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

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

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

Листопад 2020 р.

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

Повноваження

Цю публікацію було створено NIST в рамках його статутних обов'язків, передбачених Федеральним законом США про вдосконалення управління інформаційною безпекою (FISMA) від 2014 року, розділ 44 Кодексу законів США §3551 та наступних, Публічний закон (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 отримання окремого погодження від компетентних посадових осіб федеральних органів, які керують роботою 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’язуючими федеральні органи відповідно до вповноваженого рішення Міністра торгівлі. Крім того, ця настанова не повинна тлумачитися як така, що відміняє або замінює чинні повноваження Міністра торгівлі, директора OMB або іншої посадової особи федерального органу. Ця публікація може використовуватися недержавними організаціями на добровільній основі, і вона не є суб’єктом авторського права на території Сполучених Штатів Америки. Проте, NIST буде вдячний за посилання.

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

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

У цьому документі можуть бути визначені певні комерційні підприємства, обладнання або матеріали з метою належного опису експериментальної процедури або концепції. Таке визначення не має на меті рекомендування або погодження з боку NIST, і не означає що такі підприємства, матеріали або обладнання найкраще придатні для відповідної цілі.

У цій публікації можуть міститися посилання на інші публікації, які наразі розробляються NIST відповідно до покладених на нього статутних обов'язків. Інформація, що міститься в цій публікації, включаючи концепції та методики, може використовуватися федеральними органами навіть до завершення таких супутніх публікацій. Отже, до завершення кожної публікації залишаються чинними всі поточні вимоги, настанови та процедури, якщо вони існують. З метою належного планування та забезпечення переходу федеральні органи можуть виявити бажання ретельно відслідковувати процес розроблення таких нових публікацій NIST.

Протягом строків прийняття зауважень та пропозицій від громадськості організаціям рекомендується переглядати всі проекти публікації та надавати свої відгуки до NIST. Багато публікацій NIST у сфері кібербезпеки, окрім зазначених вище, можна зайти за адресою .https://csrc.nist.gov/publications

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

Доступ до всіх зауважень надається відповідно до Закону про свободу інформації (FOIA).

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

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 як Завдання та описує Знання та Навички, які створюють основу для тих, хто навчається, включаючи студентів, осіб, які шукають роботу, і працівників. Використання цих складових допоможе студентам розвивати навички, особам, які шукають роботу, виявляти 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; команда; тренінг; персонал; робоча роль.

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

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 такі заявки на патенти ITL. 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 наступні запити 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 надає та не передбачає жодної гарантії того, що для уникнення порушення патентних прав під час використання цієї публікації не потрібні будуть 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) інша 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.

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

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 про надання зауважень щодо Загальних принципів ї NICE та проекту цієї публікації, викладеного для відкритого обговорення.

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

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

Примітка для читачів

До Вашої уваги пропонуються Загальні принципи управління персоналом сфері кібербезпеки (Загальні принципи NICE), Редакція 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 Редакції 1 спрощені шляхом виключення Категорій (наприклад, забезпечення безпеки, нагляд і корпоративне управління, захист і оборона, аналіз тощо) та Сфер спеціалізації (наприклад, управління інцидентами, аналіз загроз, управління кібербезпекою тощо). З метою спрощення підходу, що передбачає динамічність, гнучкість і сумісність із іншими системами, а також модульність для організацій, у Версії 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 трудові колективи на основі цих концепцій, а також приводити їх у відповідність із цією версією Загальних принципів NICE (див. розділ 3.4).
- У Редакції 1 описано декілька способів використання складових Завдання, Знання і Навички, включаючи методики використання цих складових 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 складовими Завдання, Знання, Навички та Здібності змінилися. Складові Навички та Здібності із попередньої версії було перетворено для простоти у складову Навички, які сфокусовані на діях учня. У цій версії описані методи пов'язування складових Знання та Навички із складовою Завдання для вирішення різних питань. Перелік складових Завдання, Знання, Навички та Робочі ролі, 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. Складові Завданння, Знання і Навички (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 розповсюдженням даних про них. 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 складових кінцевим визначенням складових TKS, що наведені у цьому документі.

