NIST Special Publication 800-181

Національна освітня ініціатива у сфері кібербезпеки (NICE)
Загальні принципи управління персоналом у сфері кібербезпеки

Вільям Ньюхаус
Стефані Кіт
Бенджамін Скрібнер
Грег Вітте

Ця публікація доступна безкоштовно за посиланням:
https://doi.org/10.6028/NIST.SP.800-181

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

NIST Special Publication 800-181

Національна освітня ініціатива у сфері кібербезпеки (NICE) Загальні принципи управління персоналом у сфері кібербезпеки

Вільям Ньюхаус
Відділ прикладної кібербезпеки
Лабораторія інформаційних технологій
Стефані Кіт
Відділ кадрової стратегії та політики в області кібербезпеки
Секретаріат заступника директора з інформаційних технологій Міністерства оборони
Бенджамін Скрібнер
Відділ освіти та просвіти у сфері кібербезпеки
Управління національної оборони і програм Департаменту внутрішньої безпеки
Грег Вітте
Компанія «G2, Inc.»
Аннаполіс Джанкшен, Меріленд

Ця публікація доступна безкоштовно за посиланням:
https://doi.org/10.6028/NIST.SP.800-181

Серпень 2017 р.

Міністерство торгівлі США

Вілбур Луїс Росс-Молодший, міністр
Національний інститут стандартів і технологій
Кент Рочфорд, Директор НІСТ і заступник Міністра торгівлі в області стандартів і технологій

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Уповноважений орган

Цей документ розроблений NIST згідно його статутних обов'язків відповідно до Закону про фінансову модернізацію федеральної інформаційної безпеки (FISMA) 2014 року, 44 Кодексу законів США § 3551 і наступних параграфів, Публічного права (P.L.) 113-283. NIST відповідає за розробку стандартів та настанов з інформаційної безпеки, включаючи мінімальні вимоги до федеральних інформаційних систем, але такі стандарти та настанови не застосовуються до систем національної безпеки без офіційного затвердження відповідних федеральних посадових осіб, що керують даними системами. Ця настанова відповідає вимогам Адміністративно-бюджетного управління (OMB) Циркуляр A-130.

Жодне положення у даному документі не повинно сприйматись як таке, що суперечить обов'язковим для федеральних установ стандартам та настановам Міністра торгівлі згідно з його статутними повноваженнями. Також ці настанови не повинні тлумачитися як такі, що змінюють або відмінюють існуючі повноваження Міністра торгівлі, директора АБУ або будь-якої іншої федеральної посадової особи. Ця публікація може бути використана неурядовими організаціями на добровільній основі, та не є суб'єктом авторського права на території Сполучених Штатів. Однак, бажаним є посилання на NIST.

Спеціальне видання Національного інституту стандартів і технологій 800-181
Спеціальне видання Національного інституту стандартів і технологій 800-181, 144 сторінок (серпень 2017 р.)
CODEN: NSPUE2

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

З метою належного опису експериментальної процедури або концепції у цьому документі можуть бути ідентифіковані певні комерційні об'єкти, обладнання або матеріали. Така ідентифікація не означає рекомендацію або схвалення NIST, а також не передбачає те, що вказані об'єкти, матеріали або обладнання є найкращим для конкретної мети.

У цієї публікації можуть бути посилання на інші публікації, які на даний час розробляються NIST відповідно до його статутних обов'язків. Інформація у цій публікації, включаючи концепції та методики, може використовуватися федеральними установами ще до завершення таких супутніх публікацій. Таким чином, до завершення кожної такої публікації залишаються діючими існуючі поточні вимоги, настанови та процедури. З метою планування та переходу федеральні агентства можуть уважно стежити за розробкою цих нових публікацій NIST.

Організаціям пропонується переглянути всі проекти публікацій під час періоду надання коментарів та надати відгуки до NIST. Багато публікацій HICT з кібербезпеки, крім зазначених вище, доступні за посиланням: http://csrc.nist. gov/publications.

Адреса для відправлення коментарів до даної публікації:

Національний інститут стандартів і технологій

До уваги: NICE, Applied Cybersecurity Division, Information Technology Laboratory

100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Email: ncwf@nist.gov

Усі коментарі можуть бути опубліковані згідно до Закону про свободу інформації (FOIA).

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Звіти про технологію комп'ютерних систем

Лабораторія інформаційних технологій (ITL) при Національному інституті стандартів і технологій США сприяє покращенню економіки та суспільного добробуту населення США за допомогою технічного управління інфраструктурою вимірювань та стандартів в країні. ITL розробляє тести, методи випробувань, довідкові дані, докази реалізації концепції та технічні аналізи, спрямовані на розвиток та продуктивне використання інформаційних технологій. Обов'язки ITL включають розробку управлінських, адміністративних, технічних та фізичних стандартів та настанов для економічно ефективної системи безпеки та конфіденційності інформації, не пов’язаної з національною безпекою, в федеральних інформаційних системах. Звіти спеціального видання 800-серії містяться дослідження, настанови та роз'яснювальні заходи ITL в галузі безпеки інформаційних систем, а також стосовно її спільної діяльності з галузевими, урядовими та академічними організаціями.

Резюме

Цей документ описує Національну освітню ініціативу у сфері кібербезпеки (NICE) «Загальні принципи управління персоналом у сфері кібербезпеки (Загальні принципи NICE)», а саме довідкову структуру, яка описує міждисциплінарний характер роботи в сфері кібербезпеки. Загальні принципи NICE слугують основним довідковим ресурсом для опису та обміну інформацією про роботу у сфері кібербезпеки та знань, навичок та здібностей (KSA), необхідні для виконання завдань, які можуть посилити стан кібербезпеки в організації. Як загальний, узгоджений лексикон, що класифікує та описує роботу у сфері кібербезпеки, Загальні принципи NICE покращують комунікації стосовно того, як виявляти, набирати, розвивати та зберігати таланти у сфері кібербезпеки. Загальні принципи NICE є довідковим джерелом, за допомогою якого організації або сектори можуть розробляти додаткові публікації або інструменти, які відповідають їх потребам для визначення або надання настанов щодо різних аспектів розвитку, планування, тренінгів та навчання персоналу у сфері кібербезпеки.

Ключові слова

Здібності; кібербезпека; кіберпростір; освіта; знання; роль; навичка; область спеціалізації; завдання; тренінг; робоча роль.

Версії

Будь ласка, відвідуйте веб-сайт версій Загальних принципів NICE [1] для визначення чи були оновлення областей спеціалізацій в Загальних принципах NICE .

Додаткові матеріали

Довідкова електронна таблиця Загальних принципів NICE доступна за посиланням: https://www.nist.gov/file/372581.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Подяка

Автори висловлюють подяку приватним особам та організаціям державного і приватного секторів за значний внесок у дану роботу, а саме за помірковані та конструктивні коментарі, які підвищили загальну якість, змістовність та корисність цієї публікації. Ми вдячні Родні Петерсену, директору Національної освітньої ініціативи у сфері кібербезпеки (NICE) NIST за керівну роль та роботу. А також хочемо подякувати Тані Брюер, Діну Бушміллеру, Лінн Кларк, Джері Дамаванді, Лізі Дорр, Райану Фарр, Джиму Фоті, Джоді Гусс, Кіту Холлу, Крісу Келсаллу, Елізабет Леннон, Джеффу Маррону, Джошуа Музіканте, Стефану Олечновичу, Лорі Пфаненнштейну, Чаку Роміну, Кевіну Санчесу-Чері, Даніелю Сантосу, Стефані Шівелі, Метью Сміту, Кевіну Стейну, Блюму Суссману, Керолайн Тан, Барісу Якіну і Кларенс Вільямс за окремі внески до цього видання.

Перші Загальні принципи NICE були опубліковані для публічних коментарів у вересні 2012 року, а остаточна версія була видана у квітні 2013 року за назвою «Керівні принципи управління персоналом у сфері національної кібербезпеки, версія 1.0» [2]. Автори висловлюють подяку доктору Джейн Гомейер, Енн Кіглі, Рексу Міну, Ноелю Кайлу, Майі Янкелевіч та Пеггі Макссон за провідну роль у розробці документу, а також Монтані Вільямс і Рою Берджессу за керівну роль у розробці «Керівні принциппи управління персоналом у сфері національної кібербезпеки, версія 2.0», яка була опублікована у квітні 2014 року [3].

На завершення, автори з повагою відзначають фундаментальну роботу з комп'ютерної безпеки 1960-х років. Бачення, розуміння та цілеспрямовані зусилля основоположників комп'ютерної безпеки слугують філософсько-технічною основою завдань, знань, навичок та здатностей, зазначених у цьому виданні.

Інформація про торговельні марки

Усі торговельні марки або зареєстровані товарні знаки належать їх відповідним організаціям.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Резюме

Національна освітня ініціатива у сфері кібербезпеки (NICE), очолювана Національним інститутом стандартів і технологій (NIST) Міністерства торгівлі США – це співпраця уряду, наукової спільноти та приватного сектору з метою активізації та просування надійної мережі та екосистеми освіти, навчання та розвитку персоналу в галузі кібербезпеки. NICE виконує цю місію, погоджуючи її з урядовими, академічними та промисловими партнерами, з метою створення успішних програм на основі існуючих, сприяння змінам та інноваціям, а також забезпечення керівництва та бачення того, як збільшити кількість кваліфікованих фахівців у галузі кібербезпеки, які гарантуватимуть безпеку нашої нації.

NICE прагне розвивати цілісний персонал в сфері кібербезпеки, конкурентоспроможний в усьому світі з моменту найму до виходу на пенсію, який готовий захищати нашу державу від існуючих та виникаючих проблем з кібербезпекою. NICE сприяє загальнонаціональним ініціативам, які збільшують кількість людей, які мають знання, навички та здібності виконувати завдання, необхідні для виконання завдань у сфері кібербезпеки.

Оскільки загрози, що використовують вразливі місця у нашій кіберінфраструктурі, зростають і розвиваються, цілісний персонал у сфері кібербезпеки повинен бути спроможним проектувати, розробляти, впроваджувати та підтримувати оборонні та наступальні кіберстратегії. Цілісний персонал у сфері кібербезпеки включає в себе технічні та нетехнічні ролі, які виконують досвідчені та обізнані люди. Цілісний персонал у сфері кібербезпеки може вирішувати проблеми кібербезпеки, допомагаючи організаціям успішно реалізувати аспекти їхніх місій та бізнес-процесів, пов'язаних із кіберпростором.

Ця публікація представляє базові довідкові матеріали про підтримку персоналу, здатного задовільнити потреби організації сфері кібербезпеки, використовуючи загальний, послідовний лексикон для опису роботи у сфері кібербезпеки відповідно до категорій, спеціальностей та ролей. Це забезпечує розширений набір знань, навичок та здібностей (KSA) у сфері кібербезпеки та завдань для кожної відповідної робочої ролі. Загальні принципи NICE підтримують відповідну організаційну та галузеву комунікацію з метою освіти, тренінгів та розвитку персоналу у сфері кібербезпеки.

Користувач Загальних принципів NICE буде посилатися на нього для різних аспектів розвитку персоналу, освітніх та/або тренінгових цілей, і коли цей матеріал використовується на рівнях організації, користувач повинен підлаштовувати Загальні принципи NICE до стандартів, правил, потреб та місій своєї організації. Загальні принципи NICE є довідковою відправною точкою для змісту методології та настанов для кар'єрного росту, освіти, тренінгів та атестаційних програм.

Загальні принципи NICE - це ресурс, який зміцнить здатність організації відповідно та легко спілкуватися стосовно кібербезпеки з персоналом. Організації або сектори можуть розробляти додаткові публікації або інструменти для визначення або надання настанов стосовно різних аспектів розвитку персоналу, планування, тренінгів та освіти, що відповідають їх потребам.

Інтерактивний довідник електронних таблиць [4] доступний на веб-сайті Загальних принципів NICE.[5].

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Зміст

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Перелік додатків

Список таблиць

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

1 Вступ

Національна освітня ініціатива у сфері кібербезпеки (NICE), яка керується Національним інститутом стандартів і технологій (NIST) Міністерства торгівлі США – це співпраця уряду, наукової спільноти та приватного сектору з метою активізації та просування надійної мережі та екосистеми освіти, тренінгів та розвитку персоналу у сфері кібербезпеки. NICE виконує цю місію, за допомогою координації між урядовими, академічними та промисловими партнерами, з метою створення успішних програм на основі існуючих, сприяння змінам та інноваціям, а також забезпечення керівництва та бачення того, як збільшити кількість кваліфікованих фахівців у сфері кібербезпеки, які гарантуватимуть безпеку нашої нації та її економічну конкурентоспроможність.

NICE прагне розвивати інтегрований персонал в сфері кібербезпеки, конкурентоспроможний в усьому світі з моменту найму до виходу на пенсію, який підготований захищати нашу державу від існуючих та виникаючих проблем з кібербезпекою.

У цьому документі об’єднаний термін «персонал у сфері кібербезпеки» є скороченим описом персоналу з робочими ролями, які впливають на здатність організації захищати свої дані, системи та операції. Включені нові робочі ролі, які традиційно відомі як «захист інформаційних технологій (IT)». Ці ролі були додані до загальних принципів управління персоналом, щоб підкреслити їх важливість для загального стану кібербезпеки в організації. Окрім того, деякі робочі ролі, описані в цьому документі, включають в себе коротший термін «кібер», що містить в собі сфери, де термін «кібер» стає розмовною нормою.

Персонал у сфері кібербезпеки включає в себе не тільки технічний персонал, а й той, що застосовує знання про кібербезпеку при підготовці своєї організації до успішного виконання її місії. Добре обізнаний та кваліфікований персонал у сфері кібербезпеки потрібний для подолання ризиків кібербезпеки в рамках загального процесу управління ризиками організації.

1.1. Передумови для створення Загальних принципів NICE

Ідея створення Загальних принципів NICE з’явилась до створення NICE в 2010 році та втілилась у життя після визнання того, що персонал у сфері кібербезпеки не є визначений та оцінений. Щоб вирішити це завдання, Федеральна рада директорів з інформаційних технологій (ДІТ) поставила собі завдання в 2008 році визначити стандартні загальні принципи розуміння ролі кібербезпеки в рамках федерального уряду. Фокус-групи та експерти з численних федеральних агентств допомогли Федеральній раді ДІТ підготувати дослідницький звіт, в якому йдеться про вже проведені заходи з підвищення кваліфікації у сфері інформаційних технологій, і, відповідно до необхідності агентств, визначили тринадцять специфічних ролей для проведення заходів у сфері кібербезпеки.

Ґрунтуючись на цьому, по суті, багатопрофільному дослідженні «поля» кібербезпеки, Комплексна національна ініціатива з кібербезпеки включала в себе зосередження уваги на персоналі, що поставило декільком відомствам завдання співпрацювати для розробки системи управління персоналом у сфері кібербезпеки. Перший проект був опублікований для публічного коментаря у вересні 2011 року. Коментарі були включені до версії 1.0 [2].

На подальшому загальнодержавному розгляді США було відзначено конкретні сфери, які слід розглянути та вдосконалити. Департамент національної безпеки (DHS) зібрав інформацію та затвердив остаточні рекомендації за допомогою фокус-груп та експертів в галузі з усієї країни та у різних галузях промисловості, наукових верствах та уряді, в

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

результаті чого було створено другу версію Загальних принципів NICE, версія 2.0 [3], яка була стала публічною у 2014 році.

Секретаріат міністра оборони (OSD) поширив версію 2.0 на внутрішні контракти зі сервісними компонентами та зовнішні контракти з приватним сектором. Співавтори з DHS та NIST працювали з OSD, щоб вдосконалити публікацію та розширити її з метою підкреслення застосовності у приватному сектору та зміцнити розуміння того, що Загальні принципи NICE є довідковим ресурсом як для державного, так і для приватного секторів.

1.2. Мета та застосовність

Ця публікація слугує основним довідковим ресурсом для підтримки персоналу, здатного задовольнити потреби організації у сфері кібербезпеки. Вона забезпечує організації загальною, погодженою термінологією, що класифікує та описує роботу у сфері кібербезпеки.

Використання Загальних принципів NICE у якості фундаментального довідкового ресурсу покращить комунікацію, необхідну для виявлення, набору та розвитку талантів у сфері кібербезпеки. Завдяки Загальним принципам NICE роботодавці зможуть використовувати базову, погоджену мову в програмах професійного розвитку, для сертифікацій та академічних атестацій, а також у виборі відповідних тренінгів для свого персоналу.

Загальні принципи NICE сприяють використанню більш послідовного, порівнянного та повторюваного підходу до вибору та визначення ролей у сфері кібербезпеки для посад в організаціях. Ця публікація також надає загальний лексикон, який можуть використовувати академічні установи для розробки навчальних програм з кібербезпеки з метою кращої підготовки студентів до поточних та майбутніх потреб кібербезпеки.

Застосування загальних принципів NICE пропонує можливість описати всі роботи з кібербезпеки. Мета застосування загальних принципів NICE полягає в тому, щоб будь-яка діяльність чи посада у сфері кібербезпеки була описана шляхом вибору відповідного елементу з одного або декількох елементів Загальних принципів NICE. Для кожної роботи або посади контекст місії або бізнес-процесів та пріоритетів визначатиме, який матеріал буде обрано з загальних принципів NICE.

Застосування Загальних принципів NICE надає можливість описувати всю роботу у сфері кібербезпеки. Мета застосування Загальних принципів NICE полягає в тому, щоб будь-яка діяльність чи посада у сфері кібербезпеки була описана шляхом вибору відповідного елементу з одного або декількох складових елементів Загальних принципів NICE Для кожної роботи або посади контекст місії або бізнес-процесу та пріоритетів будуть визначатимуть те, які елементи слід обрати з Загальних принципів NICE.

Організації або сектори можуть використовувати Загальні принципи NICE для розробки додаткових публікацій або інструментів, які відповідають їх потребам, для визначення або розроблення настанов стосовно різних аспектів розвитку персоналу, планування, тренінгів та освіти.

1.3. Аудиторія/Користувачі

Загальні і принципи NICE можна розглядати як словник для управління персоналом у сфері кібербезпеки, який не потребує приписів. Користувачі Загальних принципів NICE, які посилаються на них, мають впроваджувати його на локальному рівні для різних цілей розвитку, освіти або тренінгів персоналу.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

1.3.1. Роботодавці

Використання загальної лексики Загальних принципів NICE дасть можливість роботодавцям оцінювати та розвивати свій персонал у сфері кібербезпеки. Роботодавці та керівництво організацій можуть використовувати Загальні принципи NICE для:

- Оцінювання та відстеження свого персоналу у сфері кібербезпеки, щоб отримати більш глибоке розуміння сильних сторін та прогалин у знаннях, навичках, здібностях і виконаних завданнях;
- Визначення навчальних та кваліфікаційних вимог для розвитку критично важливих знань, навичок та здібностей для виконання завдань з кібербезпеки;
- Удосконалення описів посад та вакансій, включаючи вибір необхідних KSA та завдань, як тільки будуть визначені робочі ролі та завдання;
- Визначення найбільш відповідних робочих ролей та розробки кар'єрних шляхів для управління персоналом у отриманні необхідних навичок для цих ролей; та
- Встановлення загальної термінології між менеджерами з найму та спеціалістами відділу кадрів (HR) для набору, утримання та підготовки високо спеціалізованого персоналу.

1.3.2. Сучасні та майбутні працівники у сфері кібербезпеки

Загальні принципи NICE допомагають працівникам у сфері кібербезпеки, і тим, хто бажає ними стати, визначати обов'язки в рамках категорій та робочих ролей у сфери кібербезпеки. Вони також допомагають спеціалістам відділу кадрів та методистам доводити до відома шукачам роботи та студентам зрозуміти те, які робочі ролі та необхідні знання, навички та здібності їм потрібні, аби роботодавці розглянули їх на вакантні посади у сфері кібербезпеки.

Цим працівникам надається підтримка, коли оголошення про вакансії та описи вакансій використовують загальний лексикон Загальних принципів NICE для надання чітких та послідовних описів завдань у сфері кібербезпеки, необхідних для отримання цих посад.

Коли постачальники тренінгових послуг та послуг з сертифікації у сфері кібербезпеки використовують загальний лексикон Загальних принципів NICE, спеціалісти у сфері кібербезпеки, або ті, хто бажають ними стати, зможуть знайти таких постачальників тренінгових послуг та/або послуг з сертифікації, які навчать їх виконувати завдання, необхідні для працевлаштування або отримання нових посад у сфері кібербезпеки. Використання загальної лексики допоможе студентам та фахівцям отримати KSA які, як правило, демонструються людиною, посада якої включає певну робочу роль у сфері і кібербезпеки. Це розуміння допомагає їм знайти академічні програми, які включатимуть в себе результати навчання та знання, які відповідають KSA, та завданням, які цінуються роботодавцями.

1.3.3. Педагоги/Тренери

Загальні принципи NICE надають педагогам рекомендації стосовно розробки навчальних програм, сертифікатів або програм для отримання ступені, тренінгових програм, курсів, семінарів та вправ або завдань, що охоплюють KSA та завдань, які описані в Загальних принципах NICE.

Спеціалісти з кадрового забезпечення та радники можуть використовувати Загальні принципи NICE у якості ресурсу для вивчення кар'єри.

1.3.4. Постачальники технологій

Загальні принципи NICE дозволяють постачальникам технологій визначати робочі ролі у сфері кібербезпеки, а також KSA та Завдання, пов'язані з апаратними та програмними продуктами і послугами, які вони надають. Так, постачальник технологій зможе створити довідкові матеріали, щоб допомогти персоналу у сфері кібербезпеки у правильній конфігурації та управлінні їх продуктами.

1.4. Структура даної публікації

Надалі це спеціальне видання має таку структуру:

- Розділ 2 описує такі складові Загальних принципів NICE, як: (i) Категорії; (ii) Області спеціалізації; (iii) Робочі ролі; (iv) Відповідні набори знань, навичок та здібностей (KSA); та (v) Завдання для кожної ролі.
- Розділ 3 описує використання Загальних принципів NICE
- У Розділі 4 зазначаються області, в яких інші публікації, настанови, вказівки та інструменти можуть розширити вплив Загальних принципів NICE.
- Додаток A містить перелік категорій, областей спеціалізації, робочих ролей, KSA та завдань Загальних принципів NICE.
- Додаток B містить детальний перелік робочих ролей, включаючи пов'язані з ними KSA та завдання.
- У Додатку C наведені приклади інструментів розвитку персоналу.
- У Додатку D наведені приклади настанов або керівних інструкцій, частина змісту яких перетинається зі складовими елементами Загальних принципів NICE.
- Додаток E містить перелік окремих скорочень та абревіатур, що використовуються у документі.
- Додаток F містить довідкову літературу, процитовану у цьому документі.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

2. Складові Загальних принципів NICE та їх взаємозв'язки

2.1 Складові Загальних принципів NICE

Загальні принципи NICE допомагають організувати роботу у сфері кібербезпеки та інших суміжних сферах. Цей розділ представляє та визначає основні складові Загальних принципів NICE для підтримки цих сфер.

B.7.5 Категорії

Категорії забезпечують загальну організаційну структуру Загальних принципів NICE. Існує сім категорій, і всі вони складаються з областей спеціалізації та робочих ролей. Ця організаційна структура базується на поглибленому аналізі робіт, який об'єднує роботу та працівників, які мають загальні основні функції незалежно від назв посад чи інших професійних умов.

2.1.2. Області спеціалізації

Категорії складаються з областей спеціалізації. У першій версії 1.0 «Загальних принципів управління персоналом у сфері національної кібербезпеки» [2] було виділено 31 область спеціалізації, а у другій версії 2.0 [3] – 32. Кожна область спеціалізації являє собою область зосередженої роботи або функції у сфери кібербезпеки та суміжних завдань. У попередніх версіях Загальних принципів NICE завдання та KSA були пов'язані з кожною областю спеціалізації. Тепер KSA та завдання пов'язані з робочими ролями.

2.1.3. Робочі ролі

Робочі ролі – це найбільш детальні групи у сфері кібербезпеки та суміжних сферах, які включають перелік атрибутів, необхідних для виконання певної ролі у формі знань, навичок та здібностей (KSA) та завдань, виконуваних у цій ролі.

Діяльність, яка виконується в завданні або на посаді, описується шляхом вибору однієї або кількох робочих ролей із Загальних принципів NICE, що відповідають до цій роботі або посаді для виконання місії або бізнес-процесів.

Для допомоги в організації та спілкуванні стосовно відповідальностей за кібербезпеку, робочі ролі згруповані в конкретні класи категорій та областей спеціалізації, як показано у Додатку А.

2.1.4. Знання, навички та здатність (KSA)

Знання, навички та здатність (KSA) – це атрибути, які необхідні для виконання робочих ролей, і які, як правило, демонструються через належний досвід, освіту чи тренінги.

> **Знання** – це сукупність інформації, що безпосередньо застосовується до виконання функції.
>
> **Навичка** часто визначається як спостережувана компетентність виконувати вивчену психомоторну дію. Навички в психомоторній області – це здатність фізично управляти засобом або інструментом, як рукою або молотом. Навички, необхідні для сфери кібербезпеки, менше залежать від фізичної маніпуляції інструментами і більше – від застосовуваних інструментів, загальних принципів, процесів та контролей, які впливають на стан кібербезпеки організації чи фізичної особи.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Здатність – це можливість здійснювати спостережувану поведінку або поведінку, результатом якої є спостережуваний продукт.

2.1.5. Завдання

Завдання – це специфічна визначена частина роботи, яка в поєднанні з іншими завданнями складає роботу в певної області спеціалізації або робочої ролі.

2.2. Взаємозв'язки між складовими Загальних принципів NICE

Складові Загальних принципів NICE описують роботу у сфері кібербезпеки. Як показано на Рисунку 1, кожна Категорія складається з Областей спеціалізації, кожна з яких складається з однієї або більш робочих ролей. Кожна робоча роль, у свою чергу, включає KSA та завдання.

Групування складових елементів таким чином полегшує спілкування на теми персоналу у сфері кібербезпеки та допомагає узгоджувати їх з іншими загальними принципами. Специфічний зв'язок між робочими ролями, KSA та завданнями показаний у Додатку В та у довідковій електронній таблиці [4] на сайті Загальних принципів NICE [5].

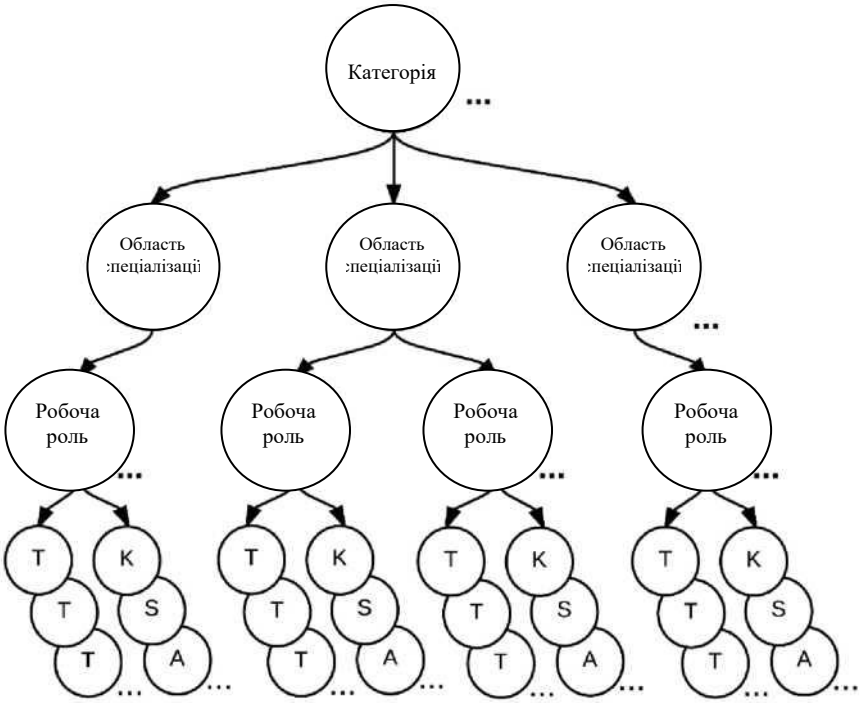

Рис. 1 – Взаємозв'язки між складовими елементами Загальних принципів NICE

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Використання Загальних принципів NICE

Використання Загальних принципів NICE для розуміння потреб організації та оцінки того, наскільки ці потреби задовольняються, може допомогти організації планувати, впроваджувати та контролювати успішну програму кібербезпеки.

3.1. Визначення потреб персоналу у сфері кібербезпеки

Сфера кібербезпеки стрімко змінюється і росте. Постійний ріст вимагає наявності кваліфікованого персоналу для виконання функцій з кібербезпеки. Після визначення організацією того, що саме необхідно для адекватного управління поточними та майбутніми ризиками, керівництво повинно враховувати здатність та необхідну кількість персоналу у сфері кібербезпеки.
На Рисунку 2 показано, що Загальні принципи NICE є центральною ланкою між роботодавцями та кваліфікованим і готовим до роботи персоналом у сфері кібербезпеки.

Рисунок 2 – Складові елементи для здатного та готового персоналу у сфері кібербезпеки

Кругові стрілки зліва на Рисунку 2 – це діяльність, яка може вплинути на здатність організації розвивати здатний та готовий персонал:

- Використання стандартного лексикону Загальних принципів NICE покращить комунікацію між педагогами, тренерами/спеціалістами з сертифікації, роботодавцями та найманими працівниками.
- Аналіз критичності виявить ті KSA та завдання, які є критичними для успішного виконання із заданою роллю, та ті KSA та завдання, які є ключовими для виконання кількох робочих ролей.
- Виконання аналізу кваліфікації надасть інформацію організації про очікуваний рівень підготовки (напр. початковий або експерт) для посад, що поєднують більше ніж одну роль. Аналіз кваліфікації повинен дозволяти уточнення вибору відповідних завдань та KSA, необхідних для робочих ролей, що складають цю посаду.

У Додатку С вказані деякі інструменти розвитку персоналу, що допомагають визначати потреби персоналу у сфері кібербезпеки.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

3.2. Набір та найм висококваліфікованого персоналу у сфері кібербезпеки

Посилання на Загальні і принципи NICE допоможе організаціям здійснити стратегічне планування та найм персоналу. Використання матеріалів Загальних принципів NICE, які використовуються під час створення або перегляду опису посад в оголошеннях про вакансії та публікаціях про роботу, допоможе кандидатам знайти конкретні посади, які їх зацікавлять та відповідатимуть їх кваліфікації і здібностям. Завдання, що використовуються для опису обов'язків та відповідальностей посад, та KSA, які використовуються для опису необхідних навичок та кваліфікації, повинні дозволяти кандидатам та спеціалістам відділу кадрів ефективніше спілкуватися. Використання термінології Загальних принципів NICE під час опису позицій та написання оголошення про вакансії дозволить досягти узгоджених критеріїв оцінки для перевірки та затвердження кандидатів.

Переглянувши перелік завдань Загальних принципів NICE, організації, стурбовані пробілами у роботі персоналу, можуть визначити специфічні завдання, які не виконуються організацією. Ці завдання допоможуть організації ідентифікувати робочу(-і) роль(-і) та область(-і) спеціалізації, які пропущені. Організація зможе мати більше можливостей взаємодіяти зі спільнотою постачальників освітніх, тренінгових та атестаційних послуг, а також послуг з сертифікації, пропозиції яких відображаються в рамках Загальних принципів NICE. Так, організація зможе визначити тренінги, які допоможуть існуючому персоналу усунути пробіли. Так само менеджери з найму персоналу, використовуючи дані Загальних принципів NICE, зможуть відібрати кандидатів, які мають KSA для виконання цих завдань з кібербезпеки.

3.3. Освіта та тренінги персоналу у сфері кібербезпеки

Визначення завдань за робочими ролями в рамках Загальних принципів NICE, дозволить викладачам готувати учнів за специфічними KSA, завдяки яким вони можуть демонструвати здатність виконувати завдання з кібербезпеки.

Академічні установи є критичними складовими підготовки та навчання персоналу у сфері кібербезпеки. Співпраця державних та приватних організацій, наприклад через програму NICE, дозволяє таким установам визначити необхідні знання та здібності. У свою чергу, розробка та доповнення навчальних програм, гармонізованих з лексиконом Загальних принципів NICE, допоможе студентам академічних установ здобувати навички, необхідні роботодавцям. Так як кількість студентів, які бажають працювати у сфері кібербезпеки, збільшується, ще більше студентів будуть залучатися до академічних програм з кібербезпеки як шлях до кар'єри.

3.4. Збереження та розвиток висококваліфікованих талантів у сфері кібербезпеки

Критичним аспектом кваліфікованого персоналу у сфері кібербезпеки є розвиток та збереження кваліфікованих талантів, які вже працюють у цієї сфері. Кожен такий працівник має існуючі стосунки, академічні знання та організаційний досвід, які важко замінити. Найм нового працівника на місце старого може призвести до нових витрат на подання оголошення про вакантну посаду, витрат на навчання, а також до зниження продуктивності праці та погіршення морального стану. Наступний перелік ілюструє шляхи, як Загальні принципи NICE підтримує утримання та розвиток талантів у сфері кібербезпеки:

- Організації можуть розробляти кар’єрні шляхи з описом кваліфікації, необхідної для поступово складних та еволюціонуючих наборів робочих ролей як ті, що перелічені в Загальних принципах NICE.
- Детальне вивчення KSA та завдань допоможе існуючому персоналу зрозуміти, які специфічні кроки необхідно зробити для розвитку своїх спроможностей щоб сприяти готовності до бажаної посади.
- Щоб дати можливість персоналу розвивати та використовувати нові навички, організація може запропонувати кадрові ротації.
- Організації можуть визначати персонал, який старанно покращує свої KSA у відповідних сферах, відзначаючи тих, хто працює добре.
- Організації можуть розробляти плани розвитку/вдосконалення персоналу для того, щоб допомогти їм скласти план, як вони можуть отримати KSA, необхідні для нових робочих ролей.
- Можуть бути можливості групових тренінгів для підготовки персоналу до підвищення загальних знань, навичок та здібностей в цих робочих ролях в організації.
- Організації можуть проводити тренінги та іспити, які базуються на специфічних навичках та здібностях у сфері кібербезпеки для оцінки рівня кваліфікації у реальному середовищі.
- Організації можуть використовувати існуючий персонал для задоволення критичних кадрових потреб у сфері кібербезпеки з використанням можливості перегляду резюме наявного персоналу для виявлення тих, хто має бажані KSA.
- Загальні принципи NICE є корисними для існуючого персоналу, які хочуть перейти отримати робочу роль у сфері кібербезпеки з іншої посади. Організація може описати KSA, які необхідні вірогідному працівнику, який має робочу роль, яка не пов’язана зі сферою кібербезпеки, щоб стати частиною персоналу у сфері кібербезпеки, що виконує завдання кібербезпеки.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Розвиток

Організації або сектори можуть використовувати Загальні принципи NICE для розробки необхідних додаткових публікацій або інструментів, які відповідають їхнім потребам, а також для визначення або розроблення настанов стосовно різних аспектів розвитку, планування, тренінгів та освіти персоналу.

Нові тематичні матеріали, які містять перехресні посилання на складові Загальних принципів NICE, будуть доступні на веб-сайті NICE [5].

Нижче наведено кілька прикладів, на основі яких можуть бути розроблені додаткові публікації чи інструменти.

4.1 Компетенції

Управління зайнятості та професійної підготовки Міністерства праці [6] визначає компетенцію як здатність застосовувати або використовувати знання, навички, здібності, поведінку та особисті характеристики для успішного виконання критичних робочих завдань, специфічних функцій або роботи на певній ролі чи посаді. На додаток до переліку технічних KSA, моделі компетентності також враховують поведінкові показники та описують нетехнічні дані, такі як персональна ефективність, академічні та робочі компетенції. Додаткова інформація про ці міркування доступна на сайті Департаменту праці «CareerOneStop» [7].

4.2 Назви посад

Назва посади – це опис роботи чи посади працівника в організації. Відповідність назв посад областям спеціальності або робочим ролям допоможе організаціям використовувати Загальні принципи NICE.

4.3 Методологія та настанови з кібербезпеки

Керівництво з кар’єрного розвитку та планування персоналу «Стратегічна мета NICE № 3» спрямоване на допомогу роботодавцям у намаганні відповідати вимогам ринку та покращувати підбір, найм, розвиток та збереження здібностей у сфері кібербезпеки. Однією з цілей цієї стратегічної мети є публікація та підвищення обізнаності про Загальні принципи NICE та заохочення прийняття. Прийняття в даному випадку означає використання Загальних принципів NICE як довідкового ресурсу для дій, пов’язаних із персоналом у сфері кібербезпеки, тренінгами та освітою.
Один із способів заохочення прийняття Загальних принципів NICE є заохочення авторів керівництва у сфері кібербезпеки або керівних документів посилатись на Загальні принципи NICE. Три приклади публікацій розглянуто у Додатку D.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Додаток А – Перелік складових Загальних принципів NICE

A.1 Категорії персоналу в Загальних принципах NICE

У Таблиці 1 наведений опис кожної Категорії в Загальних принципах NICE. Назва кожної Категорії складає абревіатуру з двох букв (наприклад SP) для швидкого посилання на Категорію та створення ідентифікаторів робочих ролей в Загальних принципах NICE (див. Таблиця 3 – Робочі ролі в Загальних принципах NICE). Перелік буде періодично оновлюватися [1]. Повне джерело останньої версії цього матеріалу можна знайти в електронній довідковій таблиці до NIST Special Publication 800-181 [4].

Таблиця 1 – Категорії персоналу в Загальних принципах NICE.

