Спеціальна публікація NIST 800-181, редакція 1

Загальні принципи управління персоналом у сфері кібербезпеки (Загальні принципи NICE)

Родні Пітерсен [Rodney Petersen]
Даніель Сантос [Danielle Santos]
Метью К. Сміт [Matthew C. Smith]
Карен А. Ветцель [Karen A. Wetzel]
Грег Вітте [Greg Witte]

Цю публікацію можна завантажити безкоштовно за адресою:
https://doi.org/10.6028/NIST.SP.800-181r1.ukr

Document translated courtesy of the Ukrainian Academy of Cybersecurity. Reviewed by Diplomatic Language Services. Official U.S. Government translation.

The official English language version of this publication is available free of charge from the National Institute of Standards and Technology (NIST): https://doi.org/10.6028/NIST.SP.800-181r1.

Спеціальна публікація NIST 800-181, редакція 1

Загальні принципи управління персоналом у сфері кібербезпеки (Загальні принципи NICE)

Родні Пітерсен [Rodney Petersen] (Директор)

Даніель Сантос [Danielle Santos] (Менеджер із комунікацій та операційної діяльності)

Карен А. Ветцель [Karen A. Wetzel] (Менеджер Загальних принципів NICE)

Національна ініціатива з поширення знань у сфері кібербезпеки (NICE)

Відділення прикладної кібербезпеки,

Лабораторія інформаційних технологій

Метью К. Сміт [Matthew C. Smith]

Грег Вітте [Greg Witte]

«Хантінгтон Інгаллс Індастріз» [Huntington Ingalls Industries]

Аннаполіс Джанкшн, штат Меріленд

Цю публікацію можна завантажити безкоштовно за адресою:
https://doi.org/10.6028/NIST.SP.800-181r1.ukr

Листопад 2020 року

Міністерство торгівлі США
Уїлбур Л. Росс мол. [Wilbur L. Ross, Jr.], Міністр

Національний Інститут Стандартів і технологій [National Institute of Standards and Technology]
Уолтер Копан [*Walter Copan*] *Директор NIST та Заступник Міністра торгівлі з юитань стандартів і технологій*

Повноваження

Цю публікацію підготовив NIST в рамках його статутних обов'язків, передбачених Федеральним законом США про вдосконалення управління інформаційною безпекою (FISMA) від 2014 року, розділом 44 Кодексу законів США §3551 *et seq.*, Публічним законом (P.L.)\113-283. NIST відповідає за розроблення стандартів та настанов у сфері інформаційної безпеки, включаючи мінімальні вимоги до федеральних інформаційних систем, але такі стандарти й настанови не застосовуються до національних систем безпеки без вираженого схвалення належних федеральних посадових осіб, які уповноважені втілювати політику щодо таких систем. Ця настанова відповідає вимогам Директиви A-130, виданої Офісом із питань управління та бюджету (OMB).

Ніщо в цієї публікації не може розглядатись як суперечливе стандартам та настановам, обов'язковим та зобов’язуючим для федеральних органів відповідно до вповноваженого рішення Міністра торгівлі. Крім того, ці настанови не повинні тлумачитися як такі, що відміняють або замінюють чинні повноваження Міністра торгівлі, директора OMB або іншої федеральної посадової особи. Ця публікація може використовуватися неурядовими організаціями на добровільній основі, і вона не є суб’єктом авторського права на території Сполучених Штатів Америки. Проте NIST буде вдячний за посилання на хей документ.

National Institute of Standards and Technology Special Publication 800-181
Natl. Inst. Stand. Technol. Spec. Publ. 800-181 Rev. 1, 27 pages (November 2020)
CODEN: NSPUE2

Цю публікацію можна завантажити безкоштовно за адресою:
https://doi.org/10.6028/NIST.SP.800-181r1.ukr

Зауваження щодо цієї публікації можна подавати за адресою:
National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
Email: NICEFramework@nist.gov

Звіти про технології комп'ютерних систем

Лабораторія інформаційних технологій (ITL) при Національному інституті стандартів і технологій США сприяє розвитку економіки США та покращенню добробуту населення шляхом технічного управління інфраструктурою країни у сфері обчислень і стандартизації. ITL розробляє тести, методи тестувань, нормативні дані, проводить дослідно-експериментальні роботи й виконує технічний аналіз із метою забезпечення розроблення та продуктивного використання інформаційних технологій. Серед обов'язків ITL – розроблення управлінських, адміністративних, технічних і фізичних стандартів та настанов щодо раціонального забезпечення безпеки та приватності даних у федеральних інформаційних системах, які не належать до інформації, пов'язаної з державною безпекою. У Спеціальній публікації серії 800 описується науково-дослідницька діяльність ITL, настанови та роз'яснювальна діяльність, присвячена інформаційній безпеці, а також співпраця із промисловістю, урядом та науковими організаціями.

Анотація

Ця публікація Національної ініціативи з поширення знань у сфері кібербезпеки (NICE) описує Загальні принципи управління персоналом у сфері кібербезпеки (Загальні принципи NICE) – основний документ для опису та розповсюдження інформації про роботу у сфері кібербезпеки. Цей документ виражає цю роботу у формі формулювання Завдань та описує формулювання Знань та Навичок, які створюють основу для тих, хто навчається, включаючи студентів, осіб, які шукають роботу, і працівників. Використання цих формулювань допоможе студентам розвивати навички, особам, які шукають роботу, демонструвати потрібну компетентність, а працівникам - виконувати завдання. Як загальний відповідний лексикон, що класифікує та описує роботу у сфері кібербезпеки, Загальні принципи NICE покращують комунікацію про те, як виявляти, наймати, розвивати й утримувати таланти у сфері кібербезпеки. Загальні принципи NICE є довідковим джерелом інформації, на основі якого організації або галузі можуть розробляти додаткові публікації або інструменти, що відповідають їхнім потребам у визначенні або наданні настанов щодо різних аспектів освіти, підготовки та розвитку працівників у сфері кібербезпеки.

Ключові слова:

Компетенція; кібербезпека; кіберпростір; освіта; знання; роль; безпека; навичка; завдання; команда; тренінг; персонал; робоча роль.

Повідомлення про розкриття патентів

ПРИМІТКА. Лабораторія інформаційних технологій (ITL) звернулась до власників заявок на патенти, використання яких може бути потрібним для дотримання настанов або вимог, що наведені у цій публікації, розкрити ITL такі заявки на патенти. Проте власники патентів не зобов'язані відповідати на запити ITL щодо патентів, а ITL не проводила жодного патентного пошуку з метою визначення того, які з патентів (за їх наявності) можуть бути пов'язані з цією публікацією.

На дату виходу публікації та наступних запитів для ідентифікації заявок на патенти, використання яких може бути потрібним для дотримання настанов або вимог, що наведені у цій публікації, на адресу ITL не надавалися дані про такі заявки на патенти.

ITL не заявляє та не припускає, що для уникнення порушення патентних прав під час використання цієї публікації не потрібні ліцензії.

Тлумачення термінів

Терміни «повинен» і «не повинен» вказують на вимоги, які мають бути дотримані з метою забезпечення відповідності цій публікації та відхилення від яких не допускається. Терміни «слід» і «не слід» вказують серед кількох можливостей на одну, що рекомендується як найбільш відповідна, без згадування або виключення інших можливостей, або на те, що певний перебіг подій є бажаним, але не обов'язково необхідним, або що (у негативній формі) якась можливість або перебіг подій не схвалюються, проте і не забороняються. Терміни «можливо» або «не потрібно» вказують на перебіг подій, що допускається в рамках цієї публікації. Терміни «може» і «не може» вказують на можливість і здатність, як матеріального, так і фізичного або причинно-наслідкового характеру.

