АГЕНТСТВО
ЄВРОПЕЙСЬКОГО СОЮЗУ
З КІБЕРБЕЗПЕКИ

ECSF

Європейська рамка компетентностей із кібербезпеки

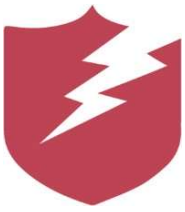
Проєкт v0.5
У процесі розроблення

КВІТЕНЬ 2022

ЗМІСТ

1. КОРОТКИЙ ОГЛЯД

Головний фахівець з інформаційної безпеки (CISO)



Фахівець із реагування на кіберінциденти

Фахівець із кіберправових питань, політики та дотримання нормативних вимог (комплаєнсу)

Фахівець з аналізу кіберзагроз

Архітектор із кібербезпеки

Аудитор із кібербезпеки

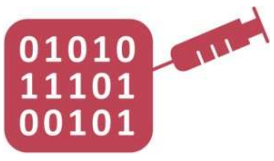
Викладач із кібербезпеки

Фахівець із впровадження кібербезпеки

Дослідник із кібербезпеки

Менеджер кіберзагроз безпекових ризиків

Слідчий із цифрової криміналістики



Тестувальник проникнення

2. ПРОФІЛІ

2.1 ГОЛОВНИЙ ФАХІВЕЦЬ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ (CISO)

Назва профілю	Головний фахівець з інформаційної безпеки (CISO)
Альтернативні назви *Перелік назв за тим самим профілем*	Директор програми з кібербезпеки, Фахівець з інформаційної безпеки (ISO), Керівник відділу інформаційної безпеки, Фахівець з IT-безпеки
Резюме *Вказує основне призначення профілю.*	Керує стратегією кібербезпеки організації та її реалізацією для належного забезпечення безпеки і захисту цифрових систем, послуг та активів.
Місія *Описує обґрунтування профілю.*	Визначає, обґрунтовує та інформує про бачення, стратегію, політику та процедури кібербезпеки. Керує впровадженням політики кібербезпеки в організації. Забезпечує обмін інформацією із зовнішніми органами та професійними організаціями.
Результат(и) *Висвітлюють профілі та пояснюють актуальність, зокрема в аспектах, не пов'язаних із кібербезпекою/ІКТ.*	• Стратегія кібербезпеки • Політика кібербезпеки
Основні завдання *Перелік типових завдань, що їх виконує Головний фахівець з інформаційної безпеки (CISO)* *Виконує такі завдання:*	• Визначати, впроваджувати, повідомляти і підтримувати цілі, вимоги, стратегії, політику кібербезпеки, узгоджені з бізнес-стратегією для підтримки цілей організації • Готувати і представляти бачення, стратегії та політики кібербезпеки для затвердження вищим керівництвом організації, а також забезпечувати їх виконання • Контролювати застосування та вдосконалення Системи управління інформаційною безпекою (СУІБ) • Навчати вище керівництво щодо кібербезпекових ризиків і загроз та їх впливу на організацію • Забезпечити узгодження з вищим керівництвом кібербезпекових ризиків організації • Розробити плани кібербезпеки • Розвивати відносини з органами та громадами, що займаються кібербезпекою • Повідомляти вищому керівництву про кібербезпекові інциденти, ризики, висновки • Стежити за розвитком кібербезпеки • Забезпечувати ресурси для реалізації стратегії кібербезпеки • Погоджувати бюджет кібербезпеки з вищим керівництвом • Забезпечувати стійкість організації до кіберінцидентів • Управляти безперервним нарощуванням потенціалу в організації • Переглядати, планувати і розподіляти відповідні ресурси кібербезпеки
Основні навички *Перелік умінь та навичок необхідних для виконання трудових функцій та обов'язків за профілем.* *Здатний:*	• Розуміти основні організаційні бізнес-процеси • Оцінювати і покращувати рівень кібербезпеки організації • Аналізувати і впроваджувати кібербезпекові стандарти, засади, політику, правила, закони, сертифікації та найкращі методи • Управляти ресурсами кібербезпеки • Розробляти, підтримувати і управляти виконанням стратегії кібербезпеки • Впливати на культуру кібербезпеки організації • Розробляти, застосовувати, контролювати і перевіряти Систему управління інформаційною безпекою (СУІБ) безпосередньо або за допомогою аутсорсингу • Переглядати і покращувати безпекові документи, звіти, угоди про рівень обслуговування, забезпечувати безпекові цілі • Застосовувати на практиці етичні вимоги щодо організації кібербезпеки • Забезпечувати практичні вирішення проблем кібербезпеки • Складати план кібербезпеки

Назва профілю	Головний фахівець з інформаційної безпеки (CISO)	
	• Комунікувати, координувати і співпрацювати із внутрішніми і зовнішніми зацікавленими сторонами • Застосовувати відповідні стандарти, сучасний досвід і юридичні вимоги щодо інформаційної безпеки • Передбачати необхідні зміни у стратегії інформаційної безпеки організації та формулювати нові плани • Визначати і застосовувати моделі зрілості для управління кібербезпекою • Передбачати майбутні кібербезпекові загрози, тенденції, потреби та виклики в організації • Управляти міждисциплінарними групами з кібербезпеки	
Основні знання *Перелік основних знань, необхідних для виконання трудових функцій та обов'язків за профілем.* *(Залежно від рівня)* *Базове розуміння:* *Розуміння:* *Знання:* *Глибокі знання:*	• Знання стандартів кібербезпеки та приватності, засад, політик, положень, законодавства, сертифікацій та найкращих практик • Розуміння етичних вимог організації кібербезпеки • Знання засобів контролю безпеки • Знання моделей зрілості кібербезпеки • Знання тактик, прийомів та процедур кібербезпеки • Знання методів/принципів управління ресурсами • Знання практик управління • Знання засад управління ризиками	
e-компетенції (з Системи e-компетенцій e-CF) *Щоб швидко знайти компетенції e-CF, зайдіть на сайт e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	D.1. Розроблення стратегії інформаційної безпеки E.3. Управління ризиками E.4. Управління взаємовідносинами E.8. Управління інформаційною безпекою E.9. Управління ІБ	Рівень 5 Рівень 4 Рівень 3 Рівень 4 Рівень 4

