Основні необхідні уміння та навички	Основні необхідні уміння та навички, притаманні аудитору інформаційних технологій (з кібербезпеки), та додатково уміти: - Розроблювати або брати участь у розробці індивідуальних/колективних планів розвитку, навчання та/або вдосконалення результатів навчання - Розроблювати чіткі вказівки і навчальні матеріали - Розроблювати або брати участь у розробці комп'ютерних навчальних модулів або курсів відповідного спрямування - Розроблювати або придбавати навчальний план, який відповідає темі та цілі на достатньому рівні - Розроблювати письмові тести для визначення рівня професійної придатності та оцінювання кваліфікації слухачів - Розроблювати критерії оцінювання результатів навчання - Брати участь у розробленні: правил оцінювання результатів навчання; внутрішніх регламентів з присвоєння/присудження кваліфікацій слухачам - Надавати технічну інформацію різним категоріям слухачів - Встановлювати ефективний зворотний зв'язок із слухачами з метою вдосконалення навчання - Розроблювати у необхідних обсягах навчальні програми на сучасних мовах програмування - Використовувати у навчальній діяльності віртуальні машини (Microsoft Hyper-V, VMWare, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud)

	- Використовувати: інструменти та методики тестування на проникнення; методи соціальної інженерії; сучасні та новітні технології у навчальних цілях - Конфігурувати і використовувати у навчальному процесі компоненти системи мережевої безпеки - Відображати дані в оригінальних форматах

44. Аналітик з безпеки інформаційних систем

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7Г1
Тип кваліфікації	Повна
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	А. Організація аналітичної діяльності з безпеки інформаційних систем А1. 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. А2. 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. 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 міждоменних рішень у безпечному середовищі А5. 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) 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 Б. Аналізування заходів та ситуації з безпекою інформаційних систем 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 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 Б3. Здатність виконувати аналізування тенденцій кіберзахисту та звітування про отримання мережевих сповіщень із різних джерел в організації, вказуючи можливі причини таких повідомлень

	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) Б5. Здатність перевіряти попередження системи виявлення вторгнень щодо мережевого трафіку за допомогою інструментів аналізування пакетів для локалізації та видалення шкідливого програмного забезпечення Б6. Здатність відновлювати втрачені дані чи інформацію про зловмисну атаку або дію на основі інформації щодо мережевого трафіку Б7. Здатність надавати допомогу в створенні сигнатур, які можна реалізувати в мережевих інструментах кіберзахисту у відповідь на нові або спостережувані загрози в мережевому середовищі В. Аналіз упереджувальних / розвідувальних заходів з безпеки інформаційних систем В1. Здатність до впровадження конкретних контрзаходів з кіберзахисту (операцій та 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, 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 (установу, підприємство) Г. Проведення моніторингу та оцінювання діяльності із забезпечення безпеки інформаційних систем Г1. Здатність розроблювати контент для засобів кіберзахисту Г2. Здатність надавати щоденні зведені звіти про мережеві події та діяльність, що стосуються практичних заходів кіберзахисту Г3. Здатність використовувати інструменти кіберзахисту для постійного моніторингу та аналізування системної активності для виявлення зловмисної діяльності

	Г4. Здатність оцінювати ефективність заходів з контролю безпеки Г5. Здатність оцінювати всі процеси керування конфігурацією Г6. Здатність оцінювати адекватні засоби контролю доступу на основі принципів найменших привілеїв і необхідності отримання відповідної інформації Г7. Здатність оцінювати та контролювати процеси кібербезпеки, пов’язані з впровадженням системи та її тестуванням
Основні необхідні знання	Знає: -Концепції комп’ютерних мереж та протоколів, а також методології мережевої безпеки; архітектури мережевої безпеки, включно з топологією, протоколами, компонентами та принципами (застосування глибинного захисту) - Принципи/методи: кібербезпеки та приватності / конфіденційності; безпеки IT (брандмауери, демілітаризовані зони, шифрування); глибинного захисту та архітектури мережевої безпеки управління мережевими системами (наскрізний моніторинг продуктивності систем) та інструменти; взаємодії людини з комп’ютером - Процеси: управління ризиками (методи оцінювання та зменшення ризику); встановлення, інтегрування, оптимізації компонентів системи - Конкретні операційні впливи за недостатності заходів із кібербезпеки - Категорії кіберзловмисників (дії зі сценаріями, інсайдерські загрози, фінансовані іншою державою) - Кіберзагрози та вразливості - Операційні системи