В рамках Загальних принципів NICE особи, які виконують роботу у сфері кібербезпеки, включаючи студентів, осіб, які шукають роботу, та працівників, називаються Учнями. Цей термін також означає, що кожен працівник навчається все своє життя.

Подяка

Загальні принципи NICE були розроблені Основним авторським колективом, що включає представників багатьох міністерств і державних органів Федерального уряду Сполучених Штатів Америки. Національний інститут стандартів і технологій США висловлює свою вдячність таким членам авторського колективу, які зробили визначний внесок у створення цієї публікації:

Уільям Ньюхаус [William Newhouse] Національний інститут стандартів і технологій США
Пем Фруджолі [Pam Frugoli] Міністерство праці США
Ліса Дорр [Lisa Dorr] Міністерство внутрішньої безпеки США
Кеннет Врумен [Kenneth Vrooman] Агентство з питань кібербезпеки та безпеки інфраструктури
Боббі Сандерс [Bobbie Sanders] Міністерство оборони США
Патрік Джонсон [Patrick Johnson] Міністерство оборони США
Метт Айснор [Matt Isnor] Міністерство оборони США
Стефані Шівлі [Stephanie Shively] Міністерство оборони США
Райан Фарр [Ryan Farr] Міністерство оборони США

Автори та Основний авторський колектив вдячні за значний внесок осіб і організацій із державного та приватного секторів, чиї глибокі та конструктивні зауваження допомогли підвищити загальну якість, ретельність викладання і корисність цієї публікації. Автори зокрема дякують за багато корисних відповідей на Запит Загальних принципів NICE про надання зауважень та на зауваження щодо проекту цієї публікації, викладеного для відкритого обговорення.

Крім того, колектив вдячний та відзначає внески осіб, які створювали попередні версії Загальних принципів управління державним персоналом у сфері кібербезпеки, що описано на сторінці Історія Ресурсного центру Загальних принципів NICE. [1]

Примітка для читачів

До Вашої уваги пропонуються Загальні принципи управління персоналом у сфері кібербезпеки (Загальні принципи NICE), Перегляд 1, Національної ініціативи з поширення знань у сфері кібербезпеки (NICE). Працівники Офісу програми NICE отримали багато відгуків від громадськості, включаючи багато відповідей на останній запит про надання загальних відгуків щодо Загальних принципів NICE, а також відповіді на проект цієї публікації, викладений для відкритого обговорення. З огляду на отримані відгуки, а також на швидкий характер розвитку і взаємопов'язаність процесів в екосистемі кібербезпеки, авторський колектив вирішив прийняти і запровадити такі параметри, як динамічність, гнучкість, сумісність із іншими системами та модульність. На основі цих параметрів Загальні принципи NICE було перероблено з метою забезпечення оптимізованого підходу до розвитку працівників, що відповідають за управління ризиками у сфері кібербезпеки. Нижче наводиться стислий огляд змін:

- Організаційні компоненти у Перегляді 1 спрощені шляхом виключення Категорій (наприклад, забезпечення безпеки, нагляд і управління, захист і оборона, аналіз тощо) та Сфер спеціалізації (наприклад, реагування на інциденти, аналіз загроз, управління кібербезпекою тощо). З метою спрощення підходу, що передбачає динамічність, гнучкість і сумісність із іншими системами, а також модульність для організацій, у Перегляді 1 представлено оптимізований набір складових, який включає Завдання, Знання та Навички. Організації, які надають перевагу використанню колишніх Категорій та Сфер спеціалізації, можуть продовжувати використовувати їх або створювати команди на основі цих концепцій, а також приводити їх у відповідність із цією версією Загальних принципів NICE (див. розділ 3.4).
- У Перегляді 1 описано декілька способів використання Завдань, Знань і Навичок, включаючи методики їх використання для створення Робочих ролей. Користувачі Робочих ролей, які описані в оригіналі документа NIST SP 800-181, можуть і надалі використовувати ці ролі; оновлення до робочих ролей можуть бути опубліковані NICE в майбутньому. [2]

Взаємозв'язки між Завданнями, Знаннями, Навичками та Здібностями змінилися. Навички та Здібності із попередньої версії було перетворено для простоти у формулюваання Навичок, які сфокусовані на діях учня. У цій версії описані методи пов'язування формулювань Знань та Навичок із формулюванням Завдань для різних результатів. Перелік Завдань, Знань, Навичок та Робочих ролей, які раніше зазначались у додатках А та В Загальних принципів від 2017 року, були виключені з цієї версії з метою спрощення підтримки Загальних принципів NICE та полегшення внесення змін і доповнень до таких переліків. Формулювання Завдань, Знань і Навичок (TKS), а також відповідні Компетенції і Робочі ролі будуть підтримуватися як окремі артефакти і вимагатимуть періодичного перегляду та оновлення у рамках визначеного процесу внесення змін та під контролем зазначення версії, що необхідно для належного управління змінами та їх розповсюдження. До того, як будуть внесені такі зміни, попередні версії цих переліків залишаються доступними для використання користувачами в Ресурсному центрі Загальних принципів NICE. Для забезпечення сумісності систем та модульності у майбутніх оновленнях буде передбачатися відповідність формулювань кінцевим визначенням формулювань TKS, що наведені у цьому документі.

- Для читачів, які зацікавлені в порівнянні стандартів, посилань або ресурсів для Загальних принципів NICE, NICE працює з онлайновою Програмою інформативних посилань (OLIR) із метою розроблення шаблонів для такого порівняння. Програма OLIR під управлінням NIST забезпечує процес приведення посилань у відповідність до документів NIST. Крім того, в рамках програми надається каталог цих посилань. [3]

Резюме

Кожен із нас окремо або спільно з іншими особами виконує важливу роботу і робить свій внесок у розвиток суспільства. Однак оскільки інформація і технології, включаючи багато новітніх типів операційної технології, стають дедалі складнішими та взаємопов'язаними між собою, може бути складно чітко описати роботу, яка виконується або яку ми бажаємо виконати, особливо у цих сферах. Національна ініціатива з освіти у сфері кібербезпеки (NICE) визначає, що особи, які виконують роботу у сфері кібербезпеки, включаючи студентів, осіб, які шукають роботу, та працівників, залишаються учнями усе своє життя за рахунок їхніх зусиль для підкреслення та вирішення наслідків залучення кібербезпеки в багатьох сферах. Ця категорія людей у цьому документі позначається і як «Учні», і як «персонал у сфері кібербезпеки», хоча останній термін не означає, що робочі ролі та зміст, які передбачені Загальними принципами NICE, поширюються лише на осіб, які займаються виключно питаннями кібербезпеки. Завдання, які виконуються цими учнями, також позначаються у цьому документі як «робота з кібербезпеки», а Загальними принципами передбачені засоби для точного описання такої роботи з метою надання підтримки учням у навчанні або підготовці, а також із метою забезпечення пошуку, найму, розвитку та утримання працівників. Загальні принципи NICE були розроблені з метою допомоги у створення довідкової таксономії, тобто спільної мови, роботи у сфері кібербезпеки та осіб, які виконують таку роботу. Загальні принципи NICE мають на меті підтримку місії NICE зі стимулювання, просування та координування потужного співтовариства, яке спільно працює над розвитком інтегрованої екосистеми освіти, тренінгів та розвитку працівників у сфері кібербезпеки. Загальні принципи NICE надають набір складових для опису завдань, знань та навичок, які потрібні для виконання роботи у сфері кібербезпеки окремими особами та колективами. Завдяки цим складовим Загальні принципи NICE надають можливість організаціям розвивати своїх працівників, яким доручається виконання роботи у сфері кібербезпеки, а також допомагає учням вивчати роботу у сфері кібербезпеки і долучатися до відповідних навчальних заходів із метою розвитку їхніх Знань і Навичок. Цей розвиток, в свою чергу, створює переваги для роботодавців та працівників для визначення кар’єрних шляхів, які документують, як саме готуватися до виконання роботи у сфері кібербезпеки, використовуючи формулювання Завдань, Знань і Навичок (TKS), прив'язаних до Робочих ролей та Компетенцій.