- Для читачів, які зацікавлені в порівнянні стандартів, довідників або ресурсів для Загальних принципів NICE, NICE працює над Програмою створення довідкових матеріалів онлайн (OLIR) із метою розроблення шаблонів для такого порівняння. Програма OLIR під управлінням NIST забезпечує процес приведення використаних джерел інформації у відповідність до документів NIST. Крім того, в рамках програми надається каталог таких використаних джерел інформації. [3]

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

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 включають багато новітніх типів операційної діяльності й обладнання, стають дедалі складнішими та взаємопов'язаними між собою, може бути складно чітко описати роботу, яка виконується або яку ми бажаємо виконати, зокрема 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 їх зусиль для підкреслення та вирішення наслідків залучення кібербезпеки в багатьох сферах. Ця категорія людей у зазначеному документі позначається або як учні, або як персонал у сфері кібербезпеки, хоча останній термін не означає, що робочі ролі та обов'язки, які передбачені Загальними принципами NICE, поширюються лише на осіб, які займаються виключно питаннями кібербезпеки. Завдання, які виконуються учнями, також позначаються у цьому документі як «робота з кібербезпеки», а Загальними принципами передбачені засоби для точного описання такої роботи з метою надання підтримки у навчанні або підготовці учням, а також із метою забезпечення пошуку, найму, розвитку або 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 власних Знань і Навичок. Цей розвиток, в свою чергу, створює додаткові переваги для роботодавців та працівників для визначення кар’єрних шляхів, які документують, як саме готуватися до виконання роботи у сфері кібербезпеки,, використовуючи дані складових 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 властивості осіб, акредитованих 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.

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

ЗМІСТ

Ця публікація можна завантажити безкоштовно, за адресою: https://doi.org/10.6028/NIST.SP.800-181r1

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 ускладняється 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 складових. Завдяки використанню концептуальних складових Загальні принципи NICE забезпечує організації можливістю 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 свого 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 Схемі 1 нижче представлено високорівневий огляд Загальних принципів NICE. Основними складовими Загальних принципів ї NICE є Завдання, Знання і Навички (TKS) (пояснені у Розділі 2), які надані разом з концепціями, які вони описують. На Схемі 1 зображено два основних типи 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.

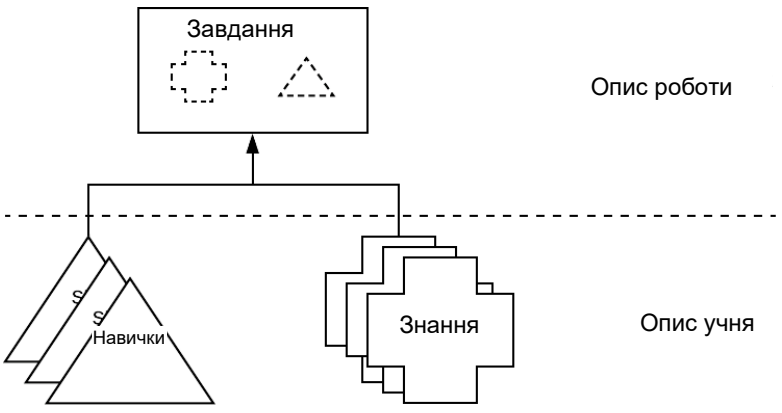

Схема 1 – Підхід із використанням складових відповідно до Загальних принципів NICE.

«Робота» – це те, чого потребує організація для досягнення цілей у сфері управління ризиками кібербезпеки. Кожна організація виконує як загальні завдання, так і 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

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

інструмент для описання своєї роботи за допомогою складових Завдань, що групуються для створення складових 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 план кар'єрного росту.

Загальні принципи NICE надають організаціям можливість описувати учнів, пов'язуючи складові Знання і Навички із окремою особою або групою осіб. Використовуючи свої Знання та Навички, учні можуть виконувати Завдання для досягнення цілей організації. Оскільки не всі організації використовують кожну концепцію, пов'язану з учнями, в Загальних принципах NICE організаціям надається гнучкий набір складових для використання 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 описи 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 контекст організаційної 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 рівнях 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 складових TKS, представлених у наступних розділах. Ці складові 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** – незважаючи на те, що кожна організація стикається з аналогічними проблемами, для всіх цих проблем не існує універсального рішення. Тому 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.

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

- **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 галузями (наприклад, приватність, управління ризиками, прикладне програмне забезпечення / розроблення).