	- Методи системного адміністрування, мережевих та операційних систем - Моделі безпеки (модель Белла-ЛаПадули, модель цілісності Біби, модель цілісності Кларка-Вілсона) - Різні типи комп'ютерних архітектур - Загальні вектори атак на мережевому рівні - Політики, процедури та правила кіберзахисту та інформаційної безпеки - Стандарти безпеки персональних даних (PII); безпеки даних індустрії платіжних карток (PCI); безпеки даних персональної медичної інформації (PHI) - Закони, нормативні акти, політики та етику, які стосуються кібербезпеки та конфіденційності - Алгоритми шифрування даних - Криптографію та концепції управління криптографічними ключами - Комп'ютерні мови, що інтерпретуються та компілюються - Процеси управління наборами, можливостей та обмежень - Методології шифрування даних - Ризики безпеки додатків (Open Web Application Security Project Top 10 list) - Результати дослідження внутрішніх загроз, звітності, інструментів дослідження та законів / норм - Нові IT)та технології кібербезпеки - Структури звітності постачальника послуг кіберзахисту та процесів у власній організації - Системи управління базами даних - 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) - Процес розробки систем - Інструменти, методи та прийоми проєктування систем безпеки - Шляхи розширення файлів (.dll, .bat, .zip, .pcap, .gzip) - Телекомунікаційні концепції (канал зв'язку, наповнення системних каналів, спектральна ефективність, мультиплексування) - Безпеку віртуальної приватної мережі (VPN) - Мережеві інструменти (ping, traceroute, nslookup) - Типи мережевого зв'язку (LAN, WAN, MAN, WLAN, WWAN) - Порти і служби Windows/Unix - Модель OSI та базові мережеві протоколи (TCP/IP) - Мережеві протоколи, такі як TCP/IP, динамічна конфігурація хоста, системи доменних імен (DNS) і служби каталогів - Методи тестування та оцінювання безпеки систем - Методи аутентифікації, авторизації та контролю доступу - Механізми доступу до мережі, ідентифікації та управління доступом (інфраструктура відкритих ключів, Oauth, OpenID, SAML, SPML) - Методології і прийоми виявлення вторгнень для виявлення вторгнень на базі хоста та мережі - Мережеві атаки, зв'язок мережевої атаки із загрозами та вразливими місцями - Вектори атаки на мережевому рівні - Етапи кібератак (розвідка, сканування, вибір вектору проникнення, отримання доступу,

	ескалація привілеїв, підтримка доступу, експлуатація мережі, приховування слідів) - Методи аналізування трафіку на рівні пакетів з використанням відповідних інструментів (Wireshark, tcpdump) - Інструменти і програми системи виявлення вторгнень (IDS) / системи попередження вторгненнь (IPS) - Комп'ютерні алгоритми - Програмну інженерію - Вбудовані системи - Вплив реалізації сигнатур для вірусів, шкідливих програм і атак - Методи формалізації відображення мережі та відтворення мережевих топологій - Інструменти командного рядка операційної системи
Основні необхідні уміння та навички	Уміє: - Визначати, як має працювати система безпеки (включно з її стійкістю і надійністю) і вплив змін умов, операцій або середовища на ці результати - Виявляти вторгнення на базі хоста та мережі за допомогою технологій виявлення вторгнень - Розпізнавати та класифікувати типи вразливостей і пов'язаних з ними атак - Використовувати методику обробки інцидентів - Проєктувати, здійснювати інтеграцію апаратних та програмних рішень - Писати код мовою програмування, що підтримується - Читати та визначати приналежність електронних підписів - Розробляти та розгортати інфраструктуру електронних підписів - Збирати дані з різноманітних ресурсів кіберзахисту - Знаходити вразливості в системах безпеки - Виконувати аналізування трафіку на рівні пакетів - Використовувати структуру та процеси звітності постачальника послуг кіберзахисту у власній організації (установі, підприємстві) - Використовувати аналізатори протоколів - Оцінювати адекватність проєктів безпеки

	- Оцінювати системи безпеки - Оцінювати засоби контролю безпеки на основі принципів кібербезпеки. (CIS, NIST SP 800-53, Cybersecurity Framework)-