Використання єдиних термінів та мови допомагає організовувати і доводити до відома відповідних осіб роботу, яка має бути виконана, та характеристики осіб, кваліфікованих для виконання такої роботи. Отже, Загальні принципи NICE допомагають спростити обмін інформацією та зосередитись на виконанні конкретних Завдань. Насамкінець, використання Загальних принципів NICE робить діяльність більш зрозумілою та послідовною на всіх організаційних рівнях, від роботи окремої особи до роботи технологічної системи, програми, організації, галузі, держави або нації.

ЗМІСТ

1 Преамбула

Технології продовжують розвиватися раніше небаченими темпами. Зокрема, радикально змінюються технології забезпечення швидкого та ефективного доступу до інформації та її обробки. Підвищується складність роботи, потрібної для розроблення, побудови, убезпечення та запровадження цих даних, мереж та систем. Крім того, складним завданням залишається описання цієї роботи та осіб, які можуть цю роботу виконувати. Ця проблема додатково ускладнюється завдяки тому, що організації використовують різні методики та методики власного розроблення, намагаючись вирішити проблеми, з якими вони стикаються.

У цій публікації Національної ініціативи з освіти у сфері кібербезпеки (NICE) представлені Загальні принципи управління персоналом у сфері кібербезпеки (Загальні принципи NICE). Загальні принципи NICE допомагають організаціям подолати проблему з описом своїх працівників для багатьох зацікавлених сторін шляхом використання підходу на основі стандартних блоків. Завдяки використанню концептуальних стандартних блоків Загальні принципи NICE забезпечують організації можливість використання спільної мови для застосування як усередині компанії, так і у спілкуванні з іншими сторонами. Цей підхід допомагає організаціям адаптувати і впроваджувати Загальні принципи NICE відповідно до їхнього унікального операційного контексту. Крім того, створюючи спільну мову, Загальні принципи NICE зменшують перешкоди на шляху залучення організацій, що мають намір долучатися до роботи інших організацій та співпрацювати з ними.

На рисунку 1 нижче представлено високорівневий огляд Загальних принципів NICE. Основними складовими Загальних принципів NICE є формулювання Завдань, Знань і Навичок (TKS) (пояснені у Розділі 2), які показані разом з концепціями, які вони описують. На рисунку 1 зображено два основних типи описуваних концепцій: «робота» та «учень». Слід зауважити, що особи, які виконують (або виконуватимуть) роботу (наприклад, студенти, поточні працівники або особи, які шукають роботу), постійно навчаються і досягають цілей та можуть перебувати на будь-якому етапі процесу навчання. Загальні принципи NICE намагаються описати як «роботу», так і «учня» узагальненими термінами, які можуть використовуватись у всіх організаціях.

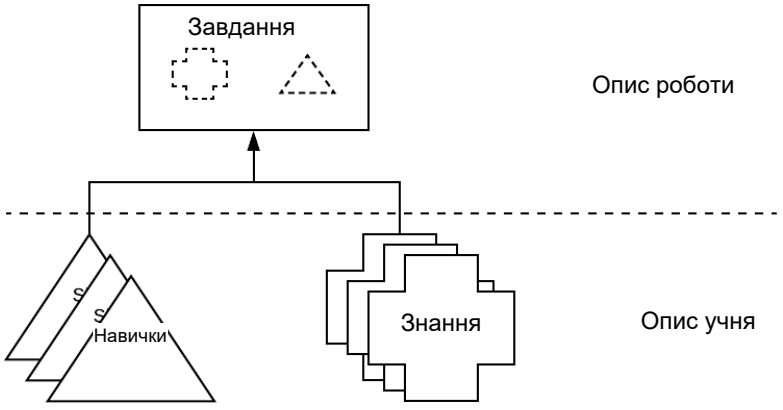

Рисунок 1. Підхід із використанням складових відповідно до Загальних принципів NICE.

«Робота» – це те, чого потребує організація для досягнення цілей у сфері управління ризиками кібербезпеки. Кожна організація виконує як загальні завдання, так і деякі завдання, пов'язані з унікальним контекстом. Наприклад, кожна організація має певну форму управлінських завдань, тоді як лише деякі організації мають завдання з «безпечного розгортання

магістральних енергетичних систем». Загальні принципи NICE надають організаціям інструмент для описання своєї роботи за допомогою формулювань Завдань, що групуються для створення формулювань Знань і Навичок.

«Учень» - це особа, яка має знання та навички. Термін *учень* застосовується до всіх людей, що описуються у цьому документі. Учень може бути студентом, особою, яка шукає роботу, працівником або іншим членом трудового колективу. В організаційному контексті учні виконують завдання. В освітньому контексті учні здобувають нові знання та навички. Усі особи вважаються учнями через те, що вони отримали певну освіту або тренінги до приймання на роботу, проходять поточні тренінги, самопідготовку або мають план кар'єрного росту.

Загальні принципи NICE надають організаціям можливість описувати учнів, пов'язуючи формулювання Знань і Навичок із окремою особою або групою осіб. Використовуючи свої Знання та Навички, учні можуть виконувати Завдання для досягнення цілей організації. Оскільки не всі організації будуть використовувати кожну концепцію, пов'язану з учнями, в Загальних принципах NICE організаціям надається гнучкий набір стандартних блоків для використання, як необхідно в їхньому унікальному контексті. Визнання ролі учня у розвитку здібностей виконувати роботу у сфері кібербезпеки також посилює придатність застосування Загальних принципів NICE для організацій, що надають послуги з освіти та тренінгів.

За допомогою опису як роботи, так і учня Загальні принципи NICE надають організаціям загальну мову для описання своєї роботи і працівників у сфері кібербезпеки. У певних частинах Загальних принципів NICE описується організаційний аспект роботи (Завдання), а в інших частинах описується контекст учня (Знання та Навички), і, насамкінець, застосований в Загальних принципах NICE підхід на основі складових дає організаціям змогу поєднати ці два контексти.

Крім того, в Загальних принципах NICE надається механізм комунікації між організаціями на рівноправному, галузевому, державному, національному або міжнародному рівні з використанням одних і тих самих складових. Завдяки цій комунікації можуть створюватись інноваційні рішення спільних проблем, зменшуватись перешкоди на шляху залучення нових організацій та фізичних осіб і підвищуватись мобільність персоналу.

1.1 Властивості, визначені в Загальних принципах NICE

Загальні принципи NICE є довідковим ресурсом для осіб, які намагаються описати роботу у сфері кібербезпеки, що виконується їхньою організацією, осіб, які виконують роботу, а також поточне навчання, яке знадобиться для ефективного виконання такої роботи. Характер роботи, а також персоналу можна описувати із використанням стандартних блоків TKS, представлених у наступних розділах. Ці стандартні блоки включають такі властивості:

- **Спритність.** Люди, процеси і технології стають зрілими і повинні адаптуватися до змін. Отже, Загальні принципи NICE дозволяють організаціям йти в ногу з екосистемою, що постійно розвивається.
- **Гнучкість.** Не зважаючи на те, що кожна організація стикається з аналогічними проблемами, для цих проблем не існує універсального рішення. Отже, Загальні принципи NICE дозволяють організаціям враховувати унікальний операційний контекст організації.
- **Сумісність.** Хоча кожне рішення загальних проблем є унікальним, ці рішення повинні узгоджувати використання відповідних термінів. Отже, Загальні принципи NICE надають організаціям змогу обмінюватися інформацією про персонал,

використовуючи спільну мову.