2.2 ФАХІВЕЦЬ ІЗ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ

Назва профілю	Фахівець із реагування на кіберінциденти	
Альтернативні назви *Перелік назв за тим самим профілем*	Оператор кіберінцидентів, Аналітик центру інформаційної безпеки (SOC), Кіберо-боронець/кіберзахисник, Аналітик журнальних файлів, Аналітик інформаційної без-пеки (Аналітик SOC), Менеджер з кібербезпеки SIEM	
Резюме *Вказує основне призначення профілю.*	Моніторинг стану кібербезпеки організації, управління інцидентами під час кібе-ратак та забезпечення безперервної роботи систем ІКТ.	
Місія *Описує обґрунтування про-філю*	Аналізує, оцінює та пом'якшує наслідки кібербезпекових інцидентів. Відстежує та оцінює стан кібербезпеки систем. Відновлює функціональність систем і процесів до робочого стану відповідно до Плану реагування на інциденти організації.	
Результат(и) *Висвітлювати профілі та по-яснювати їх актуальність, зо-крема в аспектах, не пов'яза-них із кібербезпекою/ІКТ.*	• Управління кіберінцидентами • План реагування на інциденти • Процес відновлення • Звіт про кіберінцидент • Управління вразливістю	
Основні завдання *Перелік типових завдань, що їх виконує Фахівець із ре-агування на кіберінциденти* *Виконує такі завдання:*	• Сприяти розробленню, підтримці та оцінюванню Плану реагування на ін-циденти • Розробити, впровадити й оцінити процедури, пов'язані з опрацюванням інциден-тів • Визначати, аналізувати, пом'якшувати наслідки і повідомляти про кібербезпекові інциденти • Оцінювати технічні вразливості та управляти ними • Вимірювати ефективність виявлення та реагування на кібербезпекові інциденти • Оцінювати стійкість засобів контролю кібербезпеки та заходів щодо пом'як-шення наслідків, вжитих після інциденту кібербезпеки або витоку даних • Впроваджувати і розвивати методи тестування опрацювання інцидентів • Встановити процедури аналізу результатів інцидентів та звітування про опрацю-вання інцидентів • Документувати аналіз результатів інциденту та дії з опрацювання інцидентів • Співпрацювати з центрами інформаційної безпеки (SOC) та групами реагу-вання на інциденти з комп'ютерної безпеки (CSIRT) • Співпрацювати з основним персоналом для повідомлення про інциденти безпеки відповідно до чинної нормативно-правової бази	
Основні навички *Перелік умінь та навичок не-обхідних для виконання трудо-вих функцій та обов'язків за профілем.* *Здатний:*	• Застосовувати на практиці всі технічні, функціональні та експлуатаційні аспе-кти опрацювання і реагування на інциденти кібербезпеки • Працювати над операційними системами, серверами, хмарами та відповідними інфраструктурами • Працювати під тиском • Управляти, взаємодіяти і звітувати • Працювати з файлами журналів та аналізувати їх	
Основні знання *Перелік основних знань, не-обхідних для виконання тру-дових функцій та обов'язків за профілем.* *(Залежно від рівня)* *Базове розуміння:* *Розуміння:* *Знання:* *Глибокі знання:*	• Знання методологій опрацювання кібербезпекових інцидентів • Знання практик та інструментів опрацювання кібербезпекових інцидентів • Знання комунікаційного циклу опрацювання інцидентів • Знання внутрішніх компонентів операційних систем, мережевих протоколів та сервісів • Знання тактики і техніки кібербезпекових атак • Знання кіберзагроз та вразливостей • Знання правової бази, пов'язаної з кібербезпекою та захистом даних • Знання специфіки діяльності центрів інформаційної безпеки (SOC) та груп реагування на інциденти з комп'ютерної безпеки (CSIRT)	
e-компетенції (з Системи e-компетенцій e-CF) *Щоб швидко знайти компете-нції e-CF, зайдіть на сайт e-CF Explorer: https://ecfusertool.itprofessionali sm.org/explorer*	A.7. Моніторинг технологічних тенденцій B.2. Інтеграція компонентів B.3. Тестування B.5. Виготовлення документації C.4. Управління проблемами	Рівень 3 Рівень 2 Рівень 3 Рівень 3 Рівень 4

2.3 ФАХІВЕЦЬ ІЗ КІБЕРПРАВОВИХ ПИТАНЬ, ПОЛІТИКИ ТА ДОТРИМАННЯ НОРМАТИВНИХ ВИМОГ (КОМПЛАЄНСУ)

Назва профілю	**Фахівець із кіберправових питань, політики та дотримання нормативних вимог (комплаєнсу)**
Альтернативні назви *Перелік назв за тим самим профілем*	Фахівець із захисту даних (DPO); Фахівець із захисту приватності; Консультант із кіберправа; Фахівець з управління інформацією; Фахівець із дотримання вимог до захисту даних; Юрист із питань кібербезпеки; Менеджер із дотримання вимог IT
Резюме *Вказує основне призначення профілю.*	Управляє дотриманням стандартів, правових та нормативних засад, пов'язаних із кібербезпекою, на основі стратегії організації та вимог законодавства.
Місія *Описує обґрунтування профілю.*	Контролює та забезпечує дотримання правових, нормативних засад та політик, пов'язаних із кібербезпекою і даними, відповідно до стратегії організації та вимог законодавства. Сприяє заходам організації щодо захисту даних. Надає юридичні консультації при розробленні процесів управління кібербезпекою організації.
Результат(и) *Висвітлювати профілі та пояснювати їх актуальність, зокрема в аспектах, не пов'язаних із кібербезпекою/ІКТ.*	• Політика захисту даних
Основні завдання *Перелік типових завдань, що їх виконує Фахівець із кіберправових питань, політики та дотримання нормативних вимог (комплаєнсу)* *Виконує такі завдання:*	• Забезпечувати дотримання стандартів, законів та нормативних актів у сфері приватності і захисту даних, а також надавати юридичні консультації та рекомендації щодо них • Оцінювати вплив на приватність, розробляти, підтримувати, повідомляти і навчати політиці та процедурам у сфері приватності • Забезпечувати і просувати програму приватності й захисту даних організації • Забезпечити інформування власників, розпорядників, контролерів, операторів, суб'єктів, внутрішніх і зовнішніх партнерів та організацій про права, обов'язки і відповідальність у сфері захисту даних • Виступати як головна контактна особа в питаннях реагування на запити і скарги щодо оброблення даних • Допомагати в розробленні, впровадженні, аудиті й перевірці комплаєнсу для забезпечення відповідності вимогам кібербезпеки та приватності • Брати участь у моніторингу аудитів та навчальних заходів, пов'язаних із захистом даних • Співпрацювати й обмінюватися інформацією з органами влади і професійними групами • Сприяти розробленню стратегії, політики та процедур організації кібербезпеки • Управляти юридичними аспектами відповідальності у сфері інформаційної безпеки та взаємовідносин із третіми сторонами
Основні навички *Перелік умінь та навичок необхідних для виконання трудових функцій та обов'язків за профілем.* *Здатний:*	• Мати всебічне розуміння бізнес-стратегії, моделей та продуктів, а також враховувати вимоги законодавства, нормативних актів та стандартів • Здійснювати практичну діяльність із питань захисту даних та конфіденційності, пов'язану з реалізацією організаційних процесів, фінансів та бізнес-стратегії • Управляти розробленням відповідних політик і процедур кібербезпеки та конфіденційності, які відповідають потребам бізнесу і вимогам законодавства; забезпечувати їх прийняття, розуміння та впровадження, а також доносити їх залученим сторонам • Проводити, відстежувати і переглядати оцінювання впливу на конфіденційність із використанням стандартів, засад, визнаних методологій та інструментів • Пояснювати і доносити теми захисту даних і конфіденційності до зацікавлених сторін та користувачів • Розуміти та дотримуватися етичних вимог і стандартів • Розуміти наслідки змін правової бази для стратегії та політики організації щодо кібербезпеки і захисту даних • Працювати в команді та співпрацювати з колегами