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, забезпечуючи інтеграцію кібербезпеки та управління 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 складових 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 неприбуткові організації й організацій, 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, складові 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
- Список літератури: перелік пов'язаних публікацій, посилання на які надаються у цьому документі
- Додаток А, Скорочення: Перелік скорочень та абревіатур, що використовуються у цьому документі

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

Складові Загальних принципів NICE

Загальні принципи управління персоналом у сфері кібербезпеки (Загальні принципи NICE) побудовані на основі набору окремих складових, якими описується робота, що має бути виконана (складова Завдання), а також те, що потрібно для виконання такої роботи (складові Знання та Навички). Ці складові є структурними компонентами, 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 складові мають бути настановами, які можуть бути використані для кращого розуміння, а не жорсткими структурами.

2.1 Складова Завдання

Завдання
Діяльність, спрямована на досягнення організаційних цілей.

Складова Завдання
- Простота сприйняття і розуміння
- Починаються з діяльності, яка наразі здійснюється
- Не містять цілей виконання Завдань

Як зображено на Схемі 1, складові Завдання описують роботу, тоді як складові Знання і Навички (K&S) описують учня. Складові Завдання повинні зосереджуватися на мові організації та моделях комунікації, які забезпечують цінність організації. Ці складові призначені для опису роботи, яка повинна бути виконана (у формі завдань) 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 місію. Описи Завдань мають бути простими. Незважаючи на те, що робота, яка описана в Завданні, може складатися з багатьох етапів, як це показано на прикладі нижче, сам опис повинен легко читатися та розумітися.

Складова Завдання починається з діяльності, яка має здійснюватися.

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

Складові Завдання не містять цілі, оскільки ціль може відрізнятися залежно від складових відповідного проекту і від організаційних потреб.

> Приклад: проведення інтерактивних підготовчих курсів.

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

Як показано на Схемі 1 , Завдання пов'язані з описом складових Знання і Навички. 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 складовими Знання і Навички (K&S). У прикладі з виявлення та усунення несправностей вище задля ефективного виявлення та усунення несправностей у будь-які частині програмного або апаратного забезпечення учень повинен бути ознайомлений із пов'язаними складовими Знання та

розуміти їх. Те саме можна сказати про описи складової Навички.

2.2 Складова Знання

Складові Знання пов'язані з складовими Завдання тільки тим, що завдяки розумінню, наданому у опису складової Знання, учень буде здатним виконати Завдання. Знання визначаються, як набір понять, які можна відновити з пам'яті. Складова Знання може описувати як базові, так і спеціальні поняття. Для виконання конкретного завдання можуть знадобитися декілька описів складових Знання. Так само один опис складової Знання може бути використаний для виконання багатьох різних Завдань.

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

Складова Знання
- Описуються базові або спеціальні Знання
- Для виконання Завдання можуть знадобитися декілька складових Знання
- Один і той самий опис може бути використаний для виконання багатьох різних Завдань

Опис складової Знання може бути базовим.

> Приклад: Знання загроз і вразливостей у кіберпросторі

Опис складової Знання може бути спеціальним

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

Організації, що розробляють описи складових Знання, повинні враховувати різні рівні Знань і експертизи учнів. Приклад таких різних рівнів описано у Таксономії Блума (нова редакція), де використовується мова, що забезпечує спостережливість та оцінку учня [5]

2.3 Складова Навички

Складові Навички пов'язані з складовими Завдання тим, що учень під час виконання Завдань демонструє певні Навички. Учень, який не може продемонструвати описані Навички, не зможе виконати Завдання, яке потребує відповідних Навичок. Навичка визначається, як здатність виконувати практичні завдання. Опис складової Навички можуть містити прості або складні навички. Декілька складових Навички можуть знадобитися для виконання конкретного Завдання. Так само складова Навички може застосовуватися для виконання більш ніж одного Завдання.

Навичка
Здатність виконувати практичні завдання.

Складова Навички
- Описуються прості чи складні Навички
- Для виконання Завдання можуть знадобитися декілька складових Навичок
- Один опис складової Навички може застосовуватися для виконання більш ніж одного Завдання.

Опис складової Навички може бути простим.