Категорії	Опис
Забезпечення безпеки (SP)	Концептуалізує, розробляє, та/або створює безпечні системи інформаційних технологій (IT), з відповідальністю за аспекти розвитку системи та/або мережі.
Експлуатація та обслуговування (OM)	Забезпечує підтримку, адміністрування та технічне обслуговування, необхідне для забезпечення ефективної та продуктивної роботи та безпеки системи інформаційних технологій (IT).
Нагляд і корпоративне управління (OV)	Забезпечує керування, управління, спрямування або розвиток та захист, щоб організація могла ефективно проводити заходи з кібербезпеки.
Захист і охорона (PR)	Визначає, аналізує та пом'якшує загрози внутрішнім системам інформаційних технологій (IT) та/або мережам.
Аналіз (AN)	Виконує високо спеціалізований перегляд та оцінку вхідної інформації про кібербезпеку, щоб визначити її корисність для розвідки.
Збір і обробка (CO)	Забезпечує спеціалізовані операції з заборони та дезінформації і збір інформації про кібербезпеку, яка може бути використана для розвитку розвідки.
Розслідування (IN)	Розслідує події кібербезпеки або злочини, пов'язані з системами інформаційних технологій (IT), мережами та цифровими доказами.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

A.2 Області спеціалізації в Загальних принципах NICE

В таблиці 2 наведений опис кожної Області спеціалізації в Загальних принципах NICE. Назва кожної Області спеціалізації містить абревіатуру з трьох букв (наприклад RSK) для швидкого посилання на Область спеціалізації та підтримки створення ідентифікаторів робочих ролей в Загальних принципах NICE (див. Таблиця 3 – Робочі ролі в Загальних принципах NICE). Перелік буде періодично оновлюватися [1]. Остаточне джерело найновішої версії цього матеріалу можна знайти в електронній довідковій таблиці до NIST Special Publication 800-181 [4]

Таблиця 2 – Області спеціалізації в Загальних принципах NICE

Категорії	Області спеціалізації	Опис областей спеціалізації
Забезпечення безпеки (SP)	Управління ризиками (RSK)	Контролює, оцінює та підтримує процеси документування, перевірки, оцінки та авторизації, необхідні для забезпечення того, щоб існуючі та нові системи інформаційних технологій (IT) відповідали критеріям безпеки компанії та вимогам щодо ризиків. Здійснює належне оброблення ризиків, забезпечує відповідність та впевненість з внутрішньої та зовнішньої точки зору.
	Розробка програмного забезпечення (DEV)	Розробляє та створює/програмує нові (або модифікує існуючі) комп'ютерні прикладні програми, програмне забезпечення або спеціальні програми-утиліти відповідно до кращих практик надання впевненості щодо програмного забезпечення.
	Архітектура систем (ARC)	Розробляє концепції системи та працює над фазами спроможностей життєвого циклу розробки систем; перетворює технологію та умови навколишнього середовища (наприклад, законодавчі та нормативні акти) в проекти системи і безпеки та процеси.
	Наукове дослідження технологій (TRD)	Проводить оцінку технології та процеси інтеграції; забезпечує і підтримує спроможності прототипу та/або оцінює його корисність.
	Планування вимог систем (SRP)	Консультується з клієнтами для збору та оцінки функціональних вимог та перетворює ці вимоги в технічні рішення. Надає клієнтам поради щодо застосування інформаційних систем для задоволення бізнес-потреб.
	Тестування та оцінка (TST)	Розробляє та проводить тестування систем для оцінки відповідності специфікаціям та вимогам шляхом застосування принципів та методів економічно ефективного планування, оцінки, перевірки та затвердження технічних, функціональних та експлуатаційних характеристик систем (включаючи операційну сумісність) систем або елементів систем, що інтегрують IT.
	Розробка систем (SYS)	Займається етапами розробки життєвого циклу створення систем.
Експлуатація і обслуговування (OM)	Управління даними (DTA)	Розробляє та адмініструє бази даних та/або системами управління даними, які дозволяють зберігати, запитувати, захищати та використовувати дані.
	Управління знаннями (KMG)	Керує та адмініструє процеси та інструменти, які дозволяють організації ідентифікувати, документувати та отримувати доступ до інтелектуального капіталу та інформаційного контенту.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Категорії	Області спеціалізації	Опис областей спеціалізації
	Обслуговування клієнтів та технічна підтримка (STS)	Вирішує проблеми; встановлює, налаштовує, усуває несправності та забезпечує технічне обслуговування та навчання у відповідності до вимог або запитів клієнтів (наприклад підтримку клієнтів на різних рівнях). Зазвичай надає початкову інформацію про інцидент спеціалісту з Управління інцидентами (IR).
	Обслуговування мереж (NET)	Встановлює, налаштовує, випробовує, експлуатує, обслуговує та управляє мережами та їх брандмауерами, включаючи апаратне забезпечення (наприклад, концентратори, мости, комутатори, мультиплексори, маршрутизатори, кабелі, проксі-сервери та захисні системи розподілу) та програмне забезпечення, що дозволяє розповсюдження та передачу інформації щодо усього спектру транзакцій для підтримки безпеки інформації та інформаційних систем.
	Адміністрування систем (ADM)	Встановлює, налаштовує, усуває несправності та підтримує конфігурації серверів (апаратного та програмного забезпечення), щоб забезпечити їх конфіденційність, цілісність та доступність. Керує обліковими записами, брандмауерами та патчами. Відповідальний за контроль доступу, паролі, а також створення та адміністрування облікового запису.
	Аналіз систем (ANA)	Досліджує наявні комп’ютерні системи та процедури організації і розробляє рішення для інформаційних систем, які допомагають організації працювати більш безпечно, продуктивно та ефективно. Поєднує бізнес та інформаційні технології (IT), розуміючи потреби та обмеження обох.
Нагляд і корпоративне управління (OV)	Юридичний супровід та адвокатура (LGA)	Надає юридично обґрунтовані поради та рекомендації керівництву та персоналу з різних актуальних тем у відповідній предметній сфері. Захищає правові та політичні зміни, і веде справу від імені клієнта за допомогою широкого спектру письмової та усної діяльності, включаючи юридичні документи та судові розгляди.
	Тренінги, освіта та обізнаність (TEA)	Проводить тренінги для персоналу у відповідній предметній області. Розробляє, планує, координує, забезпечує та/або оцінює тренінгові курси, методи та методики.
	Управління кібербезпекою (MGT)	Здійснює нагляд за програмою кібербезпеки інформаційної системи або мережі, включаючи управління наслідками інформаційної безпеки в рамках організації, спеціальну програму або іншу сферу відповідальності, включаючи стратегії, персонал, інфраструктуру, вимоги, політику, планування на випадок надзвичайних ситуацій, обізнаність про безпеку та інші ресурси.
	Стратегічне планування та політика (SPP)	Розробляє політики та плани та/або підтримує зміни у політиці щодо організаційних ініціатив в галузі кіберпростору або необхідних змін/вдосконалення.
	Управління працівниками з кібербезпеки (EXL)	Здійснює нагляд, управляє та/або керує роботою та працівниками, які виконують роботу з кібербезпеки, пов’язану з нею роботу, або проводять кібероперації.
	Управління проектами/програмами (PMA) та закупівля	Застосовує знання даних, інформацію, процеси, взаємодії в організації, навички та аналітичні знання, а також системи, мережі та спроможності інформаційного обміну для управління програмами закупівлі.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Категорії	Області спеціалізації	Опис областей спеціалізації
		Виконує обов'язки корпоративного управління програмами придбання апаратного та програмного забезпечення, інформаційних систем та іншими політиками управління програмами. Забезпечує пряму підтримку закупівлі систем, що використовують інформаційні технології (IT) (включаючи Системи національної безпеки), застосовуючи закони та політику, пов'язані з інформаційними технологіями, та здійснює керівництво в галузі інформаційних технологій протягом усього життєвого циклу закупівлі.
Захист і охорона (PR)	Аналіз захисту кіберпростору (CDA)	Проводить заходи захисту та використовує інформацію, зібрану з різних джерел, для ідентифікації, аналізу та звітування про події, які виникають або можуть виникнути в мережі для захисту інформації, інформаційних систем та мереж від загроз.
	Підтримка інфраструктури захисту кіберпростору (INF)	Тестує, реалізовує, використовує, підтримує, рецензує та адмініструє обладнання та програмне забезпечення інфраструктури, необхідної для ефективного управління мережею та ресурсами постачальників послуг комп'ютерної мережі. Здійснює моніторинг мережі для активного усунення несанкціонованих дій.
	Управління інцидентами (IR)	Реагує на кризові або нагальні ситуації у відповідній області для зменшення негайних та потенційних загроз. Використовує підходи, спрямовані на пом'якшення наслідків, підготовленості, реагування та відновлення, коли це потрібно, для виживання, збереження власності та інформаційної безпеки. Досліджує та аналізує всі відповідні заходи з реагування.
	Оцінка та управління вразливостями (VAM)	Здійснює оцінку загроз та вразливостей; визначає відхилення від прийнятних конфігурацій, корпоративної або локальної політики; оцінює рівень ризику; а також розробляє та/або рекомендує відповідні контрзаходи щодо пом'якшення наслідків в операційних та неопераційних ситуаціях.
Аналіз (AN)	Аналіз загроз (TWA)	Визначає та оцінює спроможності та діяльність кримінальних злочинців у сфері кібербезпеки або іноземних розвідувальних служб; готує висновки, які допомагають ініціалізувати або підтримувати правоохоронні та контррозвідувальні розслідування чи заходи.
	Аналіз вразливостей (EXP)	Аналізує зібрану інформацію для виявлення вразливостей та потенціалу для експлуатації.
	Аналіз даних з різних джерел (ASA)	Аналізує інформацію про загрози з різних джерел, напрямків та агентств у розвідувальному співтоваристві. Синтезує та розглядає розвідувальну інформацію в контексті; обмірковує можливі наслідки.
	Цілі (TGT)	Застосовує наявні знання про один або декілька регіонів, країни, недержавні організації та/або технології.
	Мовний аналіз (LNG)	Здійснює мовну, культурну та технічну експертизу для підтримки збору інформації, аналізу та іншої діяльності з кібербезпеки.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Категорії	Області спеціалізації	Опис областей спеціалізації
Збір і обробка (CO)	Збір інформації (CLO)	Збирає інформацію за допомогою відповідних стратегій та в межах пріоритетів, встановлених в процесі управління збором.
	Планування кібероперацій (OPL)	Здійснює поглиблене комплексне визначення цілей та планування системи захисту. Збирає інформацію та розробляє детальні операційні плани та розпорядження за вимогою. Здійснює стратегічне та операційне планування по всім операціям для інтеграції інформації та операцій в кіберпросторі.
	Кібероперації (OPS)	Здійснює заходи зі збору доказів щодо кримінальних та іноземних розвідувальних органів з метою пом’якшення можливих або реальних загроз, захисту від шпигунства чи інсайдерської загрози, іноземного саботажу, міжнародної терористичної діяльності або для підтримки іншої розвідувальної діяльності.
Розслідування (IN)	Кіберрозслідування (INV)	Застосовує тактики, методики та процедури повного спектру засобів і процесів розслідування, що включають в себе, але не обмежуються, методи інтерв’ю та допиту, розвідки, контррозвідки і виявлення спостереження, та належним чином збалансовує переваги обвинувачення проти збору розвідувальних даних.
	Цифрова криміналістика (FOR)	Збирає, обробляє, зберігає, аналізує та надає докази, пов’язані з комп’ютерною технікою, для підтримки зменшення вразливостей мережі та/або для кримінальних, шахрайських, контррозвідувальних або правоохоронних розслідувань.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

A.3 Робочі ролі в рамках Загальних принципів NICE

У Таблиці 3 наведений опис кожної робочої ролі в Загальних принципах NICE Кожна робоча роль ідентифікується за Категорією та областю спеціалізації та супроводжується порядковим номером (наприклад, SP-RSK-001 – це перша робоча роль в категорії SP та області спеціалізації RSK). Деякі описи робочої ролі взяті із зовнішніх джерел (наприклад, Інструкції Комітету з систем національної безпеки [CNSSI] 4009) та включають інформацію про таке джерело у стовпчику опису. Перелік буде періодично оновлюватися [1]. Остаточне джерело найновішої версії цього матеріалу можна знайти в електронній довідковій таблиці до NIST Special Publication 800-181 [4].

Таблиця 3 – Робочі ролі в Загальних принципах NICE

Категорія	Область спеціалізації	Робоча роль	Ідентифікатор робочої ролі	Опис робочої ролі
Надійне забезпечення (SP)	Управління ризиками (RSK)	Уповноважений офіційний представник/Призначена особа	SP-RSK-001	Вища посадова чи виконавча особа, що має повноваження офіційно взяти на себе відповідальність за управління інформаційною системою на прийнятному рівні ризику для операцій організації (включаючи місію, функції, імідж чи репутацію), організаційних активів, фізичних осіб, інших організацій та нації в цілому (CNSSI 4009).
		Експерт з оцінки контролів безпеки	SP-RSK-002	Здійснює незалежну комплексну оцінку управлінського, операційного та технічного контролю безпеки і покращення контролю, які використовуються в системі інформаційних технологій (IT) для визначення загальної ефективності заходів контролю (як визначено в NIST 800-37).
	Розробка програмного забезпечення (DEV)	Розробник програмного забезпечення	SP-DEV-001	Розробляє, створює, обслуговує та пише/програмує нові (або модифікує існуючі) комп'ютерні прикладні програми, програмне забезпечення або спеціальні утиліти.
		Експерт з безпеки програмного забезпечення	SP-DEV-002	Аналізує безпеку нових або існуючих комп'ютерних прикладних програм, програмного забезпечення або спеціалізованих програм-утиліт та забезпечує дієві результати.
	Системна архітектура (ARC)	Корпоративний архітектор	SP-ARC-001	Розробляє та супроводжує бізнес-, системні та інформаційні процеси для підтримки потреб підприємства; розробляє правила та вимоги до інформаційних технологій (IT), що описують базові та цільові архітектури.
		Архітектор безпеки	SP-ARC-002	Забезпечує, що вимоги безпеки зацікавлених сторін, необхідні для захисту місії організації та бізнес-процесів, належним чином враховуються в усіх аспектах архітектури підприємства, включаючи еталонні моделі, архітектури сегментів та рішень, а також системи для підтримки цих місій та бізнес-процесів.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Категорія	Область спеціалізації	Робоча роль	Ідентифікатор робочої ролі	Опис робочої ролі
	Наукове дослідження технологій (TRD)	Спеціаліст з науково-дослідних робіт	SP-TRD-001	Досліджує інжиніринг програмного забезпечення та систем, а також досліджує програмні системи для розробки нових можливостей, забезпечуючи повне впровадження кібербезпеки. Проводить комплексне дослідження технологій для оцінки потенційних вразливостей в системах кіберпростору.
	Планування вимог до систем (SRP)	Спеціаліст з планування вимог до систем	SP-SRP-001	Консультується з клієнтами для оцінки функціональних вимог та переведення функціональних вимог у технічні рішення.
	Тестування і оцінка (TST)	Спеціаліст з тестування та оцінки систем	SP-TST-001	Планує, готує та проводить тестування систем для оцінки відповідності специфікаціям та вимогам, а також аналізує/звітує щодо результатів тестування.
	Розробка систем (SYS)	Розробник системи безпеки інформаційних систем	SP-SYS-001	Проектує, розробляє, тестує та оцінює безпеку інформаційної системи протягом всього життєвого циклу розробки систем.
		Розробник систем	SP-SYS-002	Проектує, розробляє, тестує та оцінює інформаційну систему протягом всього життєвого циклу розробки систем.
Експлуатація і обслуговування (OM)	Управління даними (DTA)	Адміністратор бази даних	OM-DTA-001	Адмініструє бази даних та/або системи управління базами даних, які дозволяють безпечно зберігати, запитувати, захищати та використовувати дані.
		Спеціаліст з аналізу даних	OM-DTA-002	Досліджує дані з різних джерел з метою забезпечення обізнаності щодо безпеки та приватності. Проектує та впроваджує користувацькі алгоритми, робочі процеси та макети для складних корпоративних масивів даних, що використовуються для моделювання, пошуку даних та дослідницьких цілей.
	Управління знаннями (KMG)	Адміністратор бази знань	OM-KMG-001	Відповідальний за управління та адміністрування процесів та інструментів, які дозволяють організації ідентифікувати, документувати та отримувати доступ до інтелектуального капіталу та інформаційного контенту.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Категорія	Область спеціалізації	Робоча роль	Ідентифікатор робочої ролі	Опис робочої ролі
	Обслуговування клієнтів та технічна підтримка (STS)	Спеціаліст з технічної підтримки	OM-STS-001	Надає технічну підтримку клієнтам, які потребують допомоги з використанням апаратного та програмного забезпечення на рівні клієнта відповідно до встановлених або затверджених компонентів організаційного процесу (наприклад, Генерального Плану управління інцидентами, якщо такий передбачений).
	Обслуговування мереж (NET)	Спеціаліст з мережевих операцій	OM-NET-001	Планує, впроваджує та експлуатує мережеві служби/системи, включаючи апаратне забезпечення та віртуальні середовища.
	Адміністрування систем (ADM)	Адміністратор системи	OM-ADM-001	Відповідає за встановлення та підтримку системи або конкретних компонентів системи (наприклад, встановлення, конфігурування та оновлення апаратного та програмного забезпечення, створення та управління обліковими записами користувачів, нагляд або виконання резервного копіювання та відновлення, впровадження оперативного та технічного контролів безпеки; і дотримання політик та процедур безпеки організації).
	Аналіз систем (ANA)	Аналітик з безпеки систем	OM-ANA-001	Відповідальний за аналіз та розвиток процесів інтеграції, тестування, експлуатації та підтримки систем безпеки.
Нагляд і корпоративне управління (OV)	Юридичний супровід та адвокатура (LGA)	Юрисконсульт з інформаційного права	OV-LGA-001	Надає юридичну консультацію та рекомендації з актуальних питань, пов’язаних з інформаційним правом.
		Уповноважений з питань приватності /Менеджер з питань відповідності приватності	OV-LGA-002	Розробляє та здійснює нагляд за програмами забезпечення приватності та персоналом програми приватності, підтримуючи дотримання вимог приватності, умови корпоративного управління /політики, а також процеси управління інцидентами відповідно до потреб виконавчих керівників з приватності та безпеки, а також їхніх команд.
	Підготовка, освіта та обізнаність (TEA)	Розробник навчальної програми з кібербезпеки	OV-TEA-001	Розробляє, планує, координує та оцінює навчальні/тренінгові курси, методи та методики навчання у сфері кібербезпеки відповідно до навчальних потреб.
		Викладач сфери кібербезпеки	OV-TEA-002	Розробляє програму та проводить тренінги або навчання персоналу з кібербезпеки..

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Категорія	Область спеціалізації	Робоча роль	Ідентифікатор робочої ролі	Опис робочої ролі
	Управління кібербезпекою (MGT)	Менеджер з безпеки інформаційних систем	OV-MGT-001	Відповідальний за кібербезпеку програми, організації, системи або замкнутої групи.
		Менеджер з безпеки комунікацій (COMSEC)	OV-MGT-002	Особа, яка керує ресурсами безпеки комунікацій (COMSEC) в організації (CNSSI 4009) або ключовий розпорядник Системи управління криптографічним ключем (CKMS).
	Стратегічне планування та політика (SPP)	Розробник та менеджер персоналу у сфери кібербезпеки	OV-SPP-001	Розробляє плани, стратегії та методологію з кібербезпеки для підтримки особового складу робочої сили, персоналу, вимог до навчання та освіти та врахування змін в політиці, доктрині, матчастині, структурі з сил та вимогах щодо освіти та навчання кадрів.
		Спеціаліст зі стратегічного планування та кіберполітики	OV-SPP-002	Розробляє та підтримує плани, стратегії та політики у сфері кібербезпеки для підтримки та узгодження з ініціативами організації у сфері кібербезпеки та дотриманням регуляторних вимог.
	Виконавчий керівник з кібербезпеки (EXL)	Виконавчий керівник з кібербезпеки	OV-EXL-001	Розробляє та підтримує плани, стратегії та політики з і кібербезпеки для підтримки та узгодження з організаційними ініціативами з кібербезпеки та законодавством.
	Управління проектами/програмами (PMA) та закупівля	Менеджер програм	OV-PMA-001	Керує, координує, спілкується, інтегрує та відповідає за загальний успіх програми, забезпечуючи її узгодження з пріоритетами агентства чи підприємства.
		Менеджер IT проектів	OV-PMA-002	Безпосередньо керує проектами інформаційних технологій.
		Менеджер з підтримки продукту	OV-PMA-003	Керує набором функцій підтримки, необхідних для роботи та забезпечення готовності та операційної спроможності систем та компонентів.
		Керівник портфелю IT-інвестицій	OV-PMA-004	Управляє портфелем IT-інвестицій, який узгоджуються з загальними потребами місії та пріоритетами підприємства.
		Аудитор програми IT	OV-PMA-005	Здійснює оцінку програми IT або її окремих компонентів для визначення відповідності опублікованим стандартам.
Захист та охорона (PR)	Аналіз захисту кіберпростору (CDA)	Аналітик захисту кіберпростору	PR-CDA-001	Використовує дані, зібрані за допомогою різних інструментів кіберзахисту (наприклад, сповіщення системи виявлення атак, брандмауери, логи мережевого трафіку) для аналізу подій, що відбуваються в середовищах з метою пом’якшення загроз.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Категорія	Область спеціалізації	Робоча роль	Ідентифікатор робочої ролі	Опис робочої ролі
	Підтримка інфраструктури захисту кіберпростору (INF)	Спеціаліст з підтримки інфраструктури захисту кіберпростору	PR-INF-001	Тестує, впроваджує, розгортає, підтримує та адмініструє інфраструктурне обладнання та програмне забезпечення.
	Управління інцидентами (IR)	Спеціаліст з управління інцидентами у сфері кібербезпеки	PR-CIR-001	Досліджує, аналізує та реагує на кіберінциденти в рамках мережевого середовища або замкненої групи.
	Оцінка та управління вразливостями (VAM)	Аналітик з оцінки вразливостей	PR-VAM-001	Виконує оцінки систем та мереж у межах NE або замкненої групи та визначає, де ці системи/мережі відхиляються від прийнятних конфігурацій, політик замкненої групи чи локальних політик. Вимірює результативність ешелонованого захисту щодо відомих вразливостей.
Аналіз (AN)	Аналіз загроз (TWA)	Аналітик загроз/попереджень	AN-TWA-001	Розробляє кібер-показники для забезпечення обізнаності щодо стану високо динамічного операційного середовища. Збирає, обробляє, аналізує та поширює оцінки кіберзагрози/попереджень.
	Аналіз експлуатації (EXP)	Аналітик з експлуатації	AN-EXP-001	Співпрацює над виявленням пробілів у доступі та зборі даних, які можна заповнити за допомогою заходів зі збору та/або підготовки в кіберпросторі. Використовує всі дозволені ресурси та методи аналізу для проникнення в мережі цілі.
	Аналіз даних з різних джерел (ASA)	Аналітик даних з різних джерел	AN-ASA-001	Аналізує дані/ інформацію з одного або декількох джерел для підготовки середовища, відповідає на запити щодо інформації та подає на розгляд вимоги щодо збору та добування розвідданих для забезпечення планування і здійснення операцій.
		Спеціаліст з оцінки місії	AN-ASA-002	Розробляє плани оцінки та показники продуктивності /ефективності. Проводить стратегічну та операційну оцінки ефективності кіберподій. Визначає чи працюють системи належним чином та забезпечу\ вхідні дані для визначення операційної ефективності очікуванням.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Категорія	Область спеціалізації	Робоча роль	Ідентифікатор робочої ролі	Опис робочої ролі
	Аналіз цілей (TGT)	Розробник цілей	AN-TGT-001	Виконує аналіз цільової системи, створює та/або підтримує електронні папки цілі для включення вхідних даних з підготовки середовища та/або джерел внутрішньої або зовнішньої розвідки. Координує свої дії з партнерською діяльністю по цілі та розвідувальними організаціями та пропонує на затвердження і перевірку потенційні цілі.
		Аналітик мережі цілі	AN-TGT-002	Здійснює поглиблений аналіз збору даних та даних з відкритих джерел для забезпечення безперервності цілей, для профілювання цілей та їх діяльності; і розробляє методи отримати більше інформації про цілі. Визначає, як цілі спілкуються, рухаються, діють і живуть, базуючись на знаннях технологій, цифрових мереж та програм цілей.
	Мовний аналіз (LNG)	Багатопрофільний мовний аналітик	AN-LNG-001	Застосовує експертизу щодо мови та культури цілей/загроз та технічні знання для обробки, аналізу та/або розповсюдження розвідувальної інформації, отриманої з мовних, голосових та/або графічних матеріалів. Створює та підтримує лінгвоспецифічні бази даних та допоміжні засоби для підтримки виконання діяльності з кібербезпеки та забезпечення обміну критичними знаннями. Забезпечує предметну експертизу у інтенсивах проектах з іноземною мовою або міждисциплінарних проектах
Збір і обробка (CO)	Збір інформації (CLO)	Менеджер зі збору даних з різних джерел	CO-CLO-001	Визначає відомства зі збору даних та середовище; включає пріоритетні вимоги до інформації в систему управління збором даних; розробляє концепції для задоволення намірів керівництва. Визначає можливості наявних засобів розвідки, нові можливості збору даних; та будує і поширює плани зі збору даних. Контролює виконання завдання зі збору даних та забезпечує ефективне виконання плану зі збору даних.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Категорія	Область спеціалізації	Робоча роль	Ідентифікатор робочої ролі	Опис робочої ролі
		Менеджер з розробки вимог до збору даних з різних джерел	CO-CLO-002	Оцінює операції зі збору даних та розробляє стратегії вимог до збору даних з точки зору їхнього результату з використанням доступних ресурсів та методів покращення збору. Розробляє, підтримує, затверджує та координує подання вимог до збору даних. Оцінює продуктивність активів збору даних та операційну діяльність зі збору даних.
	Планування кібероперацій (OPL)	Спеціаліст з планування кіберрозвідки	CO-OPL-001	Розробляє детальні плани розвідки для задоволення вимог кібероперацій. Співпрацює зі спеціалістами з планування кібероперацій з метою визначення, затвердження та застосування вимог до збору та аналізу. Бере участь у виборі цілей, затвердженні, синхронізації та виконанні кібердій. Синхронізує заходи розвідки для підтримки цілей організації в кіберпросторі.
		Спеціаліст з планування кібероперацій	CO-OPL-002	Розробляє детальні плани проведення або підтримки відповідного діапазону кібероперацій за допомогою співпраці з іншими спеціалістами з планування, операторами та/або аналітиками. Бере участь у виборі цілей, затвердженні, синхронізації та інтеграції під час виконання кіберзаходів.
		Спеціаліст з планування партнерської інтеграції	CO-OPL-003	Працює над поглибленням співпраці між партнерами з кібероперацій через організаційні або національні кордони. Сприяє інтеграції партнерських кібергруп, надаючи настанови, ресурси, допомогу у розробці кращих практик та сприяння організаційної підтримки для досягнення цілей у інтегрованих кібердіях
	Кібероперації (OPS)	Кібероператор	CO-OPS-001	Здійснює збір, обробку та/або геолокацію систем для експлуатації, пошуку та/або відстеження цілей, що представляють інтерес. Виконує мережеву навігацію, тактичний криміналістичний аналіз і, у випадку поставленої задачі, виконує операції в мережі.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Категорія	Область спеціалізації	Робоча роль	Ідентифікатор робочої ролі	Опис робочої ролі
Розслідування (IN)	Кіберрозслідування (INV)	Слідчий кіберзлочинів	IN-INV-001	Визначає, збирає, аналізує та зберігає докази, використовуючи контрольовані та документально підтверджені аналітичні та слідчі методики.
	Цифрова криміналістика (FOR)	Експерт-криміналіст судової експертизи/контррозвідки	IN-FOR-001	Проводить детальні розслідування комп'ютерних злочинів, встановлює документальні чи фізичні докази, включаючи цифрові носії та лог-журнали, пов'язані з інцидентами вторгнення в кіберпростір..
		Експерт-криміналіст сфери кібербезпеки	IN-FOR-002	Аналізує цифрові докази та досліджує інциденти, пов'язані з безпекою комп'ютерів, для отримання корисної інформації з метою зменшення системної/ мережевої уразливості.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

A.4 Завдання в Загальних принципах NICE

У таблиці 4 наведено перелік всіх завдань, які були визначені у якості частина робочої ролі у сфері кібербезпеки. Кожна робоча роль містить підмножину задач, перерахованих тут. Перелік періодично оновлюватиметься [1]. Остаточне джерело найновішої версії цього матеріалу можна знайти в електронній довідковій таблиці до NIST Special Publication 800-181 [4].