- **Модульність.** Хоча ризики у сфері кібербезпеки залишаються основою цього документа, існують інші ризики, які потребують управління з боку організації на рівні підприємства. Отже, Загальні принципи NICE дозволяють організаціям обмінюватися інформацією про інші типи персоналу на рівні підприємства та між організаціями або секторами (наприклад, приватність, управління ризиками, проектування/ розроблення програмного забезпечення).

1.2 Мета і застосовність

Організації здійснюють управління багатьма різними бізнес-функціями (такими як операції, фінанси, юридичне забезпечення, управління персоналом) як частиною всього підприємства. Кожна із цих бізнес-функцій має відповідні ризики. Після того, як технології стали вирішальним чинником управління підприємством, ризики, пов'язані з кібербезпекою, також стали більш відчутними. Загальні принципи NICE допомагають організації в управлінні ризиками кібербезпеки, забезпечуючи можливості для обговорення роботи й учнів, пов'язаних із діяльністю у сфері кібербезпеки. Ці ризики у сфері кібербезпеки є важливим чинником для ухвалення рішень підприємства щодо ризиків, що описано у Міжвідомчому звіті NIST 8286 «*Інтеграція управління ризиками у сфері кібербезпеки і ризиками підприємства (ERM)*». [4]

Цей документ служить потенційною настановою для інших бізнес-функцій, які розглядають питання створення загальних принципів управління персоналом. Організації можуть підвищити ефективність шляхом використання однакових стандартних блоків для різних бізнес-функцій. Отже, будь-яка організація може використовувати цей документ.

1.3 Цільова аудиторія

Тема управління персоналом у сфері кібербезпеки охоплює багато різних типів посад, а також багато різних типів організацій. До цільової аудиторії цього документа належать органи державного сектору, приватні та некомерційні організації й організації, що надають послуги з освіти та тренінгів, розробники навчальних програм, постачальники сертифікатів, фахівці у сфері управління персоналом, менеджери з найму працівників, керівники окремих напрямів діяльності, планувальники потреб у персоналі, рекрутери та всі учні.

1.4 Структура цієї публікації

Далі ця публікація має таку структуру:

- Розділ 2. Стандартні блоки Загальних принципів NICE: визначає складові TKS в Загальних принципах NICE
- Розділ 3. Використання Загальних принципів NICE: описуються загальні підходи до використання Загальних принципів NICE
- Розділ 4. Висновки
- Посилання. Перелік пов'язаних публікацій, посилання на які надаються у цьому документі
- Додаток А. Скорочення: Перелік скорочень та абревіатур, що використовуються у цьому документі

2 Складові Загальних принципів NICE

Загальні принципи управління персоналом у сфері кібербезпеки (Загальні принципи NICE) побудовані на основі набору окремих стандартних блоків, якими описується робота, що має бути виконана (у формі Завдань), а також те, що потрібно для виконання такої роботи (через Знання та Навички). Ці складові є стандартними блоками, що сприяють використанню та впровадженню Загальних принципів NICE. Вони забезпечують механізм, за допомогою якого організації та фізичні особи можуть зрозуміти сферу застосування та зміст Загальних принципів NICE. Ці стандартні блоки мають бути настановами, які можуть бути використані для кращого розуміння, а не жорсткими структурами.

2.1 Формулювання Завдань

Завдання
Діяльність, спрямована на досягнення організаційних цілей.

Формулювання Завдань
- Легко прочитати і зрозуміти
- Починаються з діяльності, яка наразі здійснюється
- Не містять цілей завдання

Як зображено на рисунку 1, формулювання Завдань описують роботу, тоді як формулювання Знань і Навичок (K&S) описують учня. Формулювання Завдань повинні зосереджуватися на мові та моделях комунікації організації, які забезпечують цінність організації. Ці формулювання призначені для опису роботи, яка повинна бути виконана, та повинні бути узгоджені з контекстом організації.

Завдання описують роботу, яку потрібно виконати. Завдання можна визначити як діяльність, спрямовану на досягнення цілей організації, включаючи бізнес-цілі, технологічні цілі або цілі місії. Формулювання Завдань мають бути простими. Незважаючи на те, що робота, яка описана в Завданні, може складатися з багатьох етапів, як це показано на прикладі нижче, саме формулювання повинно легко читатися та розумітися.

Формулювання Завдання починається з діяльності, яка має здійснюватися.

> Приклад: **Система виявлення й усунення несправностей** в апаратному та програмному забезпеченні.

Формулювання Завдання не містить цілі, оскільки ціль може мінятися залежно від стимуляторів місії і від організаційних потреб.

> Приклад. Проведення інтерактивних практичних занять.

У наведеному вище прикладі метою цих занять може бути створення ефективного середовища для навчання, проте ціль таких курсів не включається до самого формулювання Завдання.

Як показано на рисунку 1, Завдання пов'язані з формулюваннями K&S. Учень має продемонструвати знання та навички для виконання Завдання (або йому буде поставлена мета здобути знання та навички для підготовки до виконання завдання). Складність самого Завдання пояснюється пов'язаними формулюваннями K&S. У наведеному вище прикладі виявлення та усунення несправностей, задля ефективного виявлення та усунення несправностей у будь-які частині програмного або апаратного забезпечення учень повинен бути ознайомлений із пов'язаними формулюваннями Знань та розуміти їх. Те саме можна сказати про формулювання Навичок.

2.2 Формулювання Знань

Знання
Набір понять в пам'яті, які можна відновити.

Формулювання Знань
- Описуються базові або спеціальні Знання
- Для виконання Завдання можуть знадобитися декілька формулювань Знань
- Одне формулювання може бути використане для виконання багатьох різних Завдань

Формулювання Знань пов'язані з формулюваннями Завдань тим, що тільки завдяки розумінню, наданому у формулюванні Знання, учень буде здатним виконати Завдання. Знання визначаються, як набір понять в пам'яті, які можна відновити. Формулювання Знань можуть описувати базові або спеціальні поняття. Для виконання конкретного Завдання можуть знадобитися декілька формулювань Знань. Так само одне формулювання Знань може бути використане для виконання багатьох різних Завдань.

Формулювання Знань можуть бути базовими.

> Приклад. Знання загроз і вразливостей у кіберпросторі

Формулювання Знань можуть бути спеціальними.

> Приклад. Знання про вразливості джерел розповсюдження інформації (наприклад, попередження від постачальників, інформаційні повідомлення від уряду, помилки у товаросупровідній літературі та галузеві вісники).

Організації, що розробляють формулювання Знань, повинні враховувати різні рівні знань і експертизи учнів. Приклад таких різних рівнів описано у «Таксономії Блума» [Bloom's Taxonomy] (нова редакція), де використовується мова, що забезпечує спостережливість та оцінку учня [5]

2.3 Формулювання Навичок

Навичка
Здатність виконувати спостережувану діяльність.

Формулювання Навичок
- Описуються прості чи складні навички
- Для виконання Завдання можуть знадобитися декілька формулювань Навичок
- Одне формулювання Навички може застосовуватися для виконання більш ніж одного Завдання.

Формулювання Навичок пов'язані з формулюваннями Завдань тим, що учень під час виконання завдань демонструє певні навички. Учень, який не може продемонструвати описану навичку, не зможе виконати Завдання, яке потребує цю навичку. Навичка визначається як здатність виконувати спостережувану діяльність. Формулювання Навичок можуть описувати прості або складні навички. Декілька формулювань Навичок можуть знадобитися для виконання конкретного Завдання. Так само виконання Навички може застосовуватися для виконання більш ніж одного Завдання.