> Приклад: Навички розпізнавання попереджень Системи виявлення вторгнень

Опис складової Навички може бути складним.

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

Як зображено на Схемі 1, складові Навички описують, що може зробити учень, а складові Завдання описують роботу, яку потрібно виконати. Тому важливо розділити мову, що використовується, між описом складових Навички та описом складових Завдання, і використовувати терміни, які забезпечують спостережливість та оцінку учня.

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

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

Використання Загальних принципів NICE

Варто зазначити, що хоча Загальні принципи управління персоналом у сфері кібербезпеки (Загальні принципи NICE) має 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 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 описи складових Знання і Навички із метою 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 відповідно до 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 застосування Загальних принципів NICE, які були створені для допомоги у досягненні загальних організаційних цілей. На основі цих прикладів організації або галузі можуть отримати корисну інформацію під час пошуків, як найкраще почати свою роботу, але такими прикладами не визначається єдиний спосіб використання Загальних принципів NICE.

3.1 Використання наявних складових Завдання, Знання і Навички (TKS)

Користувачі Загальних принципів NICE посилаються на одне або декілька складових Завдання, Знання і Навички (складові TKS), описаних у Розділі 2, для характеристики як роботи, так і учнів. Складові Завдання використовуються для опису роботи. Складові Завдання мають бути пов'язані з складовими Знання і Навички. Попри те, що опис складової Завдання може мати рекомендований набір пов'язаних описів складових Знання і Навички, користувачі можуть включати інші наявні описи складових Знання і Навички для приведення Завдань у відповідність до свого унікального контексту. Складові Знання і Навички використовуються для опису учнів. Складові Знання і Навички 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 організації. Наведені нижче теоретичні приклади використання показують сфери, в яких складові TKS можуть бути запроваджені:

- Програма відстеження складової Навички працівника з метою визначення кваліфікації працівника вимогам для просування по службі
- Знання, потрібні для закінчення курсу
- Щотижневий перелік Завдань, які були завершені в організації

Складові TKS та приклади можна знайти у Ресурсному центрі з розроблення Загальних принципів NICE. Ці складові, за потреби, оновлюватимуться для того, щоб іти в ногу зі змінами, які виникають внаслідок появи нових комерційних проектів, ризиків або новітніх технологій. [1]

3.2 Створення нових складових TKS

Користувачам не рекомендується змінювати текст у наявних описах складових TKS відповідно до Загальних принципів NICE. Метою складових є підтримання сумісності систем, тож зміни у контексті складових можуть призвести до подальших розбіжностей під час

використання зовнішніх джерел. У випадку виникнення потреби додати нове визначення до складових TKS для відображення унікального контексту користувача можна створити нову Складову.

Крім того, користувачі можуть створювати повністю нові складові Завдання, Знання або Навички, щоб допомогти адаптувати використання Загальних принципів NICE до локальних потреб із їхнім унікальним контекстом. Такі додаткові складові 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, допомагають учням розвивати і демонструвати Компетенції. Компетенції складаються з назви, опису Компетенції, методу оцінювання, а також із групи пов'язаних складових TKS.

Компетенція
Механізм оцінки учнів організаціями.

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

Компетенції пропонують гнучкість, дозволяючи організаціям об’єднувати різні складові TKS в загальну категорію, яка визначає широкі потреби. Хоча окреме Завдання та пов'язані з ним складові Знання і Навички можуть не змінюватись, більш широка визначена Компетенція може запровадити нові Завдання або навіть окремі складові Знання чи Навички, або може видаляти наявні, реагуючи на зміни потреб мінливої екосистеми 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 складових Завдань. Потім, організація може використовувати ці Компетенції для оцінювання того, чи здатний кандидат виконувати ці Завдання. Таке оцінювання може відбуватись у формі співбесіди, тестування кандидатів на посаду перед працевлаштуванням або спостереженням процесу навчання на робочому місці.