Таблиця 4 – Завдання в Загальних принципах NICE

Ідентифікатор завдання	Опис завдання
T0001	Знаходити та управляти необхідними ресурсами, включаючи підтримку керівництва, фінансові ресурси та ключовий персонал з питань безпеки для сприяння досягненню цілей та завдань безпеки інформаційних технологій (IT) та зниження загального ризику організації.
T0002	Знаходити необхідні ресурси, включаючи фінансові, для забезпечення безперервності функціонування операційних програм підприємства.
T0003	Консультувати вище керівництво (наприклад, директора з інформаційних технологій [CIO]) щодо рівня ризику та стану безпеки.
T0004	Консультувати вище керівництво (наприклад, CIO) щодо аналізу витрат/вигоди програм, політик, процесів, систем та елементів інформаційної безпеки.
T0005	Консультувати відповідне вище керівництво або уповноважених представників щодо змін, які впливають на стан кібербезпеки в організації.
T0006	Захищати позицію організації в судах та законодавчих процесах.
T0007	Аналізувати та визначати вимоги до даних та специфікацій.
T0008	Аналізувати та планувати очікувані зміни у вимогах щодо об’єму даних.
T0009	Аналізувати інформацію з метою визначення, рекомендацій та планування розробки нової прикладної програми або модифікації існуючої прикладної програми.
T0010	Аналізувати політику та конфігурації кіберзахисту організації та оцінювати відповідність нормативним актам та директивам організації.
T0011	Аналізувати потреби користувачів і вимоги до програмного забезпечення з метою визначення можливості розроблення в рамках обмеженого часу та витрат.
T0012	Аналізувати проектні обмеження, аналізувати компроміси та детальний проект системи та безпеки, а також розглядати підтримку життєвого циклу.
T0013	Застосовувати стандарти програмування та тестування, використовувати засоби тестування безпеки, зокрема «нечіткі» інструменти сканування коду методом статичного аналізу та здійснювати перевірку коду.
T0014	Застосовувати безпечну документацію коду.
T0015	Застосовувати політики безпеки до прикладних програм, які взаємодіють одна з одною, наприклад, прикладних програм таких як Business-to-Business (B2B).
T0016	Застосовувати політики безпеки для досягнення цілей безпеки системи.
T0017	Застосовувати сервіс-орієнтовані принципи архітектури безпеки, щоб задовольнити вимоги конфіденційності, цілісності та доступності організації.
T0018	Оцінювати ефективність заходів з кібербезпеки, які використовуються системою (системами).
T0019	Оцінювати загрози та вразливості комп’ютерної системи (систем) для розробки профілю ризику безпеки.
T0020	Розробляти контент для інструментів кіберзахисту.
T0021	Будувати, тестувати та модифікувати прототипи продуктів за допомогою робочих моделей або теоретичних моделей.
T0022	Здійснювати управління засобами контролю безпеки, які використовуються на етапі визначення вимог з метою інтеграції системи безпеки в процес, визначення ключових цілей безпеки, максимізації безпеки програмного забезпечення та мінімізації порушень планів і розкладів.
T0023	Характеризувати та аналізувати мережевий трафік з метою виявлення аномальної активності та потенційних загроз мережевим ресурсам.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор завдання	Опис завдання
T0024	Збирати та підтримувати дані, необхідні для забезпечення звітності про стан системи кібербезпеки.
T0025	Повідомляти вартість безпеки інформаційних технологій (IT) зацікавленим сторонам організації на всіх рівнях.
T0026	Складати та писати документацію щодо розробки програми, а також формувати нові редакції, додаючи коментарі до закодованих інструкцій, щоб користувачі могли зрозуміти як функціонує програма.
T0027	Проводити аналіз лог -файлів, доказів та іншої інформації для визначення найкращих методів виявлення злочинця (ів), які вторгаються в мережу.
T0028	Здійснювати та/або підтримувати дозволене тестування на проникнення до активів корпоративної мережі.
T0029	Проводити функціональне та з'єднувальне тестування для забезпечення безперервної працездатності системи.
T0030	Проводити інтерактивні тренінгові вправи для створення ефективного навчального середовища.
T0031	Опитувати потерпілих та свідків і допитувати підозрюваних.
T0032	Проводити оцінки впливу приватності (PIA) проекту безпеки прикладних програм для відповідних контролів безпеки, що захищає конфіденційність та цілісність персональних ідентифікаційних даних (PII).
T0033	Здійснювати аналіз ризиків, дослідження здійсненності та/або компромісний аналіз для розробки, документування та вдосконалення функціональних вимог та специфікацій.
T0034	Співпрацювати із системними аналітиками, інженерами, програмістами тощо, з метою розробки прикладних програм та отримання інформації про обмеження та можливості проекту, вимог до продуктивності та інтерфейсів.
T0035	Налаштовувати та оптимізовувати мережеві концентратори, маршрутизатори та комутатори (наприклад, протоколи верхнього рівня, тунелювання).
T0036	Підтверджувати відомі факти проникнення та добувати нову інформацію, якщо це можливо, після виявлення проникнення за допомогою динамічного аналізу.
T0037	Створювати шляхи доступу до інформації (наприклад, сторінки посилання), щоб полегшити доступ кінцевим користувачам.
T0038	Розробляти модель загрози, базуючись на опитуваннях та вимогах клієнтів.
T0039	Консультуватись з клієнтами з метою оцінки функціональних вимог.
T0040	Консультуватись з інженерним персоналом для оцінки інтерфейсу між апаратним та програмним забезпеченням.
T0041	Координувати та надавати експертну технічну підтримку технічним спеціалістам з кіберзахисту в масштабах усієї організації для управління інцидентами у сфері кіберзахисту.
T0042	Координувати свої дії з аналітиками системи захисту кіберпростору для управління та адміністрування оновлень правил та сигнатур (наприклад, систем виявлення проникнення /захисту, антивірусу та чорних списків) для спеціалізованих прикладних програм у сфері кіберзахисту.
T0043	Координувати свої дії з корпоративним персоналом кібербезпеки для перевірки мережевих попереджень.
T0044	Співпрацювати із зацікавленими сторонами з метою забезпечення безперервної діяльності організації в рамках програми, стратегії та виконання завдань.
T0045	Координувати свої дії з системними архітекторами та розробниками, якщо це необхідно, з метою забезпечення нагляду за розробкою проектних рішень.
T0046	Виправляти помилки, вносити відповідні зміни та здійснювати повторну перевірку програми для забезпечення отримання бажаних результатів.
T0047	Зіставляти дані про інциденти для виявлення конкретних вразливостей та надання рекомендацій для якомога швидшого відновлення роботи.
T0048	Створювати дублікати доказів (наприклад, криміналістичного образу) з гарантією виключення ненавмисних змін оригінальних доказів з метою використання їх у процесі відновлення даних та аналізу. Такі дублікати включають, але не обмежуються, жорсткі диски, дискети, компакт-диски, КПК, мобільні телефони, GPS та всі формати стрічок
T0049	Розшифровувати вилучені дані за допомогою технічних засобів.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор завдання	Опис завдання
T0050	Визначати та пріоритезувати суттєві спроможності систем або бізнес-функцій, необхідних для часткового або повного відновлення системи після її повної відмови.
T0051	Визначити відповідні рівні доступності системи на основі критичних функцій системи та переконатися, що системні вимоги визначають відповідні вимоги відновлення після аварії та безперервність операцій, включаючи будь-які відповідні вимоги щодо аварійного переходу /альтернативного сайту, вимоги до резервного копіювання та вимоги до забезпечення матеріальної підтримки для відновлення\реставрації системи.
T0052	Визначати масштаб проекту та цілі відповідно до вимог замовника.
T0053	Проектувати та розробляти продукти кібербезпеки та продукти, які сприяють кібербезпеці.
T0054	Розробляти групові політики та переліки контролю доступу для забезпечення відповідності стандартам організації, бізнес-правилам та потребам.
T0055	Проектувати апаратне забезпечення, операційні системи та прикладне програмне забезпечення для належного дотримання вимог кібербезпеки.
T0056	Розробляти або інтегрувати відповідні резервні спроможності у загальні проекти системи та забезпечувати відповідні технічні та процедурні процеси для безпечного резервного копіювання системи та захищеного зберігання резервних даних.
T0057	Проектувати, розробляти та модифікувати програмні системи, використовуючи науковий аналіз та математичні моделі для прогнозування та вимірювання результатів та наслідків проекту.
T0058	Визначати рівень впевненості розроблених можливостей на основі результатів тестування.
T0059	Розробити план розслідування потенційного злочину, порушення або підозрілої активності з використанням комп'ютерів та Інтернету.
T0060	Розвивати розуміння потреб та вимог кінцевих користувачів інформації.
T0061	Розробляти та направляти на розгляд процедури тестування та затвердження системи і документацію.
T0062	Розробляти та документувати вимоги, властивості та обмеження для процедур проектування та процесів.
T0063	Розробляти та документувати стандартні операційні процедури адміністрування систем.
T0064	Переглядати та затверджувати програми, процеси і вимоги щодо збору та зберігання даних.
T0065	Розробляти та впроваджувати процедури резервного копіювання та відновлення мережі.
T0066	Розробляти та підтримувати стратегічні плани.
T0067	Розробляти архітектури або компоненти системи відповідно до технічних умов.
T0068	Розробляти стандарти даних, політики та процедури.
T0069	Розробляти детальну проектну документацію з безпеки для специфікацій компонентів та інтерфейсів з метою підтримки проекту та розробки системи.
T0070	Розробляти плани аварійного відновлення та безперервності операцій для систем, що розробляються, та забезпечувати тестування систем до їхнього вводу у продуктивне середовище.
T0071	Розробляти/інтегрувати проекти з кібербезпеки для систем та мереж із багаторівневими вимогами безпеки або вимогами для обробки кількох рівнів класифікації даних, що застосовуються головним чином до державних організацій (наприклад, некваліфіковані, таємні та особливої важливості).
T0072	Розробляти методи моніторингу та оцінки ризиків, відповідності та зусиль щодо надання впевненості.
T0073	Розробляти нові або визначати існуючі матеріали для обізнаності та тренінгів, що підходять для цільових аудиторій.
T0074	Розробляти політику, програми та настанови для подальшого впровадження.
T0075	Надавати технічне резюме висновків відповідно до встановлених процедур звітування.
T0076	Розробляти стратегії зменшення ризиків для усунення вразливостей та рекомендувати, у випадку необхідності, зміни заходів безпеки у системі або системних компонентах.
T0077	Розробляти безпечний код та засоби обробки помилок.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор завдання	Опис завдання
T0078	Розробляти спеціальні контрзаходи з кібербезпеки та стратегії пом’якшення ризиків для систем та/або прикладних програм.
T0079	Розробляти специфікації, щоб переконатись, що зусилля щодо ризиків, ступені відповідності та надання впевненості відповідають вимогам безпеки, стійкості та надійності на рівні програмного забезпечення, системи та мережевого середовища.
T0080	Розробляти плани тестувань відповідно до специфікацій та вимог.
T0081	Діагностувати проблеми підключення до мережі.
T0082	Документувати та приводити у відповідність інформаційну безпеку організації, архітектуру кібербезпеки та вимоги техніки безпеки системи протягом всього життєвого циклу закупівлі.
T0083	Готувати звіти про попередні або залишкові ризики у сфері безпеки для роботи системи.
T0084	Застосовувати процеси управління безпечною конфігурацією.
T0085	Переконатися, що усі операції з безпеки та їх технічна підтримка належним чином задокументовані та оновлюються в разі необхідності.
T0086	Забезпечувати відповідність застосування патчів безпеки для інтегрованих у систему комерційних продуктів часовим рамкам, встановленим органом управління для призначеного операційного середовища.
T0087	Переконатися, що забезпечується дотримання ланцюга забезпечення схоронності для всіх цифрових носіїв, отриманих відповідно до Федеральних правил про докази.
T0088	Переконатися, що забезпечується зменшення встановленого ризику до прийнятного рівня за допомогою продуктів, які сприяють кібербезпеці, або інших компенсуючих технологій контролю безпеки.
T0089	Переконатися, що дії з покращення безпеки належним чином оцінюються, затверджуються та впроваджуються в разі необхідності.
T0090	Переконатися, що придбані або розроблені система (и) та архітектура (и) відповідають настановам з архітектури кібербезпеки в організації.
T0091	Переконатися, що перевірки, тести та перегляди у сфері кібербезпеки узгоджуються з мережевим середовищем.
T0092	Переконатися, що вимоги з кібербезпеки інтегровані в планування безперервного функціонування системи та/або організації (й).
T0093	Переконатися, що можливості захисту та виявлення набуті за допомогою інженерного підходу ІС та узгоджуються з архітектурою кібербезпеки на рівні організації.
T0094	Встановлювати та підтримувати канали зв’язку з зацікавленими сторонами.
T0095	Створювати загальну архітектуру інформаційної безпеки підприємства (EISA) за загальною стратегією безпеки організації.
T0096	У разі необхідності, встановлювати зв’язки між командою з управління інцидентами та іншими групами, як внутрішніми (наприклад, юридичним відділом), так і зовнішніми (наприклад, правоохоронними органами, постачальниками, фахівцями зі зв’язку з громадськістю).
T0097	Оцінювати та затверджувати програми розвитку для забезпечення належного встановлення базових засобів безпеки.
T0098	Оцінювати контракти з метою забезпечення відповідності фінансовим, юридичним та програмним вимогам.
T0099	Оцінювати витрати-вигоду, економічний аналіз та аналіз ризиків у процесі прийняття рішень.
T0100	Оцінювати такі фактори, як необхідні формати звітів, обмеження вартості та необхідність обмеження безпеки для визначення конфігурації апаратного забезпечення.
T0101	Оцінювати ефективність та комплексність існуючих програм тренінгів.
T0102	Оцінювати ефективність законів, правил, політик, стандартів чи процедур.
T0103	Вивчати відновлені дані для отримання інформації стосовно проблеми.
T0104	Об’єднувати аналізи атак на комп’ютерні мережі з кримінальними та контррозвідувальними розслідуваннями і операціями.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор завдання	Опис завдання
T0105	Визначати компоненти чи елементи, розподіляти функції безпеки для цих елементів і описувати взаємозв'язок між елементами.
T0106	Визначати альтернативні стратегії інформаційної безпеки для дотримання цілей організаційної безпеки.
T0107	Визначати та скеровувати виправлення технічних проблем, що виникають при тестуванні та впровадженні нових систем (наприклад, ідентифікувати та знаходити тимчасові рішення для несумісних протоколів зв'язку).
T0108	Ідентифікувати та надавати перевагу критичним бізнес-функціям у співпраці з зацікавленими сторонами організації
T0109	Визначати та пріоритезувати основні системні функції або підсистеми, необхідним для підтримки основних можливостей або бізнес-функцій з метою відновлення або поновлення після відмови системи або під час відновлення системи на основі загальних системних вимог щодо безперервності та доступності.
T0110	Ідентифікувати та/або визначати, чи випадок порушення безпеки є випадком порушення законодавства, що вимагає відповідних юридичних дій.
T0111	Визначати основні загальні недоліки кодування на високому рівні.
T0112	Визначати дані або інформацію доказового значення для підтримки контррозвідки та кримінальних розслідувань.
T0113	Визначати цифрові докази для вивчення та аналізу таким чином, щоб уникнути ненавмисних змін.
T0114	Визначати елементи доказу злочину.
T0115	Визначати наслідки застосування нових технологій або оновлень у програмах захисту інформаційних технологій (IT).
T0116	Визначати зацікавлених сторін організаційної політики.
T0117	Визначати наслідки порушення безпеки та застосовувати методології в рамках централізованого та децентралізованого середовища в комп'ютерних системах підприємства в процесі розробки програмного забезпечення.
T0118	Визначати проблеми безпеки у процесі стабільної роботи та управління програмним забезпеченням та вживати заходи безпеки, коли життєвий цикл продукту закінчується.
T0119	Визначати, оцінювати та рекомендувати продукти системи кібербезпеки або продукти, що сприяють кібербезпеці, для використання в системі, і гарантувати, що рекомендовані продукти відповідають організаційним вимогам щодо їхньої оцінки та затвердження.
T0120	Визначати, збирати та використовувати документальні чи фізичні докази, включаючи цифрові носії та журнали, пов'язані з інцидентами вторгнення в кіберсередовище, розслідуваннями та операціями.
T0121	Впроваджувати нові процедури проектування системи, процедури тестування та стандарти якості.
T0122	Впроваджувати проекти системи безпеки для нових або існуючих систем.
T0123	Впроваджувати для систем та/або програм спеціальні контрзаходи з кібербезпеки.
T0124	Включати рішення щодо вразливості системи у проекти систем (наприклад, Сповіщення про вразливість системи кібербезпеки).
T0125	Встановлювати та підтримувати програмне забезпечення операційної системи пристрою мережі інфраструктури (наприклад, вбудоване програмне забезпечення IOS).
T0126	Встановлювати або замінювати мережеві концентратори, маршрутизатори та комутатори.
T0127	Інтегрувати та узгоджувати політики в галузі інформаційної безпеки та/або кібербезпеки для забезпечення відповідності системного аналізу вимогам безпеки.
T0128	Інтегрувати можливості автоматичного оновлення або патчей системного програмного забезпечення, де це можливо, і розробляти процеси та процедури для ручного оновлення та виправлення системного програмного забезпечення на основі поточних та спроектованих вимог до часового ліміту патчів для операційного середовища системи.
T0129	Інтегрувати нові системи в наявну мережеву архітектуру.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор завдання	Опис завдання
T0130	Взаємодіяти з зовнішніми організаціями (наприклад, службою зі зв'язку з громадськістю, правоохоронними органами, Генеральним інспектором командних служб або компонентів) для забезпечення належного та точного розповсюдження фактів про інцидент та інших відомостей про захист комп'ютерної мережі.
T0131	Інтерпретувати та застосовувати закони, нормативні акти, політики, стандарти чи процедури до конкретних питань.
T0132	Інтерпретувати та/або затверджувати вимоги щодо безпеки спроможностей нових інформаційних технологій.
T0133	Інтерпретувати випадки невідповідності для визначення їхнього впливу на рівень ризику та/або загальну ефективність програми кібербезпеки підприємства.
T0134	Керувати та узгоджувати пріоритети безпеки інформаційних технологій (IT) зі стратегією безпеки.
T0135	Керувати та контролювати бюджет інформаційної безпеки, персонал та укладання контрактів.
T0136	Підтримувати базову безпеку системи відповідно до політики організації.
T0137	Підтримувати програмне забезпечення систем управління базами даних.
T0138	Підтримувати інструментальні засоби аудиту кіберзахисту (наприклад, спеціалізоване програмне та апаратне забезпечення для кіберзахисту) для забезпечення місій з аудиту у сфері кіберзахисту.
T0139	Забезпечувати служби реплікації каталогів, які дозволяють автоматично дублювати інформацію з резервних серверів на пересилаючі пристрої за рахунок використання способів оптимальної маршрутизації.
T0140	Забезпечувати інформаційний обмін за допомогою функцій опублікування, підписки та сповіщення, які дозволяють користувачам, при необхідності, відправляти і отримувати важливу інформацію.
T0141	Підтримувати інформаційні системи надання впевненості та матеріали акредитації.
T0142	Забезпечувати інформованість про застосовувані політики з кібербезпеки, нормативні акти і документи відповідності, що стосуються аудиту системи кіберзахисту.
T0143	Розробляти рекомендації на основі результатів тестування.
T0144	Управляти обліковими записами, мережевими правами та доступом до систем і обладнання.
T0145	Керувати та затверджувати пакети документів з акредитації (наприклад, ISO/IEC 15026-2).
T0146	Керувати компіляцією, каталогізацією, кешуванням, поширенням і пошуком інформації.
T0147	Керувати моніторингом джерел даних, що стосуються забезпечення інформаційної безпеки, з метою забезпечення обізнаності організації про ситуацію.
T0148	Організовувати опублікування настанов із захисту комп'ютерної мережі (наприклад, TCNO, концепції операцій, звіти мережевих аналітиків, NTSM, MTO) для зацікавлених сторін підприємства.
T0149	Керувати аналізом загроз або цільовим аналізом інформації про кіберзахист, а також отриманням даних про загрози в рамках підприємства.
T0150	Моніторити та оцінювати відповідність системи з інформаційними технологіями (IT) вимогам безпеки, стійкості і надійності IT.
T0151	Моніторити та оцінювати ефективність засобів кібербезпеки організації з метою гарантованого підтвердження того, що вони забезпечують необхідний рівень захисту.
T0152	Моніторити і підтримувати бази даних з метою забезпечення їх оптимальної продуктивності.
T0153	Моніторити пропускну здатність і продуктивність мережі.
T0154	Моніторити та звітувати про користування активами і ресурсами управління знаннями
T0155	Документувати та ескалювати інциденти (включаючи історію інциденту, його стан і потенційний вплив на подальші дії), які можуть чинити поточний і безпосередній вплив на середовище.
T0156	Наглядати та розробляти рекомендації стосовно управління конфігураціями.
T0157	Наглядати за виконанням програм тренінгів інформаційної безпеки та обізнаності.
T0158	Брати участь в оцінці ризику інформаційної безпеки під час проведення процедури оцінки і авторизації.
T0159	Брати участь в процесах розробки або модифікації планів і вимог програм кібербезпеки комп'ютерного середовища.
T0160	Виправляти вразливості в мережі для переконання, що інформація захищена від зовнішніх сторін.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор завдання	Опис завдання
T0161	Виконувати аналіз лог-файлів з різних джерел (наприклад, лог-файлів окремих хостів, лог-журналів мережевого трафіку, лог-журналів мережевих екранів і систем виявлення вторгнень (IDS лог-журнали) з метою визначення можливих загроз безпеці мережі.
T0162	Виконувати резервне копіювання та відновлення баз даних для забезпечення цілісності даних.
T0163	Виконувати сортування кіберінцидентів для визначення обсягу, терміновості та потенційного впливу, ідентифікації специфічної вразливості та надання рекомендації, які дозволяють оперативно усунути проблему.
T0164	Виконувати аналіз тенденцій в області кіберзахисту та звітування.
T0165	Виконувати динамічний аналіз для завантаження «образу» диска (без необхідності наявності самого жорсткого диска) з метою розуміння процесу вторгнення в природному середовищі і як користувач міг його спостерігати.
T0166	Виконувати кореляцію подій, використовуючи для цього дані, отримані з різних джерел всередині організації, з метою отримання повної інформації про ситуацію, що склалася і визначення ефективності виявленої атаки.
T0167	Виконувати аналіз підпису файлів.
T0168	Порівнювати результати обчислення хеш-функції з результатами, які зберігаються в базі даних.
T0169	Виконувати тестування кібербезпеки розроблених прикладних програм та/або систем.
T0170	Виконувати первинне накопичення і криміналістичну перевірку зображень з метою визначення можливих заходів щодо зниження/усунення несправностей в системах підприємства.
T0171	Здійснювати інтегральні тестування якості для отримання впевненості у функціональності безпеки на протистояння атакам.
T0172	Виконувати криміналістичний аналіз в режимі реального часу (наприклад, використовуючи Helix спільно з LiveView).
T0173	Виконувати аналіз відповідності плану-графіку.
T0174	Виконувати аналіз потреб з метою визначення перспектив використання нових або вдосконалених рішень для бізнес-процесів.
T0175	Виконувати в масштабі реального часу аналіз кіберінцидентів (наприклад, збір криміналістичних матеріалів, зіставлення і відстеження вторгнень, аналіз загроз і пряме відновлення системи) з метою підтримки створюваних груп реагування на інциденти (IRT).
T0176	Виконувати безпечне програмування і визначати потенційні помилки в програмних кодах з метою зменшення вразливостей.
T0177	Виконувати аналіз системи безпеки, визначати пробіли в архітектурі безпеки і розробляти план управління ризиками.
T0178	Виконувати перегляд безпеки, визначати пробіли в архітектурі безпеки, що призведе до рекомендації щодо їхнього включення в стратегію зниження ризиків.
T0179	Проводити статистичний аналіз середовища.
T0180	Здійснювати системне адміністрування спеціалізованих прикладних програм кіберзахисту та систем (наприклад, антивірусне програмне забезпечення, засоби аудиту та відновлення), або пристроїв віртуальних приватних мереж (VPN), включаючи інсталяції, налаштування, обслуговування, резервне о копіювання і відновлення.
T0181	Виконувати аналіз ризиків (наприклад, загрози, вразливості та ймовірності виникнення) щоразу, коли прикладна програма або система зазнають значних змін.
T0182	Виконувати аналіз шкідливого ПЗ 1, 2 і 3 рівнів.
T0183	Здійснювати кроки звірки шляхом порівняння реальних результатів з очікуваними, а також аналіз різниці між ними з метою визначення впливу та ризиків.
T0184	Планувати та проводити огляди авторизації безпеки та складати кейси отримання впевненості під час початкового встановлення систем та мереж.
T0185	Планувати та організовувати виконання проектів управління знаннями.
T0186	Планувати, виконувати та перевіряти надмірність даних та процедури відновлення системи.
T0187	Планувати та розробляти рекомендації щодо змін або коригувань на основі результатів застосування або системного середовища.
T0188	Готувати звітні документи з аудиторської перевірки, які містять технічні та процедурні висновки, а також рекомендувати коригування стратегій/рішень.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор завдання	Опис завдання
T0189	Підготувати детальні схеми та діаграми робочих процесів, які описують вхідні/вихідні дані та логічну операцію, та перетворювати їх у набір інструкцій, кодованих комп'ютерною мовою.
T0190	Підготувати цифрові носії для візуалізації із забезпеченням цілісності даних (наприклад, блокування записів відповідно до стандартних функціональних процедур).
T0191	Підготувати варіанти застосування, щоб обґрунтувати необхідність специфічних рішень інформаційних технологій (IT).
T0192	Підготувати, розповсюдити та підтримувати плани, інструкції, настанови та стандартні функціональні процедури стосовно безпеки функціонування мережевих систем (и).
T0193	Обстежувати місця злочину.
T0194	Документувати належним чином заходи з впровадження, функціонування та експлуатації та за необхідності, оновлювати.
T0195	Забезпечувати керований потік відповідної інформації (через веб-портали або інші засоби) на підставі вимог місії.
T0196	Надавати консультації щодо витрат на проект, концепцій проектування або змін в проекті.
T0197	Забезпечити точну технічну оцінку програмного забезпечення прикладних програм, системи чи мережі а також документувати стан його захищеності, можливостей та вразливості стосовно відповідності вимогам кібербезпеки.
T0198	Надавати щоденні підсумкові звіти про події та діяльність мережі, пов'язані з практиками кіберзахисту.
T0199	Розробити методологію кібербезпеки підприємства та управління ризиком ланцюжка постачання для розробки безперервності операційних планів.
T0200	Надавати зворотній зв'язок стосовно вимог до мережі, включаючи архітектуру мережі та інфраструктуру.
T0201	Розробляти настанови стосовно впровадження розроблених систем клієнтам або командам впровадження.
T0202	Надавати методологію з кібербезпеки керівництву.
T0203	Забезпечити вхідну інформацію стосовно вимог безпеки, які слід включити до звітів про роботу та інших відповідних документів про закупівлі.
T0204	Надавати вхідну інформацію до планів впровадження і стандартних операційних процедур.
T0205	Надавати вхідні дані для діяльності процесу загальних принципів управління ризиками та відповідну документацію (наприклад, плани забезпечення життєвого циклу системи, концепція операцій, операційні процедури і навчальні матеріали з технічного обслуговування).
T0206	Забезпечити керівництво та управління персоналом у сфері інформаційних технологій (IT), забезпечуючи, щоб обізнаність в кібербезпеці, базові знання, грамотність та тренінги операційного персоналу відповідали їх функціональним обов'язкам.
T0207	Забезпечити постійну оптимізацію та вирішення проблем.
T0208	Готувати рекомендації щодо можливих удосконалень і оновлень.
T0209	Надавати рекомендації щодо структур даних і баз даних з метою гарантованого забезпечення підготовки коректних і якісних звітних документів.
T0210	Надавати рекомендації щодо нових технологій і архітектур баз даних.
T0211	Надавати системні вихідні дані для формування вимог кібербезпеки, які повинні бути включені в операційні інструкції та інші відповідні документи, що стосуються системи постачання.
T0212	Надавати технічну допомогу відповідному персоналу з питань цифрових доказів.
T0213	Надавати технічну документацію, звіти про інциденти, результати комп'ютерних перевірок, висновки та іншу інформацію про ситуацію для головних організацій.
T0214	Отримувати і аналізувати сигнали сповіщення про мережу від різних джерел всередині організації та визначати можливі причини появи таких сигналів.
T0215	Розпізнавати можливе порушення безпеки і вживати відповідні заходи, щоб повідомити про інцидент, якщо необхідно.
T0216	Розпізнавати і точно звітувати про докази, що вказують на конкретну операційну систему.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор завдання	Опис завдання
T0217	Усувати наслідки порушення безпеки на етапі прийняття в експлуатацію програмного забезпечення, враховуючи критерії завершення, прийняття ризиків і документацію, загальні критерії та методи незалежного тестування.
T0218	Рекомендувати нові або переглядати існуючі заходи безпеки, стійкості та надійності на основі результатів перевірок.
T0219	Рекомендувати розподіл ресурсів, необхідних для безпечного функціонування та підтримки вимог організації з кібербезпеки.
T0220	Вирішувати конфлікти у законодавстві, нормативних актах, політиках, стандартах і процедурах.
T0221	Переглядати документи щодо авторизації та надання впевненості, щоб підтвердити, що рівень ризику знаходиться в допустимих межах для кожної прикладної програми, системи та мережі.
T0222	Переглядати існуючі та перспективні політики із зацікавленими сторонами.
T0223	Переглядати або здійснювати аудит програм та проектів з інформаційних технологій (IT).
T0224	Переглядати тренінгову документацію (наприклад, документи змісту курсу (CCD), плани уроків, студентські роботи, екзамени, графіки навчання [SOI] та описи курсів).
T0225	Забезпечувати захист електронного пристрою або джерела інформації.
T0226	Брати участь у відомчих і міжвідомчих радах з питань політики.
T0227	Рекомендувати політику та координувати її перегляд та затвердження
T0228	Зберігати, відновлювати та обробляти дані для аналізу можливостей системи та вимог.
T0229	Наглядати або керувати захисними чи коректувальними заходами при виявленні кіберінциденту або вразливості.
T0230	Забезпечувати розробку та виконання сценаріїв вправ.
T0231	Забезпечувати заходи щодо тестування та оцінки систем безпеки та сертифікації.
T0232	Тестувати та підтримувати мережеву інфраструктуру, включаючи програмне та апаратне забезпечення.
T0233	Відстежувати та документувати інциденти кібербезпеки з моменту їх виявлення до остаточного вирішення.
T0234	Відслідковувати результати аудиту та розробляти рекомендації, щоб забезпечити вжиття відповідних заходів щодо зменшення негативних наслідків.
T0235	Перетворювати функціональні вимоги в технічні рішення.
T0236	Перетворювати вимоги безпеки на елементи розробки прикладних програм, включаючи документування елементів зовнішніх атак на програмне забезпечення, моделювання загроз та визначення будь-яких характерних критеріїв безпеки.
T0237	Виявляти та усувати несправності у апаратному та програмному забезпеченні системи.
T0238	Витягати дані за допомогою технік «вирізання» даних (наприклад, набір інструментів для судово-криміналістичної експертизи Forensic Tool Kit [FTK], програма Foremost).
T0239	Використовувати опубліковані федеральні документи та специфічні документи організації для управління їх системами обчислювального середовища.
T0240	Перехоплювати та аналізувати мережевий трафік, пов’язаний з шкідливими діями, використовуючи засоби моніторингу мережі.
T0241	Використовувати спеціалізоване обладнання та методики каталогізації, документування, вилучення, збирання, упаковки та зберігання цифрових доказів.
T0242	Використовувати моделі та симуляції для аналізу або прогнозування продуктивності системи за різних умов експлуатації.
T0243	Перевіряти та оновлювати документацію з безпеки, яка відображає особливості проектування безпеки прикладної системи/системи.
T0244	Переконатися, що заходи безпеки прикладного програмного забезпечення /мережі/системи впроваджені, як зазначено, задокументувати можливі відхилення та рекомендувати необхідні заходи для виправлення цих відхилень.
T0245	Перевірити, що документація прикладного програмного забезпечення /мережевого/акредитації системи та надання впевненості є актуальною.
T0246	Писати та публікувати методики та настанови з кіберзахисту, а також звіти про виявлення інцидентів для відповідної аудиторії.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор завдання	Опис завдання
T0247	Писати інструктивні матеріали (наприклад, стандартні операційні процедури, технологічний посібник), щоб надавати детальні настанови для відповідної частини персоналу.
T0248	Сприяти підвищенню обізнаності керівництва щодо ситуацій безпеки та забезпечувати належні принципи безпеки в баченні та цілях організації.
T0249	Досліджувати сучасні технології щоб зрозуміти можливості необхідної системи або мережі.
T0250	Визначати стратегії кіберможливостей для розробки програмно-апаратних комплексів для замовника, ґрунтуючись на вимогах місії.
T0251	Розробити процеси відповідності безпеки та/або аудитів для зовнішніх послуг (наприклад, провайдерів хмарних послуг, центрів обробки даних).
T0252	Проводити необхідні перевірки відповідно середовищу (наприклад, технічний нагляд, огляди контрзаходів [TSCM], огляди контрзаходів TEMPEST).
T0253	Проводити зовнішній бінарний аналіз.
T0254	Переглядати стандарти політики та стратегії її впровадження, щоб забезпечити відповідність процедур та настанов політикам кібербезпеки.
T0255	Брати участь в корпоративному процесі управління ризиками щоб забезпечити зменшення ризиків безпеки, і введення даних щодо інших технічних ризиків.
T0256	Оцінювати ефективність функції закупівель з точки зору задоволення вимог інформаційної безпеки і ризиків у ланцюжку постачання через закупівельну діяльність та рекомендувати вдосконалення.
T0257	Визначати обсяг, інфраструктуру, ресурси і розмір вибірки даних, щоб забезпечити адекватну демонстрацію системних вимог.
T0258	Своєчасно виявляти, ідентифікувати і сповіщати про можливі атаки/вторгнення, аномальні процеси і неправомірні дії, та відрізнити такі інциденти і події від безпечних дій.
T0259	Використовувати засоби кіберзахисту для постійного моніторингу та аналізу діяльності системи для виявлення шкідливої діяльності.
T0260	Аналізувати виявлені шкідливі процеси, щоб визначити слабкі місця, що були використані, методи їх використання, вплив на систему та інформацію.
T0261	Допомагати у визначенні, розстановці пріоритетів і координації захисту критичної інфраструктури кіберзахисту та ключових ресурсів.
T0262	Застосовувати затверджені принципи і практики «ешелонованого» захисту (наприклад, багатоточкову систему, багаторівневу систему, відмовостійкість системи безпеки).
T0263	Визначати специфічні вимоги безпеки до системи інформаційних технологій (IT) на всіх етапах її життєвого циклу.
T0264	Переконатися, що існують плани дій та етапів або плани відновлення для усунення вразливостей, які були виявлені під час оцінки ризиків, аудиторських та інспекторських перевірок і т.п.
T0265	Забезпечувати успішне впровадження та функціональність вимог безпеки та відповідних політик і процедур інформаційних технологій (IT), які узгоджені з цілями та місією організації.
T0266	Виконувати тести на проникнення для нових або оновлених прикладних програм.
T0267	Розробляти контрзаходи і заходи щодо пом’якшення негативних наслідків від використання слабкостей і вразливостей мов програмування в системі і елементах.
T0268	Визначати і документувати те, як впровадження нових систем або інтерфейсів між системами вплине на стан захищеності діючої інфраструктури.
T0269	Проектувати і розробляти функції управління ключами (які стосуються сфери кібербезпеки).
T0270	Аналізувати потреби та вимоги користувачів з метою планування і проведення розробки системи безпеки.
T0271	Розробляти проекти з кібербезпеки з метою задоволення специфічних операційних потреб та факторів середовища (наприклад, управління доступом, автоматизовані прикладні програми, мережеві операції, високі вимог щодо цілісності, доступності, багаторівневої безпеки / обробки даних, що мають різні ступені секретності, та обробки інформації з особливим режимом зберігання)

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор завдання	Опис завдання
T0272	Забезпечувати, щоб діяльність з проектування та розвитку кібербезпеки (з наданням функціонального опису впровадження безпеки) була належним чином задокументована і оновлювалася за необхідності.
T0273	Визначати і документувати ризики ланцюжка постачання для критичних елементів системи, за необхідності.
T0274	Формувати перевірювані докази заходів безпеки.
T0275	Підтримувати необхідні заходи щодо забезпечення відповідності (наприклад, переконатися, що виконуються настанови щодо конфігурації системи безпеки, здійснюється моніторинг відповідності).
T0276	Брати участь, за необхідності, в процесі закупівлі, дотримуючись відповідних практик управління ризиків в ланцюжку постачання.
T0277	Переконатися, що усі дії з придбання, постачання, закупівлі та аутсорсингу відповідають вимогам кібербезпеки, які відповідають цілям організації.
T0278	Збирати докази вторгнень (наприклад, програмний код, шкідливе програмне забезпечення, трояни) і використовувати здобуті дані щоб уникнути потенційних інцидентів кіберзахисту в організації.
T0279	Слугувати технічним експертом, взаємодіяти з представниками правоохоронних органів та роз'яснювати деталі інцидентів за необхідності.
T0280	Постійно перевіряти організацію на відповідність політикам/настановам /процедурам/нормативним актам/законам для забезпечення відповідності.
T0281	Прогнозувати поточні потреби у послугах та забезпечувати, що припущення щодо безпеки переглядаються за необхідності.
T0282	Визначати та/або впроваджувати політики і процедури, щоб забезпечити належний захист критичної інфраструктури.
T0283	Співпрацювати із зацікавленими сторонами, щоб визначити та/або розробити відповідної технології рішень.
T0284	Проектувати і розробляти нові інструменти/технології, що стосуються кібербезпеки.
T0285	Сканувати цифрові носії на предмет наявності вірусів.
T0286	Проводити криміналістичний аналіз файлової системи.
T0287	Проводити статичний аналіз для створення «образу» диска (без необхідності наявності оригінального диска).
T0288	Виконувати статичний аналіз шкідливих програм.
T0289	Використовувати інструментальний набір криміналістичної експертизи для підтримки операцій за необхідності.
T0290	Визначати тактики, методики і процедури (TTP) для наборів вторгнень.
T0291	Досліджувати мережеві топології, щоб зрозуміти потоки даних в мережі
T0292	Надавати рекомендації щодо усунення вразливостей комп'ютерного середовища.
T0293	Визначати та аналізувати аномалії в мережевому трафіку з використанням метаданих.
T0294	Проводити дослідження, аналіз та кореляцію широкого спектра сукупностей даних, отриманих з усіх джерел (показники і попередження).
T0295	Підтверджувати попередження в системах виявлення вторгнень (IDS) на основі мережевого трафіку з використанням інструментів аналізу пакетів.
T0296	Ізолювати і видаляти шкідливе програмне забезпечення.
T0297	Визначати прикладні програми та операційні системи мережевого пристрою на основі мережевого трафіку.
T0298	Реконструювати шкідливу атаку або активність на основі мережевого трафіку.
T0299	Визначати діяльність зі створення схеми мережі та відбитків операційної системи.
T0300	Розробити і задокументувати вимоги до кваліфікації користувача (UX), включаючи вимоги до архітектури інформації та інтерфейсу користувача.
T0301	Розробляти і впроваджувати незалежні аудиторські перевірки прикладного програмного забезпечення /мереж/систем та стежити за поточними незалежними аудитами, щоб переконатися, що операційні та проектно-конструкторські (R&D) процеси та процедури відповідають організаційним та обов'язковим вимогам кібербезпеки, та чітко виконуються системними адміністраторами та іншим персоналом кібербезпеки під час виконання повсякденної діяльності.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор завдання	Опис завдання
T0302	Розробляти положення контрактів для забезпечення ланцюжків постачання, системної, мережевої і операційної безпеки
T0303	Визначати і використовувати корпоративну систему контролю версій програмного забезпечення при проектуванні і розробці захищених прикладних програм.
T0304	Впроваджувати та інтегрувати методології життєвого циклу розробки систем (SDLC) (наприклад, IBM «Rational Unified Process») в середовище розробки.
T0305	Використовувати управління конфігурацією, управління проблемами, управління потужністю та фінансове управління базами даних і системами управління даними.
T0306	Підтримувати управління інцидентами, управління послугами, управління змінами, управління релізами, управління безперервністю та управління доступністю для баз даних і систем управління даними.
T0307	Аналізувати запропоновані архітектури, розподіляти послуги безпеки і обирати механізми безпеки.
T0308	Аналізувати дані про інциденти для виявлення тенденцій.
T0309	Оцінювати ефективність засобів контролю безпеки.
T0310	Брати участь у створенні підписів, які можуть бути вбудовані в мережеві інструменти кіберзахисту у відповідь на нові або виявлені загрози всередині мережевої інфраструктури або корпоративного мережевого сегмента.
T0311	Консультуватися з клієнтами щодо проектування та підтримки програмного забезпечення..
T0312	Співпрацювати з аналітиками розвідки з метою кореляції даних при оцінці загроз.
T0313	Проектувати і документувати стандарти якості.
T0314	Розробляти умови системи безпеки, попередню концепцію проведення операцій з кібербезпеки (CONOPS), і визначати основні вимоги системи безпеки відповідно до прийнятних вимог кібербезпеки.
T0315	Розробляти і проводити технічні тренінги для навчання інших або задоволення потреб клієнтів.
T0316	Розробляти або брати участь в розробці комп'ютерних навчальних модулів або курсів.
T0317	Розробляти або брати участь у розробці завдань для курсу.
T0318	Розробляти або брати участь у розробці оцінок для курсу.
T0319	Розробляти або брати участь у розробці стандартів оцінювання та кваліфікації.
T0320	Брати участь у розробці індивідуальних/колективних планів розвитку, навчання і/або виправлення.
T0321	Розробляти або брати участь у розробці цілей і завдань навчання.
T0322	Розробляти або брати участь у розробці методичних матеріалів або програм для тренінгів на робочому місці.
T0323	Розробляти або брати участь у розробці письмових тестів для визначення рівня професійної придатності та оцінки кваліфікації учнів.
T0324	Керувати розробкою програмного забезпечення і відповідної документації.
T0325	Документувати призначення системи і попередню концепцію безпеки операцій системи.
T0326	Застосовувати процедури управління конфігурацією.
T0327	Оцінювати вразливості мережевої інфраструктури, щоб поширити можливості, які розробляються
T0328	Оцінювати архітектури і проекти безпеки для визначення адекватності проекту та архітектури безпеки, які були запропоновані або надані відповідно до вимог, що містяться в документах про придбання.
T0329	Дотримуватись стандартів і процедур життєвого циклу програмного забезпечення і інженерії систем.
T0330	Підтримувати системи гарантованої доставки повідомлень.
T0331	Підтримувати базу даних про відстеження інцидентів та про прийняті рішення.
T0332	Сповіщати уповноважених керівників, спеціалістів з реагування на інциденти, членів групи провайдера послуг з кібербезпеки про підозрювані кіберінциденти, і формулювати історію подій, статус і можливий вплив подальших заходів відповідно до плану реагування на кіберінциденти в організації.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор завдання	Опис завдання
T0334	Забезпечувати, щоб усі компоненти системи можна було інтегрувати та узгодити (наприклад, процедури, бази даних, політики, програмне та апаратне забезпечення).
T0335	Створювати, встановлювати, налагоджувати та тестувати спеціальне технічне забезпечення для кіберзахисту.
T0336	Видалено: інтегроване в T0228
T0337	Керувати та призначати задачі для програмістів, проектувальників, технологів і техніків, а також іншому інженерному та науковому персоналу.
T0338	Писати детальні функціональні специфікації, які документують процес розробки архітектури.
T0339	Очолювати зусилля по використанню системи управління знаннями та обміну інформацією в організації.
T0340	Виступати в якості першої зацікавленої сторони в основних операційних процесах та функціях інформаційних технологій (IT), які підтримують, забезпечують керівництво та моніторинг усієї діяльності, щоб послуга була надана успішно.
T0341	Підтримувати адекватне фінансування освітніх ресурсів у кіберсфері, включаючи внутрішні та галузеві курси, оплату праці інструкторів та відповідну учбово-методичну документацію.
T0342	Аналізувати джерела даних з метою розробки дієвих рекомендацій.
T0343	Аналізувати кризові ситуації з метою забезпечення суспільної та персональної безпеки, а також захисту ресурсів.
T0344	Оцінювати всі процеси управління конфігурацією (зміна конфігурації /управління релізами).
T0345	Оцінювати ефективність та дієвість навчання, відповідно до простоти використання навчальних технологій та навчання студентів, передачі знань та задоволеності.
T0346	Оцінювати поведінку окремої жертви, свідка або підозрюваного через його відношення до розслідування.
T0347	Оцінювати достовірність даних джерела та подальших висновків.
T0348	Допомагати оцінити вплив впровадження та підтримки спеціальної інфраструктури кіберзахисту.
T0349	Збирати метрики та дані про тенденції.
T0350	Проводити аналіз ринку з метою визначення, оцінки та розробки рекомендацій щодо придбання комерційних та державних готових продуктів, а також програмних продуктів з відкритим програмним кодом для їх використання всередині системи, та забезпечувати, що рекомендовані продукти відповідають прийнятим в організації вимогам до процедур оцінки і підтвердження.
T0351	Здійснювати перевірку гіпотез з використанням статистичної обробки.
T0352	Проводити оцінку потреб у навчанні та визначати вимоги.
T0353	Звертатися до системних аналітиків, інженерів, програмістів та інших для проектування прикладних програм.
T0354	Координувати та управляти усім спектром послуг, що надаються клієнтам.
T0355	Співпрацювати з внутрішніми і зовнішніми експертами з відповідних питань, щоб переконатися, що існуючі стандарти кваліфікації відображають організаційні функціональні вимоги та відповідають ґалузевим стандартам.
T0356	Співпрацювати із зацікавленими сторонами з кадрових питань організації з метою забезпечення відповідного розміщення та розподілу кадрових ресурсів.
T0357	Створювати інтерактивні навчальні вправи для формування ефективного навчального середовища.
T0358	Проектувати і розробляти процедури адміністрування системи і управління для користувачів із привілейованим доступом користувачів.
T0359	Проектувати, впроваджувати, тестувати і оцінювати захищені інтерфейси між інформаційними системами, фізичними системами і/або вбудованими технологіями.
T0360	Визначати масштаби загроз і розробляти рекомендації щодо заходів або контрзаходів для зменшення ризиків.
T0361	Розробляти і спрощувати методи збору даних.
T0362	Розробляти і впроваджувати описи стандартизованих посад на основі визначених робочих ролей кібербезпеки..

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор завдання	Опис завдання
T0363	Розробляти і аналізувати процедури підбору, найму та збереження персоналу відповідно до поточних політик кадрового забезпечення (HR).
T0364	Розробляти структуру класифікації кар'єрного росту у кіберсфері з метою формування вимог до входу в сферу та іншої номенклатури посад, наприклад кодів та ідентифікаторів.
T0365	Розробляти або брати участь у розробці політик навчання і протоколів з кіберпідготовки.
T0366	Розробляти стратегічні інсайти з великих наборів даних.
T0367	Розробити цілі та завдання для освітніх програм кібербезпеки.
T0368	Забезпечити, що сфера кіберкар'єри управляється згідно кадрових політик і директив організації.
T0369	Забезпечити, що політика і процеси управління кіберперсоналом відповідають юридичним вимогам та вимогам організації щодо рівних можливостей, різноманіття і справедливим практикам найму/ працевлаштування.
T0370	Забезпечити, що відповідні угоди про рівень обслуговування (SLA) та підкріплюючі контракти, чітко визначають для замовника опис послуги та заходи моніторингу якості послуги.
T0371	Встановлювати допустимі ліміти прикладного програмного забезпечення, мереж або систем.
T0372	Встановлювати і збирати метрики для моніторингу та підтвердження готовності персоналу кібербезпеки, включаючи аналіз даних кіберперсоналу для оцінки статусу посад, які були визначені, заповнені та зайняті кваліфікованим персоналом.
T0373	Встановлювати і контролювати процедури відмови від входу в кар'єру в кіберсфері і кваліфікаційних вимог до рівня освіти.
T0374	Встановлювати шляхи кіберкар'єри, щоб забезпечити просування по кар'єрі, планомірний розвиток та зростання як в межах одного напряму, так і за різними напрямками кар'єрного росту.
T0375	Встановлювати стандарти особового складу, персоналу і кваліфікаційних даних для підтримки вимог до управління персоналом та відповідної звітності.
T0376	Встановлювати, забезпечувати ресурсами, впроваджувати та оцінювати програми управління кіберперсоналу згідно вимог організації.
T0377	Збирати відгуки про задоволеність клієнтів та ефективність внутрішніх послуг, щоб сприяти постійному вдосконаленню.
T0378	Впроваджувати процедури оновлення підтримки систем з урахуванням ризиків для усунення системних недоліків (періодично і вибірково).
T0379	Управляти внутрішніми взаємозв'язками з власниками процесів інформаційних технологій, які підтримують послугу, допомагаючи у визначенні та узгодженні Угод про операційний рівень (OLA).
T0380	Планувати навчальні стратегії, наприклад, лекції, демонстрації, інтерактивні вправи, мультимедійні презентації, відеокурси, Web-курси для найбільш ефективного навчального середовища спільно з викладачами та тренерами.
T0381	Надавати технічну інформацію технічним та нетехнічним аудиторіям.
T0382	Відображати дані в оригінальних форматах.
T0383	Програмувати користувацькі алгоритми.
T0384	Сприяти обізнаності керівництва стосовно кіберполітики і стратегії та забезпечити відображення обґрунтованих принципів в місії, концепції і цілях організації.
T0385	Надавати дієві рекомендації для критично важливих зацікавлених сторін на основі аналізу і обробки даних.
T0386	Допомагати адвокату при проведенні кримінального розслідування в період судового розгляду.
T0387	Переглядати і застосовувати стандарти кваліфікації кар'єри в кіберсфері.
T0388	Аналізувати і застосовувати політики організації, які пов'язані з кіберперсоналом або впливають на кіберперсонал.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор завдання	Опис завдання
T0389	Переглядати звіти про ефективність послуг, де вказані усі будь-які значні проблеми і відхилення, ініціюючи, у разі необхідності, коригувальні дії та гарантуючи, що усі невирішені питання будуть відстежені.
T0390	Переглянути /оцінити ефективність кіберперсоналу для коригування навичок та/або стандартів кваліфікації.
T0391	Сприяти інтеграції кваліфікованого кіберперсоналу в процеси розробки життєвого циклу інформаційних систем.
T0392	Використовувати технічну документацію або ресурси для впровадження нових математичних методів, а також методів обробки даних або інформатики.
T0393	Підтверджувати специфікації і вимоги до можливості тестування.
T0394	Співпрацювати з менеджерами послуг і власниками продукту з метою збалансування і пріоритеризації послуг, що надаються, що, в свою чергу, дозволить задовольнити загальні вимоги, обмеження і цілі користувачів.
T0395	Писати і публікувати звіти проведених заходів.
T0396	Обробляти образ відповідними засобами в залежності цілей аналізу.
T0397	Виконувати аналіз реєстру Windows.
T0398	Здійснювати моніторинг файлів і реєстра в функціонуючій системі після виявлення вторгнення за допомогою динамічного аналізу.
T0399	Вводити інформацію про електронний носій в базу даних обліку (наприклад, база обліку і контролю виробів Product Tracker Tool) придбаних електронних носіїв.
T0400	Зіставити дані про інциденти та готувати звіти з кіберзахисту.
T0401	Підтримувати набір засобів кіберзахисту, що розгортається (наприклад, спеціалізоване програмне /технічне забезпечення для кіберзахисту) для підтримки діяльності групи управління інцидентами.
T0402	Ефективно розподілити ємність для збереження даних при проектуванні систем управління даними.
T0403	Читати, інтерпретувати, писати, модифікувати і використовувати прості скрипти (наприклад, Perl, VBScript) в ОС Windows і UNIX (наприклад, ті, що реалізують наступні функції: граматико-синтаксичний аналіз великих файлів даних, автоматизація ручних завдань і витяг/обробка віддалених даних)
T0404	Використовувати різні мови програмування для написання коду, відкриття файлів, читання файлів і запису результатів до різних файлів.
T0405	Використовувати мову з відкритим кодом, наприклад, «R», і застосувати кількісні методики (наприклад, описову і вивідну статистики, вибірку, експериментальне проектування, параметричне і непараметричне тестування відмінностей, звичайну регресію найменших квадратів, загальні лінійні методи).
T0406	Забезпечити, що діяльність з проектування та розробки належним чином задокументована (надаючи функціональний опис впровадження) та оновлена за необхідності.
T0407	Брати участь (при необхідності) в процесах придбання.
T0408	Інтерпретувати і застосовувати діючі закони, статути та нормативні документи та інтегрувати їх в політику організації.
T0409	Усувати проблеми, що виникають в процесі проектування прототипів, а також на етапах проектування, розробки і перед запуском продукту.
T0410	Визначати функціональні властивості і властивості, пов’язані із забезпеченням безпеки, з метою пошуку сприятливих можливостей для експлуатації або усунення вразливостей.
T0411	Визначати та/або розробити засоби зворотної інженерії для підвищення спроможностей і виявлення вразливостей.
T0412	Здійснити аналіз імпортних/експортних операцій з придбання систем і програмного забезпечення.
T0413	Розробляти нові можливості управління даними (наприклад, хмарне централізоване управління криптографічними ключами), щоб забезпечити підтримку мобільного персоналу.
T0414	Розробляти вимоги до ланцюжка постачання, системи, мережі, продуктивності і кібербезпеки.
T0415	Забезпечити, що вимоги до ланцюжка постачання, системи, мережі, продуктивності та кібербезпеки включені до положень контракту і встановлені..