Назва профілю	Фахівець із кіберправових питань, політики та дотримання нормативних вимог (комплаєнсу)	
Основні знання *Перелік основних знань, необхідних для виконання трудових функцій та обов'язків за профілем.* *(Залежно від рівня)* *Базове розуміння:* *Розуміння:* *Знання:* *Глибокі знання:*	• Знання в галузі інформаційної безпеки • Глибокі знання законів і нормативних актів щодо приватності та захисту даних • Глибокі знання національних, європейських та міжнародних стандартів кібербезпеки і відповідних стандартів, законодавства, політик і правил щодо приватності • Знання вимог та практики дотримання законодавства • Знання методологій оцінювання впливу на приватність • Базове розуміння процесій зберігання, оброблення і захисту даних у системах, послугах та інфраструктурах	
е-компетенції (з Системи е-компетенцій e-CF) *Щоб швидко знайти компетенції e-CF, зайдіть на сайт e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	A.1. Узгодження інформаційних систем та бізнес-стратегії D.1. Розроблення стратегії інформаційної безпеки E.8. Управління інформаційною безпекою E.9. Управління ІБ	Рівень 4 Рівень 4 Рівень 3 Рівень 4

2.4 Фахівець з аналізу кіберзагроз

Назва профілю	Фахівець з аналізу кіберзагроз
Альтернативні назви *Перелік назв за тим самим профілем*	Аналітик кібердослідних даних, Фахівець із моделювання кіберзагроз
Резюме *Вказує основне призначення профілю.*	Збирати, обробляти, аналізувати дані та інформацію для підготування оперативних звітів і їх поширення серед цільових зацікавлених сторін.
Місія *Описує обґрунтування профілю.*	Керує життєвим циклом дослідних кіберзагроз, включаючи збір інформації про кіберзагрози, аналіз та підготування оперативних даних і їх поширення серед зацікавлених сторін у сфері безпеки та кібердослідної спільноти на тактичному, оперативному і стратегічному рівнях. Визначає та контролює тактики, прийоми і процедури (TTP), які використовуються суб'єктами кіберзагроз, а також тенденції їхнього розвитку, відстежує діяльність суб'єктів загроз і спостерігає за тим, як події, що відбуваються не в кіберпросторі можуть впливати на дії, пов'язані з кіберзагрозами.
Результат(и) *Висвітлювати профілі та пояснювати їх актуальність, зокрема в аспектах, не пов'язаних із кібербезпекою/ІКТ.*	• Аналіз кібердослідних даних • Управління аналізом кіберзагроз • Звіт про кіберзагрози
Основні завдання *Перелік типових завдань, що їх виконує Фахівець з аналізу кіберзагроз* *Виконує такі завдання:*	• Розробляти, впроваджувати й управляти стратегією організації з аналізу кіберзагроз • Розробляти плани та процедури для управління аналізом загроз • Трансформувати бізнес-вимоги у вимоги до кібердослідних даних • Здійснювати збір, аналіз та підготування оперативної інформації про загрози та її поширення серед зацікавлених сторін у сфері безпеки • Виявляти й оцінювати суб'єкти кіберзагроз, які націлені на організацію • Виявляти, відстежувати й оцінювати тактики, методи і процедури (TTP), які використовуються суб'єктами кіберзагроз, шляхом аналізу даних, інформації та кібердослідних даних із відкритих і власних джерел • Складати відповідні звіти на основі кібердослідних даних щодо загроз • Розробляти і консультувати щодо планів пом'якшення наслідків на тактичному, оперативному та стратегічному рівнях • Координувати із зацікавленими сторонами обмін і використання оперативної інформації про відповідні кіберзагрози • Використовувати кібердослідні дані для підтримки й допомоги у моделюванні загроз, рекомендацій щодо зниження ризиків та пошуку кіберзагроз. • Відкрито і публічно викладати і комунікувати кібердослідні дані на всіх рівнях • Доносити до зацікавлених осіб, не пов'язаних із технічними питаннями, інформацію про належний рівень безпеки, пояснивши їм рівень ризику та його наслідки
Основні навички *Перелік умінь та навичок необхідних для виконання трудових функцій та обов'язків за профілем.* *Здатний:*	• Працювати в команді та співпрацювати з різними зовнішніми експертами з предметних областей, коли це необхідно • Збирати, аналізувати і зіставляти інформацію про кіберзагрози, що надходить із кількох джерел • Визначати TTP та кампанії суб'єктів загроз • Автоматизовувати процедури управління кібердослідними даними щодо загроз • Проводити технічний аналіз та складання звітів • Виявляти некібернетичні події, що впливають на діяльність, пов'язану з кіберсферою • Моделювати загрози, дійових осіб і TTP • Складати і доводити до відома зацікавлених сторін звіти з кібердослідними даними • Використовувати і застосовувати платформи та інструменти кібердосліджень

Назва профілю	Фахівець з аналізу кіберзагроз	
Основні знання *Перелік основних знань, необхідних для виконання трудових функцій та обов'язків за профілем.* *(Залежно від рівня)* *Базове розуміння:* *Розуміння:* *Знання:* *Глибокі знання:*	• Глибокі знання IT/OT, операційних систем та комп'ютерних мереж • Глибокі знання рішень у галузі кібербезпеки • Знання засад TTP • Знання методів роботи з великими даними та їх аналітики • Знання скриптів та мов програмування • Глибокі знання стандартів обміну кібердослідними даними • Знання останніх випадків розкриття вразливостей, інцидентів, пов'язаних із витоком даних, та геополітичних подій, що впливають на кіберризики • Знання про сучасні та постійні кіберзагрози і суб'єкти загроз • Знання статистики та методик прогнозування	
е-компетенції (з Системи е-компетенцій e-CF) *Щоб швидко знайти компетенції e-CF, зайдіть на сайт e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	B.5. Виготовлення документації D.7. Наука про дані та аналітика D.10. Управління інформацією та знаннями E.4. Управління взаємовідносинами E.8. Управління інформаційною безпекою	Рівень 3 Рівень 4 Рівень 4 Рівень 3 Рівень 4