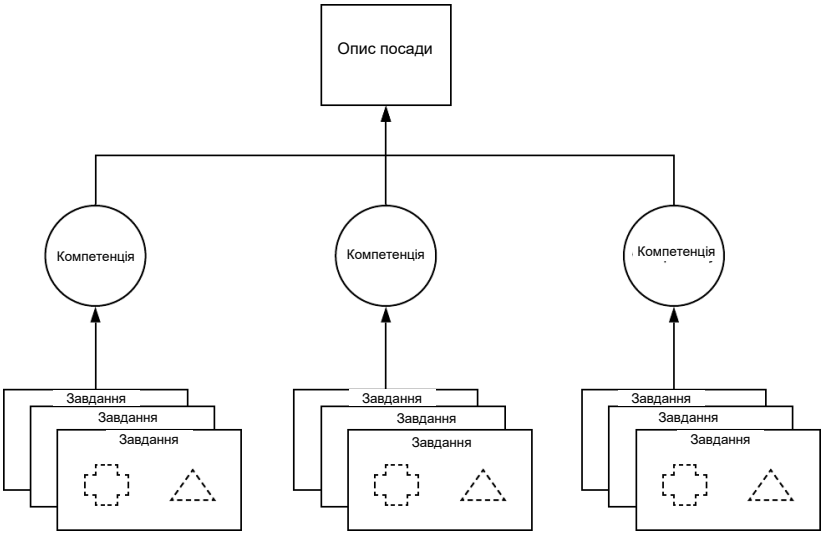

Рисунок 2 – Використання Компетенцій для оцінювання учнів шляхом опису посади

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

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

Інші організації можуть використовувати Компетенції для визначення того, чи учень досягнув визначений набір складових Навички і Знання. Ці організації можуть, як зображено у рисунку 3, обрати варіант використання Компетенцій як груп складових Знання і Навички (K&S). Ці організації можуть оцінювати учнів за цими складовими K&S. Оцінювання може проводитись у формі тестів, лабораторних демонстрацій або усного оцінювання.

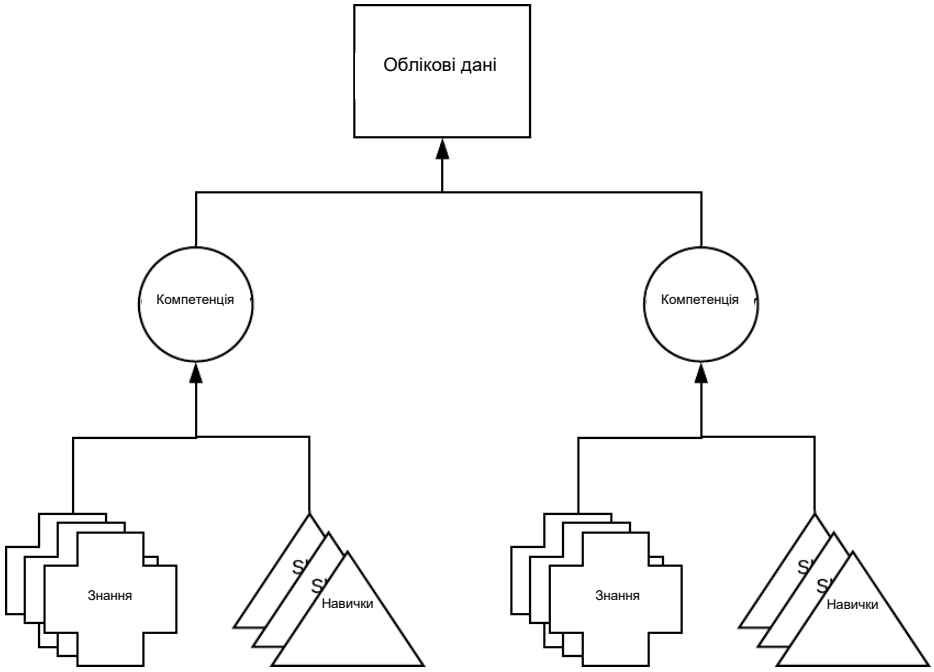

Схема 3 – Використання Компетенцій для оцінювання учнів за допомогою облікових даних

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

3.3.1 Використання наявних Компетенцій

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

- описання типів Завдань у рамках певної посади
- відстеження здібностей персоналу
- описання вимог до трудового колективу
- демонстрування здібностей учня

Хоча Компетенція має рекомендований набір пов'язаних складових TKS, користувачі можуть додавати або виключати існуючі складові, щоб адаптувати Компетенції до свого унікального контексту. Проте, користувачам не рекомендується змінювати назву або опис наявних Компетенцій Загальних принципів NICE. Компетенції призначені для підтримки сумісності тож зміни їхнього змісту можуть призвести до подальших розбіжностей під час використання зовнішніх джерел. У випадку виникнення потреби у додаванні нового визначення до Компетенції для відображення унікального контексту користувача, можна створити нову Компетенцію, що описано нижче (див. Пункт 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, дозволяє організаціям описувати Компетенцію для забезпечення відповідності мінливій екосистемі кібербезпеки. Це може бути зроблене 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 у 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 Компетенції.