Формулювання Навичок можуть бути простими.

> Приклад. Навичка розпізнавання попереджень Системи виявлення вторгнень

Формулювання Навичок можуть бути складними.

> Приклад. Навичка формування гіпотези, як саме особа, що створила загрозу, змогла обійти Систему виявлення вторгнень.

Як зображено на рисунку 1, формулювання Навичок описують, що може зробити учень, а формулювання Завдань описують роботу, яку потрібно виконати. Тому важливо розділити мову, що використовується, між формулюванням Навичок та формулюванням Завдань, і використовувати терміни, які забезпечують спостережливість та оцінку учня.

3 Використання Загальних принципів NICE

Варто зазначити, що хоча Загальні принципи управління персоналом у сфері кібербезпеки (Загальні принципи NICE) мають на меті надання користувачам загального набору складових, на основі яких можна багато чого створити, у деяких організацій може виникнути потреба розробити модель, яка тісніше пов'язана з унікальним контекстом цих організацій. Наприклад, виробниче підприємство може мати Завдання, характерні для відповідної галузі або організації, та які не описані в Загальних принципах NICE. Інші можуть вважати, що Завдання є застосовними, але їх треба відкоригувати або розробити окремі формулювання K&S з метою збільшити вірогідність виконання Завдань з огляду на їхній унікальний контекст. Самі собою складові не повинні розглядатись як незмінні; натомість, метою їхнього створення було надання організаціям або галузям спільної мови для використання у найбільш прийнятний спосіб у відповідному контексті.

Насамкінець, приклади використання складових Загальних принципів NICE, що наведені нижче, є теоретичними або концептуальними за своїм характером; організація може використовувати складові будь-якими способами, що якнайкраще відповідають потребам організації. Ці приклади мають на меті продемонструвати можливі практичні підходи до Загальних принципів NICE, які продемонстрували, що вони допомогають у досягненні загальних організаційних цілей. Вони дають організаціям або секторам, що шукають, де почати, настанови, а не єдиний спосіб використання Загальних принципів NICE.

3.1 Використання наявних формулювань Завдань, Знань і Навичок (TKS)

Користувачі Загальних принципів NICE посилаються на одне або декілька формулювань Завдань, Знань і Навичок (формулювань TKS), описаних у Розділі 2, для характеристики як роботи, так і учнів. Формулювання Завдань використовуються для опису роботи. Формулювання Завдань мають бути пов'язані з формулюваннями Знань і Навичок. Попри те, що формулювання Завдання може мати рекомендований набір пов'язаних формулювань Знань і Навичок, користувачі можуть включати інші наявні формулювання Знань і Навичок для приведення Завдань у відповідність до їхнього унікального контексту. Формулювання Знань і Навичок використовуються для опису учнів. Формулювання Знань і Навичок можуть бути використані багатьма способами з метою управління персоналом у сфері кібербезпеки. Вони можуть використовуватися частково, усі разом або взагалі не використовуватися залежно від потреб унікального контексту запроваджуючої організації. Наведені нижче теоретичні приклади використання показують сфери, в яких формулювання TKS можуть бути запроваджені:

- Програма відстеження Навички працівника з метою визначення кваліфікації для просування по службі
- Знання, потрібні для закінчення курсу
- Щотижневий перелік Завдань для завершення в організації

Формулювання та приклади TKS можна знайти у Ресурсному центрі Загальних принципів NICE. Ці формулювання, за потреби, оновлюватимуться для того, щоб іти в ногу зі змінами, які виникають внаслідок появи нових бізнес-місій, ризиків або новітніх технологій. [1]

3.2 Створення нових формулюваньTKS

Користувачів попереджують не змінювати текст у наявних формулюваннях TKS Загальних принципів NICE. Метою цих формулювань є підтримання сумісності, тож зміни їхнього змісту можуть призвести до подальших розбіжностей під час використання зовнішніх джерел. У випадку виникнення потреби змінити текст формулюваання TKS для підтримки унікального контексту користувача, можна створити нове формулювання.

Користувачі можуть також створювати повністю нові формулювання Завдань, Знань або

Навичок, щоб допомогти адаптувати використання Загальних принципів NICE до локальних потреб із їхнім унікальним контекстом. Такі додаткові формулювання допоможуть підтримувати чіткі та послідовні внутрішні обговорення щодо учнів та їхньої робочої діяльності.

3.3 Компетенції

Компетенції надають організаціям механізм оцінювання учнів. Компетенції визначаються з використанням підходу на основі інтересів роботодавця, що забезпечує врахування унікального контексту організації. Крім того, Компетенції допомагають організаціям, що надають послуги з освіти та підготовки, реагувати на потреби роботодавця або галузі шляхом розроблення навчальних програм, які допомагають учням розвивати і демонструвати Компетенції. Компетенції складаються з назви, опису Компетенції, методу оцінювання, а також із групи пов'язаних формулювань TKS.

Компетенція
Механізм оцінки учнів організаціями.

Компетенції:
- Визначаються з використанням підходу на основі інтересів роботодавця
- Орієнтовані на учня
- Спостережувані та вимірювані

Компетенції пропонують гнучкість, дозволяючи організаціям об’єднувати різні формулювання TKS у всеосяжні K&S. Хоча індивідуальне Завдання і пов‘язані з ним формулювання Знань і Навичок можуть не змінюватись, більш широко визначена Компетенція може ввести нові (чи видалити існуючі) Завдання або навіть індивідуальні Знання і Навички у відповідь на потреби, які змінюються у мінливій екосистемі кібербезпеки.

Існують різноманітні шляхи використання Компетенцій. Наприклад, як зображено на рисунку 2, організація може використовувати Компетенції в рамках процесу найму працівників, спрямованого на досягнення певних цілей організації. У цьому випадку Компетенції можна визначити і як групу пов'язаних формулювань Завдань. Потім організація може використовувати ці Компетенції для оцінювання того, чи може кандидат виконувати ці Завдання. Таке оцінювання може відбуватись у формі співбесіди, тестування кандидатів на посаду перед працевлаштуванням або спостереження процесу навчання на робочому місці.

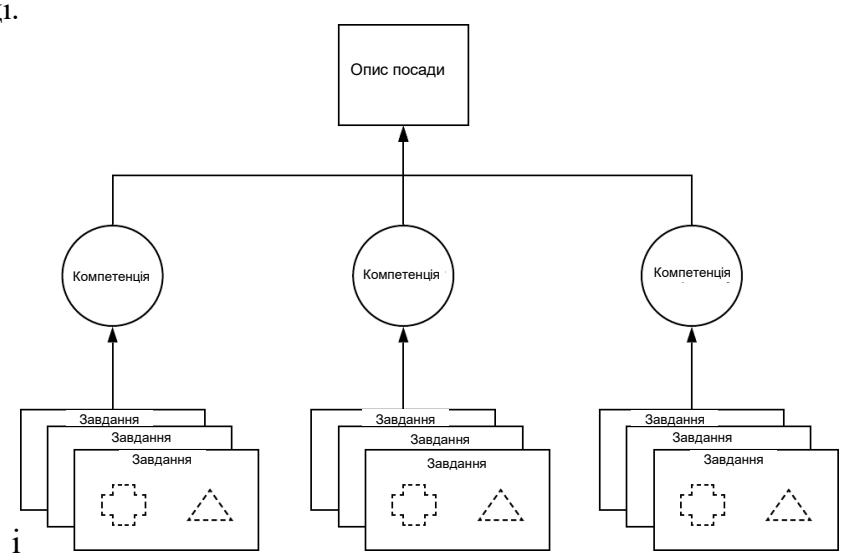

Рисунок 2. Використання Компетенцій для оцінювання учнів шляхом опису посади

Інші організації можуть використовувати Компетенції для визначення того, чи учень досягнув визначений набір Навичок і Знань. Ці організації можуть, як зображено на рисунку 3, обрати варіант використання Компетенцій як групи формулювань K&S. Ці організації можуть потім оцінювати учнів за цими формулюваннями K&S. Оцінювання може проводитись у формі тестів, лабораторних демонстрацій або усних оцінювань.