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор завдання	Опис завдання
T0416	Впроваджувати прикладні програми з відкритим ключем, шляхом використання існуючих бібліотек в інфраструктури відкритих ключів (PKI), включивши функції управління сертифікатами та функцій шифрування, за необхідності.
T0417	Ідентифікувати та задіяти послуги загальнокорпоративної безпеки в ході проектування і розробки захищених прикладних програм в (наприклад, інфраструктури відкритих ключів підприємства, сервера федеративної ідентифікації, антивірусних рішень для підприємства), за необхідності.
T0418	Встановлювати, оновлювати та усувати несправності систем/серверів.
T0419	Отримувати і підтримувати робочі знання з конституційних питань, які виникають у відповідних законах, нормативних актах, політиках, угод, стандартах, процедурах чи інших публікаціях.
T0420	Адмініструвати тестові стенди, а також тестувати та оцінювати прикладні програми, апаратну інфраструктуру, правила/підписи, контроль доступу і конфігурації платформ, що обслуговуються провайдером (ами) послуг.
T0421	Керувати індексацією/каталогізацією, зберіганням та доступом до точної інформації організації (наприклад, паперові документи, цифрові файли).
T0422	Впроваджувати стандарти управління даними, вимоги і специфікації.
T0423	Аналізувати загрози, джерелом яких є комп'ютери, для контррозвідки або кримінального розслідування.
T0424	Аналізувати та надавати інформацію зацікавленим сторонам, які будуть підтримувати розробку або модифікацію існуючих захищених прикладних програм.
T0425	Аналізувати політику організації у сфері кібербезпеки.
T0426	Аналізувати результати тестування програмного, апаратного забезпечення або сумісності.
T0427	Аналізувати потреби та вимоги користувачів для планування архітектури.
T0428	Аналізувати потреби безпеки і вимоги до програмного забезпечення з метою визначення доцільності проекту з урахуванням часових і цінових обмежень, а також мандатів безпеки.
T0429	Оцінювати потреби в політиці та співпрацювати з зацікавленими сторонами з метою розробки політик корпоративного управління діяльністю в сфері кібербезпеки.
T0430	Збирати та зберігати докази, що використовуються при розслідуванні комп'ютерних злочинів.
T0431	Перевіряти придатність, функціональність, цілісність та ефективність апаратного забезпечення системи.
T0432	Збирати та аналізувати артефакти вторгнення (наприклад, вхідний код, шкідливе програмне забезпечення та конфігурацію системи) та використовувати отримані дані, щоб уникнути потенційні інциденти кіберзахисту на підприємстві.
T0433	Здійснювати аналіз лог-журналів, доказів та іншої інформації з метою визначення найкращих методів виявлення порушника (ів), який (які) здійснив вторгнення в мережу або інші злочини.
T0434	Проводити формулювання звернень з метою відповідного інформування про можливі порушення законодавства, нормативних правових актів, або політики/інструкції.
T0435	Проводити періодичне обслуговування системи, куди входять чистка (фізична й електронна), перевірка дисків, завантажувальних програм, видалення даних і тестування.
T0436	Здійснювати пробні запуски програм і прикладного програмного забезпечення, щоб переконатися, що отримана вся необхідна інформація і настанови та рівні захищеності вірні.
T0437	Забезпечувати кореляцію тренінгів та навчання вимогам бізнесу або місії.
T0438	Формувати, редагувати і управляти списками контролю доступу до мережі у спеціалізованих системах кіберзахисту (наприклад, мережеві екрани і системи запобігання вторгнень).
T0439	Виявляти та аналізувати зашифровані дані, стенографію, альтернативні потоки даних та інші приховані дані.
T0440	Фіксувати та інтегрувати основні властивості системи або бізнес функції, які необхідні для часткового або повного відновлення системи після катастрофічного збою.
T0441	Визначати та інтегрувати середовища для поточної та майбутньої місій.
T0442	Розробляти тренінгові курси з урахуванням аудиторії і фізичного середовища.
T0443	Проводити тренінгові курси з урахуванням аудиторії і фізичних/віртуальних середовищ.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор завдання	Опис завдання
T0444	Застосовувати концепції, процедури, програмне забезпечення, обладнання та/або технологічні прикладні програми під час навчання студентів.
T0445	Розробляти/інтегрувати кіберстратегію, яка окреслює бачення, місію та цілі, які узгоджені зі стратегічним планом організації.
T0446	Проектувати, розробляти, інтегрувати і оновлювати показники захищеності системи, які забезпечують конфіденційність, цілісність, доступність, автентифікацію і безвідмовність.
T0447	Проектувати апаратне забезпечення, операційні системи і прикладні програми відповідно до вимог.
T0448	Розробити компоненти архітектури або системних компонент підприємства, необхідні для задоволення потреб користувачів.
T0449	Розробляти вимоги безпеки для забезпечення виконання вимог для всіх систем або прикладних програм.
T0450	Розробити плани і програми тренінгів на основі вимог.
T0451	Брати участь в розробці навчальних планів і програм.
T0452	Проектувати, створювати, впроваджувати та підтримувати систему управління знаннями, яка надає доступ кінцевим користувачам до інтелектуальних ресурсів організації.
T0453	Визначати і розробляти керівництва та визначати джерела інформації для виявлення та/або притягнення до відповідальності винних за вторгнення або інші протизаконні дії.
T0454	Визначати базові вимоги безпеки відповідно до діючих настанов.
T0455	Розробляти процедури тестування і перевірки автентичності програмних систем, програмування і документування.
T0456	Проводити процедури тестування і перевірки автентичності програмного забезпечення.
T0457	Розробляти процедури тестування і перевірки автентичності систем, програмування і документування.
T0458	Дотримуватись стандартних операційних процедур адміністрування систем організації.
T0459	Впроваджувати прикладні програми інтелектуального аналізу даних та сховищ даних.
T0460	Розробляти і впроваджувати програми інтелектуального аналізу даних та сховищ даних.
T0461	Впроваджувати та забезпечувати виконання політик і процедур використання локальної мережі.
T0462	Розробляти процедури і тести для перевірки відмовостійкості при перенесенні системних функцій на інший майданчик, виходячи з вимог доступності системи.
T0463	Розробляти кошторис витрат на нову (і) або модифіковану (і) систему (ми).
T0464	Розробляти детальну проектну документацію щодо створення компонентів та інтерфейсів для підтримки проектування та розробки системи.
T0465	Розробляти настанови для впровадження.
T0466	Розробляти стратегії мінімізації ризиків для зменшення витрат, графіку, продуктивності і ризиків безпеки.
T0467	Забезпечувати, що тренінги відповідають цілям і завданням тренінгів, освіти або обізнаності з кібербезпеки.
T0468	Діагностувати та усувати системні інциденти, проблеми і події, про які повідомили клієнти.
T0469	Аналізувати і повідомляти про тренди безпеки організації.
T0470	Аналізувати і повідомляти про тренди стану безпеки системи.
T0471	Документувати вихідний стан цифрових та/або пов’язаних доказів (наприклад, за допомогою цифрових фотокамер, письмових звітів, перевірки хеш-функції).
T0472	Розробляти проект, ознайомлювати персонал і публікувати політики кібербезпеки.
T0473	Документувати та оновлювати за необхідності усі напрямки діяльності, пов’язані із визначенням архітектури.
T0474	Здійснювати аналіз законодавства і готувати проекти рішень для генеральних інспекторів, уповноважених працівників з захисту даних, нагляду і перевірки дотримання персоналом відповідних вимог політик, законів і нормативних актів в сфері кібербезпеки.
T0475	Оцінювати адекватні контролі доступу, засновані на принципах мінімуму привілеїв і «необхідно знати».
T0476	Оцінювати вплив змін у законодавстві, нормативних актах, політиках, стандартах або процедурах.
T0477	Забезпечувати надійне відновлення після аварії і безперервність операцій.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор завдання	Опис завдання
T0478	Готувати настанови із застосування законодавства, нормативних актів, стандартів і процедур для керівництва, персоналу або клієнтів.
T0479	Застосовувати системи інформаційних технологій (IT) і цифрові засоби зберігання для розкриття, розслідування та/або судового переслідування кіберзлочинів, вчинених проти громадян і майна.
T0480	Визначати компоненти або елементи, розподіляти комплексні функціональні компоненти для включення в них функцій безпеки та описувати взаємозв'язки між елементами.
T0481	Визначати та вирішувати питання планування і кіберперсоналу (наприклад, набір, збереження і навчання).
T0482	Розробляти рекомендації на основі аналізу тенденцій щодо удосконалення програмних та апаратних рішень для підвищення якості обслуговування клієнтів.
T0483	Визначити потенційні протиріччя, пов'язані з впровадженням будь-яких засобів кіберзахисту (наприклад, тестування та оптимізація інструментів і підписів).
T0484	Визначати потреби у захисті (тобто, контролях безпеки) інформаційних систем та мережі, а також належним чином їх документувати.
T0485	Впроваджувати заходи безпеки для усунення вразливостей, зниження ризиків і вносити рекомендації щодо змін в систему або її компоненти за необхідності.
T0486	Впроваджувати вимоги Загальних принципів управління ризиками (RMF)/ Оцінку та авторизацію безпеки (SA&A) для спеціальних систем кіберзахисту на підприємстві, а також документувати і вести записи про них.
T0487	Сприяти впровадженню нових або переглянутих законів, нормативних актів, керівних документів, розпоряджень, політик, стандартів або процедур.
T0488	Впроваджувати проекти нової (их) або існуючої (их) системи (м).
T0489	Впроваджувати заходи безпеки відповідно до встановлених процедур для забезпечення конфіденційності, цілісності, доступності, автентифікації і відмовостійкості.
T0490	Встановлювати та налаштовувати системи управління базами даних та програмне забезпечення.
T0491	Встановлювати та налаштовувати апаратне та програмне забезпечення, а також периферійне обладнання для користувачів системи відповідно до стандартів організації.
T0492	Забезпечувати інтеграцію та впровадження системи междоменних рішень (CDS) у безпечне середовище.
T0493	Керувати та контролювати бюджет, укомплектування персоналом та підписання контрактів.
T0494	Адмініструвати облікові записи, мережеві права і доступ до систем і обладнання.
T0495	Керувати пакетами документів з акредитації (наприклад, ISO/IEC 15026-2).
T0496	Управляти активами/проводити інвентаризацію активів, що належать до ресурсів інформаційних технологій (IT).
T0497	Управляти процесом планування використання IT, щоб переконатися, що розроблені рішення відповідають вимогам замовника.
T0498	Управляти системними/серверними ресурсами, включаючи продуктивність, ємність, доступність, ремонтопридатність і здатність відновлюватись.
T0499	Зменшувати/виправляти недоліки в системі безпеки, виявлені при тестуванні рівня захищеності системи /сертифікації, та/або розробляти рекомендації для вищого керівника або уповноваженої особи щодо прийняття ризиків.
T0500	Модифікувати та підтримувати існуюче програмне забезпечення, щоб виправити помилки, адаптувати його до нового обладнання або оновити інтерфейси і підвищити продуктивність.
T0501	Моніторити та підтримувати конфігурацію системи/сервера.
T0502	Моніторити і звітувати про продуктивність комп'ютерної системи на рівні клієнта.
T0503	Моніторити зовнішні джерела даних (наприклад, сайти постачальників засобів кіберзахисту, груп реагування на надзвичайні комп'ютерні події, центр безпеки) для підтримки поточного стану загроз кіберзахисту, та визначення того, які проблеми безпеки можуть вплинути на підприємство.
T0504	Аналізувати і моніторити кібербезпеку, пов'язану з практиками впровадження і тестування системи.
T0505	Моніторити неухильне виконання політик, принципів і практик при наданні послуг з планування та управління.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор завдання	Опис завдання
T0506	Знаходити консенсус із зацікавленими сторонами щодо запропонованих змін політики
T0507	Наглядати за встановленням, впровадженням, налаштуванням та підтримкою компонентів системи.
T0508	Переконатися, що мінімальні вимоги безпеки застосовані для всіх прикладних програм.
T0509	Виконувати оцінку ризиків інформаційної безпеки.
T0510	Координувати функції реагування на інциденти.
T0511	Виконувати тестування системи у процесі її розробки.
T0512	Здійснювати тестування сумісності систем, які здійснюють обмін електронною інформацією з іншими системами.
T0513	Проводити експлуатаційне тестування.
T0514	Діагностувати несправне апаратне забезпечення системи/сервера.
T0515	Виконувати ремонт несправного апаратного забезпечення системи/сервера.
T0516	Виконувати безпечне тестування, огляд та/або оцінку програм, щоб виявити потенційні недоліки в кодах і пом’якшити вразливості.
T0517	Інтегрувати результати щодо ідентифікації пробілів в архітектурі безпеки.
T0518	Здійснювати огляди безпеки та виявляти пробіли в архітектурі безпеки.
T0519	Планувати і координувати реалізацію методик і форматів проведення класних занять (наприклад, лекції, демонстрації, інтерактивні заняття, мультимедійні презентації) з метою створення найбільш ефективного навчального середовища.
T0520	Планувати позакласні заняття з використанням методик і форматів навчання (наприклад, відеокурси, навчання у наставників, Web-курси).
T0521	Планувати стратегію впровадження, щоб забезпечити, що компоненти підприємства можуть бути інтегровані та узгоджені.
T0522	Готувати юридичні та інші необхідні документи (наприклад, показання, зведення, поручительства, заяви, скарги, клопотання, розкриття).
T0523	Готувати звіти для документування розслідування, здійснюваного відповідно до правових стандартів і вимог.
T0524	Сприяти обміну знаннями між власниками/користувачами інформації через операційні процеси і системи організації.
T0525	Надавати методологію з кібербезпеки підприємства та управління ризиками ланцюжка постачання.
T0526	Надавати рекомендації з кібербезпеки керівництву на основі значних загроз і вразливостей.
T0527	Забезпечувати вхідні дані для планів впровадження і стандартні операційні процедури, які стосуються безпеки інформаційних систем.
T0528	Забезпечувати вхідні дані для планів впровадження, стандартних операційних процедур, експлуатаційної документації та навчально-методичних матеріалів.
T0529	Надавати методологію щодо політики керівництву з кібербезпеки, персоналу і користувачам.
T0530	Проводити аналіз тенденцій і звітувати про їхній вплив.
T0531	Вирішувати проблеми з апаратним /програмним інтерфейсом та проблеми сумісності.
T0532	Оглядати криміналістичні образи та інші джерела даних (наприклад, мінливі дані) для відновлення потенційно важливої інформації.
T0533	Оглядати, здійснювати або брати участь в аудитах кіберпрограм і кіберпроектів.
T0534	Проводити періодичні огляди/перегляди змісту курсу на предмет їх достовірності, повноти і актуальності (наприклад, змістовні матеріали курсу, плани занять, посібники, іспити, розклад занять і опис програм).
T0535	Розробляти рекомендації щодо переглядів навчальних планів і програм на основі відгуків про попередні навчальні заняття.
T0536	Виконувати обов’язки внутрішнього консультанта і радника в своїй експертній області (наприклад, технічній області, області авторського права, електронних носіях).
T0537	Підтримувати директора з інформаційних технологій у формуванні політик, які стосуються кібербезпеки.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор завдання	Опис завдання
T0538	Надавати підтримку процедур тестування і оцінки.
T0539	Проводити тестування, оцінку та перевірку програмного та/або апаратного забезпечення з метою визначення їх відповідності встановленим специфікаціям і вимогам.
T0540	Записувати та управляти даними тестування.
T0541	Відстежувати системні вимоги з метою проектування компонентів та виконувати аналіз недоліків розробки.
T0542	Перетворювати запропоновані спроможності в технічні вимоги.
T0544	Підтверджувати стабільність, сумісність, портативність і/або масштабованість архітектури системи.
T0545	Співпрацювати із зацікавленими сторонами щодо врегулювання інцидентів в області комп'ютерної безпеки і вимог щодо усунення вразливостей.
T0546	Писати і публікувати рекомендації з кібербезпеки, а також звітні документи і експертні доклади з результатами аналізу інцидентів для відповідної аудиторії.
T0547	Досліджувати і оцінювати наявні технології і стандарти з метою задоволення вимог замовника.
T0548	Забезпечувати консультації і дані для планів аварійного відновлення, непередбачених обставин та безперервності операцій.
T0549	Проводити оцінку технічних (оцінка технології) і нетехнічних (оцінка людей і операцій) ризиків і вразливостей пріоритетних технологічних областей (наприклад, локальне комп'ютерне середовище, мережа та інфраструктура, межі закритої групи, допоміжна інфраструктура та прикладні програми).
T0550	Розробляти рекомендації щодо вибору ефективних, з точки зору витрат, контролей захищеності з метою зниження ризиків (наприклад, захист інформації, систем і процесів).
T0551	Розробляти і публікувати документи щодо управління безпекою ланцюжка постачання та управління ризиками.
T0552	Аналізувати та затверджувати політики управління безпекою ланцюжка постачання і управління ризиками.
T0553	Застосовувати функції кібербезпеки (наприклад, шифрування, контроль доступу і управління ідентифікацією) з метою зниження можливостей використання.
T0554	Визначати і документувати програмні коригування або версії програми, які залишають вразливості.
T0555	Документувати те, як впровадження нової системи або нового інтерфейсу між системами впливає на поточну або цільову інфраструктуру, включаючи, але не обмежуючись станом безпеки.
T0556	Оцінювати і проектувати функції управління безпекою, пов'язані з кіберпростором.
T0557	Інтегрувати функції управління ключами, пов'язані з кіберпростором.
T0558	Аналізувати потреби та вимоги користувачів з метою планування та подальшої розробки системи.
T0559	Розробляти проекти з метою задоволення специфічних операційних потреб і факторів середовища (наприклад, контроль доступу, автоматизовані прикладні програми, мережеві операції).
T0560	Брати участь в розробці проектів з кібербезпеки з метою задоволення специфічних операційних потреб і факторів середовища (наприклад, контроль доступу, автоматизовані прикладні програми, мережеві операції, високі вимоги щодо цілісності та доступності, багаторівневий захист/обробка даних, що мають різні ступені секретності, і обробка секретної інформації з особливим режимом зберігання).
T0561	Надавати точні характеристики цілей.
T0562	Адаптувати операції або плани зі збору даних з метою усунення виявлених проблем/викликів, а також з метою синхронізації збору даних з загальними операційними вимогами.
T0563	Забезпечувати вхідні дані для аналізу, проектування, розробки або набуття можливостей, які використовуються для досягнення поставлених цілей.
T0564	Проводити аналіз зворотного зв'язку з метою визначення того, наскільки продукти і послуги задовольняють вимоги.
T0565	Аналізувати вхідні запити на збір інформації.
T0566	Аналізувати внутрішню операційну архітектуру, інструменти та процедури для визначення способів підвищення продуктивності.
T0567	Аналізувати цільову операційну архітектуру для визначення способів отримання доступу.

Ідентифікатор завдання	Опис завдання
T0568	Аналізувати плани, директиви, настанови і політики, що стосуються факторів, які можуть вплинути на операційну структуру і вимоги щодо управлінням збору даних (наприклад, тривалість, обсяг, комунікативні вимоги, міжвідомчі/міжнародні угоди).
T0569	Відповідати на запити щодо отримання інформації.
T0570	Застосовувати і використовувати авторизовані кіберспроможності з метою забезпечення доступу до цільових мереж.
T0571	Застосовувати експертизу політики і процесів з метою сприяння розробці, узгодженню та планування внутрішнього кадрового забезпечення, і/або протоколів про угоду.
T0572	Застосовувати збір кіберданих, готувати середовище та проводити експертизу з метою забезпечення можливості проведення нових операцій та /або продовження операцій збору, або з метою виконання вимог замовників.
T0573	Оцінювати та застосовувати фактори операційного середовища і ризиків для процесу управління збором даних.
T0574	Застосовувати і дотримуватись чинних статутів, законів, нормативних документів і політик.
T0575	Координувати розвідувальні заходи у підтримку оперативного планування діяльності.
T0576	Оцінювати розвідку з усіх джерел і рекомендувати цілі для підтримки цілей кібероперацій.
T0577	Оцінювати ефективність існуючих систем обміну інформацією та систем управління інформацією.
T0578	Оцінювати ефективність ресурсів збору інформації відповідно до затверджених специфікацій.
T0579	Оцінювати цільові вразливості та/або оперативні можливості з метою визначення напрямку дій.
T0580	Оцінювати ефективність збору даних у заповненні пріоритетних пробілів в інформації, використовуючи для цього наявні можливості і методи, та відповідно коригувати стратегії збору та вимоги до збору даних.
T0581	Допомагати і надавати консультації міжвідомчим партнерам у визначенні та розробці кращих практик для полегшення операційної підтримки для досягнення цілей організації.
T0582	Проводити експертизу з метою визначення напрямку подальших дій.
T0583	Проводити предметну експертизу з метою розробки загальної оперативної картини.
T0584	Підтримувати загальну картину розвідувальних заходів.
T0585	Проводити предметну експертизу з метою розробки спеціальних індикаторів кібероперацій.
T0586	Сприяти координації, підтвердженню і управлінню вимогами, планам та/або заходам зі збору даних з усіх джерел.
T0587	Сприяти розробці і уточненню пріоритезації вимог до інформації.
T0588	Проводити експертизу з метою розробки показників ефективності та показників продуктивності.
T0589	Брати участь в процесі визначення недоліків у зборі розвідувальної інформації.
T0590	Забезпечувати синхронізацію планів підтримки розвідки між організаціями- партнерами.
T0591	Проводити аналіз діяльності з використання цільової інфраструктури.
T0592	Забезпечувати вхідні дані з метою визначення критеріїв успіху, пов’язаних з кіберзахистом.
T0593	Готувати резюме загроз і/або цілі поточної ситуації.
T0594	Створювати і підтримувати електронні цільові папки.
T0595	Класифікувати документи відповідно до настанов з класифікації.
T0596	Закривати запити на отримання інформації після їх задоволення.
T0597	Співпрацювати з аналітиками розвідки/ цільовими організаціями, залученими у пов’язані області.
T0598	Співпрацювати з організаціями-розробниками з метою створення та розгортання інструментів, необхідних для досягнення поставлених цілей.
T0599	Співпрацювати з іншими замовниками, розвідкою та цільовими організаціями, залученими у пов’язані кібербласті.
T0600	Співпрацювати з іншими зовнішніми і внутрішніми організаціями-партнерами щодо цільового та оперативних питань.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор завдання	Опис завдання
T0601	Співпрацювати з іншими членами команди або партнерськими організаціями з метою розробки різнопланової програми інформаційних матеріалів (наприклад, Web-сторінки, брифінги, друковані матеріали).
T0602	Співпрацювати з замовником з метою визначення вимог до інформації.
T0603	Інформувати керівництво, а також внутрішніх і зовнішніх клієнтів про нові розробки, досягнення, проблеми і пройдені уроки.
T0604	Порівнювати розподілені та наявні активи для потреб процесу збору інформації відповідно до вимог.
T0605	Накопичувати досвід, отриманий під час реалізації заходів щодо забезпечення збору даних, з метою вирішення поставлених перед організацією завдань.
T0606	Накопичувати, інтегрувати та/або інтерпретувати дані, здобуті з різних джерел, для забезпечення розвідувальних заходів або отримання даних про вразливість для специфічних цілей.
T0607	Ідентифікувати та проводити аналіз цільових комунікацій з метою визначення інформації, необхідної для забезпечення і проведення операцій.
T0608	Проводити аналіз фізичних та логічних цифрових технологій (наприклад, бездротового зв'язку, СКАДА, телекомунікацій) з метою визначення потенційних шляхів доступу.
T0609	Надавати доступ до бездротових комп'ютерних і цифрових мереж.
T0610	Збирати та обробляти дані, передані через бездротові комп'ютерні і цифрові мережі.
T0611	Проводити оцінку закінчення операцій.
T0612	Здійснювати експлуатацію бездротових комп'ютерних і цифрових мереж.
T0613	Проводити офіційне та неофіційне узгодження вимог до збору даних відповідно до встановлених настанов і процедур.
T0614	Проводити незалежний поглиблений цільовий аналіз і технічний аналіз, включаючи цільову специфічну інформацію (наприклад, культурну, організаційну, політичну), у результаті якого може бути отриманий доступ.
T0615	Проводити поглиблене дослідження та аналіз.
T0616	Проводити мережеву розвідку і аналізи вразливостей систем у мережі.
T0617	Проводити аналіз вузлів.
T0618	Проводити заходи в мережі з метою контролю і отримання даних з розгорнутих технологій.
T0619	Проводити заходи в мережі та за її межами з метою контролю і отримання даних з розгорнутих автоматизованих технологій.
T0620	Збирати дані з відкритих джерел за допомогою різних онлайн інструментів.
T0621	Проводити контроль якості, щоб визначити достовірність і актуальність інформації, яка зібрана про мережі.
T0622	Розробляти, оглядати та впроваджувати настанови з планування на всіх рівнях з метою підтримки кібероперацій.
T0623	Проводити обстеження комп'ютерних і цифрових мереж.
T0624	Проводити цільові дослідження і аналіз.
T0625	Враховувати результативність та ефективність активів і ресурсів збору даних, якщо/коли вони застосовуються відповідно до вимог пріоритетності інформації.
T0626	Формувати плани та матриці збору даних з використанням встановлених настанов і процедур.
T0627	Брати участь у плануванні кризової діяльності для кібероперацій.
T0628	Брати участь у розробці засобів підтримки прийняття рішень організації за необхідності.
T0629	Брати участь у розробці, кадровому забезпеченні та координації політик кібероперацій, стандартів продуктивності, планів та пакетів схвалення з відповідними внутрішніми і/або зовнішніми посадовими особами, які приймають рішення.
T0630	Включати розвідувальні заходи в проекти планів проведення кібероперацій.
T0631	Узгоджувати розподіл ресурсів зібраних активів з урахуванням пріоритетних вимог до збирання інформації, з керівниками, що визначають порядок збирання.
T0632	Координувати включення плану зі збору даних у відповідну документацію.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор завдання	Опис завдання
T0633	Узгоджувати перевірку цілій з відповідними партнерами.
T0634	Змінювати задачу або переорієнтовувати засоби та ресурси зі збору даних.
T0635	Співпрацювати з партнерами розвідувального напрямку і сфери кіберзахисту з метою отримання необхідної важливої інформації.
T0636	Співпрацювати зі спеціалістами з планування розвідувальних заходів, щоб забезпечити отримання менеджерами зі збору даних вимог до інформації.
T0637	Співпрацювати з командою спеціалістів з планування розвідувальних заходів для оцінки можливості вирішувати поставлені розвідувальні завдання.
T0638	Координувати, розробляти та відстежувати вимоги до розвідки.
T0639	Узгоджувати, синхронізувати та складати відповідні розвідувальні розділи в планах кібероперацій
T0640	Використовувати дані розвідки для протидії потенційним цільовим атакам
T0641	Створювати стратегії комплексної експлуатації, які визначають експлуатаційні технічні або операційні вразливості.
T0642	Підтримувати обізнаність про внутрішні та зовнішні кіберструктури організації, сильні сторони, укомплектованість персоналом, використовувані технології.
T0643	Розгортати інструменти проти цілі та здійснювати їх утилізацію відразу після використання (наприклад, бекдори, сніфери).
T0644	Виявляти експлойти проти цільових мереж і хостів, та реагувати відповідним чином
T0645	Визначати порядок подальших дій при внесенні змін до мети, настанов і операційного середовища.
T0646	Визначати існуючі бази даних Web-сторінок, бібліотеки і сховища управління збором інформації.
T0647	Визначати, як ідентифіковані фактори впливають на постановку завдань, збір, обробку, використання та поширення форм архітектур.
T0648	Визначати індикатори (наприклад, критерії оцінки ефективності), які є найбільш придатними для визначення цілей кібероперацій.
T0649	Визначати організації та/або інстанції, які уповноважені на збір даних і володіють повністю доступними засобами для збору.
T0650	Визначати, які технології використовує певна ціль.
T0651	Розробляти метод порівняння звітів зі збору інформації з невиконаними вимогами для визначення пробілів в інформації.
T0652	Розробляти матеріали для цільової розвідки з усіх джерел.
T0653	Застосовувати аналітичні методики, щоб отримати більше цільової інформації.
T0654	Розробляти і підтримувати плани запобіжних і/або кризових заходів.
T0655	Розробляти і переглядати специфічні настанови з кібероперацій для інтеграції у більш широку діяльність з планування.
T0656	Розробляти і переглядати настанови з розвідки для інтеграції у підтримку планування та виконання кібероперацій.
T0657	Розробляти координуючі інструкції щодо порядку збору даних в кожній фазі операції.
T0658	Розробляти плани та настанови з кібероперацій щоб переконатися, що рішення про виконання та розподіл ресурсів відповідають цілям організації.
T0659	Розробляти детальну розвідувальну підтримку вимог до кібероперацій.
T0660	Розробляти вимоги до інформації, необхідні для відповідей на пріоритетні запити інформації.
T0661	Розробляти показники результативності та показники продуктивності.
T0662	Розподіляти активи збору даних на основі настанов керівництва, пріоритетів і оперативних акцентів.
T0663	Розробляти матеріали для оцінки результативності озброєності або оперативної оцінки.
T0664	Розробляти нові методики для отримання і підтримки доступу до цільових систем.
T0665	Розробляти або брати участь в розробці стандартів надання, відправлення запитів і/або отримання підтримки з боку зовнішніх партнерів з метою синхронізації кібероперацій.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор завдання	Опис завдання
T0666	Розробляти або формувати стратегії, політики і напрямки діяльності в рамках міжнародного співробітництва з метою вирішення завдань організації.
T0667	Розробляти потенційні напрямки діяльності.
T0668	Розробляти процедури для встановлення зворотного зв'язку з менеджерами зі збору даних, управлінню активами і центрами обробки, експлуатації і поширення інформації.
T0669	Розробляти стратегію і процеси для розробки планів взаємодії з партнерами, проведення операцій і розвитку можливостей.
T0670	Розробляти, впроваджувати та рекомендувати зміни до відповідних процедур планування та політик.
T0671	Розробляти, підтримувати, і оцінювати угоди із зовнішніми партнерами з питань взаємодії в сфері кібербезпеки.
T0672	Розробляти, документувати та затверджувати стратегію і плани проведення кібероперацій.
T0673	Розповсюджувати звіти з питань збору даних особам, які приймають рішення.
T0674	Розповсюджувати повідомлення про завдання та плани зі збору даних.
T0675	Проводити і документувати оцінку результатів збору даних з використанням встановлених процедур.
T0676	Розробляти вимоги до збору і проведення розвідки.
T0677	Редагувати або виконувати прості скрипти (наприклад, Perl, VBScript) в ОС Windows і UNIX.
T0678	Залучати клієнтів до розуміння їх потреб і зацікавленості в результатах розвідувальних заходів.
T0679	Забезпечувати ефективний перехід від оперативного планування до відповідності поточних операцій.
T0680	Переконатися, що діяльність з планування розвідки інтегрована та синхронізована з графіками оперативного планування.
T0681	Встановлювати альтернативні напрямки обробки, використання і поширення інформації з метою вирішення виявлених питань і проблем.
T0682	Підтверджувати зв'язок між вимогами до запитів на збір даних і вимогами до критичної інформації та пріоритетними вимогами керівництва до розвідувальних заходів.
T0683	Встановлювати заходи з управління обробкою, експлуатацією та розповсюдженням з використанням затверджених настанов і/або процедур.
T0684	Оцінювати оперативні ефекти, які забезпечує кібердіяльність.
T0685	Оцінювати процеси прийняття рішень щодо загроз.
T0686	Ідентифікувати вразливості загроз.
T0687	Ідентифікувати загрози, викликані вразливостями в системі стеження «Blue Force».
T0688	Оцінювати наявні можливості щодо бажаних ефектів, щоб рекомендувати ефективні рішення.
T0689	Оцінювати обсяг даних, зібраних та/або наданих розвідкою, який задовольняє запити на отримання інформації.
T0690	Оцінювати оцінки розвідки для підтримки циклу планування.
T0691	Оцінювати умови, які впливають на використання наявних спроможностей кіберрозвідки.
T0692	Генерувати та оцінювати ефективність стратегій аналізу мережі.
T0693	Оцінювати ступінь відповідності операцій зі збору інформації оперативним вимогам.
T0694	Оцінювати ефективність операцій зі збору інформації відповідно до плану.
T0695	Досліджувати метадані та матеріали перехоплення з точки зору розуміння важливості визначення цілій.
T0696	Застосовувати мережеві пристрої, пристрої захисту та/або термінали з використанням різних методів або засобів.
T0697	Спрощувати доступ за допомогою фізичних і/або безпровідних засобів.
T0698	Сприяти безперервному оновленню вихідних даних для розвідки, систем стеження і візуального спостереження в інтересах фахівців оперативної відеозйомки.
T0699	Сприяти співробітництву між внутрішніми і зовнішніми посадовими особами, які приймають рішення для синхронізації та інтеграції основних напрямків діяльності на підтримку цілій.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор завдання	Опис завдання
T0700	Сприяти обміну «кращими практиками » і «отриманими уроками» у спільноті кібероперації.
T0701	Співпрацювати з розробниками, передаючи їм цільову і технічну інформацію при розгляді вимог до розроблюваних інструментів для покращення розробки інструментів.
T0702	Формулювати стратегії збору даних, ґрунтуючись на знанні наявних можливостей дисциплін розвідки та методах збору інформації, які об'єднують можливості мультидисциплінарного збору даних і доступу до цілей і їх спостережень.
T0703	Збирати та аналізувати дані (наприклад, показники ефективності) з метою визначення ефективності, та готувати звітні документи для проведення подальших заходів.
T0704	Включати плани підтримки кібероперацій і безпеки зв'язку до цілій організації.
T0705	Включати розвідку і контррозвідку в процес розробки плану.
T0706	Збирати дані про мережі за допомогою звичайних і альтернативних способів (наприклад, аналіз соціальних мереж, ланцюжки дзвінків, аналіз трафіку).
T0707	Формувати запити на інформацію.
T0708	Визначати тактику та методологію загрози.
T0709	Визначати всі доступні можливості і обмеження розвідки, проведеної партнерами, які підтримують кібероперації.
T0710	Визначати та оцінювати усі критичні спроможності, вимоги і вразливості загрози.
T0711	Визначати, розробляти, оцінювати і пріоритезувати відповідні вимоги щодо розвідки або інформації.
T0712	Визначати та управляти пріоритетами в області забезпечення безпеки при взаємодії з зовнішніми партнерами.
T0713	Визначати та подавати на розгляд вимоги до розвідувальних заходів з метою розробки пріоритетних вимог до інформації.
T0714	Визначати платформи співпраці, які можуть сприяти узгодженню процесів, функцій і результатів з певними організаціями і функціональними групами.
T0715	Визначати недоліки та потенційні стратегії збору інформації про цілі.
T0716	Визначати вимоги і процедури координації з призначеними органами зі збору інформації.
T0717	Визначати критичні компоненти цілі.
T0718	Визначати недоліки і вади в розвідувальних заходах.
T0719	Визначати пробіли і недоліки кіберрозвідки для оперативного кіберпланування.
T0720	Визначати пробіли у власному розумінні технології цілі і розробці інноваційних підходів до збору даних.
T0721	Визначати питання та проблеми, які можуть вплинути і/або істотно знизити ефективність архітектур обробки, експлуатації та розповсюдження.
T0722	Визначати компоненти мережі і їх функціональність для аналізу та розробки цілі.
T0723	Визначати потенційні напрямки зі збору даних з метою їх застосування відповідно до пріоритетних вимог до інформації.
T0724	Виявляти сильні сторони та вразливості мережі.
T0725	Ідентифікувати та знижувати ризики для здатності управління збором інформації для підтримки плану, операцій та циклу цілі.
T0726	Виявляти потреби, обсяг і часові рамки для підготовленої продукції застосовного середовища розвідки.
T0727	Ідентифікувати, визначати місце та відслідковувати цілі за допомогою методик геопросторового аналізу.
T0728	Забезпечувати введення або розробляти напрямки дій, виходячи з факторів загрози.
T0729	Інформувати зовнішніх партнерів про можливі наслідки введення нових або коригування існуючих політики та настанов з проведення спільних кібероперацій.
T0730	Інформувати зацікавлені сторони (наприклад, спеціалістів зі збору інформації, розпорядників активами, центри обробки, експлуатації і розповсюдження) про результати оцінки, використовуючи встановлені процедури.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор завдання	Опис завдання
T0731	Відправляти запити, щоб керувати завданнями і надавати допомогу з управління зборами даних.
T0732	Інтегрувати процеси планування /визначення цілій з іншими організаціями
T0733	Інтерпретувати результати оцінювання підготовки середовища з метою визначення подальших дій.
T0734	Видавати запити на отримання інформації.
T0735	Керувати та узгоджувати розвідувальну підтримку оперативного планування.
T0736	Керувати або дозволяти проведення операцій для підтримки цілей організації та вимог цілей.
T0737	Пов'язувати вимоги щодо пріоритетного збору даних з оптимальними активами і ресурсами.
T0738	Підтримувати обізнаність про досягнення в апаратних та програмних технологіях (наприклад, брати участь в тренінгах і або конференціях, читати) і їх можливі наслідки.
T0739	Налагоджувати взаємозв'язки з внутрішніми і зовнішніми партнерами, що залучаються до кіберпланування або суміжних сфер.
T0740	Підтримувати ситуаційну обізнаність і функціональність органічної операційної інфраструктури.
T0741	Підтримувати ситуаційну обізнаність про вимоги до розвідки, пов'язаних з кібербезпекою та відповідних завдань.
T0742	Підтримувати ситуаційну обізнаність про можливості та діяльність партнерів.
T0743	Підтримувати ситуаційну обізнаність щоб визначити, чи потребують зміни в операційному середовище перегляду і коригування плану.
T0744	Підтримувати перелік цілей (а саме, Обмежений список цілей (RTL), Загальний список цілей (JTL), Список ймовірних цілей (CTL) та ін.).
T0745	Розробляти рекомендації для настанов зі збору даних відповідно до вимог замовника.
T0746	Змінювати вимоги до збору даних за необхідності.
T0747	Моніторити і оцінювати інтегровані кібероперації з метою визначення можливостей досягнення цілей організації.
T0748	Моніторити та звітувати про зміни в розташуванні, діяльності, тактиці, спроможностях, цілях і т.п. загроз, що стосуються визначеного набору проблем щодо попередження кібероперацій.
T0749	Моніторити та звітувати про підтверджені загрозливі дії.
T0750	Моніторити завершення перерозподілених зусиль зі збору інформації.
T0751	Моніторити Web-сайти відкритих джерел на предмет вороже налаштованого контенту, яка торкається інтересів організації або партнерів.
T0752	Моніторити операційне середовище та звітувати про ворожу діяльність згідно встановлених керівництвом вимогам до пріоритетної інформації.
T0753	Моніторити функціональний стан і ефективність обробки, експлуатації та архітектури розповсюдження.
T0754	Моніторити мережі цілей для індикації та оповіщення про зміни комунікацій цілій або збої в обробці.
T0755	Моніторити операційне середовище щодо потенційних та ризиків для процесу управління операціями зі збору інформації.
T0756	Здійснювати експлуатацію та підтримку автоматизованих систем для отримання і здійснення доступу до цільових систем.
T0757	Забезпечувати оптимізацію поєднання активів і ресурсів збору даних для підвищення ефективності та продуктивності щодо суттєвої інформації, пов'язаної з пріоритетними вимогами до розвідки.
T0758	Здійснювати вчасно інтегровану, об'єднану, розвідувальну інформацію про кібероперації з усіх джерел та/або надавати показники і попередження про результати розвідки (наприклад, оцінку загроз, брифінги, дослідження розвідки, дослідження країн).
T0759	Сприяти аналізу і вдосконаленню політики, включаючи оцінку наслідків прийняття або відмови від такої політики.
T0760	Надавати експертні знання за тематикою командам планування, координаційним групам і оперативним групам за необхідності.