Приклад аналізу даних 1

Таблиця 1 нижче за текстом є інформативною та містить відправну точку для формування Компетенції. Компетенція за прикладом 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 Завдання, що відповідає бізнес цілям. (Зверніть увагу, що у Таблиці 1 використовуються Завдання з загальних принципів NICE версії 2017 року. [2])

Таблиця 1 – Приклад створення нової Компетенції «Аналіз даних у рамках наявних завдань відповідно до Загальних принципів NICE 2017 р.»

Назва Компетенції: Приклад аналізу даних 1
Опис Компетенції: Збирання, створення або аналізування якісної або кількісної інформації чи даних із різних джерел із метою прийняття рішення, надання рекомендації та/або складання звітів, інструктажів, резюме та іншої документації.
Метод оцінювання: Лабораторна демонстрація
Складові Завдання
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).

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

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

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», визначену роботодавцем.

Деталізована Компетенція «Аналіз даних» може бути набагато ширшою. За допомогою нумерації складових Завдання у рамках Компетенції, організація може визначити бажану сферу застосування Компетенції. Для простоти використання посилання на Завдання використовують ідентифікатори (ID) завдань відповідно до Загальних принципів 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 описи складових Знання і Навички для формування Компетенції.

Таблиця 2 – Приклад створення нової Компетенції

«Аналіз даних із додатковими Завданнями»

Назва Компетенції: Приклад аналізу даних 2
Опис Компетенції: Збирання, створення або аналізування якісної або кількісної інформації чи даних із різних джерел із метою прийняття рішення, надання рекомендації та/або підготування звітів, інструктажів, резюме та іншої документації.
Метод оцінювання: Тестування
Складові 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 даних та стандартизації даних.
K0338 |Знання методик розумного аналізу даних.

У цьому прикладі Таблиця 2 показує Компетенцію «аналіз 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», що визначена органом сертифікації.

(Зауважте, що у таблиці 2 використовуються описи складових Знання і Навички із 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 описами складових Знання, Навички та Здібності, в Загальних принципах NICE використовується більш динамічний підхід через Завдання. Робочі ролі складаються із Завдання, яке визначають роботу, що має бути виконана; Завдання включають пов'язані складових Знання і Навички, що відображають здатність учнів виконувати такі Завдання. Такий перехідний підхід, зображений на рисунку 3, підвищує гнучкість і спрощує комунікацію.