2.5 АРХІТЕКТОР ІЗ КІБЕРБЕЗПЕКИ

Назва профілю	Архітектор із кібербезпеки
Альтернативні назви *Перелік назв за тим самим профілем*	Архітектор рішень у галузі кібербезпеки, Дизайнер кібербезпеки, Архітектор безпеки даних
Резюме *Вказує основне призначення профілю.*	Планує та проєктує рішення щодо забезпечення безпеки (інфраструктури, системи, активи, програмне забезпечення, апаратне забезпечення і послуги) та засоби контролю кібербезпеки.
Місія *Описує обґрунтування профілю.*	Розробляє рішення на основі принципів безпеки і конфіденційності за проєктом. Створює і постійно вдосконалює архітектурні моделі та розробляє відповідну архітектурну документацію і специфікації. Координувати безпечне розроблення, інтеграцію та підтримку компонентів кібербезпеки згідно зі стандартами та іншими відповідними вимогами.
Результат(и) *Висвітлювати профілі та пояснювати їх актуальність, зокрема в аспектах, не пов'язаних із кібербезпекою/ІКТ.*	• Архітектура кібербезпеки • Вимоги до кібербезпеки
Основні завдання *Перелік типових завдань, що їх виконує Архітектор із кібербезпеки* *Виконує такі завдання:*	• Розробити і запропонувати безпечну архітектуру для реалізації стратегії організації • Розробити архітектуру кібербезпеки організації з урахуванням вимог безпеки та конфіденційності • Підготувати архітектурну документацію та специфікації • Представити зацікавленим сторонам проєкт архітектури безпеки високого рівня • Створити безпечне середовище під час життєвого циклу розроблення систем, послуг і продуктів • Координувати розроблення, інтеграцію та обслуговування компонентів кібербезпеки, забезпечуючи дотримання специфікацій кібербезпеки • Проаналізувати й оцінити кібербезпеку архітектури організації • Убезпечувати архітектуру рішень шляхом перевірки безпеки та сертифікації • Співпрацювати з іншими групами та колегами • Оцінити вплив рішень у галузі кібербезпеки на дизайн і продуктивність архітектури організації • Адаптувати архітектуру організації до нових загроз • Оцінити реалізовану архітектуру для підтримки належного рівня безпеки
Основні навички *Перелік умінь та навичок необхідних для виконання трудових функцій та обов'язків за профілем.* *Здатний:*	• Проводити аналіз вимог користувачів і бізнесу • Складати архітектурні та функціональні специфікації • Проєктувати системи та архітектури на основі принципів кібербезпеки, що забезпечують приватність і безпеку «за проєктом» та «за замовчуванням» • Управляти і комунікувати з виконавцями та персоналом IT/OT • Звітувати, комунікувати і робити презентації для зацікавлених сторін • Пропонувати архітектури кібербезпеки на основі потреб і бюджету зацікавлених сторін • Вибирати відповідні специфікації, процедури та засоби контролю • Забезпечити стійкість у місцях збою у всій архітектурі • Забезпечити керівництво технологічним проєктуванням • Координувати інтеграцію рішень щодо забезпечення безпеки
Основні знання *Перелік основних знань, необхідних для виконання трудових функцій та обов'язків за профілем.* *(Залежно від рівня)* *Базове розуміння:* *Розуміння:*	• Розуміння ризиків місії та бізнес-цілей організації • Розуміння стандартів та вимог щодо безпеки • Знання життєвого циклу безпечного розроблення • Знання еталонних моделей безпекової архітектури та рішень у галузі безпеки • Знання технологій та рішень у галузі безпеки • Знання кібербезпекових ризиків та загроз • Знання останніх тенденцій у галузі кібербезпеки • Розуміння стандартів та вимог, пов'язаних із кібербезпекою • Знання старих методів забезпечення безпеки • Знання технологій підвищення приватності (PET)

Назва профілю	Архітектор із кібербезпеки	
Знання: *Глибокі знання:*	• Знання методологій «приватність за проєктом» (privacy-by-design)	
е-компетенції (з Системи е-компетенцій e-CF) *Щоб швидко знайти компетенції e-CF, зайдіть на сайт e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	A.5. Архітектурний дизайн A.6. Дизайн застосунків B.1. Розроблення застосунків B.3. Тестування B.6. Інженерія систем ІКТ	Рівень 5 Рівень 3 Рівень 3 Рівень 3 Рівень 4

2.6 АУДИТОР ІЗ КІБЕРБЕЗПЕКИ

Назва профілю	Аудитор із кібербезпеки
Альтернативні назви *Перелік назв за тим самим профілем*	Аудитор інформаційної безпеки, Менеджер з аудиту кібербезпеки, Аудитор процедур і процесів кібербезпеки, Аудитор з перевірки вихідного коду, Аудитор з оцінювання ризиків та відповідності, вимогам інформаційної безпеки, Аналітик з оцінювання захисту даних
Резюме *Вказує основне призначення профілю.*	Виконувати аудит кібербезпеки в екосистемі організації.
Місія *Описує обґрунтування профілю.*	Проводить незалежні огляди для оцінювання ефективності процесів та засобів контролю і загальної відповідності політикам організації у галузі законодавства та нормативно-правової бази. Оцінює, тестує та перевіряє продукти, пов'язані з кібербезпекою (системи, апаратне забезпечення, програмне забезпечення і сервіси), функції та політики, що забезпечують відповідність інструкціям, стандартам і нормам.
Результат(и) *Висвітлювати профілі та пояснювати їх актуальність, зокрема в аспектах, не пов'язаних із кібербезпекою/ІКТ.*	• План аудиту кібербезпеки • Аудит кібербезпеки
Основні завдання *Перелік типових завдань, що їх виконує Аудитор із кібербезпеки* *Виконує такі завдання:*	• Розробити політику, процедури, стандарти і рекомендації з аудиту організації • Визначити методології та практику, що використовуються для аудиту систем • Визначити цільове середовище та управляти аудиторською діяльністю • Визначити обсяг аудиту, цілі та критерії для проведення аудиту • Розробити план аудиту з описом засад, стандартів, методології, процедур та аудиторських тестів • Переглядати об'єкт оцінювання, цілі та вимоги безпеки на основі профілю ризику • Перевіряти відповідність чинним законам і нормам, пов'язаним із кібербезпекою • Перевіряти відповідність застосовним стандартам, пов'язаним із кібербезпекою • Виконати план аудиту і зібрати докази та заміри • Підтримувати і захищати цілісність аудиторських записів • Готувати і надавати звіти про оцінку відповідності, забезпечення, аудит, сертифікацію і технічне обслуговування
Основні навички *Перелік умінь та навичок необхідних для виконання трудових функцій та обов'язків за профілем.* *Здатний:*	• Організовувати і працювати систематично і чітко, ґрунтуючись на фактичних даних • Дотримуватись і застосовувати на практиці основні положення, стандарти і методології аудиту • Застосовувати інструменти і методи аудиту • Аналізувати бізнес-процеси, оцінювати й аналізувати безпеку програмного чи апаратного забезпечення, а також технічні та організаційні засоби контролю • Повідомляти, пояснювати й адаптувати юридичні та нормативні вимоги і потреби бізнесу • Систематично та чітко планувати і проводити інтерв'ю • Збирати, оцінювати, підтримувати й захищати аудиторську інформацію • Добросовісно, неупереджено та незалежно проводити аудит
Основні знання *Перелік основних знань, необхідних для виконання трудових функцій та обов'язків за профілем.* *(Залежно від рівня)* *Базове розуміння:* *Розуміння:* *Знання:* *Глибокі знання:*	• Знання рішень у галузі кібербезпеки, технічних та організаційних засобів контролю • Знання систем контролю безпеки, стандартів • Знання методик оцінки відповідності • Глибокі знання системи аудиту, стандартів, методологій та сертифікації • Знання техніки проведення інтерв'ю