Ідентифікатор завдання	Опис завдання
T0761	Надавати предметні експертні знання та підтримку форумів з планування/ форумам з розвитку і робочим групам належним чином.
T0763	Проводити заходи з довгострокового стратегічного планування за участю внутрішніх і зовнішніх партнерів з кібердіяльності.
T0764	Надавати предметні експертні знання щодо планування зусиль за участю внутрішніх і зовнішніх партнерів з кібероперацій.
T0765	Проводити предметну експертизу розробки вправ.
T0766	Пропонувати політику взаємодії, яка регулює взаємодію із зовнішніми групами координації.
T0767	Виконувати аналіз контенту та/або метаданих для досягнення цілей організації.
T0768	Здійснювати кібердіяльність з метою руйнування/видалення інформації, що міститься в комп'ютерах і обчислювальних мережах.
T0769	Проводити заходи з автоматизації націлювання.
T0770	Характеризувати Web-сайти.
T0771	Проводити предметну експертизу характеризацій вебсайту.
T0772	Готувати і проводити предметну експертизу в інтересах відповідних заходів.
T0773	Розставляти пріоритети серед вимог до збору інформації для комп'ютерних платформ, що використовуються для збору даних, з урахуванням можливостей таких платформ.
T0774	Обробляти відфільтровані дані, призначені для аналізу та/або розповсюдження між замовниками.
T0775	Проводити реконструкції мережі.
T0776	Випускати результати аналізу системи цілі.
T0777	Описувати обов'язки мережевих або системних адміністраторів і їх діяльність.
T0778	Описувати цілі та їхню діяльність.
T0779	Надавати консультації/допомогу посадовим особам, які приймають рішення з питань проведення операцій і розвідувальних заходів, щодо розподілу активів і ресурсів збору даних у відповідь на динамічні оперативні ситуації.
T0780	Надавати консультативну та адвокатську підтримку для популяризації плану збирання, як невід'ємної складової компоненти стратегічних планів та інших адаптивних планів.
T0781	Розробляти рекомендації з досягнення мети та проведення повторних кібероперацій.
T0782	Забезпечити аналіз та підтримку оцінки результативності.
T0783	Забезпечувати поточну розвідувальну підтримку критичним внутрішнім / зовнішнім зацікавленим сторонам.
T0784	Розробляти настанови з кіберзаходів і консультувати щодо вхідних даних для планів підтримки розвідки.
T0785	Здійснювати оцінку і зворотний зв'язок, необхідні для поліпшення результативності розвідки, звітності за результатами розвідки, вимог до збору даних і операцій.
T0786	Надавати інформацію та оцінки з метою інформування керівництва і клієнтів; розробки та уточнення цілей; забезпечення планування та проведення операцій; а також оцінки результатів операцій.
T0787	Надавати вхідні дані для розробки та уточнення цілей, пріоритетів, стратегій, планів і програм кібероперацій.
T0788	Надавати вхідні дані та брати участь в процедурах оцінки результативності після дії.
T0789	Надавати вхідні дані та брати участь в розробці планів та настанов.
T0790	Надавати вхідні дані для оцінки ефективності визначення цілі для схвалення керівництвом.
T0791	Надавати вхідні дані для адміністративних і логічних елементів плану оперативної підтримки.
T0792	Здійснювати аналіз розвідувальних заходів для підтримки призначених навчань, заходів з планування і операцій, залежних від часу їх проведення.
T0793	Забезпечувати ефективність проведення навчань і/або операцій, які залежать від часу.
T0794	Розробляти рекомендації щодо операцій та повторення.
T0795	Забезпечувати підтримку планування між внутрішніми і зовнішніми партнерами.
T0796	Надавати актуальні геоінформаційні дані в режимі реального часу.
T0797	Розробляти цільові рекомендації, які відповідають поставленим керівництвом цілям.
T0798	Забезпечувати цільові продукти та цільову підтримку за призначенням

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор завдання	Опис завдання
T0799	Забезпечувати чутливе до часу визначення цілей
T0800	Своєчасно повідомляти про загрозливі або ворожі наміри або дії, які можуть вплинути на цілі, ресурси або спроможності організації.
T0801	Розробляти рекомендації щодо вдосконалення, адаптації, припинення або виконання оперативних планів в залежності від ситуації.
T0802	Переглядати відповідні джерела інформації, щоб визначити достовірність і актуальність зібраної інформації.
T0803	Реконструювати мережі в форматі діаграм або звітів.
T0804	Документувати заходи зі збору інформації та/або підготовку середовища щодо цілей протягом проведення операцій, спрямованих на досягнення кіберефектів.
T0805	Готувати звіти на основі розвідданих про значні мережеві події і вторгнення.
T0806	Готувати запити на обробку, використання і розподіл специфічної тематичної інформації, отриманої під час збору даних, використовуючи специфічні тематичні активи і ресурси здобутих даних відповідно до затверджених настанов і/або процедур.
T0807	Досліджувати тенденції розвитку каналів зв'язку в сучасних технологіях (в комп'ютерних і телефонних мережах, супутникових, кабельних і бездротових системах передачі) відкритих і закритих джерелах.
T0808	Переглядати та розуміти цілі, поставлені керівництвом організації, а також настанови з планування.
T0809	Переглядати спроможності розподілених активів збору інформації.
T0810	Переглядати настанову зі збору розвідувальної інформації на предмет її точності/застосовності.
T0811	Переглядати перелік вимог зі збору пріоритетної інформації та важливих даних.
T0812	Переглядати та оновлювати загальний план зі збору інформації за необхідності.
T0813	Переглядати, затверджувати, пріоритезувати та подавати на розгляд операційні вимоги для дослідження, розробки і/або набуття кіберспроможностей.
T0814	Переглядати матрицю збору даних на основі наявності оптимальних активів і ресурсів.
T0815	Видаляти зайву та мінімізувати інформацію з метою захисту джерел і методів.
T0816	Розробляти план заходів щодо проведення кіберрозвідки.
T0817	Слугувати як провідник інформації від команд партнерів, визначаючи експертів у відповідній області, які можуть допомогти у розслідуванні складних або незвичайних подій.
T0818	Підтримувати зв'язок із зовнішніми партнерами.
T0819	Запитувати і доводити до завершення зворотній зв'язок від клієнтів щодо якості, своєчасності та ефективності збору даних відповідно до вимог збору.
T0820	Конкретизувати зміни в планах зі збору даних і/або операційному середовищі, які потребують повторного виконання завдань або перенаправлення активів збору і ресурсів.
T0821	Конкретизувати заходи зі збору специфічної тематичної інформації та/або завдань, які повинні бути виконані найближчим часом.
T0822	Направляти інформаційні запити у підрозділ з управління вимогами до збору даних для обробки як запити на збір даних.
T0823	Направляти або відповідати на запити щодо врегулювання конфліктних ситуацій в кібероперацiях.
T0824	Брати участь в ідентифікації та документуванні побічних ефектів.
T0825	Синхронізувати кібердіяльність щодо міжнародної взаємодії та відповідні потреби в ресурсах.
T0826	Синхронізувати кіберчастини планів співпраці в сфері кібербезпеки.
T0827	Синхронізувати комплексне застосування всіх доступних активів збору власної і партнерської розвідки використовуючи наявні можливості та методи співпраці.
T0828	Тестувати і оцінювати локально розроблені засоби з метою з оперативного використання.
T0829	Тестувати інструменти і методики, розроблені всередині організації, проти інструментів цілі.
T0830	Відстежувати статус запитів на отримання інформації, включаючи ті, які розглядаються як запити на збір даних, а також виконання технологічних вимог, використовуючи встановлені процедури.
T0831	Перекладати запити зі збору даних в застосовні вимоги до збору специфічної інформації.
T0832	Використовувати результати зворотного зв'язку (наприклад, отриманий урок), щоб визначити можливості підвищення ефективності та результативності управління збором даних.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор завдання	Опис завдання
T0833	Підтверджувати запити на отримання інформації відповідно до встановлених критеріїв.
T0834	Тісно співпрацювати зі спеціалістами з планування, аналітиками розвідки і співробітниками зі збору даних з метою забезпечення точності і актуальності вимог до розвідки і планів зі збору даних.
T0835	Тісно співпрацювати зі спеціалістами з планування, аналітиками і менеджерами зі збору даних, щоб виявити пробіли у розвідці та забезпечити точність і актуальність вимог до розвідки.
T0836	Документувати отримані уроки, які відображають результати подій та/або навчань.
T0837	Консультувати менеджерів та операторів з мовних та культурних питань, які впливають на досягнення цілей організації.
T0838	Аналізувати і обробляти інформацію на основі використання мовної та/або культурологічної експертизи.
T0839	Оцінювати, документувати та застосовувати мотивацію і/або світогляд цілей для сприяння аналізу, визначення мети і проведення заходів зі збору даних.
T0840	Співпрацювати з внутрішніми та/або зовнішніми організаційними структурами з метою підвищення ефективності збору, аналізу і розповсюдження даних.
T0841	Проводити дослідження цілей на основі різних джерел з використання матеріалів відкритих джерел мовою цілі.
T0842	Проводити аналіз комунікацій цілей для виявлення необхідної інформації на підтримку цілей організації.
T0843	Проводити аналіз якості та забезпечувати зворотний зв’язок щодо розшифрованих або переведених матеріалів.
T0844	Оцінювати та інтерпретувати метадані з метою визначення закономірностей, аномалій або подій, для оптимізації процесу таргетування, аналізу і обробки.
T0845	Визначати тактики і методології кіберзагроз.
T0846	Ідентифікувати цільові комунікації в рамках глобальної мережі.
T0847	Підтримувати обізнаність щодо інструментів, прийомів та характеристик цільових мереж (наприклад, пропускна здатність, функціональна можливість,, маршрути і критичні вузли), і їх потенційних наслідків на таргетування, аналіз і збір даних.
T0848	Забезпечити зворотний зв’язок зі спеціалістами зі збору даних, щоб покращити майбутній збір даних та аналіз.
T0849	Проводити ідентифікацію іноземної мови та діалекту по вхідним даним.
T0850	Проводити або підтримувати технічний аналіз мережі і картографію.
T0851	Забезпечувати формування вимог і зворотний зв’язок з метою оптимізації розвитку засобів обробки мов.
T0852	Проводити аналіз соціальних мереж і документувати результати аналізу за необхідності.
T0853	Сканувати, ідентифікувати і пріоритезувати графіку (включаючи міжкомп’ютерні комунікації) і/або голосовий мовний матеріал.
T0854	Відправляти критичну або інформацію, що залежить від часу, відповідним замовникам.
T0855	Розшифровувати голосові мовні матеріали мовою цілі.
T0856	Здійснювати переклад (наприклад, дослівний, по суті та/або анотація) цільового графічного матеріалу
T0857	Здійснювати переклад (наприклад, дослівний, по суті та/або анотація)цільових голосових матеріалів.
T0858	Виявляти іноземну термінологію в комп’ютерних програмах (наприклад, коментарі, назви змінні).
T0859	Проводити мовний аналіз в режимі реального часу (наприклад, під час проведення операцій).
T0860	Визначити кібер/технологічну термінологію цільовою мовою
T0861	Співпрацювати з головним юрисконсультом, представниками зовнішніх зв’язків і бізнесів для забезпечення, що існуючі і нові послуги задовольняють вимоги приватності і безпеки даних.
T0862	Співпрацювати з юрисконсультом і керівництвом, головними відділами і комітетами, щоб переконатися, що організація має і підтримує відповідну угоду щодо забезпечення приватності і конфіденційності, форми авторизації та інформаційні повідомлення та матеріали, які відображають поточні корпоративні та правові методики і вимоги.

Ідентифікатор завдання	Опис завдання
T0863	Співпрацювати з відповідними регуляторними органами для забезпечення того, що програми, політики і процедури, які стосуються свобод громадян та приватності, вирішуються комплексно і всебічно.
T0864	Взаємодіяти з регуляторними органами та органами з акредитації.
T0865	Співпрацювати зі зовнішніми організаціями з метою налагодження взаємозв'язків з регуляторними органами та іншими державними чиновниками, які відповідають за вирішення питань щодо приватності та безпеки даних.
T0866	Підтримувати знання про діючі федеральні та регіональні закони щодо приватності та стандартів з акредитації та моніторити досягнення в технологіях приватності інформації для забезпечення адаптації та відповідності організації.
T0867	Забезпечити, щоб усі системи обробки та/або бази даних були зареєстровані в місцевих органах приватності /захисту даних.
T0868	Співпрацювати з бізнес-групами та вищим керівництвом, щоб забезпечити обізнаність щодо «кращих практик » з питань приватності та безпеки даних.
T0869	Співпрацювати з вищим керівництвом організації для створення загального для організації комітету з нагляду за приватністю.
T0870	Виконувати обов'язки керівника комітету з нагляду за приватністю.
T0871	Співпрацювати над політиками та процедурами у сфері кіберприватності та кібербезпеки.
T0872	Співпрацювати з фахівцями із кібербезпеки в процесі оцінки ризиків безпеки для вирішення питань дотримання приватності та зменшення ризиків.
T0873	Співпрацювати з вищим керівництвом з метою розробки стратегічних планів збору даних, використання і розподілу інформації таким способом, щоб максимально підвищити її оперативну цінність при дотриманні відповідних нормативних вимог приватності
T0874	Надавати стратегічні настанови корпоративним керівникам організації щодо інформаційних ресурсів і технологій.
T0875	Надавати допомогу керівнику з безпеки з питань розробки та впровадження інформаційної інфраструктури.
T0876	Співпрацювати з головним комплаєнс-менеджером щодо процедур документування і підготовки звітів про саморозкриття будь-яких доказів порушення приватності.
T0877	Співпрацювати з наявними підрозділами організації з нагляду за дотриманням прав споживачів на отримання доступу до інформації.
T0878	Слугувати у якості сполучної ланки щодо забезпечення приватності інформації для користувачів технологічних систем
T0879	Слугувати у якості сполучної ланки з відділом інформаційних систем.
T0880	Розробляти матеріали для тренінгів з приватності та інших комунікацій для покращення розуміння працівниками політик приватності в організації, практик і процедур обробки даних, та юридичних зобов'язань.
T0881	Контролювати, направляти, проводити або забезпечувати проведення початкового тренінгу або орієнтації на приватність всіх працівників, волонтерів, підрядників, контрагентів, ділових партнерів та інших відповідних третіх сторін.
T0882	Проводити регулярні тренінги з приватності та обізнаності.
T0883	Співпрацювати з зовнішніми відомствами для розвитку взаємозв'язків з компаніями-замовниками та іншими неурядовими організаціями, зацікавленими у вирішенні проблем приватності і безпеки даних, а також для управління участю компанії в публічних заходах, що стосуються питань приватності та безпеки даних.
T0884	Співпрацювати з адміністрацією компанії, юрисконсультом та іншими зацікавленими сторонами, щоб представляти інтереси організації щодо приватності інформації зі зовнішнім суб'єктами, включаючи урядові органи, які зобов'язуються прийняти або внести зміни в законодавство, нормативні акти або стандарти з питань приватності.
T0885	Періодично звітувати раді директорів, виконавчому директору (CEO) та іншим відповідальним особам про стан програми з приватності.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор завдання	Опис завдання
T0886	Співпрацювати з представниками зовнішнього відомства, щоб реагувати на запити преси та інші запити, що стосуються персональних даних клієнтів і співробітників організації.
T0887	Очолювати програму приватності в організації.
T0888	Направляти та наглядати за спеціалістами з приватності та координувати програми приватності та безпеки даних з вищими керівниками глобально, щоб забезпечити узгодженість в усієї організації.
T0889	Забезпечувати відповідність практикам з приватності та послідовному застосуванню санкцій в разі недотримання політик приватності для усіх осіб у штаті організації, допоміжних трудових ресурсів, розширеного штату та для всіх ділових партнерів у взаємодії з відділами кадрового забезпечення, менеджером з питань безпеки інформації, адміністрації та юрисконсульта відповідним чином.
T0890	Розробляти відповідні санкції за недотримання корпоративних політик і процедур
T0891	Розглядати заяви про невиконання корпоративних політик приватності або повідомлення про інформаційну практику.
T0892	Розробляти та координувати управління ризиками і відповідність загальним принципам для приватності.
T0893	Проводити комплексний аналіз проектів даних компанії і проектів приватності та переконатися, що вони відповідають корпоративним цілям і політикам приватності та безпеки даних.
T0894	Розробляти і управляти процедурами всього підприємства для забезпечення розвитку нових продуктів та послуг відповідно до політик приватності і юридичних зобов'язань компанії.
T0895	Формувати процес прийому, документування, відстеження, розслідування та прийняття рішень щодо всіх претензій, які торкаються політик і процедур приватності організації.
T0896	Встановлювати разом з керівництвом та операціями механізм відстеження доступу до медичної інформації, що охороняється, в межах компетенцій організації та відповідно до вимог законодавства, і надавати кваліфікованим співробітникам можливості перегляду або отримання звітних документів за такою діяльністю.
T0897	Забезпечити керування плануванням, проектуванням і оцінкою проектів, пов'язаних із забезпеченням приватності і безпеки.
T0898	Розробляти програму внутрішнього аудиту приватності.
T0899	Періодично переглядати програму приватності на основі змін в законодавстві, нормативних актах або політиці організації.
T0900	Розробляти настанови та брати участь у визначенні, впровадженні та підтримки політик і процедур приватності інформації організації в координації з керівництвом, адміністрацією та юрисконсультом організації.
T0901	Забезпечити, що використання технологій зберігає, а не руйнує захист приватності під час використання, збору та розкриття персональних даних.
T0902	Моніторити розробку систем і операції для забезпечення відповідності вимогам безпеки та приватності.
T0903	Проводити оцінку впливу на приватність запропонованих правил щодо приватності персональних даних, включаючи тип зібраних персональних даних і кількість людей, яких це стосується
T0904	Проводити періодичну оцінку впливу на приватність інформації та поточну діяльність з моніторингу з координації іншими функціями організації і оперативною оцінкою.
T0905	Аналізувати усі плани з інформаційної безпеки системи, щоб забезпечити узгодження між практиками безпеки та приватності.
T0906	Співпрацювати з усіма працівниками організації, залученими до будь-яких аспектів оприлюднення захищеної інформації для забезпечення відповідності політикам, процедурам організації, і вимогам законодавства.
T0907	Реєструвати та адмініструвати індивідуальні запити на розголошення або розкриття персональних і/або захищених даних.
T0908	Розробляти і управляти процедурами перевірки і аудиту постачальників на предмет їх відповідності вимогам політик приватності і безпеки даних та вимогам законодавства.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

ID завдання	Опис завдання
T0909	Брати участь у впровадженні і поточному моніторингу відповідності всіх угод з торговими партнерами і бізнес спільнотами, щоб забезпечити вирішення усіх проблем приватності, вимог та відповідальності.
T0910	Виконувати обов'язки консультанта або співпрацювати з консультантом стосовно контрактів з бізнес партнерами.
T0911	Зменшувати наслідки використання або розкриття персональних даних співробітниками або бізнес партнерами.
T0912	Розробляти і застосовувати процедури, пов'язані з коригуванням діяльності.
T0913	Адмініструвати діяльність щодо усіх скарг, що стосуються політик і процедур з приватності організації, у координації та співпраці з іншими подібними функціями, та, за необхідності, з юрисконсультом.
T0914	Дотримуватись прийнятої в організації програми приватності, тісно взаємодіючи з уповноваженим із приватності, директором із інформаційної безпеки та іншими керівниками, щоб забезпечити дотримання федеральних і державних законів і нормативних актів з приватності.
T0915	Ідентифікувати та усувати потенційні пробіли відповідності у компанії і/або у зонах ризику для забезпечення повного дотримання нормативних вимог з приватності.
T0916	Управляти інцидентами і порушеннями приватності спільно з уповноваженим з приватності, головним керівником з інформаційної безпеки, юрисконсультом і підрозділами компанії.
T0917	Співпрацювати з головним керівником з інформаційної безпеки, щоб забезпечити узгодженість між практиками безпеки і приватності.
T0918	Розробляти, впроваджувати та підтримувати корпоративні політики і процедури щодо дотримання нормативних актів з приватності.
T0919	Переконатися, що компанія підтримує відповідні повідомлення про приватність та конфіденційність, форми згоди та форми авторизації та інші матеріали.
T0920	Розробляти і підтримувати відповідну комунікацію та тренінги для заохочення та освіти всього персоналу і членів правління з питань дотримання приватності та вимог, і наслідків в разі недотримання вимог.
T0921	Визначати вимоги партнерів по бізнесу, пов'язані з програмою забезпечення приватності організації.
T0922	Розробити і управляти процесами отримання, документування, відстеження, розслідування, і за необхідності прийняття коригувальних заходів, які стосуються політик і процедур з приватності.
T0923	Співпрацювати з відповідними регуляторними відомствами та іншими законодавчими органами та відповідальними особами організації, при проведенні будь-яких перевірок відповідності або розслідувань.
T0924	Проводити поточний моніторинг дотримання приватності.
T0925	Моніторити досягнення в технологіях приватності інформації, щоб забезпечити прийняття та дотримання організацією.
T0926	Розробляти або брати участь в розробці матеріалів для тренінгів з приватності та інших засобів комунікацій, щоб покращити розуміння працівниками політик,, практик і процедур обробки даних і юридичних зобов'язань.
T0927	Призначати групу експертів з безпеки інформаційних технологій і керувати нею.
T0928	Співпрацювати з ключовими зацікавленими сторонами з метою створення програми управління кіберризиками.
T0929	Визначати та призначати осіб на певні ролі, пов'язані з виконанням Загальних принципів управління ризиками.
T0930	Розробити стратегію управління ризиками організації, яка включає визначення прийняття ризиків.
T0931	Визначати місії, бізнес функції і місію/бізнес процеси, які буде підтримувати система.
T0932	Визначати зацікавлених сторін, які мають інтереси до безпеки при розробленні, впровадженні, функціонуванні або підтримці системи.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор завдання	Опис завдання
T0933	Визначати зацікавлених сторін, які мають інтереси до безпеки при розробленні, впровадженні, функціонуванні або підтримці системи.
T0934	Визначати активи зацікавлених сторін, які потребують захисту.
T0935	Проводити початкову оцінку ризиків активів зацікавлених сторін та оновлювати оцінку ризиків на регулярної основі.
T0936	Визначати потреби у захисті та вимоги до безпеки для зацікавлених сторін.
T0937	Визначати розміщення системи в архітектурі підприємства.
T0938	Визначати загальні для всієї організації контролі, які можуть бути успадковані системами організації.
T0939	Проводити категоризацію безпеки другого рівня для систем організації з однаковим рівнем впливу.
T0940	Визначати кордони системи.
T0941	Визначати вимоги до безпеки, які застосовуються до системи і організації.
T0942	Визначати типи інформації, яка підлягає обробці, зберіганню або передачі системою.
T0943	Здійснювати категоризацію системи і документувати результати категоризації безпеки як частину системних вимог.
T0944	Описувати характеристики системи.
T0945	Реєструвати систему у відповідних програмах організацій /офісах управління.
T0946	Обирати контролі безпеки для системи і документувати функціональний опис запланованих впроваджень контролів безпеки.
T0947	Розробляти стратегію моніторингу результативності контролів безпеки; координувати стратегію на системному рівні зі стратегією моніторингу на рівні організації та місії/ бізнес-процесу.
T0948	Переглядати та затверджувати плани безпеки.
T0949	Впроваджувати контролі безпеки, описані у плані безпеки або іншій документації системи.
T0950	Документувати зміни у процесі планового впровадження контролів безпеки та встановлювати базову лінію конфігурації для системи.
T0951	Розробляти, переглядати та затверджувати план оцінки контролів безпеки у системі і організації.
T0952	Оцінювати контролі безпеки відповідно до процедур оцінювання, визначених в плані оцінки безпеки.
T0953	Готувати звіт за результатами оцінки безпеки, документуючи проблеми, висновки і рекомендації з оцінки контролю безпеки.
T0954	Проводити початкову діяльність до усунення проблем безпеки на основі висновків і рекомендацій, представлених у звіті про оцінку безпеки; проводити повторну оцінку виправлених засобів контролю.
T0955	Готувати план заходів та контрольні точки на основі висновків і рекомендацій, представлених у звіті про оцінку безпеки, за винятком будь-яких вжитих заходів усунення проблем.
T0956	Сформувати перелік авторизації і відправити його уповноваженій особі для затвердження.
T0957	Виявляти ризик, викликаний функціонуванням або використанням системи, або забезпеченням або використанням загальних контролів.
T0958	Визначати та впроваджувати переважний напрямок дій у відповідь на виявлений ризик.
T0959	Визначати, чи є ризик, викликаний функціонуванням або використанням системи, або забезпеченням або використанням загальних контролів, прийнятним.
T0960	Моніторити зміни в системі і в середовищі її функціонування.
T0961	Оцінювати контролі безпеки, що використовуються в системі і успадковані нею, відповідно до стратегії моніторингу, прийнятої в організації.
T0962	Реагувати на ризик на основі результатів поточної діяльності з моніторингу, оцінки ризиків і невиконаних пунктів плану дій та контрольних точок.

Ідентифікатор завдання	Опис завдання
T0963	Оновлювати план безпеки, звіт про оцінку безпеки і план дій та етапів на основі результатів, отриманих в процесі безперервного моніторингу.
T0964	Звітувати уповноваженій особі про стан безпеки системи (включаючи ефективність контролів безпеки) на постійній основі відповідно до стратегії моніторингу.
T0965	Переглядати стан безпеки системи (включаючи ефективність контролів безпеки) на постійній основі, щоб визначити, чи є ризик залишається прийнятним.
T0966	Впроваджувати стратегію видалення системи, яка виконує необхідні дії, коли система вилучається з обслуговування.
T0967	Підтримувати та сприяти безперервному моніторингу в організації.
T0968	Призначати за потреби персонал до відповідних робочих груп безперервного моніторингу.
T0969	Визначати вимоги до звітності для підтримки діяльності з ів безперервного моніторингу.
T0970	Формувати систему критеріїв та показників для оцінки ефективності програми безперервного моніторингу.
T0971	Визначати, як інтегрувати програму безперервного моніторингу в більш широкі структури безпеки і політики корпоративного управління ї організації.
T0972	Використовувати показники оцінки і ранжування безперервного моніторингу при прийнятті інвестиційних рішень в області інформаційно безпеки з метою вирішення постійних питань.
T0973	Переконатися, що персонал безперервного моніторингу має підготовку і ресурси (наприклад, персонал і бюджет) для виконання покладених на нього обов'язків.
T0974	Співпрацювати з аналітиками ризиків організації, щоб забезпечити, що звітність по безперервному моніторингу охоплює відповідні структури організації.
T0975	Співпрацювати з аналітиками ризиків організації, щоб переконатися, що показники ризиків є реалістичними для підтримки безперервного моніторингу.
T0976	Співпрацювати зі посадовими особами організації, щоб забезпечити, що дані, отримані за допомогою інструментів безперервного моніторингу, забезпечують ситуаційну обізнаність про рівні ризику.
T0977	Встановлювати тригери неприпустимих порогових значень ризиків для даних безперервного моніторингу.
T0978	Співпрацювати зі посадовими особами організації над встановленням категорій звітності на системному рівні, які можуть використовуватися в програмі безперервного моніторингу організації.
T0980	Призначати кваліфіковану особу в якості відповідального за керування та впровадження програми безперервного моніторингу.
T0981	Визначати зацікавлені сторони в програмі безперервного моніторингу та організовувати процес їхнього інформування про програму.
T0982	Визначати вимоги до звітності організації, орієнтованої на безпеку, які виконуються програмою безперервного моніторингу.
T0983	Використовувати дані, отримані в ході безперервного моніторингу, в процесі прийняття рішень щодо інвестування в сферу інформаційної безпеки з метою подолання існуючих проблем.
T0984	Визначати в програмі безперервного моніторингу тригери, які можуть використовуватися для визначення неприпустимого ризику та вжиття заходів щодо його усунення.
T0985	Формувати системи показників і критеріїв якості з метою оцінки ефективності програми безперервного моніторингу.
T0986	Співпрацювати з керівниками з безпеки з метою формування відповідних вимог до звітності по безперервному моніторингу на системному рівні.
T0987	Використовувати інструменти і технології безперервного моніторингу з метою оцінки ризиків на постійній основі.
T0988	Встановлювати відповідні вимоги до звітності відповідно до критеріїв, зазначених в програмі безперервного моніторингу для використання в автоматизованій оцінки контролів
T0989	Використовувати неавтоматизовані методи оцінки, коли дані з інструментів та технологій безперервного моніторингу, не відповідають вимогам до їх повноти або якості.
T0990	Розробляти спільно з групою зовнішнього аудиту процедури обміну інформацією стосовно програми безперервного моніторингу, та її впливу на оцінку контролів безпеки.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор завдання	Опис завдання
T0991	Визначати вимоги до звітності для використання в автоматизованій оцінці контролю для підтримки безперервного моніторингу.
T0992	Визначати, як будуть використовуватися результати безперервного моніторингу в поточній авторизації.
T0993	Організовувати процеси і процедури контролю доступу до інструментів і технологій безперервного моніторингу.
T0994	Забезпечувати управління контролем доступу до інструментів и технологій безперервного моніторингу належним чином.
T0995	Організовувати процес надання технічної допомоги фахівцям з пом'якшення за безперервного моніторингом.
T0996	Координувати роботу з різними користувачами щодо вимог до звітності безперервного моніторингу.
T0997	Встановлювати відповідальність за забезпечення впровадження кожного інструменту або кожної технології безперервного моніторингу.
T0998	Взаємодіяти з робочою групою з розроблення показників і критеріїв для підтримки безперервного моніторингу.
T0999	Формувати та керувати процесом включення нового ризику для забезпечення безперервного моніторингу.
T1000	Визначати проблеми конфігурації безперервного моніторингу і створювати підгрупи для координації.
T1001	Розробляти вимоги до вимірювання/забезпечення продуктивності інструментів і технологій безперервного моніторингу.
T1002	Використовувати систему показників та критеріїв для мотивації та оцінки ефективності при вирішенні проблем безперервного моніторингу.
T1003	Співпрацювати з менеджерами безпеки (тобто, власниками системи, менеджерами безпеки інформаційної системи тощо), щоб формувати відповідні вимоги до звітності безперервного моніторингу на системному рівні.
T1004	Використовувати інструменти безперервного моніторингу для оцінки ризиків на постійній основі.
T1005	Використовувати дані безперервного моніторингу в процесі прийняття рішень щодо інвестування в безпеку з метою подолання існуючих проблем.
T1006	Відповідати на проблеми, виявлені під час безперервного моніторингу, здійснювати ескалацію та координувати відповідь.
T1007	Переглядати результати безперервного моніторингу і своєчасно пом'якшувати ризики на регулярній основі.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

A.5 Опис знань в рамках Керівних принципів НОІСК

В Таблиці 5 наведений перелік різних видів інформації, знання якої застосовується під час виконання конкретної функції. Вибіркові ідентифікатори знань/описи з даного переліку відповідають кожній робочій ролі з детального переліку робочих ролей в Додатку В. Перші шість знань відносяться до усіх робочих ролей сфери кібербезпеки. Перелік періодично оновлюватиметься [1]. Джерело найновішої версії цього матеріалу можна знайти в електронній довідковій таблиці до спеціального видання НІСТ 800-181 [4].

Таблиця 5 – Опис знань в Загальних принципів NICE

Ідентифікатор знання	Опис
K0001	Знання концепцій і протоколів комп'ютерних мереж, а також методології забезпечення мережевої безпеки.
K0002	Знання процесів управління ризиками (наприклад, методів оцінки та зниження ризиків).
K0003	Знання законів, нормативних актів, політик і етичних норм, і як вони пов'язані з кібербезпекою і приватністю.
K0004	Знання принципів кібербезпеки і приватності.
K0005	Знання кіберзагроз та вразливостей.
K0006	Знання конкретних операційних наслідків в результаті помилок кібербезпеки.
K0007	Знання методів автентифікації, авторизації та контролю доступу.
K0008	Знання прикладних бізнес процесів і функцій в організації -замовнику.
K0009	Знання вразливостей прикладних приграм.
K0010	Знання методів, принципів і концепцій комунікацій, які підтримують інфраструктуру мережі.
K0011	Знання спроможностей та прикладних програм мережевого обладнання, включаючи маршрутизатори, комутатори, мости, сервери, засоби передачі і відповідне технічне обладнання.
K0012	Знання аналізу спроможностей і вимог.
K0013	Знання оцінок систем кіберзахисту і вразливостей, а також їх можливостей.
K0014	Знання складних структур даних.
K0015	Знання комп'ютерних алгоритмів.
K0016	Знання принципів комп'ютерного програмування.
K0017	Знання концепцій і методик обробки цифрових даних, що використовуються в кримінальних розслідуваннях.
K0018	Знання алгоритмів шифрування.
K0019	Знання концепцій криптографії та управління криптографічними ключами.
K0020	Знання політик адміністрування даних і стандартизації даних.
K0021	Знання резервного копіювання та відновлення даних.
K0022	Знання принципів збору і зберігання даних.
K0023	Знання систем управління базами даних, мов побудови запитів, взаємозв'язків між таблицями і уявлення таблиць.
K0024	Знання систем баз даних.
K0025	Знання управління цифровими правами.
K0026	Знання безперервності бізнесу та операційних планів відновлення безперервності після катастроф.
K0027	Знання корпоративної архітектури інформаційної безпеки організації.
K0028	Знання вимог до процедур оцінки і валідації, прийнятих в організації.
K0029	Знання процедур підключення до локальної мережі організації та до глобальних мереж.
K0030	Знання електротехніки, використовуваної в архітектурі комп'ютера (наприклад, друковані плати, процесори, мікросхеми та технічне забезпечення).
K0031	Знання корпоративних систем обміну повідомленнями і відповідного програмного забезпечення.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор знання	Опис
K0032	Знання стійкості і надмірності.
K0033	Знання механізмів контролю доступу до хостів /мереж (наприклад, списки контролю доступу, списки повноважень).
K0034	Знання мережевих служб і протоколів інформаційного обміну, які забезпечують мережеву комунікацію.
K0035	Знання процедур інсталяції, інтеграції та оптимізації компонентів системи.
K0036	Знання принципів взаємодії людина-комп'ютер.
K0037	Знання процесу оцінки стану безпеки і процесу авторизації.
K0038	Знання принципів кібербезпеки і приватності, застосовуваних під час управління ризиками, пов'язаних із використанням, обробкою, зберіганням і передачею інформації або даних.
K0039	Знання принципів і методів кібербезпеки та приватності, які застосовуються при розробці програмного забезпечення.
K0040	Знання джерел поширення інформації про вразливість (наприклад, попередження, рекомендації, списки помилок і бюлетені).
K0041	Знання категорій інцидентів, процедур і термінів реагування на інциденти.
K0042	Знання методології реагування на інциденти і обробки даних інцидентів.
K0043	Знання принципів і методів аналізу прийнятих в галузевих стандартах або в організації.
K0044	Знання принципів і методів кібербезпеки та приватності, а також організаційних вимог (щодо забезпечення конфіденційності, цілісності, доступності, автентифікації і неспростовності).
K0045	Знання принципів створення систем інформаційної безпеки (NIST SP 800-160).
K0046	Знання методології виявлення вторгнень і способів виявлення вторгнень до хостів і мережі.
K0047	Знання архітектурних концепцій та загальних принципів інформаційних технологій (IT).
K0048	Знання вимог в рамках Загальних принципів управління ризиками (RMF)
K0049	Знання принципів і методів забезпечення безпеки інформаційних технологій (IT) (наприклад, мережеві екрани, ДМЗ, шифрування).
K0050	Знання принципів і концепцій мережевих зв'язків на локальних і глобальних рівнях, включаючи управління пропускної здатністю (трафіком).
K0051	Знання мов програмування низького рівня (наприклад, асемблер).
K0052	Знання математики (наприклад, логарифмів, тригонометрії, лінійної алгебри, математичного аналізу, статистики і операційного аналізу).
K0053	Знання критеріїв або показників продуктивності і доступності систем.
K0054	Знання сучасних галузевих методів оцінки, впровадження та розповсюдження інструментів та процедур оцінки безпеки інформаційних технологій (IT), моніторингу, виявлення та усунення несправностей, що використовують концепції та можливості на основі стандартів.
K0055	Знання мікропроцесорів.
K0056	Знання управління мережевим доступом, ідентифікацією, та доступом (наприклад, інфраструктура відкритих ключів, автентифікація об'єктів, відкриті ідентифікатори, мова розмітки для контролю захищеності, мова розмітки для надання послуг).
K0057	Знання обладнання та функцій апаратного забезпечення мереж.
K0058	Знання методів аналізу мережевого трафіку.
K0059	Знання нових і виникаючих інформаційних технологій (IT) та технологій кібербезпеки.
K0060	Знання операційних систем.
K0061	Знання теорії управління потоками в мережах (наприклад, протоколу управління передачею (TCP), протоколу міжмережевого обміну даними (IP), моделі взаємодії відкритих систем (OSI), бібліотеки інфраструктури інформаційних технологій, поточної версії [ITIL]).
K0062	Знання аналізу на мережевому (пакетному) рівні.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор знання	Опис
K0063	Знання концепцій паралельних і розподілених обчислень.
K0064	Знання інструментів та методик налаштування продуктивності.
K0065	Знання засобів контролю доступу, адаптивних до ризиків і заснованих на політиці.
K0066	Знання оцінки впливу на приватність.
K0067	Знання інженерних концепцій розробки процесів і процедур.
K0068	Знання структур і логіки мов програмування.
K0069	Знання мов формування запитів, наприклад, структурована мова запитів (SQL).
K0070	Знання загроз і вразливостей безпеки систем і прикладного програмного забезпечення (наприклад, переповнення буфера, мобільний код, міжсайтові сценарії, процедурна мова/мова структурованих запитів [PL/SQL] та ін'єкції, перегони фронтів, прихований канал, повтор, атаки на повернення, шкідливий код).
K0071	Знання концепцій технології віддаленого доступу.
K0072	Знання принципів і способів управління ресурсами.
K0073	Знання способів управління безпечною конфігурацією (наприклад, Посібники з технічного впровадження безпеки (STIGs), кращі практики кібербезпеки на сайті «cisecurity.org»).
K0074	Знання основних концепцій управління безпекою (наприклад, Управління версіями, патч-менеджмент).
K0075	Знання засобів, методів і способів проектування систем безпеки.
K0076	Знання теорії, концепцій і методів адміністрування серверів і проектування систем.
K0077	Знання операційних систем сервера і клієнта.
K0078	Знання інструментів діагностики і методик виявлення несправностей в серверах.
K0079	Знання принципів налагодження програмного забезпечення.
K0080	Знання інструментів, методів і методик проектування програмного забезпечення.
K0081	Знання моделей розробки програмного забезпечення (наприклад, каскадна модель, спіральна модель).
K0082	Знання технології побудови програмного забезпечення
K0083	Знання джерел, характеристик і принципів застосування активів даних організації.
K0084	Знання принципів і методів структурного аналізу.
K0086	Знання інструментів, методів і методик проектування систем, включаючи автоматизовані системи аналізу і інструменти проектування.
K0087	Знання стандартів, політик і авторизованих підходів до проектування системного ПЗ, прийнятих в організації (наприклад, стандарти міжнародної організації зі стандартизації [ISO]).
K0088	Знання концепцій адміністрування систем.
K0089	Знання інструментів діагностики систем і методик визначення несправностей.
K0090	Знання принципів управління життєвим циклом системи, включаючи забезпечення безпеки та експлуатаційної придатності ПЗ.
K0091	Знання методів тестування та оцінки систем.
K0092	Знання процесів інтеграції технологій.
K0093	Знання концепцій телекомунікацій (наприклад, комунікаційні канали, бюджетування системних каналів зв'язку, спектральна ефективність, мультиплексування).
K0094	Знання можливостей і функціональних характеристик, пов'язаних з технологіями формування контенту (наприклад, Web-сайти, контент яких можуть коригувати користувачі, соціальні мережі, системи формування контенту, блоги).
K0095	Знання спроможностей та функціональності, пов'язаних з різними технологіями для систематизації і управління інформацією (наприклад, бази даних, механізми створення закладок).
K0096	Знання спроможностей та функціональності різних технологій спільної обробки даних (наприклад, групового програмного забезпечення SharePoint).
K0097	Знання характеристик фізичних і віртуальних електронних засобів зберігання даних.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор знання	Опис
K0098	Знання структури і процедур підготовки звітних документів постачальником, який надає послуги з кіберзахисту в рамках власної організації
K0100	Знання архітектури інформаційних технологій (IT) підприємства.
K0101	Знання корпоративних цілей і завдань, пов'язаних з використанням IT в організації.
K0102	Знання технологічних процесів систем.
K0103	Знання типів і періодичності планової підтримки апаратного забезпечення.
K0104	Знання безпеки віртуальних приватних мереж (VPN).
K0105	Знання вебсервісів (наприклад, сервіс-орієнтована архітектура, Simple Object Access Protocol і мова опису вебсервісу).
K0106	Знання того, що являє собою мережева атака, і який існує зв'язок між мережевими атаками і загрозами та вразливостями.
K0107	Знання розслідувань інсайдерських загроз, звітів, інструментів розслідування та законів/нормативних актів
K0108	Знання концепцій, термінології і операцій широкого спектра засобів масової комунікації (комп'ютерні і телефонні мережі, супутникові, волоконно-оптичні та бездротові).
K0109	Знання фізичних компонентів і архітектури комп'ютера включаючи функції різних компонентів і периферійних пристроїв (наприклад, процесорів, мережевих адаптерів, сховищ даних).
K0110	Знання тактики, способів і процедур протистояння.
K0111	Знання інструментів мережі (наприклад, утиліта ping, трасування (прокладка) маршруту, nslookup).
K0112	Знання принципів системи ешелонованого захисту і архітектури безпеки мережі.
K0113	Знання різних типів мереж зв'язку (наприклад, LAN, WAN, MAN, WLAN, WWAN).
K0114	Знання електронних пристроїв (наприклад, обчислювальні системи/компоненти, засоби контролю доступу, цифрові камери і сканери, електронні блокноти, жорсткі диски, карти пам'яті, модеми, компоненти мережі, мережеве прикладне програмне забезпечення, засоби контролю, принтери, змінні пристрої зберігання, телефони, копіри, факсимільні апарати та ін.).
K0115	Знання тих технологій, які можуть бути використані.
K0116	Знання розширень файлів (наприклад, .dll, .bat, .zip, .pcap, .gzip).
K0117	Знання реалізацій файлових систем (наприклад, Файлова система нової технології [NTFS], Таблиця розміщення файлів [FAT], Розширення файлу [EXT]).
K0118	Знання процедур вилучення і зберігання цифрових доказів.
K0119	Знання методологій проведення хакерських атак.
K0120	Знання того, як інформаційні потреби і вимоги до збору інформації задовольняються і відслідковуються, а також як їм присвоюються пріоритети в рамках всього підприємства.
K0121	Знання принципів і методик управління програмами та проектами з інформаційної безпеки.
K0122	Знання умов дослідження технічного обладнання, операційних систем і мережевих технологій.
K0123	Знання правового корпоративного управління, пов'язаного з законністю (наприклад, правила доказування).
K0124	Знання декількох когнітивних доменів, а також інструментів і методів, які застосовуються для навчання в кожному домені.
K0125	Знання процесів збору, форматування, доставки і зберігання електронних доказів протягом усього ланцюжка постачання.
K0126	Знання методик управління ризиками в ланцюжку постачання (NIST SP 800-161).
K0127	Знання суті та функції відповідної інформаційної структури (наприклад, національної інформаційної інфраструктури).
K0128	Знання типів і збору постійних даних