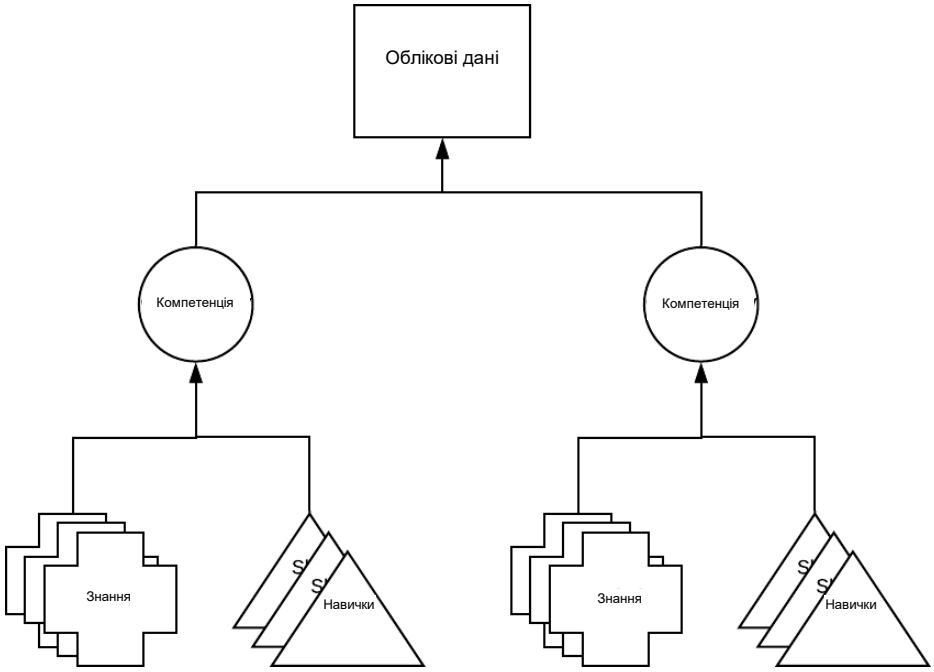

Рисунок 3. Використання Компетенцій для оцінювання учнів за допомогою облікових даних

Наведені вище приклади є умовними. Вони можуть використовуватися частково, усі разом або взагалі не використовуватися, залежно від унікального контексту організації, що впроваджує цей підхід.

3.3.1 Використання наявних Компетенцій

Компетенції Загальних принципів NICE є для організацій шляхом узгодження із Загальними принципами NICE на високому рівні, не вдаючись у деталі формулювань TKS. Компетенції є спосіб опису процесу оцінювання учня. Підтримуючи групи формулювань TKS, визначених організацією, Компетенції допомагають організаціям лаконічно спілкуватися та ефективно організовувати свою роботу у сфері кібербезпеки, щоб забезпечити прискорений погляд на персонал. Інші потенційні можливості використання Компетенцій включають

- Опис типів Завдань у рамках певної посади
- Відстеження здібностей персоналу
- Опис вимог команди
- Демонстрування здібностей учня

Хоча Компетенція має рекомендований набір пов'язаних формулювань TKS, користувачі можуть додавати або виключати існуючі формулювання, щоб адаптувати Компетенції до свого унікального контексту. Проте користувачів попереджують не змінювати назву або опис наявної Компетенції Загальних принципів NICE. Компетенції призначені для підтримки сумісності. тож зміни їхнього змісту можуть призвести до подальших розбіжностей під час використання зовнішніх джерел. У випадку потреби змінити текст Компетенції для підтримки унікального контексту користувача можна створити нову Компетенцію, як описано нижче (див. Розділ 3.3.2).

3.3.2 Створення нових Компетенцій

Деяким організаціям може знадобитися описати Компетенцію для конкретного контексту своєї роботи у сфері кібербезпеки. Загальні принципи NICE, які розроблені з урахуванням принципу спритності, дозволяють організаціям описувати Компетенцію для забезпечення відповідності мінливій екосистемі кібербезпеки. Це може бути зроблено шляхом зміни існуючої Компетенції для задоволення локальних потреб або шляхом створення абсолютно нової Компетенції.

Нижче наводяться два умовних приклади для пояснення можливих процесів використання Компетенцій. Ці два приклади зосереджені на аналізі даних для того, щоб показати, що однакові Компетенції можуть бути використані за допомогою різних підходів. Крім того, використання цих прикладів показано на рисунку 2 та рисунку 3 для того, щоб надихнути читача на потенційне впровадження. У прикладах використовується таблична структура відображення Компетенції. Такий табличний підхід є одним із багатьох підходів, які можуть використовуватись організацією, яка прагне запровадження Компетенцій.

Приклад аналізу даних 1

Таблиця 1 нижче за текстом є інформативною та містить відправну точку для формування Компетенції. Компетенція у Прикладі аналізу даних 1 має назву та опис, що дозволяє організації швидко визначити Компетенцію як таку, що має цінність для їхньої організаційної структури та контексту. Використовуючи метод оцінки «лабораторна демонстрація», організація оцінює учня шляхом створення змодельованого робочого середовища для виконання Завдань, що відповідає її бізнес-цілям. (Зверніть увагу на те, що у Таблиці 1 використовуються Завдання з Загальних принципів NICE версії 2017 року. [2])

Таблиця 1. Приклад створення нової Компетенції аналізу даних з наявними Завданнями Загальних принципів NICE 2017 року

Назва Компетенції: Приклад аналізу даних 1
Опис Компетенції: Збирання, створення або аналіз якісної і кількісної інформації і даних із різних джерел з метою прийняття рішення, надання рекомендації та/або складання звітів, інструктажів, резюме та іншої кореспонденції.
Метод оцінювання: Лабораторна демонстрація
Формулювання Завдань
T0007 | Аналіз та визначення вимог до даних і характеристик даних.
T0405 | Використання мови з відкритим кодом, такої, як R, і застосування кількісних методик (наприклад, описова і дедуктивна статистика, вибірка, експериментальні плани, параметричні та непараметричні тести різниці, звичайні регресії найменших квадратів, довільна пряма).

У прикладі, описаному в Таблиці 1, організація може надати учневі комп'ютер, у який завантажено певний набір даних і який підключений до лабораторної мережі. Після цього учневі надається певний час для демонстрації своєї здатності використовувати мови з відкритим кодом для застосування кількісних методик оброблення даних. Ключовою частиною цього оцінювання може бути аналіз набору даних для того, щоб переконатися, що ці дані відповідають певним специфікаціям даних перед завершенням аналізу. В рамках цього оцінювання учень демонструє Компетенцію «Приклад аналізу даних 1», як визначено роботодавцем.

Повна деталізована Компетенція аналізу даних може бути набагато ширшою. За допомогою нумерації формулювань Завдань у рамках Компетенції організація може визначити бажану сферу застосування Компетенції. Для простоти використання посилання на Завдання вказані в їхніх ідентифікаторах (ID) Завдань відповідно в Загальних принципах NICE від 2017 року.