Назва профілю	Аудитор із кібербезпеки	
е-компетенції (з Системи е-компетенцій e-CF) *Щоб швидко знайти компетенції e-CF, зайдіть на сайт e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	B.3. Тестування B.5. Виготовлення документації E.3. Управління ризиками E.6 Управління якістю ІКТ E.8. Управління інформаційною безпекою	Рівень 4 Рівень 3 Рівень 4 Рівень 4 Рівень 4

2.7 ВИКЛАДАЧ ІЗ КІБЕРБЕЗПЕКИ

Назва профілю	Викладач із кібербезпеки
Альтернативні назви *Перелік назв за тим самим профілем*	Фахівець з обізнаності з кібербезпекою, Інструктор з кібербезпеки, Професор із кібербезпеки, Лектор із кібербезпеки
Резюме *Вказує основне призначення профілю.*	Підвищує рівень знань, навичок та компетенції людей у галузі кібербезпеки.
Місія *Описує обґрунтування профілю.*	Проєктує, розробляє і проводить інформаційні, навчальні та освітні програми з питань кібербезпеки і захисту даних. Використовує відповідні методи, прийоми та інструменти навчання і підготовки для транслювання та підвищення культури кібербезпеки, можливостей, знань і навичок людських ресурсів. Пропагує важливість кібербезпеки та закріплює її в організації.
Результат(и) *Висвітлювати профілі та пояснювати їх актуальність, зокрема в аспектах, не пов'язаних із кібербезпекою/ІКТ.*	• Обізнаність із кібербезпекою • Тренінги з кібербезпеки • Освіта в галузі кібербезпеки
Основні завдання *Перелік типових завдань, що їх виконує Викладач із кібербезпеки* *Виконує такі завдання:*	• Розробляти, оновлювати й надавати навчальні програми і навчальні матеріали з кібербезпеки та захисту даних для навчання і підвищення обізнаності на основі змісту, методів, інструментів, потреб студентів • Організовувати, розробляти і проводити заходи, семінари, курси, практичні тренінги з підвищення обізнаності з питань кібербезпеки та захисту даних • Відстежувати, оцінювати і звітувати про ефективність навчання • Оцінювати і звітувати про результати діяльності студента • Шукати нові підходи до освіти, навчання та підвищення обізнаності • Проєктувати, розробляти і забезпечувати кібербезпекові симуляції, віртуальні лабораторії або середовища кібернетичного діапазону • Надавати рекомендації щодо програм сертифікації кібербезпеки для фізичних осіб • Постійно підтримувати і вдосконалювати знання; заохочувати і розширювати можливості постійного вдосконалення потенціалу кібербезпеки та нарощування можливостей
Основні навички *Перелік умінь та навичок необхідних для виконання трудових функцій та обов'язків за профілем.* *Здатний:*	• Визначати потреби в обізнаності, навчанні та освіті в галузі кібербезпеки • Аналізувати і проводити навчання і тренінги з кібербезпеки • Проєктувати, розробляти і реалізовувати навчальні плани і програми з кібербезпеки відповідно до потреб організації та окремих осіб • Розробляти актуальні вправи та сценарії з кібербезпеки для симуляцій, віртуального або кібер-середовища • Забезпечувати навчання для отримання професійних сертифікацій із кібербезпеки та захисту даних • Проводити навчання, використовуючи різні навчальні ресурси • Розробити програми оцінювання заходів із підвищення обізнаності, навчання та освіти • Розповсюджувати або писати публікації, звіти, навчальні матеріали • Визначати й обирати відповідні педагогічні підходи для цільової аудиторії • Мотивувати і стимулювати учнів

Назва профілю	Викладач із кібербезпеки	
Основні знання *Перелік основних знань, необхідних для виконання трудових функцій та обов'язків за профілем.* *(Залежно від рівня)* *Базове розуміння:* *Розуміння:* *Знання:* *Глибокі знання:*	• Знання педагогічних методів • Глибокі знання в галузі підвищення обізнаності з кібербезпекою, розробленні програм для навчання і тренінгів • Знання професійних стандартів, методів оцінювання результатів навчання та сертифікацій у сфері кібербезпеки • Знання сучасних методів, інструментів і методик практичного навчання та тренінгів із кібербезпеки • Знання правової бази, нормативно-правових актів, стандартів, пов'язаних із кібербезпекою • Знання систем кібербезпеки, методологій, засобів контролю та найкращих практик	
e-компетенції (з Системи e-компетенцій e-CF) *Щоб швидко знайти компетенції e-CF, зайдіть на сайт e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	D.3. Надання освіти і навчання D.9. Розвиток персоналу E.8. Управління інформаційною безпекою	Рівень 3 Рівень 3 Рівень 3