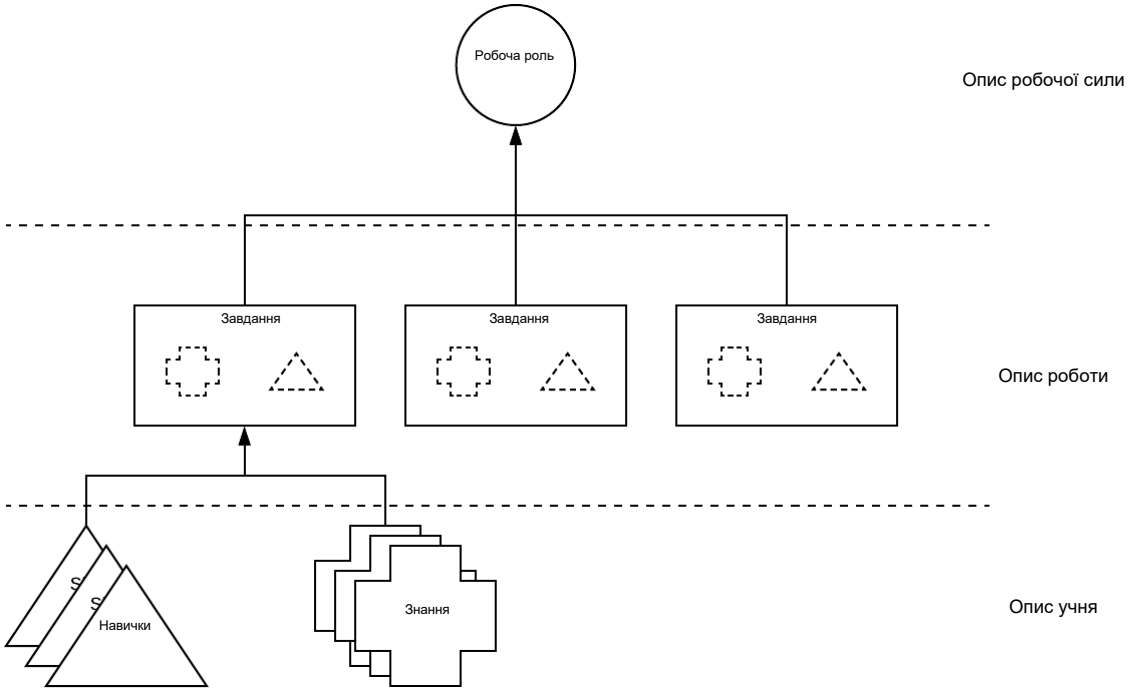

Схема 4 – Зв'язок Робочих ролей зі складовими

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

Окрема Робоча роль (наприклад, Розробник Програмного Забезпечення) може застосовуватися для тих, хто має багато різних посад (наприклад, програміст, кодувальник, розробник прикладного програмного забезпечення). І навпаки, багато ролей можуть бути об'єднані для створення певної роботи. Такий адитивний підхід підтримує модульність й відображає той факт, що всі учні у складі трудового колективу виконують різноманітні та численні завдання в різних робочих ролях, незалежно від займаних посад. 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.

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

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

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 складових Загальних принципів NICE можна знайти в Ресурсному Загальних принципів NICE. [1]

Користувачів застерігають від внутрішньої модифікації назви або опису існуючих Робочих ролей. Робочі ролі призначені для підтримки сумісності, і тому зміни у їхньому змісті можуть призвести до подальших розбіжностей. Якщо виникає потреба у додаванні нової складової, 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 різними 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 завершена. Такий підхід може вважатися підходом «згори донизу».

Таблиця 3 – Приклад створення команди з розробки безпечного програмного забезпечення на основі Робочих ролей відповідно до Загальних принципів NICE 2017 р.

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

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

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, створенні 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 р. 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 системи безпеки
Виявлення	PR-CDA-001 | Аналітик із питань кібернетичної оборони
Реагування	PR-CIR-001| Відповідальний за усунення інцидентів у сфері кібернетичної оборони
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, приклад команди створений з використання підходу, орієнтованого на роботу. Використовуючи ядро Загальних принципів з удосконалення кібербезпеки критичної інфраструктури (Загальні принципи кібербезпеки) обираються цілі у сфері кібербезпеки, визначаються Завдання, спрямовані на досягнення цих цілей, і обираються Робочі 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 на основі Компетенцій

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 проблем. Цей підхід можна назвати «знизу догори». Отже, команда, яка створена у такий спосіб, може допомагати визначати учнів, які можуть взяти участь у роботі команди у майбутньому. Такі учні можуть або не можуть бути пов'язані з певною Робочої роллю і просто мати Компетенції, потрібні для сприяння досягненню організаційних цілей.

Наприклад команда із кібербезпеки у сфері оборони, що використовує свої Навички для імітування технік 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 розповсюдження даних про учнів (і про роботу, яку учні виконуватимуть) з метою досягнення цілей організації.

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

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

Висновки

Завдяки застосуванню підходу з використанням складових, описаного в Загальних принципах NICE, користувачі можуть скористатися послідовним методом організації та обговорення роботи, що має бути виконана, на основі складових Завдання, 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, 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.

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

Посилання

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

[2] Newhouse WD, Witte GA, Scribner B, Keith S (2017) National Initiative forCybersecurity 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 EnterpriseRisk 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

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

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	Складові Знання і Навички
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	Складові Завдання, Знання і Навички

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, які можна відновити з пам'яті.

Навичка Здатність виконувати практичні задачі.

Завдання Діяльність, спрямована на досягнення цілей організації.

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