Приклад аналізу даних 2

У Таблиці 2 нижче за текстом показані інша відправна точка для створення Компетенції. Приклад є інформативним; опис є таким самим, як і в Таблиці 1, однак у цьому прикладі використовуються формулювання Знань і Навичок для формування Компетенції.

Таблиця 2. Приклад створення нової Компетенції аналізу даних із додатковими Завданнями

Назва Компетенції: Приклад аналізу даних 2
Опис Компетенції: Збір, синтез або аналіз якісної і кількісної інформації і даних із різних джерел із метою прийняття рішення, надання рекомендації та/або підготування звітів, доповідей, резюме та іншої кореспонденції.
Метод оцінювання: Тестування
Формулювання K&S
S0013 | Навички подання запитів та розроблення алгоритмів із метою аналізування структур даних.
S0021 | Навички проектування структури аналізу даних (тобто типів даних, які мають бути створені під час тесту, і порядку аналізу таких даних).
S0091 | Навички аналізування мінливих даних.
K0020 |Знання політик адміністрування та стандартизації даних.
K0338 |Знання методик глибинного аналізу даних.

У цьому прикладі Таблиця 2 показує Компетенцію аналізу даних. Ця Компетенція може бути створена органом сертифікації, який надає тест для оцінювання учнів. Тест може проводитися у паперовому форматі або в комп’ютерному форматі. Проходячи тест, учень демонструє Компетенцію «Приклад аналізу даних 2», як визначено органом сертифікації.

(Зауважте, що у таблиці 2 використовуються формулювання K&S Загальних принципів NICE версії 2017 року. [2])

3.4 Робочі ролі

Робочі ролі широко використовуються в Загальних принципах NICE. Робочі ролі є способом опису групи робіт, за яку хтось відповідає або є підзвітним.

Хоча попередні версії загальних принципів управління персоналом також пов'язували Робочі ролі з параметрами Знань, Навичок та Здібності, Загальні принципи NICE заохочують більш динамічний підхід через Завдання. Робочі ролі складаються із Завдань, які визначають роботу, що має бути виконана; Завдання включають пов'язані формулювання Знань і Навичок, які відображають здатність учнів виконувати такі Завдання. Такий перехідний підхід, зображений на рисунку 3, підвищує гнучкість і спрощує комунікацію.

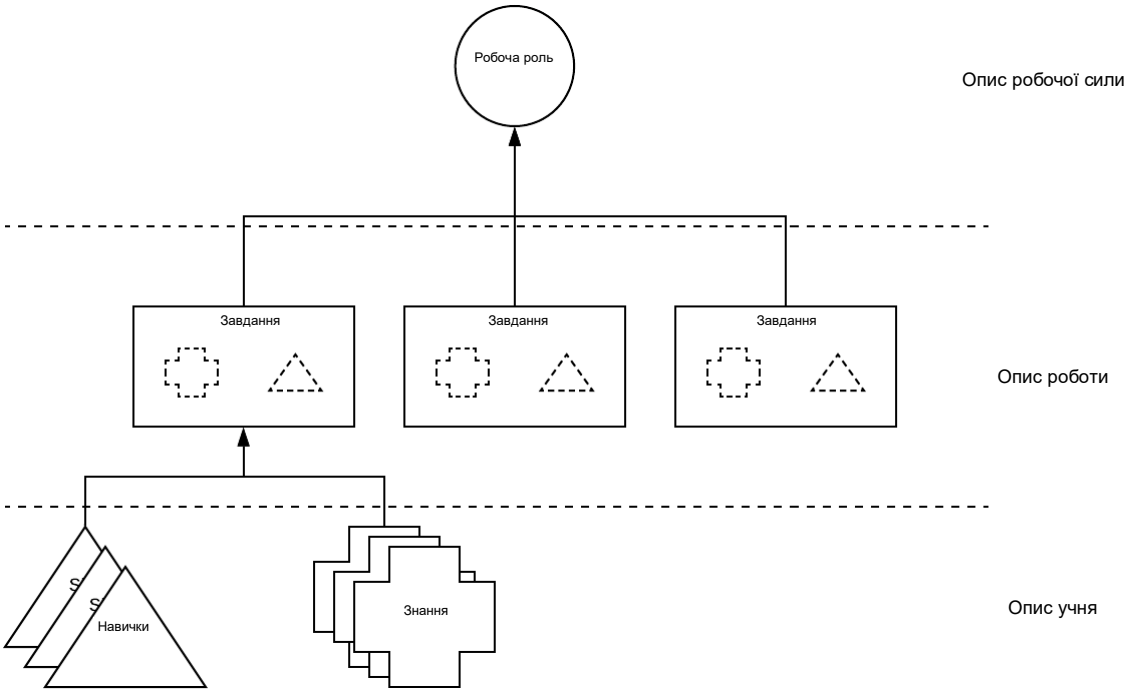

Рисунок 4. Зв'язок Робочих ролей зі стандартними блоками

Назви Робочих ролей не співпадають із назвами посад. Деякі Робочі ролі можуть співпадати з назвою посад залежно від використання назв посад в організації. Крім того, Робочі ролі не співпадають із назвами професій.

Одна Робоча роль (наприклад, Розробник Програмного Забезпечення) може застосовуватися до працівників з багатьма різними назвами посад (наприклад, програміст, кодувальник, розробник прикладного програмного забезпечення). І навпаки, багато ролей можуть бути об'єднані для створення певної посади. Такий адитивний підхід підтримує кращу модульність й відображає той факт, що всі учні у складі колективу виконують численні завдання в різних ролях, незалежно від назви посади. Аналогічно, в Загальних принципах NICE не визначаються рівні професійної підготовки (наприклад, Базовий, Середній, Вищий). Такі параметри, а також визначення рівня професійної підготовки учня, який виконує Завдання, залишилися іншим моделям або ресурсам.

3.4.1 Використання існуючих Робочих ролей

Кожна Робоча роль призначена для досягнення цілей через виконання Завдань. Хоча Робоча роль може мати попередньо визначений набір пов'язаних Завдань, користувачі можуть включати інші існуючі Завдання для адаптації Робочих ролей до свого унікального контексту. Аналогічно, користувач може мати бажання залучити одну із перерахованих Робочих ролей або включати додаткові Робочі ролі для підтримки додаткових цілей. Поточний набір компонентів Загальних принципів NICE можна знайти в Ресурсному центрі Загальних принципів NICE. [1]

Користувачів застерігають проти внутрішньої модифікації назви та опису існуючих Робочих ролей. Робочі ролі призначені для підтримки сумісності, і тому зміни у їхньому змісті можуть призвести до подальших розбіжностей. Якщо виникає потреба змінити текст, можна створити нову Робочу роль, як описано нижче.

3.4.2 Створення нової Робочої ролі

Користувачі можуть також створювати нові Робочі ролі, щоб допомогти використанню Загальних принципів NICE для їхнього унікального контексту. Такі додаткові Робочі ролі сприятимуть зрозумілим та послідовним обговоренням роботи у сфері кібербезпеки всередині організації.

3.5 Команди

Багато організацій використовують команди для колективного вирішення складних проблем, об'єднуючи людей із доповнюючими навичками та досвідом. Використовуючи різні ресурси і погляди, команди допомагають організаціям комплексно управляти ризиками. Команди використовують переваги спеціалізації знань та процесів кожного члена команди для ефективного розподілу роботи. Команди можуть бути визначені на основі Робочих ролей або Компетенцій.

3.5.1 Створення команд з Робочими ролями

Підхід до створення команд, орієнтований на Робочі ролі, допомагає організаціям визначати, які типи Робочих ролей потрібні для досягнення поставлених цілей. Оскільки самі Робочі ролі складаються із Компетенцій, цей підхід до створення команд починається з роботи, яка має бути виконана. Такий підхід може вважатися підходом «згори донизу».