2.8 ФАХІВЕЦЬ ІЗ ВПРОВАДЖЕННЯ КІБЕРБЕЗПЕКИ

Назва профілю	Фахівець із впровадження кібербезпеки
Альтернативні назви *Перелік назв за тим самим профілем*	Фахівець із впровадження інформаційної безпеки, Експерт із рішень у галузі кібербезпеки, Розробник кібербезпеки, Інженер із безпеки, Інженер із розроблення, безпеки та експлуатації (DevSecOps).
Резюме *Вказує основне призначення профілю.*	Розробляти, впроваджувати і використовувати кібербезпекові рішення (системи, активи, програмне забезпечення, засоби контролю та сервіси) на інфраструктурах і продуктах.
Місія *Описує обґрунтування профілю.*	Забезпечує пов'язане з кібербезпекою технічне розроблення, інтеграцію, тестування, впровадження, експлуатацію, технічне обслуговування, моніторинг і підтримку кібербезпекових рішень. Забезпечує дотримання специфікацій та вимог відповідності, гарантує надійну роботу й вирішує технічні проблеми, необхідні для рішень (системи, активи, програмне забезпечення, засоби контролю та сервіси), інфраструктур і продуктів організації, пов'язаних із кібербезпекою.
Результат(и) *Висвітлювати профілі та пояснювати їх актуальність, зокрема в аспектах, не пов'язаних із кібербезпекою/ІКТ.*	• Розроблення рішень у галузі кібербезпеки • Розгортання рішень у галузі кібербезпеки • Використання рішень у галузі кібербезпеки
Основні завдання *Список типових завдань, що їх виконує профіль.* *Має такі завдання:*	• Розробляти, впроваджувати, підтримувати, оновлювати, тестувати кібербезпекові продукти • Надавати користувачам і клієнтам підтримку з питань кібербезпеки • Інтегрувати кібербезпекові рішення та забезпечувати їх надійну роботу • Безпечно налаштовувати системи, послуги та продукти • Підтримувати і покращувати безпеку систем, послуг і продуктів • Впроваджувати процедури та засоби кібербезпеки • Контролювати і забезпечувати ефективність запроваджених засобів контролю кібербезпеки • Документувати і звітувати про безпеку систем, послуг і продуктів • Тісно співпрацювати з персоналом IT/OT щодо дій, пов'язаних із кібербезпекою • Впроваджувати, застосовувати й управляти оновленнями продуктів для усунення технічних вразливостей
Основні навички *Перелік умінь та навичок необхідних для виконання трудових функцій та обов'язків за профілем.* *Здатний:*	• Документувати, звітувати і комунікувати з різними зацікавленими сторонами • Інтегрувати кібербезпекові рішення в інфраструктуру організації • Налаштовувати рішення відповідно до політики безпеки організації • Оцінювати безпеку та продуктивність рішень • Розробляти й тестувати безпечний код і скрипти • Виявляти і вирішувати проблеми, пов'язані з кібербезпекою • Співпрацювати з іншими учасниками команди та колегами
Основні знання *Перелік основних знань, необхідних для виконання робочих функцій та обов'язків за профілем.* *(Залежно від рівня) Базове розуміння: Розуміння: Знання: Глибокі знання:*	• Знання життєвого циклу розроблення систем • Знання мов програмування • Знання безпеки операційних систем • Знання безпеки комп'ютерних мереж • Знання засобів контролю безпеки • Знання наступальних та оборонних методів забезпечення безпеки • Знання практик безпечного кодування • Знання методологій та практики тестування

Назва профілю	Фахівець із впровадження кібербезпеки	
е-компетенції (з Системи е-компетенцій е-CF) *Щоб швидко знайти компетенції e-CF, зайдіть на сайт e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	A.5. Архітектурний дизайн A.6. Дизайн застосунків B.1. Розроблення застосунків B.3. Тестування B.6. Інженерія систем ІКТ	Рівень 3 Рівень 3 Рівень 3 Рівень 3 Рівень 4

2.9 ДОСЛІДНИК ІЗ КІБЕРБЕЗПЕКИ

Назва профілю	Дослідник із кібербезпеки
Альтернативні назви *Перелік назв за тим самим профілем*	Інженер-дослідник у галузі кібербезпеки, Головний науковий співробітник (CRO) з кібербезпеки, Старший науковий співробітник із кібербезпеки, Фахівець із досліджень та розроблень (R&D) у галузі кібербезпеки, Науковий співробітник у галузі кібербезпеки, Фахівець із досліджень та інновацій / експерт із кібербезпеки, Науковий співробітник із кібербезпеки
Резюме *Вказує основне призначення профілю.*	Досліджувати галузь кібербезпеки та включати результати в кібербезпекові рішення.
Місія *Описує обґрунтування профілю.*	Проводить фундаментальні/базові та прикладні дослідження і сприяє інноваціям у галузі кібербезпеки шляхом співпраці з іншими зацікавленими сторонами. Аналізує тенденції та наукові висновки у сфері кібербезпеки.
Результат(и) *Висвітлювати профілі та пояснювати їх актуальність, зокрема в аспектах, не пов'язаних із кібербезпекою/ІКТ.*	• Дослідження в галузі кібербезпеки
Основні завдання *Перелік типових завдань, що їх виконує Дослідник із кібербезпеки* *Виконує такі завдання:*	• Аналізувати й оцінювати технології, рішення, розробки і процеси в галузі кібербезпеки • Проводити дослідження, інновації та розроблення на теми, пов'язані з кібербезпекою • Проявляти і генерувати ідеї досліджень та інновацій • Розвивати актуальні теми, пов'язані з кібербезпекою • Допомагати в розробленні інноваційних рішень, пов'язаних із кібербезпекою • Проводити експерименти і розробляти підтвердження концепції, пілотні проєкти і прототипи для рішень у галузі кібербезпеки • Обирати і застосовувати засади, методи, стандарти, інструменти і протоколи, включаючи створення і тестування підтвердження концепції для підтримки проєктів • Сприяти створенню сучасних бізнес-ідей, послуг та рішень у сфері кібербезпеки • Допомагати в нарощуванні потенціалу, пов'язаного з кібербезпекою, включаючи підвищення обізнаності, теоретичну підготовку, практичне навчання, тестування, наставництво, нагляд і обмін • Виявляти міжсекторальні досягнення в галузі кібербезпеки і застосовувати їх в іншому контексті або пропонувати інноваційні підходи та рішення • Управляти або брати участь в інноваційних процесах і проєктах, включаючи управління проєктами та бюджетування • Публікувати і презентувати наукові роботи та результати досліджень і розроблень
Основні навички *Перелік умінь та навичок необхідних для виконання трудових функцій та обов'язків за профілем.* *Здатний:*	• Генерувати нові ідеї та втілювати теорію у практику • Розбирати й аналізувати системи, виявляти слабкі місця, розробляти вимоги до безпеки і приватності, визначати ефективні або неефективні відповідні рішення • Аналізувати і вирішувати складні проблеми та завдання в галузі безпеки • Постійно відстежувати нові досягнення та інновації в галузі кібербезпеки • Повідомляти і поширювати наукові результати • Доводити обґрунтованість результатів дослідження • Співпрацювати з іншими учасниками команди