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор знання	Опис
K0129	Знання інструментів командного рядка (наприклад, mkdir, mv, ls, passwd, grep).
K0130	Знання технологій віртуалізації і розробки та підтримки віртуальних машин.
K0131	Знання методик збору веб-пошти, пошуку/аналізу інструментів та файлів cookie.
K0132	Знання тих системних файлів, які містять відповідну інформацію (наприклад, файли журналів та файли реєстру, файли конфігурації), а також, де можна знайти такі системні файли.
K0133	Знання типів цифрових даних, що використовуються в криміналістиці, а також способів їх розпізнавання.
K0134	Знання портативних засобів проведення криміналістичної експертизи.
K0135	Знання методик Web-фільтрації.
K0136	Знання спроможностей різних систем і методів електронної комунікації (наприклад, e-mail, VOIP, IM, Direct Video Broadcasts, Web-форуми, пряме відео-трансляції).
K0137	Знання діапазону існуючих мереж (наприклад, PBX, LAN, WAN, WiFi, SCADA).
K0138	Знання WiFi.
K0139	Знання інтерпретованих і компільованих комп'ютерних мов.
K0140	Знання методик безпечного кодування.
K0141	Вилучено – Інтегровано в опис знання K0420
K0142	Знання процесів управління зборами, спроможностей і обмежень.
K0143	Знання зовнішніх систем збору даних, включаючи збір, фільтрацію та вибір трафіку.
K0144	Знання соціальної динаміки комп'ютерних зловмисників у глобальному контексті.
K0145	Знання інструментів кореляції подій безпеки
K0146	Знання основних бізнес-процесів і місії організації.
K0147	Знання виникаючих безпеки, ризиків і вразливостей.
K0148	Знання нормативних актів експортно-імпортного контролю та відповідальних установ, з метою зниження ризиків ланцюжка постачання.
K0149	Знання підходу організації до прийняття ризиків та/або управління ризиками.
K0150	Знання програми, робочих ролей і відповідальності при управлінні інцидентами в організації.
K0151	Знання поточних і виникаючих загроз/векторів загроз.
K0152	Знання принципів і методів безпеки інформаційних технологій (IT), які пов'язані з програмним забезпеченням (наприклад, модульність, розбивка на рівні, абстрагування, приховування даних, простота/мінімізація).
K0153	Знання процесу гарантованого забезпечення якості програмного забезпечення.
K0154	Знання стандартів, процесів і практик управління ризиками в ланцюжку постачання.
K0155	Знання законодавства про електронні докази..
K0156	Знання правових основ доказування і судочинства.
K0157	Знання політик, процедур і нормативних актів з інформаційної безпеки та кіберзахисту.
K0158	Знання політик безпеки користувача організації, що використовує інформаційні технології (наприклад, створення облікового запису, правила паролів, контроль доступу).
K0159	Знання технології передачі голосу по IP (VoIP).
K0160	Знання поширених векторів атак на мережевому рівні.
K0161	Знання різних класів атак (наприклад, пасивні, активні, інсайдерські, наступальні, розподілені атаки).
K0162	Знання типів порушників, які здійснюють кібератаки (наприклад, недосвідчені хакери), інсайдерські атаки, спонсоровані і не спонсоровані державами).
K0163	Знання вимог до закупівлі критичних інформаційних технологій.
K0164	Знання вимог до функціональності, якості та безпеки та як вони будуть виконуватися по відношенню до конкретних компонентів, що постачаються (тобто, елементи та процеси).
K0165	Знання оцінки ризиків/загроз.
K0167	Знання методик адміністрування системи, мережі та захисту операційних систем.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор знання	Опис
K0168	Знання діючих законів, законодавчих актів парламенту (наприклад, статті 10, 18, 32, 50 кодексу США), директив президента, постанов і розпоряджень органів виконавчої влади та/або кодексу і процедур адміністративного/кримінального права.
K0169	Знання політик, вимог і процедур безпеки ланцюжка постачання інформаційних технологій (IT) та управління ризиками ланцюжка постачання.
K0170	Знання систем критичної інфраструктури з інформаційно-комунікаційними технологіями, які були розроблені без розгляду безпеки системи.
K0171	Знання методик зворотного інжинірингу технічного обладнання.
K0172	Знання проміжного програмного забезпечення (наприклад, шини обслуговування організації і черги повідомлень).
K0174	Знання мережевих протоколів.
K0175	Знання методик зворотного інжинірингу програмного забезпечення.
K0176	Знання схем розширеної мови розмітки (XML).
K0177	Знання етапів кібератак (наприклад, розвідка, сканування, перерахування, отримання доступу, ескалація привілеїв, підтримка доступу, використання мережі, приховування слідів).
K0178	Знання методології, інструментів і практик безпечного розгортання програмного забезпечення
K0179	Знання концепцій архітектури безпеки мережі, включаючи топологію, протоколи, компоненти і принципи (наприклад, прикладна система ешелонованого захисту).
K0180	Знання принципів, моделей, інструментів та методів управління мережевими системами (наприклад, наскрізний моніторинг продуктивності систем).
K0182	Знання інструментів та методів вирізання даних (наприклад, «Foremost»).
K0183	Знання концепцій зворотного інжинірингу.
K0184	Знання тактик, способів і процедур протидії кримінальному розслідуванню.
K0185	Знання конфігурації проектування лабораторії криміналістичної експертизи та прикладних програм підтримки (наприклад, VMWare, Wireshark).
K0186	Знання процедур та інструментів налагодження.
K0187	Знання типів файлів, якими зловживають порушники для аномального функціонування системи.
K0188	Знання інструментів аналізу шкідливих програм (наприклад, Oily Debug, Ida Pro).
K0189	Знання шкідливих програм, які виявляють віртуальні машини (наприклад, відоме шкідливе ПЗ з підтримкою віртуальної машини, відоме шкідливе ПЗ з підтримкою відлагоджувальника, шкідливе розпаковане ПЗ, яке шукає послідовності, які пов’язані з віртуальною машиною і які відображаються на екрані вашого комп’ютера).
K0190	Знання методологій шифрування.
K0191	Вплив електронного підпису на віруси, шкідливі програми та атаки.
K0192	Знання портів і служб, що надаються ОС Windows/Unix.
K0193	Знання додаткових функцій безпеки від виправлення даних в базах даних.
K0194	Знання хмарних технологій управління знаннями та концепцій, пов’язаних з безпекою, корпоративним управлінням, постачанням і адмініструванням.
K0195	Знання стандартів і методології класифікації даних на основі чутливості та інших факторах ризику.
K0196	Знання нормативних актів, що регулюють експортно-імпортні операції, пов’язані з криптографією та іншими технологіями безпеки.
K0197	Знання інтерфейсів прикладних програм для доступу до даних (наприклад, «Java Database Connectivity» [JDBC]).
K0198	Знання концепцій вдосконалення процесів організації та моделей зрелості процесів (наприклад, і Capability Maturity Model Integration (CMMI) for Development, CMMI for Services, and CMMI for Acquisitions)
K0199	Знання концепцій архітектури безпеки і еталонних моделей архітектури підприємства (наприклад, Zachman, Federal Enterprise Architecture [FEA]).

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор знання	Опис
K0200	Знання концепцій управління послугами для мереж і в відповідних стандартів (наприклад, бібліотека інфраструктури інформаційних технологій [ITIL], поточна версія).
K0201	Знання методик і концепцій заміни симетричних ключів.
K0202	Знання концепцій і функцій прикладних програм мережевих екранів (наприклад, єдиної точки автентифікації/аудиту/реалізації політики, сканування повідомлень на наявність шкідливого вмісту, знеособлення даних з метою задоволення вимог стандартів PCI та DII, сканування захисту від втрати даних, прискорених криптографічних операцій, протокол захисту інформації SSL, REST/JSON-обробка).
K0203	Знання моделей системи безпеки (наприклад, модель Белла-Лападули, моделі забезпечення цілісності «Biba» і Кларка-Вілсона).
K0204	Знання методик оцінки навчання (рубрики, плани оцінювання, тестування, вікторини).
K0205	Знання методик зміцнення базової системи, мережі і операційної системи.
K0206	Знання принципів і методів етичних хакерських атак.
K0207	Знання основ аналізу схемотехніки.
K0208	Знання освітніх комп'ютерних послуг і послуг дистанційної освіти.
K0209	Знання методик організації прихованих каналів зв'язку.
K0210	Знання концепцій резервного копіювання та відновлення даних.
K0211	Знання вимог до конфіденційності, цілісності та доступності.
K0212	Знання програмного забезпечення з підтримкою кібербезпеки.
K0213	Знання моделей проектування та оцінки освітнього процесу (наприклад, модель розробки навчальних програм «ADDIE», системно-орієнтована модель Сміта/Рагана, модель Роберта М. Ганьє, модель багаторівневої оцінки Дональда Киркпатріка).
K0214	Знання методології оцінки загальних принципів управління ризиками
K0215	Знання політики навчання організації.
K0216	Знання рівнів навчання (тобто, системи освіти, розробленою Бенджаміном Блумом).
K0217	Знання систем управління навчанням та їх використання в управлінні навчанням.
K0218	Знання стилів навчання (наприклад, асиміляторний, слуховий і кінестетичне навчання).
K0220	Знання режимів навчання (наприклад, механічне запам'ятовування, спостереження).
K0221	Знання моделі OSI і базових мережевих протоколів (наприклад, протоколів TCP/IP).
K0222	Знання відповідних законів, органів юстиції, обмежувальних заходів і нормативних актів, що стосуються заходів кіберзахисту.
K0223	Видалено – інтегровано в опис знання K0073
K0224	Знання концепцій системного адміністрування операційних систем (і не тільки), Unix/Linux, IOS, Android і Windows.
K0226	Знання систем навчання, які застосовуються в організації.
K0227	Знання різних типів комп'ютерних архітектур.
K0228	Знання таксономії та семантичної онтології.
K0229	Знання прикладних програм, які можуть реєструвати помилки, позаштатні ситуації, збої в прикладних програмах та вести лог- журнал.
K0230	Знання моделей хмарних послуг і того, як такі моделі можуть обмежувати процедури управління інцидентами.
K0231	Знання протоколів, процесів та методик антикризового управління.
K0233	Знання загальних принципів персоналу у сфері національної кібербезпеки, робочих ролей, а також завдань, знань, навичок та здатностей, які до них відносяться.
K0234	Знання всього спектру кіберможливостей (наприклад, захист, атаки, експлуатація).
K0235	Знання того, як використовувати науково-дослідні центри, аналітичні центри, наукові дослідження та промислові системи.
K0236	Знання того, як використовувати Hadoop, Hive, Java, Python, SQL і Pig для аналізу даних.
K0237	Знання кращих галузевих практик служби підтримки.
K0238	Знання теорії і принципів машинного навчання.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор знання	Опис
K0239	Знання методик і методів виробництва, комунікації та розповсюдження медіа, включаючи альтернативні способи інформування за допомогою передачі текстових, мовних і візуальних повідомлень.
K0240	Знання багаторівневих систем безпеки та рішень для захищеного інформаційного обміну між доменами.
K0241	Знання прийнятих в організації політик, процесів і процедур кадрового забезпечення.
K0242	Знання політик безпеки в організації.
K0243	Знання політик, процесів і процедур тренінгів та навчання в організації
K0244	Знання фізичної та фізіологічної поведінки, які можуть вказувати на підозрілі або ненормальні дії.
K0245	Знання принципів і процесів проведення тренінгів та оцінки потреб у навчанні.
K0246	Знання відповідних концепцій, процедур, програмного забезпечення, обладнання і прикладних технологічних програм.
K0247	Знання процесів, засобів і спроможностей віддаленого доступу, пов’язаних з підтримкою клієнтів.
K0248	Знання теорії і практики стратегії.
K0249	Знання технологій, процесів і стратегій підтримки.
K0250	Знання процесів тестування і оцінювання учнів.
K0251	Знання судового процесу, включаючи надання фактів і доказів.
K0252	Знання принципів і методів тренінгів та освіти для розробки навчально-методичних матеріалів для індивідуального і групового навчання та освіти, а також вимірювання результатів навчання і освіти.
K0253	Видалено – Інтегровано в опис знання K0227
K0254	Знання бінарного аналізу.
K0255	Знання концепцій мережевої архітектури, включаючи топологію, протоколи та компоненти.
K0257	Знання вимог до постачання/закупівлі інформаційних технологій (IT).
K0258	Знання процедур, принципів і методології тестування (наприклад, Capabilities and Maturity Model Integration (CMMI)).
K0259	Знання концепцій і методології аналізу шкідливого ПЗ.
K0260	Знання стандартів безпеки персональних ідентифікаційних даних (PII).
K0261	Знання стандартів безпеки даних в сфері платіжних карт (PCI).
K0262	Знання стандартів безпеки медичних персональних даних (PHI).
K0263	Знання політик, вимог і процедур управління ризиками інформаційних технологій (IT).
K0264	Знання процесу планування захисту програм (наприклад, політики безпеки ланцюжків постачання інформаційних технологій / політика управління ризиками, Методи боротьби з підробками та вимоги).
K0265	Знання інфраструктури, що підтримує інформаційні технології (IT) для забезпечення захисту, продуктивності та надійності.
K0266	Знання того, як оцінити надійність постачальника і/або продукту.
K0267	Знання законів, політик, процедур чи корпоративного управління, що стосуються кібербезпеки критичних інфраструктур.
K0268	Знання криміналістичної процедури ідентифікації слідів.
K0269	Знання архітектури систем мобільного зв’язку.
K0270	Знання процесу життєвого циклу постачання/закупівлі.
K0271	Знання структури та властивостей операційної системи (наприклад, управління процесами, структура каталогів, встановлених застосунків).
K0272	Знання інструментів аналізу мереж для виявлення вразливостей в ПЗ, яке забезпечує комунікацію.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор знання	Опис
K0274	Знання технологій запису передаваних сигналів (наприклад, bluetooth, радіочастотна ідентифікація (RFID), мережі з інфрачервоним діапазоном передачі (IR), WiFi, пейджингові системи передачі, стільникові системи мобільного зв'язку, антени супутникового зв'язку, голосовий зв'язок (VoIP)) та методики «перешкод», які забезпечують передачу небажаної інформації або не дозволяють інстальованим системам функціонувати коректно.
K0275	Знання методик управління конфігураціями.
K0276	Знання системи управління безпекою.
K0277	Знання сучасних і перспективних засобів шифрування (наприклад, система шифрування стовпців і таблиць, шифрування файлів і дисків) в базах даних (наприклад, вбудовані функції управління криптографічними ключами).
K0278	Знання сучасних і перспективних функцій безпеки відновлення даних в базах даних.
K0280	Знання теорії, концепцій і методів системної інженерії систем.
K0281	Знання каталогів послуг інформаційних технологій (IT).
K0282	Видалено – Інтегровано в опис знання K0200
K0283	Знання варіантів застосування спільної роботи і синхронізації контенту різних платформ (наприклад, мобільні системи, персональний комп'ютер, хмарні системи).
K0284	Знання способів розробки і застосування системи управління обліковими даними користувачів.
K0285	Знання способів впровадження систем депонування ключів з метою забезпечення локального шифрування даних.
K0286	Знання багаторівневих типологій (наприклад, включаючи ОС сервера і клієнта).
K0287	Знання використовуваної в організації програми класифікації інформації і процедур розкриття.
K0288	Знання стандартних галузевих моделей захисту.
K0289	Знання засобів діагностики систем/серверів і методик визначення несправностей.
K0290	Знання методів тестування та оцінки захищеності систем.
K0291	Знання концепцій і моделей IT архітектури підприємства (наприклад, базовий рівень, затверджений дизайн, цільові архітектури).
K0292	Знання процедур і процесів управління інцидентами, проблемами і подіями.
K0293	Знання інтеграції цілей і завдань організації в архітектуру.
K0294	Знання експлуатації, підтримки і безпеки IT-систем, які необхідні для належного функціонування обладнання.
K0295	Знання принципів забезпечення конфіденційності, цілісності та доступності.
K0296	Знання спроможностей, прикладних програм і потенційних вразливостей мережевого обладнання, включаючи концентратори, маршрутизатори, комутатори, мости, сервери, носії передачі і супутнє апаратне обладнання.
K0297	Знання розробки контрзаходів для виявлених ризиків безпеки.
K0298	Знання контрзаходів щодо виявлених ризиків безпеки.
K0299	Знання того, як повинна функціонувати система безпеки (включаючи її можливості відмовостійкості та надійності), а також як вплинуть на неї зміни умов, операцій та інфраструктури.
K0300	Знання планування мережі і відтворення мереж.
K0301	Знання аналізу на пакетному рівні за допомогою відповідних інструментів (наприклад, Wireshark, tcpdump).
K0302	Знання основ функціонування комп'ютерів.
K0303	Знання інструментів для сегментування мереж.
K0304	Знання концепцій і практик обробки цифрових криміналістичних даних
K0305	Знання способів маскування даних (наприклад, алгоритми шифрування і стенографія).
K0308	Знання криптології.
K0309	Знання перспективних технологій, які можуть бути використані в подальшому.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор знання	Опис
K0310	Знання методологій зламу.
K0311	Знання галузевих показників, корисних для визначення тенденцій розвитку технологій.
K0312	Знання принципів, політик і процедур збору криміналістичних даних, включаючи юридичні повноваження і обмеження.
K0313	Знання зовнішніх організацій і академічних установ, діяльність яких спрямована на дослідження кіберпростору (наприклад, з програмами з кібербезпеки/тренінгами, та дослідженнями та розробками).
K0314	Знання потенційних вразливостей кібербезпеки в галузевих технологіях.
K0315	Знання основних методів, процедур і способів збору інформації, звітності, її обробки і спільного використання.
K0316	Знання бізнес планів чи планів військових операцій, планів і наказів на проведення кібероперацій, політики і встановлених правил взаємодії.
K0317	Знання процедур, які використовуються при документуванні та запитів повідомлень про інциденти, проблеми та події.
K0318	Знання інструментів командного рядка операційної системи
K0319	Знання можливостей технічної доставки та її обмежень
K0320	Знання критеріїв оцінки та підтвердження автентичності, прийнятих в організації.
K0321	Знання інженерних концепцій, що застосовуються до комп'ютерної архітектури і відповідного комп'ютерного обладнання/програмного забезпечення.
K0322	Знання вбудованих систем.
K0323	Знання методології відмовостійкості систем.
K0324	Знання інструментів та прикладного програмного забезпечення Системи виявлення вторгнень (IDS) та Системи запобігання вторгнень (IPS).
K0325	Знання теорії інформації (наприклад, кодування джерела, канальне кодування, теорія складності алгоритмів і стиснення даних).
K0326	Знання демілітаризованих зон.
K0330	Знання успішних можливостей для визначення рішень менш загальних і більш складних системних проблем.
K0332	Знання мережевих протоколів, таких, як TCP/IP, динамічного конфігурування вузлів, системи доменних імен (DNS) і послуг, що надаються Службою каталогів.
K0333	Знання процесів проектування мереж, включаючи розуміння цілей системи безпеки, операційних цілей та компромісів.
K0334	Знання аналізу мережевого трафіку (інструменти, методології, процеси).
K0335	Знання сучасних і перспективних кібертехнологій.
K0336	Знання методів автентифікації доступу.
K0337	Видалено – інтегровано в опис знання K0007.
K0338	Знання способів збору даних.
K0339	Знання того, як використовувати інструменти аналізу мережі для визначення вразливостей.
K0341	Знання іноземних політик розкриття інформації і нормативних документів з контролю експортно-імпортних операцій, пов'язаних з кібербезпекою.
K0342	Знання принципів, інструментів та методик тестування на проникнення.
K0343	Знання методів аналізу першопричин.
K0344	Знання середовища загроз організації.
K0346	Знання принципів і методів інтеграції системних компонентів.
K0347	Знання і розуміння розробки операцій.
K0349	Знання типів, процесів адміністрування, функцій і системи управління контентом Web-сайтів (CMS).
K0350	Знання прийнятої організацією системи планування.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор знання	Опис
K0351	Знання чинних законодавчих актів, законів, нормативних актів та політик, які регулюють кібертаргетинг та експлуатацію.
K0352	Знання форм потреб у підтримці розвідки, тем та напрямків розвідки.
K0353	Знання можливих ситуацій, які могли б привести до зміни органів управління збором даних.
K0354	Знання відповідних процедур звітності і розповсюдження інформації.
K0355	Знання процедур звітності та розповсюдження інформації з усіх джерел.
K0356	Знання аналітичних інструментів та методик для мовних, голосових і/або графічних матеріалів.
K0357	Знання аналітичних конструкцій та їх використання для оцінки операційного середовища.
K0358	Знання аналітичних стандартів і призначення ступенів довіри до матеріалів розвідки.
K0359	Знання прийнятних процесів поширення розвідувальної інформації.
K0361	Знання доступності, можливостей і обмежень активів.
K0362	Знання методів і способів проведення атак (розподілені атаки типу «відмова в обслуговуванні», метод грубої сили, перехоплення трафіку та ін.).
K0363	Знання процедур аудиту та логування (включаючи серверне логування).
K0364	Знання доступних баз даних і інструментів, які необхідні для оцінки відповідних завдань зі збору даних.
K0367	Знання тестування на проникнення.
K0368	Знання закладок, здатних забезпечувати збір даних і/або підготовку діяльності.
K0371	Знання принципів розробки системи збору інформації (наприклад, розпізнавання набраного номеру, аналіз соціальних мереж).
K0372	Знання концепцій програмування (наприклад, рівні, структури, мови з компіляцією або інтерпретацією).
K0373	Знання основного прикладного програмного забезпечення (наприклад, сховища даних і резервного копіювання, прикладних баз даних), а також типів вразливостей, які виявлені в цих прикладних програмах.
K0375	Знання вразливостей бездротових прикладних програм.
K0376	Знання внутрішніх і зовнішніх замовників та партнерських організацій, включаючи їх інформаційні потреби, цілі, структури, можливості тощо.
K0377	Знання стандартів, політик і процедур маркування за класифікацією та контролем.
K0379	Знання організацій-замовників, включаючи їх інформаційні потреби, цілі, структури, можливості тощо.
K0380	Знання інструментів та середовищ для спільної роботи.
K0381	Знання супутньої шкоди та оцінювання впливу.
K0382	Знання можливостей збору даних та обмежень.
K0383	Знання можливостей збору даних, доступу, специфікацій продуктивності та обмежень, які використовуються для виконання плану збору.
K0384	Знання функцій управління збором даних (наприклад, посади, функції, відповідальність, продукти, вимоги до звітності).
K0385	Видалено – Інтегровано в опис знання K0142
K0386	Знання інструментів управління збором даних.
K0387	Знання процесу планування збору та плану збору інформації.
K0388	Знання методик збору/аналізу даних та інструментів для чатів/списку друзів в соціальних мережах, виникаючих технології, голосового зв'язку і доставки даних Media Over IP, VPN, VSAT /бездротових систем, Web-пошти та файлів cookie.
K0389	Знання джерел збору, включаючи традиційні і не традиційні джерела.
K0390	Знання стратегій збору даних.
K0391	Знання систем, можливостей і процесів збору даних.
K0392	Знання загальних видів зараження комп'ютерів/мереж (віруси, закладки типу «троянський кінь» та ін.), а також методів зараження (через порти, прикріплені файли та ін.).
K0393	Знання загальномережевих пристроїв та їх конфігурацій.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор знання	Опис
K0394	Знання загальних баз даних і інструментів звітності.
K0395	Знання фундаментальних основ комп'ютерних мереж (тобто, основних компонентів комп'ютерної мережі, типів мереж і ін.).
K0396	Знання концепцій комп'ютерного програмування, включаючи комп'ютерні мови, програмування, тестування, налагодження і типи файлів.
K0397	Знання концепцій безпеки в операційних системах (наприклад, Linux, Unix).
K0398	Знання концепцій, що стосуються Web-сайтів (наприклад, Web-сервери/сторінки, хостинг, DNS, реєстрація, Web-мови, наприклад, HTML).
K0399	Знання процедур планування кризових дій та в умовах обмеженого часу.
K0400	Знання процедур планування кібероперацій в кризових ситуаціях.
K0401	Знання критеріїв оцінки результатів збору даних.
K0402	Знання факторів критичності і вразливості (наприклад, цінність, відновлення, запас, контрзаходи) при виборі цілі і можливості застосування до кібердомену.
K0403	Знання криптологічних характеристик, обмежень і внеску в кібероперації.
K0404	Знання поточних вимог до збирання інформації.
K0405	Знання сучасних комп'ютерних наборів вторгнень.
K0406	Знання існуючого програмного забезпечення та методології активного захисту та системного зміцнення.
K0407	Знання потреб інформації клієнтів.
K0408	Знання принципів, можливостей, обмежень та наслідків кібердій (наприклад, кіберзахисту, збору інформації, підготовки середовища, кібератаки),
K0409	Знання можливостей кіберрозвідки/збору інформації та сховищ даних..
K0410	Знання законодавства в кіберсфері і його впливу на планування кібероперацій.
K0411	Знання законодавства та правових аспектів в кіберсфері і їх впливу на планування кібероперацій.
K0412	Знання кіберлексики/термінології.
K0413	Знання цілей, політик і законності кібероперацій.
K0414	Знання процесів підтримки або стимулювання кібероперацій.
K0415	Знання термінології/лексики кібероперацій.
K0416	Знання кібероперацій.
K0417	Знання термінології передачі даних (наприклад, мережеві протоколи, Ethernet, IP, шифрування, оптичні пристрої, знімні носії).
K0418	Знання процесу обробки потоку даних під час збору інформації з термінальної мережі або середовища.
K0419	Знання процедур адміністрування і підтримки баз даних.
K0420	Знання теорії баз даних.
K0421	Знання баз даних, порталів та відповідних засобів поширення.
K0422	Знання процесів і процедур усунення конфліктних ситуацій.
K0423	Знання звітності щодо усунення конфліктних ситуацій, включаючи взаємодію з зовнішніми організаціями.
K0424	Знання способів заборони і дезінформації.
K0425	Знання різних цілей організації на всіх рівнях, включаючи рівень підлеглих, рівень рівнозначних співробітників і рівень керівників.
K0426	Знання способів динамічного і підготованого таргетингу.
K0427	Знання алгоритмів шифрування і кіберможливостей/інструментів (наприклад, SSL, PGP).
K0428	Знання алгоритмів і інструментів шифрування для бездротових локальних мереж (WLANs).
K0429	Знання управління інформацією всього підприємства.
K0430	Знання стратегій і методик ухилення.
K0431	Знання сучасних/перспективних технологій комунікації.
K0432	Знання існуючих, майбутніх і довготривалих проблем, пов'язаних зі стратегією, політикою і організацією кібероперацій.
K0433	Знання умов криміналістичної експертизи структури і функцій операційної системи.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор знання	Опис
K0435	Знання фундаментальних кіберконцепцій, принципів, обмежень і ефектів.
K0436	Знання фундаментальних концепцій, термінології/лексикону (тобто, підготовка середовища, кібератаки, кіберзахист), принципів, можливостей, обмежень і ефектів кібероперацій.
K0437	Знання головних компонентів Системи наглядового контролю та збору даних (SCADA).
K0438	Знання архітектури мобільного стільникових зв'язку (наприклад, LTE, CDMA, GSM/EDGE і UMTS/HSPA).
K0439	Знання регулюючих органів для таргетингу.
K0440	Знання засобів безпеки на хостах, і того, як ці засоби впливають на експлуатацію та зниження вразливостей.
K0442	Знання того, як об'єднані технології впливають на кібероперації (наприклад, цифрові, телефонні, бездротові).
K0443	Знання про те, як концентратори, комутатори, маршрутизатори працюють разом у проекті мережі.
K0444	Знання того, як працюють прикладні Інтернет програми (SMTP-протокол, електронна пошта на базі HTTP-протоколу, електронна пошта в Інтернеті, клієнти чата, VOIP).
K0445	Знання того, як сучасні цифрові і телефонні мережі впливають на кібероперації.
K0446	Знання того, як сучасні бездротові комунікаційні системи впливають на проведення кібероперацій.
K0447	Знання того, як збирати, аналізувати і ідентифікувати цінну інформацію про цілі інтересів з метаданих (наприклад, електронна пошта, HHTP-протокол).
K0448	Знання того, як встановлювати пріоритети ресурсів.
K0449	Знання того, як витягувати, аналізувати і використовувати метадані.
K0450	Видалено – Інтегровано в опис знання K0036
K0451	Знання процесів ідентифікації і звітності.
K0452	Знання впровадження ОС Unix і Windows, які надають послуги автентифікації і логування (протокол RADIUS), DNS-служби, електронну пошту, Web-послуги, FTP-сервера, DHCP-протоколу, мережевого екрану і SNMP- протоколу.
K0453	Знання індикаторів та попереджень.
K0454	Знання потреб інформації.
K0455	Знання концепцій інформаційної безпеки, які сприяють технологіям та методам.
K0456	Знання можливостей і обмежень розвідки.
K0457	Знання рівнів впевненості розвідки.
K0458	Знання розвідувальних дисциплін.
K0459	Знання вимог зайнятості розвідки (тобто, матеріально-технічне забезпечення, підтримка зв'язку, маневреності, правові обмеження тощо).
K0460	Знання розвідувальної підготовки середовища і аналогічних процесів.
K0461	Знання виробничих процесів розвідки.
K0462	Знання принципів, політик, процедур і засобів розвідувальної звітності, включаючи формати звітів, критерії звітності (вимоги і пріоритети), практики розповсюдження і юридичні повноваження та обмеження.
K0463	Знання систем розробки вимог до розвідувальних заходів.
K0464	Знання розвідувальної підтримки планування, виконання та оцінки.
K0465	Знання можливостей і інструментів кібероперацій внутрішніх і зовнішніх організацій-партнерів.
K0466	Знання розвідувальних процесів внутрішніх і зовнішніх організацій -партнерів та розробка вимог до інформації та цінної інформації.
K0467	Знання можливостей і обмежень внутрішніх і зовнішніх організацій-партнерів (тих, хто має завдання, збирає, обробляє і відповідає за розповсюдження інформації
K0468	Знання звітності внутрішніх і зовнішніх організацій-партнерів.
K0469	Знання внутрішньої тактики прогнозування і/або моделювання спроможностей та дій загроз.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор знання	Опис
K0470	Знання Інтернету та протоколів маршрутизації.
K0471	Знання адресації в Інтернет-мережі (IP-адреси, маршрутизація на основі безкласових IP-адрес, система нумерації TCP/UDP-портів).
K0472	Знання систем виявлення вторгнень і розробки сигнатур.
K0473	Знання наборів вторгнень.
K0474	Знання ключових учасників кіберзагроз та їх активів.
K0475	Знання основних факторів операційного середовища і загроз.
K0476	Знання інструментів та методик обробки мов.
K0477	Знання намірів і цілей лідерства.
K0478	Знання юридичних аспектів таргетингу.
K0479	Знання аналізу та характеристик шкідливого програмного забезпечення.
K0480	Знання шкідливих програм.
K0481	Знання методів і методик, що використовуються для виявлення різних дій з експлуатації.
K0482	Знання методів визначення стану та доступності активів, які використовуються системою збору даних.
K0483	Знання методів інтеграції і узагальнення інформації з будь-яких потенційних джерел.
K0484	Знання сутності збору даних (процес, завдання, організація, цілі та ін.).
K0485	Знання адміністрування мереж.
K0486	Знання побудови і топології мережі.
K0487	Знання безпеки мережі (наприклад, шифрування, мережеві екрани, автентифікація, сервери-пастки, захист периметра).
K0488	Знання впровадження системи безпеки мережі (наприклад, підсистема IDS, виявлення вторгнень, розташована в IP-вузлі, система попередження вторгнень IPS, списки доступу), включаючи знання їх функцій і розміщення компонентів в мережі.
K0489	Знання топології мережі.
K0490	Видалено – Інтегровано в опис знання K0058
K0491	Знання основ мереж і Інтернет-комунікацій (тобто, пристроїв, конфігурації пристроїв, технічного та програмного забезпечення, прикладних програм, портів/протоколів, адресації, архітектур та інфраструктури мережі, маршрутизації, операційних систем тощо).
K0492	Знання нетрадиційних методологій збору даних.
K0493	Знання прихованих технологій (наприклад, TOR/Onion/анонімайзери, VPN/VPS, шифрування).
K0494	Знання цілей, ситуації, операційного середовища, статусу, розташування і можливостей збору інформації внутрішніх і зовнішніх організацій-партнерів, доступних для підтримки планування.
K0495	Знання поточних і майбутніх операцій.
K0496	Знання обмежень оперативних активів
K0497	Знання процедур оцінювання оперативної ефективності.
K0498	Знання оперативного планування.
K0499	Знання безпеки операцій.
K0500	Знання систем, їх можливостей і процесів збору інформації в організації та/або у організації-партнера.
K0501	Знання програм, стратегій і ресурсів кібероперацій в організації.
K0502	Знання інструментів і/або методів підтримки прийняття рішень в організації.
K0503	Знання прийнятих в організації форматів звітних документів про готовність ресурсів і активів, а також їх оперативну значимість і вплив на систему збору інформації на основі розвідувальних заходів.
K0504	Знання розв’язуваних організацією проблем і завдань, кібероперацій, а також нормативних правових актів і політичних директив, що регулюють проведення кібероперацій.
K0505	Знання завдань організації і пов’язаних з їх вирішенням потреб зі збору інформації.
K0506	Знання цілей організації, визначених керівництвом пріоритетів і ризиків при прийнятті рішень.
K0507	Знання про експлуатацію цифрових мереж організації або партнера.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор знання	Опис
K0508	Знання політик організації і концепцій планування співпраці з внутрішніми і/або зовнішніми організаціями.
K0509	Знання повноважень організації і організації-партнера, відповідальності та внесків у досягнення поставлених цілей.
K0510	Знання політик, засобів, спроможностей і процедур організації та організації-партнера.
K0511	Знання ієрархії організації та процесів прийняття кіберрішень.
K0512	Знання концепцій планування в організації.
K0513	Знання пріоритетів організації, юридичних повноважень та процесів виконання вимог.
K0514	Знання організаційних структур та пов’язаних з ними розвідувальних можливостей.
K0516	Знання фізичних та логічних мережевих пристроїв та інфраструктури, включаючи концентратори, комутатори, маршрутизатори, брандмауери тощо
K0517	Знання процесу затвердження перегляду після впровадження (PIR).
K0518	Знання про ініціювання планування діяльності.
K0519	Знання адаптивного планування, планування в кризових умовах та планування з урахуванням обмеженого часу.
K0520	Знання принципів та практик, пов’язаних із розвитком цілі, а саме знання, асоціації, системи зв’язку та інфраструктура цілі.
K0521	Знання пріоритетної інформації, способів її отримання, місця її публікації, способів доступу до неї, тощо
K0522	Знання потреб та архітектури здійснення та поширення розробки.
K0523	Знання виробів і номенклатури виробів основних компаній-вендорів (наприклад, комплекси безпеки -Trend Micro, Symantec, McAfee, Outpost і Panda), а також того, як ці продукти впливають на експлуатацію та зменшують вразливості.
K0524	Знання відповідних законів, правил та політик.
K0525	Знання необхідних продуктів планування розвідувальних заходів, пов’язаних з оперативним плануванням кібероперацій.
K0526	Знання стратегій досліджень та управління знаннями.
K0527	Знання стратегій управління ризиками та стратегії їх зменшення.
K0528	Знання супутникових систем зв’язку.
K0529	Знання розробки сценаріїв.
K0530	Знання опцій апаратного та програмного забезпечення безпеки, включаючи мережеві артефакти, які вони ініціалізуються, та їхній вплив на експлуатацію.
K0531	Знання впливу безпеки на конфігурації програмного забезпечення..
K0532	Знання спеціалізованої мови цілі (наприклад, скорочення, жаргон, технічні терміни, кодові слова).
K0533	Знання специфічних ідентифікаторів цілей і їх застосування.
K0534	Знання процесів управління персоналом, призначення і розміщення.
K0535	Знання стратегій і інструментів дослідження цілі.
K0536	Знання структури, методів і стратегії застосування інструментів експлуатації (наприклад, сніфери, клавіатурне перехоплення) та методик (наприклад, отримання доступу через бекдор, збір/ вилучення даних, аналіз вразливостей інших систем у мережі).
K0538	Знання організаційних структур, критичних можливостей та критичних вразливостей цілі та загрози.
K0539	Знання профілів комунікацій цілі та їх ключових елементи (наприклад, асоціації, діяльність, інфраструктура зв’язку цілі).
K0540	Знання інструментів та методик комунікацій цілі
K0541	Знання культурних посилань, діалектів, виразів, ідіом та скорочень цілі
K0542	Знання розвитку цілі (тобто, концепцій, ролей, відповідальності,, продуктів тощо).