45. Провідний аналітик з безпеки інформаційних систем

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7Г1
Тип кваліфікації	Часткова додаткова
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	Трудові функції А, Б,В та Г, притаманні "Аналітику з безпеки інформаційних систем", та додатково: Д. Координація діяльності із забезпечення безпеки інформаційних систем Д1. Здатність координувати роботу з персоналом із забезпечення кібербезпеки всієї організації для перевірки мережевих сповіщень Д2. Здатність надавати керівникам рекомендації щодо кібербезпеки Д3. Здатність надавати керівникам рекомендації щодо кібербезпеки на основі інформації про значні загрози і вразливості Д4. Здатність працювати із заінтересованими сторонами для усунення інцидентів кібербезпеки та забезпечення захисту у відповідності до вимог щодо усунення вразливостей Д5. Здатність надавати рекомендації до планів аварійного відновлення, непередбачених випадків та забезпечення безперервності операцій
Основні необхідні знання	Основні необхідні знання, притаманні аналітику з безпеки інформаційних систем, та додатково знати: - Процеси управління безпекою - Конкретні операційні впливи за недостатності заходів з кібербезпеки

	- Різні класи атак (пасивні, активні, інсайдерські, суміжні, розподільні атаки) - Процеси управління ризиками (методи оцінювання та зменшення ризику)
Основні необхідні уміння та навички	Основні необхідні уміння та навички, притаманні аналітику з безпеки інформаційних систем, та додатково уміти: - Використовувати структуру та процеси звітності постачальника послуг кіберзахисту у власній організації - Оцінювати засоби контролю безпеки на основі принципів кібербезпеки - Проєктувати, інтегрувати апаратні та програмні рішення - Оцінювати адекватність проєктів безпеки - Збирати дані з різноманітних ресурсів кіберзахисту

46. Фахівець з підтримки інфраструктури кіберзахисту

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7Г2
Тип кваліфікації	Повна
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	Трудові функції А, Б та В, притаманні "Молодшому фахівцю з підтримки інфраструктури кіберзахисту ", та додатково: Г. Приймати участь у визначенні, розстановці пріоритетів і координації захисту критичної інфраструктури кіберзахисту та ключових ресурсів (Т0261) Д. Координація дій з аналітиками системи захисту кіберпростору для управління та адміністрування оновлень правил та сигнатур для спеціалізованих прикладних програм у сфері кіберзахисту (Т0042)
Основні необхідні знання	
Основні необхідні уміння та навички	

47. Провідний фахівець з підтримки інфраструктури кіберзахисту

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7Г2
Тип кваліфікації	Часткова додаткова
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	Трудові функції А, Б, В, Г та Д, притаманні "Фахівцю з підтримки інфраструктури кіберзахисту ", та додатково: Е. Впровадження на підприємстві (в установі, організації) новітніх технологій та напрацювань у сфері підтримки інфраструктури кіберзахисту (Т0486)
Основні необхідні знання	
Основні необхідні уміння та навички	

48. Фахівець з реагування на інциденти кібербезпеки

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7ГЗ
Тип кваліфікації	Повна
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	Трудові функції А, Б та В, притаманні "Молодшому фахівцю з реагування на інциденти кібербезпеки", та додатково: Г. Реалізація на підприємстві (в установі, організації) повноважень технічного експерта, взаємодія з представниками правоохоронних органів та за необхідності роз'яснення для них деталей інцидентів, співпраця з аналітиками розвідки з метою кореляції даних при оцінці загроз (Т0279, Т0312) Д. Координація функції реагування на інциденти та надання експертну технічної підтримки профільним фахівцям в масштабах підприємства (установи, організації) для управління інцидентами у сфері кіберзахисту (Т0041, Т0510)
Основні необхідні знання	
Основні необхідні уміння та навички	

49. Провідний фахівець з реагування на інциденти кібербезпеки

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7ГЗ
Тип кваліфікації	Часткова додаткова
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	Трудові функції А, Б, В, Г та Д, притаманні "Фахівцю з реагування на інциденти кібербезпеки", та додатково: Е. Розроблення та запровадження на практиці методик та настанов з кіберзахисту, а також звітів про виявлення інцидентів для відповідної аудиторії (Т0246)
Основні необхідні знання	
Основні необхідні уміння та навички	

50. Аналітик з оцінки вразливостей

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7Г4
Тип кваліфікації	Повна
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	А. Здійснення та/або підтримування дозволеного тестування на проникнення до активів корпоративної мережі (Т0028) Б. Проведення необхідних перевірок стану кіберзахисту відповідно середовищу, аналіз політики та конфігурації кіберзахисту підприємства (установи, організації) та оцінювання їх відповідності нормативним актам та її директивам (Т0252, Т0010) В. Проведення оцінювання технічних і нетехнічних ризиків і вразливостей пріоритетних технологічних областей (Т0549) Г. Забезпечення поінформованості про застосовувані політики з кібербезпеки, нормативні акти і документи відповідності, що стосуються аудиту системи кіберзахисту (Т0142)
Основні необхідні знання	
Основні необхідні уміння та навички	