Назва профілю	Дослідник із кібербезпеки	
Основні знання *Перелік основних знань, необхідних для виконання трудових функцій та обов'язків за профілем.* *(Залежно від рівня)* *Базове розуміння:* *Розуміння:* *Знання:* *Глибокі знання:*	• Знання досліджень, розроблень та інновацій (RDI), що стосуються питань кібербезпеки • Знання методів, методологій, інструментів та прийомів кібербезпеки • Знання в галузі управління проєктами та бюджетування • Знання програм та грантів • Розуміння питань авторського права і прав інтелектуальної власності, стандартів та оформлення патентів • Розуміння багатодисциплінарного аспекту кібербезпеки • Розуміння відповідального розкриття інформації, пов'язаної з кібербезпекою • Розуміння загроз і ризиків шпигунства та примусу в міжнародних дослідженнях	
е-компетенції (з Системи е-компетенцій е-CF) *Щоб швидко знайти компетенції e-CF, зайдіть на сайт e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	A.7. Моніторинг технологічних тенденцій A.9. Інновації D.7. Наука про дані та аналітика C.4. Управління проблемами D.10. Управління інформацією та знаннями	Рівень 5 Рівень 5 Рівень 4 Рівень 3 Рівень 3

2.10 МЕНЕДЖЕР КІБЕРБЕЗПЕКОВИХ РИЗИКІВ

Назва профілю	Менеджер кібербезпекових ризиків
Альтернативні назви *Перелік назв за тим самим профілем*	Аналітик ризиків інформаційної безпеки, Консультант із захисту від кібербезпекових ризиків, Фахівець з оцінки кібербезпекових ризиків, Аналітик впливу на кібербезпеку
Резюме *Вказує основне призначення профілю.*	Управляти ризиками, пов'язаними з кібербезпекою організації, відповідно до стратегії організації. Розробляти, підтримувати, інформувати про процеси і звіти з управління ризиками.
Місія *Описує обґрунтування профілю.*	Постійно керує (виявляє, аналізує, оцінює, визначає, пом'якшує) ризики, пов'язані з кібербезпекою інфраструктур, систем і послуг ІКТ, плануючи, застосовуючи, звітуючи та повідомляючи про аналіз, оцінювання та усунення ризиків. Встановлює стратегію управління ризиками для організації та забезпечує збереження ризиків на прийнятному для організації рівні шляхом вибору дій щодо зниження ризиків і засобів контролю.
Результат(и) *Висвітлювати профілі та пояснювати їх актуальність, зокрема в аспектах, не пов'язаних із кібербезпекою/ІКТ.*	• Управління кібербезпековими ризиками
Основні завдання *Перелік типових завдань, що їх виконує Менеджер кібербезпекових ризиків* *Виконує такі завдання:*	• Розробити стратегію управління кібербезпековими ризиками організації • Управляти інвентаризацією активів організації • Виявляти й оцінювати загрози і вразливості систем ІКТ, пов'язані з кібербезпекою • Ідентифікувати ландшафт загроз, включаючи профілі зловмисників, та оцінювати потенціал атак • Оцінювати кібербезпекові ризики і пропонувати найбільш придатні варіанти управління ризиками, включаючи засоби контролю безпеки, пом'якшення та уникнення ризиків, які найкраще відповідають стратегії організації • Відстежувати ефективність контролю кібербезпеки та рівні ризику • Забезпечити, щоб усі кібербезпекові ризики залишалися на прийнятному рівні для активів організації • Розробляти, підтримувати, звітувати і комунікувати про повний цикл управління ризиками
Основні навички *Перелік умінь та навичок необхідних для виконання трудових функцій та обов'язків за профілем.* *Здатний:*	• Впроваджувати засади, методології і рекомендації щодо управління кібербезпековими ризиками та забезпечувати відповідність нормам і стандартам • Аналізувати і консолідувати методи управління якістю та ризиками організації • Давати можливість власникам бізнес-активів, керівникам та іншим зацікавленим сторонам приймати обґрунтовані з погляду ризиків рішення щодо управління та зменшення ризиків • Давати можливість співробітникам розуміти, вживати і дотримуватися заходів контролю • Створювати середовище усвідомлення кібербезпекових ризиків • Комунікувати, презентувати і звітувати перед відповідними зацікавленими сторонами • Пропонувати й управляти варіантами розподілу ризиків

Назва профілю	Менеджер кібербезпекових ризиків	
Основні знання *Перелік основних знань, необхідних для виконання трудових функцій та обов'язків за профілем.* *(Залежно від рівня)* *Базове розуміння:* *Розуміння:* *Знання:* *Глибокі знання:*	• Глибокі знання основ управління ризиками, стандартів, методологій, інструментів, рекомендацій та найкращих практик • Знання кіберзагроз, класифікацій загроз та репозиторіїв уразливостей • Знання варіантів і найкращих практик розподілу ризиків • Знання технічних та організаційних заходів контролю, які допомагають знизити кібербезпекові ризики до належного рівня • Знання технологій та засобів контролю, пов'язаних із кібербезпекою • Знання принципів, методів та політик в галузі моніторингу, впровадження, тестування та оцінювання ефективності засобів контролю	
e-компетенції (з Системи e-компетенцій e-CF) *Щоб швидко знайти компетенції e-CF, зайдіть на сайт e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	E.3. Управління ризиками E.5. Удосконалення процесів E.7. Управління змінами в бізнесі E.9. Управління ІБ	Рівень 4 Рівень 3 Рівень 4 Рівень 4