Таблиця 3. Приклад Команди з розробки безпечного програмного забезпечення на основі Робочих ролей відповідно до Загальних принципів NICE 2017 року

Етап життєвого циклу	Робоча роль
Розроблення	SP-ARC-002 | Розробник архітектури системи безпеки
Побудова	SP-DEV-001 | Розробник програмного забезпечення
Розгортання	OM-NET-001 | Фахівець із мережевих операцій
Експлуатація	OM-STS-001 | Фахівець з технічної підтримки
Технічне обслуговування	OM-DTA-001 | Адміністратор баз даних
Виведення з експлуатації	OV-LGA-001 | Юридичний радник із кібернетичних питань

У Таблиці 3 вище показаний спосіб створення Команди із розроблення безпечного програмного забезпечення. Робочі ролі посилаються на ідентифікатори робочих ролей, наведених в Загальних принципах NICE версії 2017 року. Команди, створені в такий спосіб, починають із визначення роботи, яка має бути виконана. У цьому прикладі команда із розроблення безпечного програмного забезпечення організована за етапами життєвого циклу. У першому рядку показано, що команда розглядатиме цілі етапу Розроблення, включаючи планування, і, отже, буде потрібен Розробник архітектури системи безпеки. Таблиця 3 є інформативним прикладом і не охоплює всі Робочі ролі, які можуть бути присутніми або потрібні для цієї команди. Для отримання додаткової інформації див. *Інструкцію з розроблення надійного програмного забезпечення NIST.* [6]

Таблиця 4. Приклад створення команди із питань кібербезпеки, що використовує Робочі ролі відповідно до Загальних принципів NICE версії 2017 року та нові Робочі ролі

Функція відповідно до Загальних принципів кібербезпеки	**Робоча роль**
Ідентифікація	Нова Робоча роль 1 | Менеджер із ризиків
Захист	SP-RSK-002 | Оцінювач контролю безпеки
Виявлення	PR-CDA-001 | Аналітик із питань кіберзахисту
Реагування	PR-CIR-001| Відповідальний за усунення інцидентів кіберзахисту
Відновлення	Нова Робоча роль 2 | Спеціаліст із питань комунікацій

Таблиця 4 описує приклад Команди із кібербезпеки. Як і у випадку із командою з розроблення безпечного програмного забезпечення, команду у прикладі створено з використанням підходу, орієнтованого на роботу. Використовуючи Ядро *Загальних принципів удосконалення кібербезпеки критичної інфраструктури (Загальні принципи кібербезпеки),* обираються цілі у сфері кібербезпеки, визначаються Завдання, спрямовані на досягнення цих цілей, і обираються Робочі ролі, щоб визначити ролі, які будуть потрібні для досягнення цих цілей. [7] Таблиця 4 є інформативним прикладом і не охоплює усі Робочі ролі, які можуть бути присутніми або потрібними для цієї команди. Дві нові Робочі ролі додані для демонстрування змішаного підходу до використання існуючих Робочих ролей (п. 3.4.1) та створення нових Робочих ролей (п. 3.4.2). За допомогою створення нових Робочих ролей цей приклад демонструє гнучкий і динамічний підхід до використання Загальних принципів NICE.

3.5.2 Створення команд з Компетенціями

Команди також можуть формуватися на основі Компетенцій. Цей підхід створення команди визнає, що окремі Завдання можуть бути невідомими, проте відомі типи Компетенцій, потрібні для вирішення проблеми. Цей підхід можна назвати «знизу догори». Отже, команда, яка створена у такий спосіб, може допомогти визначати учнів, які можуть взяти участь у роботі Команди у майбутньому. Такі учні можуть або не можуть бути пов'язані з певною Робочої роллю, а просто можуть мати Компетенції, потрібні для сприяння досягненню організаційних цілей.

Наприклад команда захисної кібербезпеки, що використовує свої Навички для імітування методів атаки супротивника (тобто «Червона команда»), може складатися з таких умовних Компетенцій:

- Планування операції
- Правила проведення операції
- Тест на проникнення
- Збір даних
- Використання вразливостей

Створюючи команди або інші TKS групи, кожна організація може використовувати Загальні принципи NICE таким чином, щоб якнайкраще відповідати використанню та розповсюдженню даних про учнів (і про роботу, яку учні виконуватимуть) з метою досягнення цілей організації.

4 Висновки

Завдяки застосуванню підходу з використанням стандартних блоків, описаного в Загальних принципах NICE, користувачі можуть скористатися послідовним методом організації та обговорення роботи, що має бути виконана, на основі формулювань Завдань, а також спираючись на Знання і Навички окремих учнів, які виконують цю роботу. Загальні принципи NICE допомагають спрямувати зусилля роботодавців на опис роботи у сфері кібербезпеки, а організаціям, що надають послуги з освіти та тестування для підготовки працівників у сфері кібербезпеки, та учням виявити свої здібності під час виконання роботи у сфері кібербезпеки.

Здатність описувати Завдання, Знання і Навички є важливою для забезпечення комплексного розуміння роботи і персоналу. Загальні принципи NICE забезпечують розширений довідковий ресурс, який може застосовуватись і використовуватись різними організаціями або галузями для опису роботи, яка має виконуватись у багатьох сферах. Переваги для цих організацій підтримують місію NICE - активізувати, просувати та координування потужну спільноту, яка спільно працює над розвитком інтегрованої екосистеми освіти, тренінгів та розвитку персоналу у сфері кібербезпеки.

Посилання

[1] National Initiative for Cybersecurity Education (2020) *NICE Framework Resource Center*. Доступно за адресою: https://www.nist.gov/nice/framework

[2] Newhouse WD, Witte GA, Scribner B, Keith S (2017) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181. https://doi.org/10.6028/NIST.SP.800-181

[3] National Institute of Standards and Technology (2020) *National Online Informative References Program*. Доступно за адресою: https://csrc.nist.gov/projects/olir

[4] Stine K, Quinn S, Witte G, Gardner RK (2020) Integrating Cybersecurity and Enterprise Risk Management (ERM). (National Institute of Standards and Technology,Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8286. https://doi.org/10.6028/NIST.IR.8286

[5] Krathwohl, D. R. (2002). A revision of Bloom's taxonomy: An overview. *Theory Into Practice*, 41(4), 212-218. Доступно за адресою: https://www.depauw.edu/files/resources/krathwohl.pdf

[6] Dodson DF, Souppaya MP, Scarfone KA (2020) Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF).(National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper. https://doi.org/10.6028/NIST.CSWP.04232020

[7] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD).https://doi.org/10.6028/NIST.CSWP.04162018

Додаток A Скорочення

Окремі скорочення та абревіатури, що були використані, визначені нижче.

ERM	Управління ризиком підприємства
FISMA	Федеральний закон США про вдосконалення управління інформаційною безпекою
FOIA	Закон про свободу інформації
ITL	Лабораторія інформаційних технологій NIST
K&S	Формулювання Знань і Навичок
NICE	Національна ініціатива з поширення знань у сфері кібербезпеки
NIST	Національний інститут стандартів і технологій США
OLIR	Довідкові матеріали онлайн
OMB	Відділ із питань управління та бюджету
SSDF	Загальні принципи розроблення безпечного програмного забезпечення
TKS	Формулювання Завдань, Знань і Навичок

Додаток Б Глосарій

Для ознайомлення з повними глосарієм, будь ласка, відвідайте https://csrc.nist.gov/glossary.

Компетенція Механізм для оцінки учнів організаціями.

Знання Набір понять в пам'яті, які можна відновити.

Навичка Здатність виконувати практичні задачі.

Завдання Діяльність, спрямована на досягнення цілей організації.