51. Провідний аналітик з оцінки вразливостей

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7Г4
Тип кваліфікації	Часткова додаткова
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	Трудові функції А, Б, В та Г , притаманні " Аналітику з оцінки вразливостей ", та додатково: Д. Підготовка рекомендацій щодо вибору ефективних, з точки зору витрат, контролів захищеності з метою зниження ризиків (Т0550)
Основні необхідні знання	
Основні необхідні уміння та навички	

52. Аналітик загроз безпеки

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7Д1
Тип кваліфікації	Повна
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	А. Проведення предметної експертизи розвідувальних даних щодо загроз з метою розробки загальної оперативної картини (Т0583) Б. Підготовка інтегрованої, об'єднаної, розвідувальної інформацію про кібероперації з усіх джерел та/або надання показників і попереджень про результати розвідки (Т0758) В. Моніторинг та звітування про підтверджені загрозливі дії (Т0749) Г. Брати участь в процесі визначення недоліків у зборі розвідувальної інформації (Т0589) Д. Забезпечення поточної розвідувальної підтримки критичним внутрішнім / зовнішнім зацікавленим сторонам (Т0783)
Основні необхідні знання	
Основні необхідні уміння та навички	

53. Провідний аналітик загроз безпеки

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7Д1
Тип кваліфікації	Часткова додаткова
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	Трудові функції А, Б, В, Г та Д , притаманні " Аналітику загроз безпеки", та додатково: Е. Оцінювання процесів прийняття рішень щодо загроз (Т0685)
Основні необхідні знання	
Основні необхідні уміння та навички	

54. Дізнавач (сфера кібербезпеки та захисту інформації)

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7Є1
Тип кваліфікації	Повна
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	---------
Основні необхідні знання	---------
Основні необхідні уміння та навички	**---------**

55. Слідчий з кіберзлочинів

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7Є1
Тип кваліфікації	Повна
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	---------
Основні необхідні знання	----------
Основні необхідні уміння та навички	**----------**

56. Експерт-криміналіст (сфера кібербезпеки та захисту інформації)

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7Є2
Тип кваліфікації	Повна
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	---------
Основні необхідні знання	---------
Основні необхідні уміння та навички	**----------**

57. Експерт-криміналіст судової експертизи (сфера кібербезпеки та захисту інформації)

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	7
Рівень ГРК КБ	7Є2
Тип кваліфікації	Повна
Код КП	2139.2
Назва освітньої кваліфікації	Магістр
Перелік трудових функцій та професійних компетентностей	--------
Основні необхідні знання	--------
Основні необхідні уміння та навички	**---------**

58. Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	8
Рівень ГРК КБ	8B5
Тип кваліфікації	Повна
Код КП	1239
Назва освітньої кваліфікації	Доктор філософії
Перелік трудових функцій та професійних компетентностей	А. Створення та підтримання у дієздатному стані загальної архітектури інформаційної безпеки підприємства (установи, організації) (T0095) Б. Нагляд за діяльністю підпорядкованого персоналу, направленою на забезпечення ефективного функціонування системи кібербезпеки В. Формування раціонального розподілу ресурсів, необхідних для безпечного функціонування та підтримки вимог підприємства (установи, організації) з кібербезпеки (T0219) Г. Співпраця із зацікавленими сторонами з метою забезпечення безперервної діяльності підприємства (установи, організації) в рамках програми, стратегії та виконання завдань (T0044) Д. Консультування вищого керівництва щодо рівня ризику та стану безпеки, аналізу витрат/зисків, програм, політик, процесів, систем та елементів інформаційної безпеки (T0003, T0004)
Основні необхідні знання	
Основні необхідні уміння та навички	

59. Керівник підприємства (установи, організації) (сфера захисту інформації)

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	8
Рівень ГРК КБ	8В5
Тип кваліфікації	Повна
Код КП	1210.1
Назва освітньої кваліфікації	Доктор філософії
Перелік трудових функцій та професійних компетентностей	--------
Основні необхідні знання	-------
Основні необхідні уміння та навички	**--------**

60. Заступник керівника підприємства (установи, організації) (сфера захисту інформації)

Характеристики професійної кваліфікації	**Значення та опис**
Рівень НРК	8
Рівень ГРК КБ	8В5
Тип кваліфікації	Часткова
Код КП	1210.1
Назва освітньої кваліфікації	Доктор філософії
Перелік трудових функцій та професійних компетентностей	--------
Основні необхідні знання	--------
Основні необхідні уміння та навички	**--------**