2.11 СЛІДЧИЙ ІЗ ЦИФРОВОЇ КРИМІНАЛІСТИКИ

Назва профілю	Слідчий із цифрової криміналістики	
Альтернативні назви *Перелік назв за тим самим профілем*	Аналітик із цифрової криміналістики, Фахівець із кібербезпеки та криміналістики, Консультант із комп'ютерної криміналістики	
Резюме *Вказує основне призначення профілю.*	Забезпечити, щоб у процесі розслідування кіберзлочинів було виявлено всі цифрові докази, які підтверджують зловмисну діяльність.	
Місія *Описує обґрунтування профілю.*	Встановлює зв'язок між артефактами та фізичними особами, отримує, відновлює, ідентифікує і зберігає дані, включаючи прояви, входи, виходи і процеси досліджуваних цифрових систем. Здійснює аналіз, реконструкцію та інтерпретацію цифрових доказів на основі якісного висновку. Надає неупереджений якісний висновок без інтерпретації отриманих результатів.	
Результат(и) *Висвітлювати профілі та пояснювати їх актуальність, зокрема в аспектах, не пов'язаних із кібербезпекою/ІКТ.*	• Цифровий криміналістичний аналіз	
Основні завдання *Перелік типових завдань, що їх виконує Слідчий із цифрової криміналістики* *Виконує такі завдання:*	• Розробити політику, плани та процедури цифрових криміналістичних розслідувань • Ідентифікувати, відновлювати, вилучати, документувати й аналізувати цифрові докази • Зберігати і захищати цифрові докази та надавати їх уповноваженим зацікавленим сторонам • Перевіряти середовище на наявність ознак несанкціонованих і незаконних дій • Систематично і чітко документувати, звітувати і представляти результати цифрового криміналістичного аналізу • Обирати і налаштовувати методи криміналістичного тестування, аналізу та звітності	
Основні навички *Перелік умінь та навичок необхідних для виконання трудових функцій та обов'язків за профілем.* *Здатний:*	• Працювати етично та незалежно; не піддаватися впливу та не бути упередженим під впливом внутрішніх чи зовнішніх суб'єктів • Збирати інформацію, зберігаючи її цілісність • Визначати, аналізувати і зіставляти події • Пояснювати і подавати цифрові докази простим, зрозумілим та доступним способом • Розробляти і комунікувати детальні та аргументовані звіти про розслідування	
Основні знання *Перелік основних знань, необхідних для виконання трудових функцій та обов'язків за профілем.* *(Залежно від рівня)* *Базове розуміння:* *Розуміння:* *Знання:* *Глибокі знання:*	• Знання методів цифрової криміналістики, передового досвіду та методик • Знання методик цифрового криміналістичного аналізу • Знання техніки цифрового криміналістичного тестування • Знання методик та процедур кримінального розслідування • Знання інструментів аналізу шкідливих програм • Знання класифікації кіберзагроз та вразливостей • Глибокі кзнання тактики і техніки кібербезпекових атак • Знання правової бази, пов'язаної з кібербезпекою та захистом даних • Знання внутрішніх компонентів операційних систем, мережевих протоколів та сервісів	
e-компетенції (з Системи e-компетенцій e-CF) *Щоб швидко знайти компетенції e-CF, зайдіть на сайт e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	A.7. Моніторинг технологічних тенденцій B.3. Тестування B.5. Виготовлення документації E.3. Управління ризиками	Рівень 3 Рівень 4 Рівень 3 Рівень 3

2.12 ТЕСТУВАЛЬНИК ПРОНИКНЕННЯ

Назва профілю	Тестувальник проникнення
Альтернативні назви *Перелік назв за тим самим профілем*	Етичний хакер-пентестер, Аналітик вразливостей, Тестер кібербезпеки, Експерт із активної кібербезпеки, Експерт із оборонної кібербезпеки, Експерт «червоної команди»
Резюме *Вказує основне призначення профілю.*	Оцінювати ефективність контролю безпеки, виявляти й використовувати вразливості кібербезпеки, оцінюючи їхню критичність у разі використання суб'єктами загроз.
Місія *Описує обґрунтування профілю.*	Планує, проєктує, впроваджує і виконує дії з тестування на проникнення та сценарії атак для оцінки ефективності впроваджених або запланованих заходів безпеки. Визначає вразливі місця або збої технічних та організаційних засобів контролю, які впливають на конфіденційність, цілісність і доступність продуктів ІКТ (наприклад, систем, апаратного забезпечення, програмного забезпечення та сервісів).
Результат(и) *Висвітлювати профілі та пояснювати їх актуальність, зокрема в аспектах, не пов'язаних із кібербезпекою/ІКТ.*	• Технічна оцінка кібербезпеки
Основні завдання *Перелік типових завдань, що їх виконує Тестувальник проникнення* *Виконує такі завдання:*	• Визначати, аналізувати й оцінювати технічні та організаційні вразливості кібербезпеки • Визначати вектори атак, виявляти і демонструвати використання технічних вразливостей кібербезпеки • Тестувати системи та операції на відповідність нормативним стандартам • Обирати і розроблювати відповідні методи тестування на проникнення • Організувати плани тестування і процедури тестування на проникнення • Встановити процедури аналізу та звітності результатів тестування на проникнення • Документувати і звітувати зацікавленим сторонам про результати тестування на проникнення • Впровадити інструменти і програми тестування на проникнення
Основні навички *Перелік умінь та навичок необхідних для виконання трудових функцій та обов'язків за профілем.* *Здатний:*	• Розробляти коди, скрипти і програми • Проводити соціальну інженерію • Визначати і використовувати вразливі місця • Проводити етичне зламування • Думати творчо і нестандартно • Вирішувати й усувати проблеми • Комунікувати і звітувати • Ефективно використовувати інструменти тестування на проникнення • Адаптувати і налаштовувати інструменти і методи тестування на проникнення
Основні знання *Перелік основних знань, необхідних для виконання трудових функцій та обов'язків за профілем.* *(Залежно від рівня)* *Базове розуміння:* *Розуміння:* *Знання:* *Глибокі знання:*	• Глибокі знання векторів кібербезпекових атак • Глибокі знання IT/OT пристроїв, операційних систем та комп'ютерних мереж • Глибокі знання інструментів, методів і методологій тестування на проникнення • Знання скриптів та мов програмування • Знання вразливостей системи безпеки • Знання найкращих практик із кібербезпеки

Назва профілю	Тестувальник проникнення	
е-компетенції (з Системи е-компетенцій е-CF) *Щоб швидко знайти компетенції e-CF, зайдіть на сайт e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	B.2. Інтеграція компонентів B.4. Тестування B.5. Впровадження рішень B.6. Виготовлення документації B.3. E.3. Управління ризиками	Рівень 4 Рівень 4 Рівень 2 Рівень 3 Рівень 4

XX-00-00-000-XX-X

ПРО ENISA

Агентство Європейського Союзу з кібербезпеки (ENISA) – це агентство Європейського Союзу, покликане забезпечити високий загальний рівень кібербезпеки в Європі. Агентство Європейського Союзу з кібербезпеки, засноване у 2004 році та підсилене Законом ЄС про кібербезпеку, сприяє кіберполітиці ЄС, підвищує надійність продуктів, послуг і процесів ІКТ за допомогою схем сертифікації кібербезпеки, співпрацює з державами-учасницями та органами ЄС та допомагає Європі підготуватися для кібервикликів майбутнього. Шляхом обміну знаннями, нарощування потенціалу та підвищення обізнаності Агентство співпрацює зі своїми головними зацікавленими сторонами для зміцнення довіри до пов'язаного сегменту економіки, підвищення стійкості інфраструктури Союзу та, зрештою, створення цифрової безпеки європейського суспільства і громадян. Більше інформації про ENISA та його роботу можна знайти тут: www.enisa.europa.eu.

ENISA
Агентство Європейського Союзу з кібербезпеки

Офіс в Афінах
Агамемнонос 14, Халандрі 15231, Аттікі, Греція

Офіс в Іракліоні
95 Ніколау Пластіра
700 13 Вассіліка Вутон, Ірактіон, Греція

ISBN 000-00-0000-000-0 DOI: 0000.0000/000000