Ідентифікатор знання	Опис
K0543	Знання орієнтовного часу ремонту та відновлення цілі.
K0544	Знання методик збору розвідданих та оперативної підготовки та життєвих циклів цілі.
K0545	Знання мови (в) цілі.
K0546	Знання розробки списків цілі (обмежений, повний, список кандидатів).
K0547	Знання методів і процедур цілі
K0548	Знання кіберсуб'єктів та процедур цілі чи загрози.
K0549	Знання процедур перевірки та підтвердження цілі
K0550	Знання цілі, включаючи пов'язані з нею поточні події, профіль комунікацій, виконавців кібератак та історії (мови, культури) і/або структуру повноважень.
K0551	Знання циклів таргетингу
K0552	Знання механізмів виконання завдань.
K0553	Знання процесів виконання завдань для органічних та підпорядкованих активів збирання.
K0554	Знання процесів виконання завдань, збору і обробки даних, використання і розповсюдження інформації.
K0555	Знання мережевих протоколів TCP/IP.
K0556	Знання основ телекомунікацій.
K0557	Знання збору даних від термінальної мережі або у середовищі (процес, цілі, організація, цілі тощо.).
K0558	Знання доступних інструментів та прикладних програм, пов'язаних з вимогами до збору даних та управлінням даними.
K0559	Знання основної структури, архітектури та проектів конвергентних прикладних програм.
K0560	Знання основної структури, архітектури та проектів сучасних мереж зв'язку.
K0561	Знання основ захисту мережі (наприклад, шифрування, брандмауери, автентифікація, сервери-пастки, захист периметру).
K0562	Знання можливостей і обмежень нових та перспективних систем збору даних, доступності та/або процесів.
K0563	Знання можливостей, обмежень і методології виконання завдань внутрішнього і зовнішнього збору даних і того, як вони використовуються в планових кіберзаходах.
K0564	Знання характеристик цільових мереж зв'язку (наприклад, ємність, функціональність, шляхи, критичні вузли).
K0565	Знання загальних мережевих протоколів та протоколів маршрутизації (наприклад, TCP/IP), послуг (наприклад, веб-пошти, DNS) та їх взаємодії для забезпечення мережевих зв'язків.
K0566	Знання вимог до критичної інформації і того, як ці вимоги використовуються при плануванні.
K0567	Знання потоку даних від джерела збору до сховищ та інструментів.
K0568	Знання системи управління збором даних та повноважень збору даних
K0569	Знання існуючої архітектури створення завдань, збору інформації, обробки, експлуатації і розповсюдження даних.
K0570	Знання факторів загрози, які могли б вплинути на операції зі збору даних..
K0571	Знання циклу зворотного зв'язку в процесах збору даних.
K0572	Знання функцій і можливостей внутрішніх груп, які імітують загрозливу діяльність на користь організації.
K0573	Знання фундаментальних основ цифрової криміналістики для отримання дієвої розвідки.
K0574	Знання про вплив мовного аналізу на функції мережевого оператора.
K0575	Знання впливу оцінок кадрового забезпечення внутрішніх і зовнішніх партнерів.
K0576	Знання інформаційного середовища.
K0577	Знання загальних принципів, процесів і відповідних систем розвідки.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор знання	Опис
K0578	Знання розробки вимог до розвідки і запиту на інформаційні процеси
K0579	Знання організації, робочих ролей і відповідальності вищих, нижчих та суміжних підрозділів.
K0580	Знання встановленого в організації формату плану заходів зі збору даних.
K0581	Знання циклів планування, операцій і таргетингу, встановлених в організації.
K0582	Знання процесу планування та кадрового процесу.
K0583	Знання планів/директив/настанов, які описують цілі організації.
K0584	Знання прийнятих в організації політик/процедур тимчасової передачі повноважень зі збору інформації.
K0585	Знання структури організації і того, яке вона має відношення до всього спектру кібероперацій, включаючи функції, відповідальності та внутрішні взаємозв'язки між окремими внутрішніми елементами.
K0586	Знання результатів ходу операції і аналізу її проведення.
K0587	Знання пробних версій, баз даних, інструментів та прикладних програм POC, необхідних для підготовки середовища, та засобів спостереження.
K0588	Знання вимог до пріоритетної інформації, одержуваної від підлеглих, допоміжних і керівних структур організації.
K0589	Знання процесу оцінки продуктивності та впливу операцій.
K0590	Знання процесів синхронізації процедур оперативної оцінки з процесом вимагання критичної інформації.
K0591	Знання службових обов'язків і можливостей системного аналізу та оцінки значущості отриманих результатів.
K0592	Знання мети і внеску шаблонів цілі.
K0593	Знання всього спектру кібероперацій, а також потреб, тематики і пріоритетних областей розвідувальних заходів.
K0594	Знання взаємозв'язків між кінцевими станами, цілями, результатами і напрямками операції, тощо.
K0595	Знання взаємозв'язків між оперативними завданнями, вимогами до розвідки і розвідувальними завданнями.
K0596	Знання процесу запиту інформації.
K0597	Знання ролі мережевих операцій у підтримці та сприянні іншим операціям організації.
K0598	Знання структури та змісту специфічних планів, настанов і повноважень, прийнятих в організації.
K0599	Знання структури, архітектури і проектування сучасних цифрових і телефонних мереж.
K0600	Знання структури, архітектури і проектування сучасних бездротових систем зв'язку.
K0601	Знання систем/архітектур/систем зв'язку, які використовуються для координації.
K0602	Знання дисциплін і можливостей збору даних.
K0603	Знання шляхів, якими цілі або загрози використовують Інтернет-мережу.
K0604	Знання систем загроз та/або цілей.
K0605	Знання попереджень, оповіщення, змішування та надмірності.
K0606	Знання процесів і методів розшифрування стенограм (наприклад, дослівно, суть, резюме).
K0607	Знання процесів і методик перекладу.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор знання	Опис
K0608	Знання структур і компонентів ОС Unix/Linux і Windows (наприклад, управління процесами, структура каталогів, вбудовані прикладні програми).
K0609	Знання технологій віртуальних машин.
K0610	Знання продуктів віртуалізації (Vmware, Virtual PC)
K0611	Видалено – Інтегроване в опис знання K0131
K0612	Знання того, що являє собою «загроза» для мережі.
K0613	Знання корпоративних спеціалістів в області оперативного планування і того, як і де можна з ними зв'язатися і які результати можна очікувати від них.
K0614	Знання бездротових технологій зв'язку (наприклад, стільникові, супутникові, GSM-системи), включаючи базову структуру, архітектуру і побудову сучасних бездротових систем зв'язку.
K0615	Знання заяв на розкриття приватності на основі чинного законодавства.
K0616	Знання основ і процесів безперервного моніторингу, його процесів та діяльності програми безперервної діагностики і пом'якшення (CDM).
K0617	Знання процедур оцінки автоматизованих засобів контролю захищеності.
K0618	Знання про управління апаратними активами і відстеження розміщення і конфігурації мережевих пристроїв і програмного забезпечення у відділах, їхню локацію, апаратуру, та потенційно, для підтримки бізнес-функцій.
K0619	Знання про управління програмними активами і відстеження розміщення і конфігурації мережевих пристроїв і програмного забезпечення у відділах, їхню локацію, та потенційно для підтримки бізнес-функцій.
K0620	Знання технологій і інструментів безперервного моніторингу.
K0621	Знання процедури оцінки ризиків.
K0622	Знання засобів контролю, пов'язаних з використанням, обробкою, зберіганням та передачею даних.
K0623	Знання методологій оцінки ризиків.
K0624	Знання ризиків безпеки прикладних програм (Open Web Application Security Project Top 10 list).
K0625	Знання про те, що виправлення та оновлення програмного забезпечення недоцільні для деяких мережевих пристроїв.
K0626	Знання механізмів безпечного оновлення даних.
K0627	Знання важливості фільтрації вхідного трафіку з метою захисту від автоматизованих загроз, які використовують підроблені мережеві адреси.
K0628	Знання організації кіберзмагань як способу розвитку навичок шляхом надання практичного досвіду в симульованих, реальних ситуаціях.
K0629	Знання складання чорних/білих списків.
K0630	Знання новітніх методик і методів вторгнення та задокументованих зовнішніх вторгнень поза організацією.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

A.6 Опис навичок в Загальних принципах NICE

В Таблиці 6 наведений перелік необхідних навичок з кібербезпеки. Навичка – це характерна компетенція для здійснення вивченої психомоторної дії. Окремі описи з даного переліку відповідають кожній робочій ролі з детального переліку робочих ролей в Додатку В. Перелік періодично оновлюватиметься [1]. Джерело останньої версії цього матеріалу можна знайти в електронній довідковій таблиці до NIST Special Publication 800-181 [4].

Таблиця 6 – Опис навичок в Загальних принципах NICE

Ідентифікатор навички	Опис
S0001	Навичка проводити сканування вразливостей і розпізнання вразливостей в системах безпеки.
S0002	Навичка розподілу ємності сховища при проектуванні систем управління даними.
S0003	Навичка ідентифікації, захоплення, вмісту і звітності про шкідливі програми.
S0004	Навичка аналізу пропускної здатності мережевого трафіку і характеристик продуктивності мережі.
S0005	Навичка застосування та інтеграції IT до запропонованих рішень.
S0006	Навичка застосування принципів конфіденційності, цілісності та доступності.
S0007	Навичка застосування контролю доступу до хосту /мережі (наприклад, список контролю доступу).
S0008	Навичка застосування специфічних принципів і методик системного аналізу в організації.
S0009	Навичка оцінки надійності системи та проектів.
S0010	Навичка аналізу можливостей і вимог.
S0011	Навичка проводити пошук інформації.
S0012	Навичка проводити зіставлення знань (наприклад, карта сховищ знань).
S0013	Навичка проведення запитів і розробки алгоритмів аналізу структур даних.
S0014	Навичка проводити налагодження програмного забезпечення.
S0015	Навичка здійснення заходів з тестування.
S0016	Навичка налаштування і оптимізації програмного забезпечення
S0017	Навичка розробки і застосування математичних або статистичних моделей.
S0018	Навичка розробки політик, які відображають цілі системи безпеки.
S0019	Навичка створення програм, які затверджують і обробляють множинні вхідні дані, включаючи аргументи командного рядка, змінні середовища і вхідні потоки.
S0020	Навичка розробки і використання електронних підписів.
S0021	Навичка проектування структури аналізу даних (тобто типи даних, які тест повинен генерувати, і як аналізувати такі дані).
S0022	Навичка розробки контрзаходів для виявлення ризиків безпеки.
S0023	Навичка розробки контролів безпеки на основі принципів і доктрин кібербезпеки.
S0024	Навичка проектування інтеграції апаратних і програмних рішень.
S0025	Навичка виявлення вторгнення на хостах або мережі, за допомогою технологій виявлення вторгнень (наприклад, Snort).
S0026	Навичка визначення необхідного рівня складності тесту для конкретної системи.
S0027	Навичка визначення, як буде функціонувати система безпеки (включаючи її властивості відмовостійкості і надійності), та як зміни умов, операцій або середовища вплинуть на ці результати.
S0028	Навичка розробки словників даних.
S0029	Навичка розробки моделей даних.
S0030	Навичка розробки сценаріїв тестування на основі операцій
S0031	Навичка розробки і застосування засобів контролю доступу в системах безпеки.
S0032	Навичка розробки, тестування і впровадження планів реагування на нештатні ситуації і відновлення мережевої інфраструктури.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор навички	Опис
S0033	Навичка діагностування проблем з підключенням.
S0034	Навичка визначення потреби в забезпеченні безпеки систем інформаційних технологій (тобто контролів безпеки).
S0035	Навичка створення схеми маршрутизації.
S0036	Навичка оцінки адекватності проектів безпеки.
S0037	Навичка створення запитів та звітів.
S0038	Навичка визначення показників або індикаторів продуктивності системи та дій, спрямованих на підвищення або виправлення продуктивності, виходячи з призначення системи.
S0039	Навичка визначення можливих причин зниження продуктивності або доступності системи ініціювати дії, необхідні для пом'якшення цієї ситуації.
S0040	Навичка впровадження, підтримки і вдосконалення визнаних практик безпеки мережі.
S0041	Навичка встановлення, налаштування та усування несправностей в компонентах LAN та WAN, таких як маршрутизатори, концентратори та комутатори.
S0042	Навичка підтримки баз даних (тобто резервне копіювання, відновлення, видалення даних, файли лог-журналу тощо).
S0043	Навичка підтримки служби каталогів (наприклад, Microsoft Active Directory, LDAP тощо.).
S0044	Навичка імітувати поведінку загроз.
S0045	Навичка оптимізації продуктивності бази даних.
S0046	Навичка виконання аналізу на рівні пакетів за допомогою відповідних інструментів (наприклад, Wireshark, tcpdump).
S0047	Навичка збереження цілісності доказів відповідно до стандартних оперативних процедур або національних стандартів.
S0048	Навичка інтеграційного тестування системах.
S0049	Навичка вимірювання та звітування про інтелектуальний капітал
S0050	Навичка моделювання проектів і побудови сценаріїв їх використання (наприклад, універсальна мова моделювання).
S0051	Навичка використання інструментів та методик тестування на проникнення.
S0052	Навичка використання методів соціальної інженерії. (наприклад, фішинг, приманка, несанкціоноване проходження тощо).
S0053	Навичка налаштування датчиків.
S0054	Навичка використання методології обробки інцидентів.
S0055	Навичка використання методик управління знаннями
S0056	Навичка використання інструментів управління мережею для аналізу структур мережевого трафіку (наприклад, простого протоколу управління мережею).
S0057	Навичка використання аналізаторів протоколу.
S0058	Навичка використання відповідних інструментів для відновлення програмного, апаратного та периферійного обладнання системи.
S0059	Навичка використання пристроїв віртуальних приватних мереж (VPN) і шифрування.
S0060	Навичка написання програм на сучасних мовах програмування (наприклад, Java, C ++).
S0061	Навичка написання планів проведення тестування.
S0062	Навичка аналізу дампів пам'яті з метою вилучення інформації.
S0063	Навичка збору даних з різних ресурсів кіберзахисту.
S0064	Навичка розробки і виконання навчальних планів і програм технічної підготовки.
S0065	Навичка ідентифікації та витягування даних, що представляють інтерес для криміналістичної експертизи, на різних електронних носіях (тобто криміналістичної експертиза електронних засобів).
S0066	Навичка у визначення пробілів в технічних можливостях.
S0067	Навичка визначення, модифікації і маніпулювання з відповідними системними компонентами у ОС Windows, Unix або Linux (наприклад, паролі, облікові записи користувачів, файли).
S0068	Навичка збору, обробки, пакування, транспортування і зберігання електронного доказу для запобігання модифікації, втрати, фізичного пошкодження або знищення даних.
S0069	Навичка створення і налаштування робочої станції для криміналістів.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор навички	Опис
S0070	Навичка розмовляти з іншими, щоб ефективно передавати інформацію.
S0071	Навичка користування наборами криміналістичних інструментів (наприклад, EnCase, Sleuthkit, FTK).
S0072	Навичка використання наукових підходів і методик при вирішенні проблем.
S0073	Навичка використання віртуальних машин (наприклад, Microsoft Hyper-V, VMWare vSphere, Citrix XenDesktop/Server, Amazon Elastic Compute Cloud, тощо).
S0074	Навичка фізичного демонтажу ПК.
S0075	Навичка проведення криміналістичної експертизи в кількох середовищах операційних систем (наприклад, системи мобільного зв'язку).
S0076	Навичка налаштування і використання програмних засобів захисту комп'ютерів (наприклад, програмні фільтри, антивірусна програма й антишпигунське ПЗ).
S0077	Навичка захисту мережевих комунікацій.
S0078	Навичка розпізнавання та класифікації різних типів вразливостей і пов'язаних з ними атак.
S0079	Навичка захисту мережі від шкідливого ПЗ (наприклад, NIPS, захист від шкідливого ПЗ, обмеження/запобігання впливу зовнішніх пристроїв, фільтрації спаму).
S0080	Навичка проводити оцінки збитків.
S0081	Навичка використання інструментів мережевого аналізу для визначення вразливостей (наприклад, fuzzing, nmap, тощо).
S0082	Навичка оцінки планів проведення тестування на предмет придатності і повноти.
S0083	Навичка інтегрування засобів тестування безпеки методом «чорного ящика» в процес забезпечення якості різних версій ПЗ.
S0084	Навичка конфігурування і використання компонентів системи мережевої безпеки (наприклад, мережеві екрани, віртуальні приватні мережі, системи виявлення вторгнень).
S0085	Навичка проведення аудитів або оглядів технічних систем.
S0086	Навичка оцінки надійності постачальника і/або продукту
S0087	Навичка поглибленого аналізу виявленої шкідливої програми/коду (наприклад, криміналістичний аналіз шкідливого ПЗ).
S0088	Навичка використання засобів бінарного аналізу (наприклад, Hexedit, коди команд xxd і hexdump Free BSD).
S0089	Навичка застосування односпрямованих хеш-функцій (наприклад, SHA і MD5).
S0090	Навичка аналізу аномального програмного коду для визначення, чи шкідливий він, чи безпечний.
S0091	Навичка аналізу швидко змінюваних даних.
S0092	Навичка ідентифікації методів обфускації.
S0093	Навичка інтерпретації результатів роботи налагоджувача з метою визначення тактики, техніки та процедури.
S0094	Навичка читання шістнадцяткових даних.
S0095	Навичка ідентифікації загальних методів кодування (наприклад, Виключна диз’юнкція (операція XOR), Американський стандартний код для інформаційного обміну [ASCII], Unicode, Base64, Uuencode, кодування уніфікованого локатору ресурсів [URL]).
S0096	Навичка читання та інтерпретування сигнатур (наприклад, мережева система запобігання і виявлення вторгнень з відкритим вихідним кодом).
S0097	Навичка застосування засобів контролю захищеності.
S0100	Навичка використання або розробки освітніх заходів (наприклад, програм навчання, навчальних ігор, інтерактивних занять).
S0101	Навичка використання технології в освітніх цілях (наприклад, інтерактивні дошки, Web-сайти, комп'ютери, проектори).
S0102	Навичка використання технічних можливостей доставки.
S0103	Навичка оцінка прогностичної сили і універсальності моделі.
S0104	Навичка проведення аналізу готовності до випробування
S0106	Навичка здійснення попередньої обробки даних (наприклад, умовний розрахунок, зниження розмірності, нормування, перетворення, розпакування, фільтрація, згладжування).
S0107	Навичка розробки і документування стратегій комплексного тестування та оцінювання ПЗ.
S0108	Навичка розробки кваліфікаційних стандартів для трудових ресурсів і займаних посад.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор навички	Опис
S0109	Навичка розпізнання прихованих структур або взаємозв'язків.
S0110	Навичка визначення вимог до інфраструктури тестування і оцінювання (співробітники, полігони, засоби, прилади).
S0111	Навичка взаємодії з замовниками.
S0112	Навичка управління активами, ресурсами для тестування і спеціалістами з тестування з метою забезпечення гарантій ефективного проведення тестових заходів.
S0113	Навичка перетворення формату даних з метою забезпечення їх стандартного відображення.
S0114	Навичка здійснення аналізу чутливості.
S0115	Навичка розробки звітних документів за результатами тестування і оцінювання.
S0116	Навичка розробки багаторівневих рішень безпеки/міждоменних рішень.
S0117	Навичка здійснення оцінки ресурсів, необхідних для тестування і оцінювання.
S0118	Навичка розробки семантичних онтологій, «зрозумілих» для ЕОМ.
S0119	Навичка регресійного аналізу (наприклад, ієрархічний поетапний метод, узагальнений лінійний метод, метод найменших квадратів, деревовидні методи, логістичний метод).
S0120	Навичка аналізу реєстраційних записів з метою встановлення доказів здійснених вторгнень.
S0121	Навичка застосування технік підвищення вимог до системи, мережі і ОС (наприклад, виключення незатребуваних послуг, парольних політик, сегментація мережі, використання журналу реєстрації, мінімум привілеїв і т.п.).
S0122	Навичка застосування методів проектування.
S0123	Навичка аналізу перетворень (наприклад, агрегування, ущільнення, обробка).
S0124	Навичка усування неполадок і діагностування аномалій функціонування інфраструктури системи кібербезпеки на основі її аналізу.
S0125	Навичка використання основних описових статистичних даних та методів (наприклад, нормальний розподіл, розподіл моделей, розподільчі схеми).
S0126	Навичка використання засобів аналізу даних (наприклад, «Excel», «STATA SAS», «SPSS»).
S0127	Навичка використання інструментів звірки даних.
S0128	Навичка використання ІТС, призначених для кадрового забезпечення та обслуговування кадрових органів.
S0129	Навичка застосування технік ідентифікації і видалення сторонніх користувачів.
S0130	Навичка написання сценаріїв (шаблонів) для Web-сайтів/порталів з використанням мов R, Python, PIG, HIVE, SQL і т.п.
S0131	Навичка аналізу шкідливого ПЗ.
S0132	Навичка проведення бітового аналізу.
S0133	Навичка обробки цифрових доказів, включаючи захист та створення юридично обґрунтованих копій доказів.
S0134	Навичка проведення оглядів систем.
S0135	Навичка розробки плану тестування системи безпеки (наприклад, окремого компонента, процесу інтеграції, системи, процесу приймання системи).
S0136	Навичка використання принципів, моделей, методів і засобів управління мережевими системами (наприклад, наскрізний моніторинг пропускної здатності системи).
S0137	Навичка проведення оцінок вразливості програмних додатків..
S0138	Навичка використання шифрування інфраструктури відкритих ключів (PKI) та можливостей цифрового підпису в програмних додатках (наприклад, ел. пошта S/MIME, SSL-трафік).
S0139	Навичка використання моделей системи безпеки (наприклад, модель Белла-Лападули, моделі забезпечення цілісності «Biba» і Кларка-Вілсона).
S0140	Навичка застосування процесів технічної розробки систем.
S0141	Навичка оцінки проектів систем безпеки.
S0142	Навичка проведення дослідження з метою усунення нестандартних проблем, що виникли на рівні клієнта.
S0143	Навичка проведення планування, управління та обслуговування систем/серверів
S0144	Навичка виправлення фізичних та технічних проблем, що впливають на роботу системи/сервера.
S0145	Навичка інтегрування та застосування політики, яка відповідає цілям безпеки системи

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор навички	Опис
S0146	Навичка розробки політик, які дозволяють системам відповідати вимогам щодо пропускної здатності (наприклад, маршрутизація трафіку, договір про рівень послуг, технічні вимоги до центрального процесора).
S0147	Навичка оцінки засобів контролю безпеки на основі принципів і доктрин кібербезпеки (наприклад, стандарти «CIS CSC», NIST SP 800-53, Керівні принципи кібербезпеки і т.п.).
S0148	Навичка проектування інтеграції технологічних процесів і рішень, включаючи застарілі системи і сучасні мови програмування.
S0149	Навичка розробки програмних додатків, які можуть реєструвати і обробляти помилки, винятки і збої в додатках, а також вести журнали реєстрації.
S0150	Навичка впровадження і тестування планів реагування на нештатні ситуації і відновлення мережевої інфраструктури.
S0151	Навичка діагностування несправних системних компонентів (тобто серверів).
S0152	Навичка перекладу функціональних вимог в потреби захисту (тобто, контролі безпеки).
S0153	Навичка ідентифікації та прогнозування системної/серверної роботи, доступності, можливостей або проблем з налаштуванням.
S0154	Навичка встановлення оновлень системи та компонентів (наприклад, серверів, пристроїв, мережевих пристроїв).
S0155	Навичка моніторингу та оптимізації роботи системи/сервера.
S0156	Навичка здійснення аналізу на мережевому (пакетному) рівні.
S0157	Навичка відновлення систем/серверів після виявленого збою (наприклад, ПЗ для відновлення, відмовостійкі кластери, дублювання/«зеркалювання» і т.п.).
S0158	Навичка адміністрування ОС (наприклад, ведення облікових записів, резервне копіювання даних, підтримання продуктивності системи, інсталяція і настройка нового апаратного/програмного забезпечення).
S0159	Навичка налаштування і підтвердження мережевих робочих станцій і зовнішніх пристроїв відповідно до затверджених стандартів та/або технічних завдань.
S0160	Навичка використання проектного моделювання (наприклад, універсальна мова моделювання).
S0161	Видалено – Інтегровано в опис навички S0160
S0162	Навичка організації підмереж.
S0163	Видалено – Інтегровано в опис навички S0060
S0164	Навичка оцінки практичного застосування криптографічних стандартів.
S0166	Навичка визначення технічних проблем в системі доставки..
S0167	Навичка виявлення вразливостей в захищених системах (наприклад, сканування вразливостей і перевірка відповідності).
S0168	Навичка створення фізичних або логічних підмереж, які відокремлюють внутрішню локальну мережу (LAN) від інших ненадійних мереж.
S0169	Навичка проведення аналізу тенденцій.
S0170	Навичка налаштування та використання компонентів захисту комп'ютера (наприклад, апаратних брандмауерів, серверів, маршрутизаторів, у відповідних випадках).
S0171	Навичка проведення оцінки впливу/ризику.
S0172	Навичка застосування безпечних методів кодування.
S0173	Навичка використання інструментів співвіднесення подій сфери кібербезпеки.
S0174	Навичка застосування безпечних способів кодування
S0175	Навичка аналізу першопричин.
S0176	Навичка організації процесів планування, включаючи підготовку функціональних і спеціальних планів підтримки, підготовки і забезпечення ділового листування, а також процесів кадрового забезпечення.
S0177	Навичка аналізу мереж зв'язку цілі.
S0178	Навичка аналізу найважливіших мережевих даних (наприклад, файлів налаштувань маршрутизаторів, протоколів маршрутизації).
S0179	Навичка аналізу засобів мовної обробки з метою подальшого вдосконалення розробки таких засобів.
S0180	Видалено – Інтегровано в опис навички S0062

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор навички	Опис
S0181	Навичка аналізу даних, зібраних на основі перехоплення трафіку.
S0182	Навичка аналізу внутрішніх та зовнішніх зв'язків цілі, зібраних з бездротових локальних мереж.
S0183	Навичка аналізу даних, зібраних з термінальної мережі або мережевого середовища.
S0184	Навичка аналізу трафіку з метою визначення мережевих пристроїв.
S0185	Навичка застосування аналітичних методів, які зазвичай використовуються з метою забезпечення планування та обгрунтування рекомендованих стратегій і програм заходів.
S0186	Навичка застосування процедур кризового планування.
S0187	Навичка застосування різних аналітичних методів, засобів і способів (наприклад, конкуруючі гіпотези, послідовність міркувань, виявлення відмови і обману, низька ймовірність події з сильним впливом на систему, аналіз мережі/віртуального з'єднання або каналу зв'язку, баєсове виведення, Delphi-аналіз і розпізнавання образів).
S0188	Навичка оцінки системи орієнтирів цілі (наприклад, мотивація, технічна спроможність, організаційна структура, уразливості).
S0189	Навичка оцінки і/або розрахунку результатів, отриманих в період проведення і після закінчення кібероперацій.
S0190	Навичка оцінки сучасних засобів з метою визначення необхідності їх подальшого вдосконалення.
S0191	Навичка оцінки придатності доступних аналітичних засобів в різних ситуаціях.
S0192	Навичка аудиту мережевих екранів, периметрів, маршрутизаторів і систем виявлення вторгнень.
S0193	Навичка дотримання юридичних обмежень по відношенню до інформації про ціль.
S0194	Навичка проведення невідстежуваного дослідження.
S0195	Навичка проведення дослідження з використанням усіх доступних джерел.
S0196	Навичка проведення дослідження з використанням Web-сайтів/сторінок, що не індексуються пошуковими системами (deep web).
S0197	Навичка аналізу соціальних мереж, списків друзів і/або аналіз файлів cookie.
S0198	Навичка аналізу соціальних мереж.
S0199	Навичка формування і витягування важливої інформації з перехоплених IP-пакетів.
S0200	Навичка формування вимог до системи збору даних з метою забезпечення заходів зі збору даних.
S0201	Навичка розробки планів для забезпечення віддалених операцій (тобто, тобто, гарячі/теплі/холодні/альтернативні місця, відновлення після аварії).
S0202	Навичка збору (наприклад, системи пошуку файлів) і аналізу даних.
S0203	Навичка визначення і опису всіх необхідних аспектів операційного середовища.
S0204	Навичка відображення джерела даних або побічних даних на схемі мережі.
S0205	Навичка визначення відповідних варіантів таргетингу шляхом оцінки наявних можливостей щодо бажаних результатів.
S0206	Навичка визначення встановлених патчів на різних операційних системах та ідентифікації патч-сигнатур.
S0207	Навичка визначення ступеня впливу різних налаштувань маршрутизаторів і мережевих екранів на зразки трафіку і пропускну здатність мережі як у середовищах локальної мережі, так і в глобальній мережі.
S0208	Навичка визначення місця розташування мережевих пристроїв.
S0209	Навичка розробки і реалізації програми комплексної оцінки кібероперацій для аналізу і підтвердження функціональних характеристик, що визначають ефективність.
S0210	Навичка розробки звітних документів за результатами розвідки.
S0211	Навичка розробки або підготовки рекомендацій щодо застосування аналітичних методів або рішень для подолання проблем або ситуацій, пов'язаних з недостатністю інформації або в тих випадках, коли таких проблем і ситуацій раніше не існувало.
S0212	Навичка своєчасного розповсюдження даних, отриманих в результаті успішних розвідувальних операцій..
S0213	Навичка документування і поширення складної технічної інформації і програм.
S0214	Навичка оцінки значимості результатів розвідки.
S0215	Навичка оцінки та інтерпретації метаданих.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор навички	Опис
S0216	Навичка оцінки наявних можливостей з урахуванням бажаних результатів з метою забезпечення ефективності проведених заходів.
S0217	Навичка оцінки джерела даних на предмет їх корисності, надійності і об’єктивності.
S0218	Навичка оцінки інформації на предмет її надійності, достовірності та корисності.
S0219	Навичка оцінки інформації з метою визначення її корисності, пріоритетності тощо.
S0220	Навичка використання/запитування інформації з баз даних системи збору даних, що належить організації і/або організації-партнеру.
S0221	Навичка витягування інформації з перехоплених IP-пакетів.
S0222	Навичка комплексного аналізу.
S0223	Навичка розробки оперативних планів на підтримку вимог місії та цілей.
S0224	Навичка охоплення комунікацій цілі.
S0225	Навичка визначення комунікаційних мереж цілі.
S0226	Навичка визначення характеристик мережі цілі.
S0227	Навичка визначення альтернативних аналітичних трактувань з метою мінімізації виникнення непередбачених ситуацій.
S0228	Навичка визначення критично важливих компонентів цілі для включення критично важливих компонентів цілі в кіберпросторі.
S0229	Навичка визначення кіберзагроз, які можуть «поставити під удар» інтереси організації та/або партнера.
S0230	Видалено – Інтегровано в опис навички S0066
S0231	Навичка визначення того, як ціль передає інформацію.
S0232	Навичка визначення проблем і обмежень розвідки.
S0233	Навичка визначення мовних проблем, які можуть вплинути на рішення задач, що стоять перед організацією.
S0234	Навичка визначення орієнтувань для розробки цілі.
S0235	Навичка визначення регіональних мов і діалектів, які не належать цілі.
S0236	Навичка ідентифікації пристроїв, що працюють на кожному рівні моделей протоколів.
S0237	Навичка ідентифікації, розміщення та відстеження цілі за допомогою методик геопросторового аналізу.
S0238	Навичка встановлення пріоритетів інформації, яка стосується операцій..
S0239	Навичка трактування компільованих й інтерпретованих мов програмування..
S0240	Навичка інтерпретації метаданих і змісту, що застосовуються в системах збору інформації.
S0241	Навичка інтерпретації результатів трасування і того, як вони використовуються при аналізі і реконструкції мереж.
S0242	Навичка інтерпретації результатів, отриманих сканером вразливостей, з метою виявлення вразливостей.
S0243	Навичка управління знаннями, включаючи методики технічної документації (наприклад, сторінку Wiki).
S0244	Навичка управління відносинами з клієнтами, включаючи визначення потреб/вимог клієнтів, управління очікуваннями клієнта та демонстрацію відданості досягненню якісних результатів.
S0245	Навичка навігації програмного забезпечення для візуалізації мережі.
S0246	Навичка нормалізації чисел.
S0247	Навичка здійснення синтезу даних з наявних даних для забезпечення нових або продовження проведеного збору інформації.
S0248	Навичка аналізу системи цілі.
S0249	Навичка підготовки і проведення брифінгів.
S0250	Навичка складання планів та відповідної кореспонденції.
S0251	Навичка визначення пріоритету матеріалу мовою цілі.
S0252	Навичка обробки зібраних даних для подальшого аналізу.
S0253	Навичка аналізу питань, пов'язаних з ціллю (наприклад, мова, культура, спілкування).
S0254	Навичка проведення аналізу, що допомагає при написанні поетапних звітів після проведеного заходу.
S0255	Навичка надання інформації геолокацію в режимі реального часу, використовуючи інфраструктуру цілі.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор навички	Опис
S0256	Навичка забезпечення розуміння систем цілі або загрози шляхом ідентифікації та аналізу зв'язків фізичних, функціональних або поведінкових відносин.
S0257	Навичка читання, інтерпретації, складання, внесення змін і виконання простих скриптів (наприклад, PERL, VBS) в ОС Windows і UNIX (наприклад, такі, які дозволяють вирішити наступні завдання: аналіз великих файлів даних, автоматизація ручних завдань і отримання /обробка віддалених даних).
S0258	Навичка виявлення та інтерпретації шкідливої мережевої активності у трафіку.
S0259	Навичка розпізнавати методики заборони і дезінформації цілі.
S0260	Навичка розпізнавати можливості центрального моменту та суттєву інформацію.
S0261	Навичка визнавати актуальність інформації.
S0262	Навичка виявлення суттєвих змін в моделях комунікацій цілі.
S0263	Навичка розпізнавання технічної інформації, яка може бути використана для потенційних клієнтів при проведенні аналізу метаданих.
S0264	Навичка розпізнавання технічної інформації, яка може бути використана для потенційних клієнтів для здійснення віддалених операцій (дані, які включають користувачів, паролі, адреси електронної пошти, діапазон IP-адрес цілі, частота поведінки DNI, поштові сервери, сервери доменів, інформація в SMTP-заголовку).
S0265	Навичка виявляти технічну інформацію, яка може бути використана для розробки цілі, включаючи розробку розвідки.
S0266	Навичка програмування на відповідних мовах (наприклад, «C ++», Python тощо.).
S0267	Навичка використання віддаленого командного рядка та графічного інтерфейсу користувача (GUI).
S0268	Навичка дослідження суттєвої інформації.
S0269	Навичка дослідження вразливостей та експлойтів, які використовуються у трафіку.
S0270	Навичка зворотного інжинірингу розробки (наприклад, hex editing, утиліти бінарної компресії, налагодження та аналіз рядків) з метою визначення функцій і належності видалених інструментів.
S0271	Навичка аналізу і редагування результатів процедури оцінювання.
S0272	Навичка аналізу і редагування результатів розвідки, отриманих з різних джерел при проведенні кібероперацій.
S0273	Навичка аналізу і редагування планів.
S0274	Навичка аналізу і редагування матеріалів цілі.
S0275	Навичка адміністрування серверів.
S0276	Навичка обстеження, збору та аналіза метаданих бездротової локальної мережі.
S0277	Навичка синтезу, аналізу і розстановки пріоритетів у наборах даних.
S0278	Навичка адаптування аналізу до необхідних рівнів (наприклад, класифікаційного та організаційного).
S0279	Навичка визначення цілей з метою безпосередній підтримки операцій зі збору даних.
S0280	Навичка визначення аномалій в цільової мережі (наприклад, вторгнення, потік даних або їх обробки, цільове впровадження нових технологій).
S0281	Навичка розробки технічної документації.
S0282	Навичка тестування і оцінювання інструментів для впровадження.
S0283	Навичка розпізнавання комунікацій мовою цілі.
S0284	Навичка перекладу цільових графічних і/або мовних матеріалів
S0285	Навичка використання булевих операторів для побудови простих і складних запитів.
S0286	Навичка використання баз даних для визначення актуальної для цілі інформації.
S0287	Навичка використання геопросторових даних та застосування геопросторових ресурсів.
S0288	Навичка використання кількох аналітичних інструментів, баз даних і методик (наприклад, Analyst's Notebook, A-Space, Anchory, M3, дивергентне/конвергентне мислення, діаграми зв'язків, матриці тощо.).
S0289	Навичка використання кількох пошукових систем (наприклад, Google, Yahoo, LexisNexis, DataStar) і інструментами при проведенні пошуку джерел з відкритим кодом.
S0290	Навичка використання анонімних мереж.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор навички	Опис
S0291	Навичка використання методів дослідження, включаючи дослідження декількох різних джерел з метою реконструкції цільової мережі.
S0292	Навичка використання баз даних та пакетів програмного забезпечення для таргетингу.
S0293	Навичка використання інструментів, методик і процедур для віддаленої експлуатації та забезпечення утримання на цілі.
S0294	Навичка використання інструментів трасування маршрутів та інтерпретації отриманих результатів в разі їх використання для аналізу або реконструкції мережі.
S0295	Навичка використання різних інструментів різних відкритих джерел для збору даних (он-лайн торгівля, DNS, електронна пошта, тощо).
S0296	Навичка використання зворотного зв'язку з метою вдосконалення процесів, продуктів і послуг
S0297	Навичка використання віртуальних колективних робочих просторів і/або інструментів (наприклад, IWS, VTC,, чат- кімнати, SharePoint).
S0298	Навичка перевірки цілісності всіх файлів (наприклад, контрольні суми, виключне АБО, безпечне хеши, контрольні обмеження тощо).
S0299	Навичка аналізу, створення шаблонів і геолокації бездротових мереж цілі.
S0300	Навичка розробки (і подання) вимог для подолання пробілів у технічних можливостях.
S0301	Навичка зрозумілої, переконливої і системної подачі фактів та ідей в письмовій формі.
S0302	Навичка написання звітів про результативність.
S0303	Навичка формування, аналізу і редагування результатів кіберрозвідки/оцінки даних з декількох джерел.
S0304	Навичка отримання доступу до інформації про доступні поточні активи та їх використання.
S0305	Навичка отримання доступу до баз даних, в яких зберігаються плани/директиви/методологія.
S0306	Навичка аналізу стратегічних настанов з питань, які вимагають роз’яснення і/або додаткової методології.
S0307	Навичка аналізу джерел сили і морального духу цілі чи загрози.
S0308	Навичка передбачати вимоги до використання можливостей розвідки.
S0309	Навичка передбачати ключові дії цілі або загрози, які, швидше за все, потребують від керівництва прийняття будь-яких рішень.
S0310	Навичка використання аналітичних стандартів для оцінки результатів розвідки.
S0311	Навичка використання можливостей, обмежень і методик постановки завдань платформ, датчиків, архітектур та апаратів, для їх застосування до цілей організації.
S0312	Навичка застосування процесу оцінки продуктивності та впливу кібероперацій.
S0313	Навичка формулювання потреб/вимог та інтеграції нових і сучасних можливостей збору даних, доступів та/або процесів до збору даних.
S0314	Навичка формулювання можливостей розвідувальних заходів для підтримки виконання плану.
S0315	Навичка формулювання потреб спільних планувальників для аналітиків з усіх джерел.
S0316	Навичка пов’язувати пробіли розвідки та вимоги до пріоритетної інформації та спостережуваними даними.
S0317	Навичка порівняння показників/ результатів спостереження з вимогами.
S0318	Навичка концептуалізації процесу розвідки в багатьох доменах та вимірах.
S0319	Навичка перетворювати вимоги до розвідки на завдання розвідки.
S0320	Навичка координації розробки спеціалізованих розробок розвідки.
S0321	Навичка узгодження пріоритетів розвідки з розміщенням ресурсів/активів розвідки
S0322	Навичка створення показників для оцінки оперативних досягнень/успіхів.
S0323	Навичка створення і підтримки актуальних планових документів та відстеження послуг/розробок.
S0324	Навичка визначення доцільності збору інформації.
S0325	Навичка розробки плану збору даних, який чітко відображає забезпечення, яке може бути використано для збору необхідної інформації.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор навички	Опис
S0326	Навичка визначення різниці між умовними і фактичними ресурсами та їх придатності до плану, що розробляється.
S0327	Навичка забезпечення того, щоб стратегія зі збору даних використовувала усі доступні ресурси.
S0328	Навичка оцінки факторів операційного середовища стосовно цілей і вимог до інформації.
S0329	Навичка оцінки запитів на отримання інформації з метою визначення наявності необхідної інформації для відповіді.
S0330	Навичка оцінки можливостей, обмежень і методологій постановки завдань для скоординованих, обмежених місцями збору, національних, коаліційних та інших можливостей системи збору даних.
S0331	Навичка усного та письмового викладення даних про зв'язок між обмеженнями можливостей розвідки та ризиками під час прийняття рішень і впливом на загальний хід операції.
S0332	Навичка збору даних з доступних інструментів та прикладних програм відповідно до вимог збору даних та управління операціями зі збору даних.
S0333	Навичка графічного відображення матеріалів системи забезпечення процесу прийняття рішень, що містять оцінки даних розвідки і можливостей партнерів.
S0334	Навичка визначення і впровадження процесів постановки завдань, збору, обробки та розподілу даних, а також використання вразливостей за відповідними напрямами.
S0335	Навичка визначення проблем розвідки.
S0336	Навичка визначати, коли задоволені вимог до пріоритетної інформації.
S0337	Навичка впровадження встановлених процедур оцінки управління збором даних і операційною діяльністю.
S0338	Навичка інтерпретації методології планування для визначення необхідного рівня аналітичного забезпечення.
S0339	Навичка інтерпретації звітних матеріалів про готовність, їх оперативну значимість і вплив на системи збору даних на розвідку.
S0340	Навичка моніторингу та факторів середовища цілі або загрози.
S0341	Навичка моніторингу наслідків загроз в системах партнерів, а також проведення безперервної оцінки таких наслідків.
S0342	Навичка оптимізації продуктивності системи збору даних за допомогою повторного налаштування, тестування і регулювання.
S0343	Навичка управляти командами з планування розвідки, заходами зі збору та розробки і моніторити статус.
S0344	Навичка підготовки та подання звітів, презентацій і брифінгів, включаючи використання візуальних допоміжних засобів або технології проведення презентацій.
S0345	Навичка співвідносити ресурси/активи розвідки з передбачуваними вимогами до розвідки.
S0346	Навичка прийняття рішень у разі виникнення суперечливих вимог до збору даних.
S0347	Навичка огляду характеристик продуктивності та історичних даних про активи збору.
S0348	Навичка конкретизації заходів зі збору даних і/або постановки завдань, які обов'язково повинні бути проведені найближчим часом.
S0349	Навичка синхронізації процедур функціональної оцінки та процесу, який вимагає отримання критично важливої інформації.
S0350	Навичка узгодження заходів діяльності з планування з потрібною підтримкою розвідки.
S0351	Навичка переводити можливості, обмеження та методології постановки завдань у власних системах збору даних, на місці здійснення операцій, у національних системах, коаліційних та інших.
S0352	Навичка використання засобів спільних та середовища під час операцій зі збору інформації.
S0353	Навичка використання систем і/або інструментів відстеження вимог збору даних і визначення того, наскільки вони виконуються.
S0354	Навичка розробки політик, що відображають основні завдання забезпечення приватності в бізнесі.
S0355	Навичка обговорення угод з постачальниками та оцінки практик приватності постачальників.

Ідентифікатор навички	Опис
S0356	Навичка комунікації з керівниками всіх рівнів, включаючи членів правління (наприклад, навички міжособистісного спілкування, доступність, уміння ефективно сприймати мову виступаючих, відповідне аудиторії використання стилю і мови виступу).
S0357	Навичка прогнозування нових загроз безпеки.
S0358	Навичка обізнаності про виникнення технічних інфраструктур.
S0359	Навичка використання критичного мислення при аналізі організаційних моделей і взаємозв'язків.
S0360	Навичка аналізу і оцінки можливостей та інструментів проведення кібероперацій внутрішніх і зовнішніх партнерів.
S0361	Навичка аналізу і оцінки процесів розвідки та розробки вимог до інформації та суттєвої інформації внутрішніх і зовнішніх партнерів.
S0362	Навичка аналізу і оцінки можливостей і обмежень внутрішніх і зовнішніх партнерів (тобто тих, які відповідають за постановку завдань, збір, обробку, експлуатацію та розповсюдження).
S0363	Навичка аналізу і оцінки звітності внутрішніх і зовнішніх партнерів.
S0364	Навичка забезпечення розробки ідей про контекст середовища загроз організації.
S0365	Навичка проектування реагування на інциденти в моделях хмарних послуг.
S0366	Навичка виявляти успішні спроможності знаходити рішення для менш загальних і більш складних системних проблем.
S0367	Навичка застосування принципів кібербезпеки і приватності при формуванні організаційних вимог (які стосуються конфіденційності, цілісності, доступності, автентифікації і неспростовності).
S0368	Навичка використовувати скоринг ризику для інформування підходів, основаних на продуктивності та ефективності витрат, при наданні допомоги організаціям при визначенні, оцінці та управлінні ризиками кібербезпеки.
S0369	Навичка визначати джерела, характеристики і використання даних-активів організації.
S0370	Навичка використовувати у власній організації структури і процеси підготовки звітів про кіберзахист постачальника послуг.
S0371	Навичка реагування і проведення локальних заходів у відповідь на сигнали сповіщення про загрозу, поширені постачальниками послуг.
S0372	Навичка перекладати, відстежувати і пріоритезувати потреби в інформації і вимоги до збору даних розвідки серед розширеної організації.
S0373	Навичка забезпечити, що інформація про підзвітність зібрана для інформаційних систем та компонентів інформаційних та комунікаційних технологій інфраструктури ланцюжка постачання
S0374	Навичка виявляти проблеми кібербезпеки і приватності, які виникають при з'єднаннях внутрішніх та зовнішніх замовників та організацій-партнерів.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

A.7. Опис здатностей в Загальних принципах NICE

В Таблиці 7 наведений перелік здібностей з кібербезпеки. Здатність – це компетентність виконувати спостережувану поведінку або поведінку результатом якої є спостережуваний продукт. Окремі описи здатностей з цього переліку включені до кожної робочої ролі у детальному переліку робочих ролей у Додатку В. Перелік періодично оновлюватиметься [1]. Джерело останньої версії цього матеріалу можна знайти в електронній довідковій таблиці до NIST 800-181 [4].

Таблиця 7 – Опис здатностей в Загальних принципах NICE

Ідентифікатор здатності	Опис
A0001	Здатність виявляти системні проблеми безпеки на основі аналізу даних вразливостей та конфігурації.
A0002	Здатність узгоджувати відповідну технологію сховищ знань для певного застосунку або середовища.
A0003	Здатність визначати достовірність інформації про тенденції розвитку технологій.
A0004	Здатність розробляти навчальні програми, які описують тему на відповідному рівні для цільової аудиторії.
A0005	Здатність дешифрувати сукупність даних.
A0006	Здатність готувати та проводити навчальні та брифінги з обізнаності щоб забезпечити, що користувачі систем, мереж і даних дотримуються політик і процедур безпеки
A0007	Здатність адаптувати аналіз коду для особливостей специфічного застосунку.
A0008	Здатність застосовувати методи, стандарти та методики для опису, аналізу та документування архітектури корпоративної інформаційної технології організації (наприклад, The Open Group Architecture Framework [TOGAF], Department of Defense Architecture Framework [DoDAF], Federal Framework Architecture Framework [FEAF]).
A0009	Здатність застосовувати стандарти управління ризиками для ланцюжка постачання.
A0010	Здатність аналізувати шкідливе ПЗ.
A0011	Здатність чітко та стисло відповідати на питання.
A0012	Здатність ставити уточнюючі питання.
A0013	Здатність впевнено і систематизовано доводити складну інформацію, концепції або ідеї в усній і письмовій формах і/або за допомогою наочних засобів.
A0014	Здатність ефективно спілкуватися під час письма.
A0015	Здатність проводити процедури сканування вразливостей і розпізнавання вразливостей в системах безпеки.
A0016	Здатність сприяти дискусіям в невеликих групах.
A0017	Здатність оцінювати рівень розуміння і знань учня.
A0018	Здатність готувати та представляти брифінги.
A0019	Здатність розробляти технічну документацію.
A0020	Здатність встановлювати ефективний зворотний зв’язок зі студентами з метою вдосконалення навчання.
A0021	Здатність використовувати і розуміти складні математичні концепції (наприклад, дискретна математика).
A0022	Здатність застосовувати принципи навчання дорослих.
A0023	Здатність розробляти обґрунтовані і надійні оцінки.
A0024	Здатність розробляти чіткі вказівки і навчальні матеріали..
A0025	Здатність точно визначати інциденти, проблеми та події в системі обробки звернень клієнтів.
A0026	Здатність аналізувати тестові дані.
A0027	Здатність використовувати цілі і завдання організації при розробці і підтримці архітектури.
A0028	Здатність оцінювати та прогнозувати вимоги до персоналу для досягнення цілей організації.
A0029	Здатність будувати складні структури даних і високорівневі мови програмування.
A0030	Здатність збирати, перевіряти і підтверджувати дані тестування.
A0031	Здатність проводити та впроваджувати маркетингові дослідження для урядових та галузевих можливостей, а також відповідного ціноутворення.
A0032	Здатність розробляти навчальні програми для їх використання у віртуальному середовищі.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор здатності	Опис
A0033	Здатність розробляти політику, плани і стратегії відповідно до законодавства, регуляторних актів, політик і стандартів на підтримку кібердіяльності організації.
A0034	Здатність розробляти, оновлювати та/або підтримувати стандартні операційні процедури (SOP).
A0035	Здатність розкрити проблему і перевірити взаємозв'язки між даними, які, на перший погляд, здаються не пов'язаними між собою.
A0036	Здатність високорівнево визначати основні загальні проблеми коду.
A0037	Здатність задіяти кращі практики і отримані уроки зовнішніх організацій і освітніх установ які мають справу з ситуаціями кібербезпеки.
A0038	Здатність проводити оптимізацію системи відповідно до вимог продуктивності підприємства.
A0039	Здатність контролювати розробку та оновлення оцінки витрат на життєвий цикл.
A0040	Здатність переводити дані і результати тестування в оціночні висновки.
A0041	Здатність використовувати інструменти візуалізації даних (наприклад, Flare, HighCharts, AmCharts, D3.js, Processing, Google Visualization API, Tableau, Raphael.js,).
A0042	Здатність розвивати можливості кар'єрного росту.
A0043	Здатність проводити криміналістичну експертизу в середовищах Windows і Unix/Linux.
A0044	Здатність застосовувати структури і логіку мов програмування (наприклад, аналіз коду джерела).
A0045	Здатність оцінити /забезпечити надійність постачальника та/або продукту.
A0046	Здатність моніторити і оцінювати можливий вплив виникаючих технологій на закони, нормативні акти та/або політики.
A0047	Здатність розробляти безпечне програмне забезпечення відповідно до методологій, інструментів і практик розробки безпечного програмного забезпечення.
A0048	Здатність застосовувати концепції архітектури безпеки мереж, включаючи топологію, протоколи, компоненти і принципи (наприклад, застосунки з «ешелонованим захистом).
A0049	Здатність застосовувати інструменти, методи і техніки розробки безпечних систем.
A0050	Здатність застосовувати інструменти, методи і техніки проектування систем, включаючи інструменти автоматизованого аналізу та проектування систем.
A0051	Здатність виконувати процеси інтеграції технологій.
A0052	Здатність експлуатувати мережеве обладнання, включаючи концентратори, маршрутизатори, комутатори, мости, сервери, засоби передачі та відповідне апаратне обладнання.
A0053	Здатність визначати достовірність даних про тенденції трудових ресурсів.
A0054	Здатність застосовувати методології проектування навчальних систем (ISD).
A0055	Здатність користуватися загальнодоступними мережевими інструментами (наприклад, ping, traceroute, nslookup).
A0056	Здатність забезпечити практики безпеки протягом усього процесу закупівель.
A0057	Здатність розробити навчальну програму, яка відповідає темі на відповідному рівні для цільової аудиторії.
A0058	Здатність використовувати командний рядок ОС (наприклад,ipconfig, netstat, dir, nbtstat).
A0059	Здатність налаштовувати маршрути локальної мережі/ глобальної мережі організації.
A0060	Здатність будувати архітектури та загальні принципи.
A0061	Здатність проектувати архітектури та загальні принципи.
A0062	Здатність моніторити показники або індикатори продуктивності та доступності системи.
A0063	Здатність керувати різними системами і методами електронної комунікації (наприклад, електронна пошта, VOIP, IM, Web-форуми, Direct Video Broadcasts).
A0064	Здатність інтерпретувати та переводити вимоги замовника в операційні можливості

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор здатності	Опис
A0065	Здатність моніторити потоки трафіку, що проходять через мережу.
A0066	Здатність збирати точні та повні дані з джерел, які використовуються для результатів розвідки, оцінки та/або планування.
A0067	Здатність адаптуватися та працювати в різноманітних, непередбачуваних, складних швидкоплинних робочих середовищах.
A0068	Здатність застосовувати затверджені процеси планування і кадрового забезпечення.
A0069	Здатність застосовувати навички і стратегії спільної роботи.
A0070	Здатність застосовувати навички критичного читання/мислення.
A0071	Здатність застосовувати мовну та культурологічну експертизу для аналізу.
A0072	Здатність чітко викладати вимоги до розвідки в коректно сформульованих питаннях дослідницької роботи і змінних параметрах даних, що відслідковуються для відстеження вхідних запитів.
A0073	Здатність чітко викладати вимоги до розвідки в коректно сформульованих питаннях дослідницької роботи та запитах на інформації.
A0074	Здатність ефективно співпрацювати з іншими.
A0076	Здатність координувати та співпрацювати з аналітиками щодо розробки вимог спостереження і суттєвої інформації.
A0077	Здатність координувати кібероперації з іншими функціями організації або підтримуючою діяльністю.
A0078	Здатність координувати, співпрацювати та розповсюджувати інформацію серед підпорядкованих, суміжних організацій та організацій вищого рівня.
A0079	Здатність коректно використовувати кожну організацію чи елемент у плані та матриці збору даних.
A0080	Здатність розробляти або рекомендувати аналітичні підходи або рішення для подолання проблем або ситуацій, для яких недостатньо інформації або немає прецедента.
A0081	Здатність розробляти або рекомендувати рішення планування для проблем або ситуацій, для яких немає прецеденту.
A0082	Здатність ефективно співпрацювати через віртуальні команди.
A0083	Здатність оцінювати інформацію на предмет її надійності, достовірності і актуальності.
A0084	Здатність оцінювати, аналізувати та синтезувати великі об’єми даних (які можуть бути фрагментованими і суперечливими) в високоякісні і об’єднані продукти таргетингу/розвідки.
A0085	Здатність застосовувати судження, коли політики визначені некоректно.
A0086	Здатність розширювати доступ до мережі шляхом проведення цільового аналізу і збору даних для визначення цілей, що представляє інтерес.
A0087	Здатність концентрувати зусилля у дослідницькій області з метою задоволення потреб замовника в процесі прийняття рішень.
A0088	Здатність ефективно працювати у динамічному, швидкоплинному середовищі.
A0089	Здатність працювати в колективі, постійно звертаючись за консультаціями до аналітиків і експертів (внутрішніх і зовнішніх організацій) для використання аналітичного і технічного досвіду.
A0090	Здатність визначати зовнішніх партнерів зі спільними інтересами в проведенні кібероперацій.
A0091	Здатність виявляти пробіли розвідки.
A0092	Здатність ідентифікувати/описувати вразливості цілі.
A0093	Здатність ідентифікувати/описувати методики /методи ведення технічної експлуатації цілі.
A0094	Здатність інтерпретувати і застосовувати закони, нормативні акти, політики та методології, що стосуються кіберцілей організації.
A0095	Здатність інтерпретувати і перетворювати вимоги замовника в оперативні дії.
A0096	Здатність інтерпретувати і розуміти складні концепції, що швидко змінюються.
A0097	Здатність моніторити операції системи і реагувати на події у відповідь на тригери та/або спостереження за трендами або незвичайною діяльністю.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор здатності	Опис
A0098	Здатність брати участь в якості члена груп планування, координаційних і оперативних груп за необхідності.
A0099	Здатність виконувати тактики, методи та процедури збору даних в мережі, включаючи можливості/інструменти дешифрування.
A0100	Здатність проводити процедури бездротового збору даних, включаючи можливості/інструменти дешифрування.
A0101	Здатність розпізнавати і пом'якшувати когнітивні упередження, які можуть вплинути на аналіз.
A0102	Здатність розпізнавати і з пом'якшувати дезінформацію у звітності і аналізі.
A0103	Здатність переглядати оброблені матеріали мови цілі на предмет точності і повноти.
A0104	Здатність обирати відповідні програмні закладки для досягнення оперативних цілей.
A0105	Здатність адаптувати технічну та планувальну інформацію до рівня розуміння замовника.
A0106	Здатність критично мислити.
A0107	Здатність мислити як порушник.
A0108	Здатність розуміти цілі та результати.
A0109	Здатність використовувати кілька джерел розвідки в усіх напрямках розвідувальних дисциплін.
A0110	Здатність моніторити зміни в законодавстві сфери приватності для забезпечення адаптованості та відповідності діяльності організації.
A0111	Здатність взаємодіяти з департаментами і бізнес підрозділами для впровадження принципів і програм забезпечення приватності в організації та узгодження завдань забезпечення приватності з цілями безпеки.
A0112	Здатність моніторити досягнення у технологіях приватності інформації для забезпечення адаптації та відповідності організації.
A0113	Здатність визначати, чи порушує інцидент безпеки принцип приватності або правовий стандарт, що потребує прийняття конкретних юридичних рішень.
A0114	Здатність розробити або придбати навчальну програму, яка відповідає темі на відповідному рівні для цілі
A0115	Здатність взаємодіяти з департаментами і бізнес підрозділами для впровадження принципів і програм приватності в організації та узгодження цілей приватності з цілями безпеки організації.
A0116	Здатність правильно та ефективно обирати пріоритети і розподіляти ресурси кібербезпеки.
A0117	Здатність встановлювати зв'язки між стратегією, бізнесом і технологією в контексті динаміки організації.
A0118	Здатність розуміти технологічні задачі і завдання управління та керівництва, пов'язані з процесами і рішенням проблем організації.
A0119	Здатність розуміти основні поняття і проблеми, пов'язані з діяльністю організації в кіберпросторі та її впливом.
A0120	Здатність ділитися змістовною інформацією про контекст середовища загроз для організації, що покращує її позицію управління ризиками.
A0121	Здатність розробити реагування на інциденти для моделей хмарних послуг.
A0122	Здатність проектувати можливості пошуку рішень для менш поширених і більш складних системних проблем.
A0123	Здатність застосовувати принципи кібербезпеки і приватності при формуванні вимог організації (стосовно конфіденційності, цілісності, доступності, автентифікації і неспростовності).
A0124	Здатність встановлювати та підтримувати автоматизовані оцінки контролів безпеки.
A0125	Здатність написати заяву про розкриття приватності на основі чинного законодавства.
A0126	Здатність відстежувати місце розташування та конфігурацію мережевих пристроїв та програмного забезпечення по відділах, локаціях, об'єктах, тим самим підтримуючи виконання бізнес-функції.
A0127	Здатність впроваджувати технології і інструментів безперервного моніторингу.
A0128	Здатність застосовувати методики виявлення вторгнень з боку хоста та мережі за допомогою технологій виявлення вторгнень

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор здатності	Опис
A0129	Здатність забезпечити інтеграцію процесів управління інформаційною безпекою з процесами стратегічного та операційного планування.
A0130	Здатність забезпечити, щоб вищі посадові особи організації забезпечували інформаційну безпеку для інформації та систем, що підтримують операції та активи, які знаходяться під їх контролем.
A0131	Здатність забезпечити наявність в організації належним чином підготовленого персоналу, здатного дотримуватися вимог безпеки, передбачених законодавством, розпорядженнями, політиками, директивами, інструкціями, стандартами і настановами.
A0132	Здатність координуватися з вищим керівництвом організації, щоб забезпечити всеосяжний, загально корпоративний і цілісний підхід стосовно ризику, тобто підхід, який забезпечує більш глибоке розуміння інтегрованих операцій організації.
A0133	Здатність координуватися з вищим керівництвом організації для розробки стратегії управління ризиками організації, яка визначає стратегічний погляд організації на ризики, пов'язані з безпекою.
A0134	Здатність координуватися з вищим керівництвом організації для полегшення обміну інформацією, пов'язаною з ризиками, між уповноваженими офіційними особами та іншими вищими керівниками організації.
A0135	Здатність координуватися з вищим керівництвом організації, щоб забезпечити нагляд за усіма заходами, пов'язаними з управлінням ризиками у всій організації, щоб забезпечити послідовні і ефективні рішення щодо прийняття ризиків.
A0136	Здатність координуватися з вищим керівництвом організації для забезпечення того, що рішення про авторизацію враховують всі фактори, необхідні для успіху місії та бізнесу.
A0137	Здатність співпрацювати з вищим керівництвом організації з метою проведення спільної корпоративної конференції з обговорення всіх можливих джерел ризиків (включаючи агрегований ризик) для операцій, що проводяться організацією, і активів, окремих осіб, інших організацій і нації в цілому.
A0138	Здатність співпрацювати з вищим керівництвом організації для сприяння співробітництва та співпраці між уповноваженими посадовими особами, включаючи дії стосовно авторизації, які вимагають спільної відповідальності.
A0139	Здатність координуватися з вищим керівництвом організації, щоб забезпечити, що спільна відповідальність за підтримку місії/бізнес-функцій організації з використанням зовнішніх постачальників систем, послуг та застосунків отримує необхідну видимість та донесена до відповідних органів, які приймають рішення.
A0140	Здатність співпрацювати з вищим керівництвом організації для визначення позиції ризику організації на основі сукупного ризику від експлуатації та використання систем, за які відповідає організація.
A0141	Здатність тісно співпрацювати з уповноваженими посадовими особами або їх офіційними представниками, щоб допомогти забезпечити ефективне впровадження загальної програми безпеки організації та забезпеченні належного захисту усіх систем та середовищ організації.
A0142	Здатність тісно співпрацювати з уповноваженими посадовими особами або їх офіційними представниками, щоб допомогти забезпечити інтеграцію усіх міркувань безпеки в цикли розробки програм/планів/бюджетів, архітектури підприємства і життєві цикли придбання/розробки системи.
A0143	Здатність тісно співпрацювати з уповноваженими посадовими особами або їх офіційними представниками, щоб допомогти забезпечити, що системи і загальні контролі безпеки організації включені в затверджені плани безпеки і отримана діюча авторизація на їх експлуатацію.
A0144	Здатність тісно співпрацювати з уповноваженими посадовими особами або їх офіційними представниками, щоб допомогти забезпечити ефективне, економічне та своєчасне виконання заходів безпеки у всій організації.
A0145	Здатність тісно співпрацювати з уповноваженими посадовими особами або їх офіційними представниками, щоб допомогти забезпечити централізовану звітність про діяльність з безпеки.

Ідентифікатор здатності	Опис
A0146	Здатність встановлювати правила щодо належного використання та захисту інформації, а також збереження відповідальності навіть після поширення або надання інформації іншим організаціям.
A0147	Здатність затверджувати плани безпеки, меморандуми про домовленість або взаєморозуміння, плани дій та етапів, а також визначати, чи вимагають повторної авторизації важливі зміни в операційних системах або середовищах.
A0148	Здатність слугувати основною сполучною ланкою між архітектором підприємства та інженером систем безпеки та співпрацювати з власниками систем, постачальниками загальних контролів та працівниками системи безпеки щодо розподілу контролів безпеки на системні, гібридні або загальні контролі.
A0149	Здатність, тісно співпрацюючи з працівниками системи безпеки, консультувати посадових осіб, директорів інформаційних технологій, директорів із інформаційної безпеки та відповідальної посадової особи з управління ризиками/виконавчого ризику (функції) щодо питань безпеки (наприклад, встановлення периметру системи, оцінки ступеня слабкості та недоліків у системі, планів дій і контрольних точок, підходів до виявлених вразливостей).
A0150	Здатність проводити заходи з побудови безпеки системи (NIST SP 800-160).
A0151	Здатність збирати і доопрацьовувати вимоги до системи безпеки та забезпечувати ефективну інтеграцію таких вимог в складові продукти і системи через цілеспрямовану безпечну архітектуру, проектування, розробку і налаштування.
A0152	Здатність застосовувати кращі практики впровадження контролів безпеки в систему, включаючи методологію розробки ПЗ; принципи проектування системи і безпеки; проектування безпеки, безпечну архітектуру і методики безпечного кодування.
A0153	Здатність координувати їх діяльність щодо безпеки з архітекторами безпеки, директорами із інформаційної безпеки, власниками системи, постачальниками загальних контролів та працівниками безпеки.
A0154	Здатність проводити всебічну оцінку застосованих в системі або успадкованих системою управлінських, операційних і технічних контролів безпеки і їх удосконалень для визначення результативності контролів (тобто якою мірою контроль безпеки впроваджений коректно, функціонує як передбачено, чи досягається бажаний результат, що задовольняє вимогам безпеки для системи).
A0155	Здатність проводити оцінку суттєвості слабких місць або недоліків, виявлених в системі та її середовищі функціонування, і рекомендувати коригуючі дії для вирішення виявлених вразливостей.
A0156	Здатність готувати заключний звіт з оцінки безпеки, включаючи результати і висновки оцінки.
A0157	Здатність оцінювати план безпеки з метою забезпечення в наявності всього набору контролів безпеки системи, які задовольняють заявленим вимогам безпеки.
A0158	Здатність забезпечувати належний розгляд функціональних вимог та вимог безпеки в контрактах та відповідність контрактора функціональним вимогам та вимогам безпеки, зазначеним у контракті.
A0159	Здатність інтерпретувати інформацію, зібрану мережевими інструментами (наприклад, nslookup, ping, та traceroute).
A0160	Здатність перекладати, відстежувати та пріоритезувати інформаційні потреби та вимоги до збору розвідки в розширеній організації.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ідентифікатор здатності	Опис
A0161	Здатність впроваджувати вимоги до інформаційної безпеки у процес закупівлі; використовуючи застосовні базові контролі безпеки у якості одного із джерел вимог безпеки; забезпечуючи надійний процесу контролю якості програмного забезпечення; і встановлюючи різні джерела (наприклад, маршрути доставки для критичних елементів системи).
A0162	Здатність забезпечити безпеку інформаційної системи, персоналу закупівель, юрисконсульта та інших відповідних консультантів і зацікавлених осіб, які беруть участь в процесі прийняття рішень від визначення /перегляду концепцій системи, а також тих, хто бере участь у прийнятті або затвердженні кожної точки прийняття рішень протягом усього життєвого циклу систем.
A0162	Здатність розпізнавати унікальні аспекти середовища та ієрархії безпеки комунікацій (COMSEC).
A0163	Здатність інтерпретувати термінологію, методологію та процедури комунікаційної безпеки (COMSEC).
A0164	Здатність визначати ролі і обов’язки для призначеного персоналу безпеки комунікацій (COMSEC).
A0165	Здатність керувати процедурою матеріального обліку, контролю та використання безпеки комунікацій (COMSEC).
A0166	Здатність ідентифікувати типи інцидентів безпеки комунікацій (COMSEC), та як про них звітують.
A0167	Здатність визначати важливість аудиту матеріалів та рахунків безпеки комунікацій (COMSEC).
A0168	Здатність визначати вимоги до внутрішнього процесу обліку для безпеки комунікацій (COMSEC).
A0170	Здатність виявляти системи критичної інфраструктури з інформаційно-телекомунікаційними технологіями, які були спроектовані без врахування безпеки системи.
A0171	Здатність проводити оцінку потреб у навчанні та освіті.
A0172	Здатність налаштовувати фізичну або логічну підмережу, що відокремлює внутрішню локальну мережу (LAN) від інших ненадійних мереж.
A0173	Здатність розпізнавати зміни у системі або середовищі, які можуть змінити залишкові ризики по відношенню до ризик-апетиту.
A0174	Здатність знаходити і орієнтуватися в дарквебі, використовуючи анонімну (TOR) мережу з метою визначення місця розташування ринків і форумів.
A0175	Здатність перевіряти цифрові носії на декількох платформах операційних систем.
A0176	Здатність підтримувати бази даних (тобто, резервування, відновлення, видалення даних, файли логу транзакцій тощо).

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Додаток B – Детальний перелік робочих ролей

У даному додатку знаходиться детальний опис кожної робочої ролі Загальних принципів NICE. У переліку нижче надана наступна інформація стосовно робочих ролей:

- Назва робочої ролі;
- Унікальний ідентифікатор робочої ролі в Загальних принципах NICE, створений на основі абревіатур категорій та областей спеціалізації, до яких відноситься робоча роль;
- Область спеціалізації, до якої належить робоча роль;
- Категорія, до якої належить робоча роль;
- Опис робочої ролі;
- Перелік завдань в Загальних принципах NICE, які повинна виконувати особа, що займає посаду з кібербезпеки і виконує певну робочу роль;
- Перелік знань в Загальних принципах NICE, які повинна демонструвати особа, що займає посаду з кібербезпеки і виконує певну робочу роль;
- Перелік навичок в Загальних принципах NICE, якими повинна володіти особа, що займає посаду з кібербезпеки і виконує певну робочу роль; та
- Перелік здатностей в Загальних принципах NICE, які повинна демонструвати особа, що займає посаду з кібербезпеки і виконує певну робочу роль.

У таблицях нижче описані робочі ролі в Загальних принципах NICE з переліком завдань, знань, навичок та здатностей. Джерело останньої версії цього матеріалу можна знайти в електронній довідковій таблиці до NIST Special Publication 800-181 [4]. Електронна довідкова таблиця містить більш докладний список завдань, знань, навичок та здатностей. Робочі ролі періодично оновлюватимуться [1].

B.1 Забезпечення безпеки (SP)

Робоча роль	**Уповноважений офіційний представник/Призначена особа**
Ідентифікатор Робочої ролі	**SP-RSK-001**
Область спеціалізації	**Управління ризиками (RSK)**
Категорія	**Забезпечення безпеки (SP)**
Опис Робочої ролі	Вища посадова чи виконавча особа, що має повноваження офіційно взяти на себе відповідальність за управління інформаційною системою на прийнятному рівні ризику для операцій організації (включаючи місію, функції, імідж чи репутацію), організаційних активів, фізичних осіб, інших організацій та нації в цілому (CNSSI 4009).
Завдання	T0145, T0221, T0371, T0495
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0013, K0019, K0027, K0028, K0037, K0038, K0040, K0044, K0048, K0049, K0054, K0059, K0070, K0084, K0089, K0101, K0126, K0146, K0168, K0169, K0170, K0179, K0199, K0203, K0260, K0261, K0262, K0267, K0295, K0322, K0342, K0622, K0624
Навички	S0034, S0367
Здатності	A0028, A0033, A0077, A0090, A0094, A0111, A0117, A0118, A0119, A0123, A0170

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Робоча роль	**Експерт з оцінки контролів безпеки**
Ідентифікатор Робочої ролі	**SP-RSK-002**
Область спеціалізації	**Управління ризиками (RSK)**
Категорія	**Забезпечення безпеки (SP)**
Опис Робочої ролі	Здійснює незалежну комплексну оцінку управлінського, операційного та технічного контролю безпеки і покращення контролю, які використовуються в системі інформаційних технологій (IT) для визначення загальної ефективності заходів контролю (як визначено в NIST 800-37).
Завдання	T0145, T0184, T0221, T0244, T0251, T0371, T0495, T0177, T0178, T0181, T0205, T0243, T0255, T0264, T0265, T0268, T0272, T0275, T0277, T0309, T0344
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0008, K0009, K0010, K0011, K0013, K0018, K0019, K0018, K0021, K0024, K0026, K0027, K0028, K0029, K0037, K0038, K0040, K0044, K0048, K0049, K0054, K0056, K0059, K0070, K0084, K0089, K0098, K0100, K0101, K0126, K0146, K0168, K0169, K0170, K0179, K0199, K0203, K0260, K0261, K0262, K0267, K0287, K0322, K0342, K0622, K0624
Навички	S0001, S0006, S0027, S0034, S0038, S0073, S0078, S0097, S0100, S0110, S0111, S0112, S0115, S0120, S0124, S0128, S0134, S0135, S0136, S0137, S0138, S0141, S0145, S0147, S0171, S0172, S0173, S0174, S0175, S0176, S0177, S0184, S0232, S0233, S0234, S0235, S0236, S0237, S0238, S0239, S0240, S0241, S0242, S0243, S0244, S0248, S0249, S0250, S0251, S0252, S0254, S0271, S0273, S0278, S0279, S0280, S0281, S0296, S0304, S0305, S0306, S0307, S0325, S0329, S0332, S0367, S0370, S0374
Здатність	A0001, A0011, A0012, A0013, A0014, A0015, A0016, A0018, A0019, A0023, A0026, A0030, A0035, A0036, A0040, A0056, A0069, A0070, A0082, A0083, A0084, A0085, A0086, A0087, A0088, A0089, A0090, A0091, A0092, A0093, A0094, A0095, A0096, A0098, A0101, A0106, A0108, A0109, A0117, A0118, A0119, A0111, A0112, A0114, A0115, A0116, A0119, A0123, A0170

Робоча роль	**Розробник програмного забезпечення**
Ідентифікатор Робочої ролі	**SP-DEV-001**
Область спеціалізації	**Розробка програмного забезпечення (DEV)**
Категорія	**Забезпечення безпеки (SP)**
Опис Робочої ролі	Розробляє, створює, обслуговує та пише/програмує нові (або модифікує існуючі) комп’ютерні прикладні програми, програмне забезпечення або спеціальні утиліти.
Завдання	T0009, T0011, T0013, T0014, T0022, T0026, T0034, T0040, T0046, T0057, T0077, T0100, T0111, T0117, T0118, T0171, T0176, T0181, T0189, T0217, T0228, T0236, T0267, T0303, T0311, T0324, T0337, T0416, T0417, T0436, T0455, T0500, T0553, T0554
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0014, K0016, K0027, K0028, K0039, K0044, K0050, K0051, K0060, K0066, K0068, K0070, K0073, K0079, K0080, K0081, K0082, K0084, K0086, K0105, K0139, K0140, K0152, K0153, K0154, K0170, K0179, K0199, K0202, K0260, K0261, K0262, K0263, K0322, K0332, K0342, K0343, K0624
Навички	S0001, S0014, S0017, S0019, S0022, S0031, S0034, S0060, S0135, S0138, S0149, S0174, S0175, S0367
Здатність	A0007, A0021, A0047, A0123, A0170

Робоча роль	**Експерт з оцінки безпеки програмного забезпечення**
Ідентифікатор Робочої ролі	**SP-DEV-002**
Область спеціалізації	**Розробка програмного забезпечення (DEV)**
Категорія	**Забезпечення безпеки (SP)**
Опис Робочої ролі	Аналізує безпеку нових або існуючих комп'ютерних прикладних програм, програмного забезпечення або спеціалізованих програм-утиліт та забезпечує дієві результати.
Завдання	T0013, T0014, T0022, T0038, T0040, T0100, T0111, T0117, T0118, T0171, T0181, T0217, T0228, T0236, T0266, T0311, T0324, T0337, T0424, T0428, T0436, T0456, T0457, T0516, T0554
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0014, K0016, K0027, K0028, K0039, K0044, K0050, K0051, K0060, K0066, K0068, K0070, K0073, K0079, K0080, K0081, K0082, K0084, K0086, K0105, K0139, K0140, K0152, K0153, K0154, K0170, K0178, K0179, K0199, K0202, K0260, K0261, K0262, K0263, K0322, K0342, K0343, K0624
Навички	S0001, S0022, S0031, S0034, S0083, S0135, S0138, S0174, S0175, S0367
Здатність	A0021, A0123, A0170

Робоча роль	**Корпоративний архітектор**
Ідентифікатор Робочої ролі	**SP-ARC-001**
Область спеціалізації	**Системна архітектура (ARC)**
Категорія	**Забезпечення безпеки (SP)**
Опис Робочої ролі	Розробляє та супроводжує бізнес-, системні та інформаційні процеси для підтримки потреб підприємства; розробляє правила та вимоги до інформаційних технологій (IT), що описують базові та цільові архітектури.
Завдання	T0051, T0084, T0090, T0108, T0196, T0205, T0307, T0314, T0328, T0338, T0427, T0440, T0448, T0473, T0517, T0521, T0542, T0555, T0557
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0024, K0027, K0028, K0030, K0035, K0037, K0043, K0044, K0052, K0056, K0060, K0061, K0063, K0074, K0075, K0082, K0091, K0093, K0102, K0170, K0179, K0180, K0198, K0200, K0203, K0207, K0211, K0212, K0214, K0227, K0240, K0264, K0275, K0286, K0287, K0291, K0293, K0299, K0322, K0323, K0325, K0326, K0332, K0333, K0487, K0516
Навички	S0005, S0024, S0027, S0050, S0060, S0122, S0367, S0374
Здатність	A0008, A0015, A0027, A0038, A0051, A0060, A0123, A0170

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Робоча роль	**Архітектор безпеки**
Ідентифікатор Робочої ролі	**SP-ARC-002**
Область спеціалізації	**Системна архітектура (ARC)**
Категорія	**Забезпечення безпеки (SP)**
Опис Робочої ролі	Забезпечує, що вимоги безпеки зацікавлених сторін, необхідні для захисту місії організації та бізнес-процесів, належним чином враховуються в усіх аспектах архітектури підприємства, включаючи еталонні моделі, архітектури сегментів та рішень, а також системи для підтримки цих місій та бізнес-процесів.
Завдання	T0050, T0051, T0071, T0082, T0084, T0090, T0108, T0177, T0196, T0203, T0205, T0268, T0307, T0314, T0328, T0338, T0427, T0448, T0473, T0484, T0542, T0556
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0008, K0009, K0010, K0011, K0012, K0013, K0015, K0018, K0019, K0024, K0026, K0027, K0030, K0035, K0036, K0037, K0043, K0044, K0052, K0055, K0056, K0057, K0059, K0060, K0061, K0063, K0071, K0074, K0082, K0091, K0092, K0093, K0102, K0170, K0180, K0198, K0200, K0202, K0211, K0212, K0214, K0227, K0240, K0260, K0261, K0262, K0264, K0275, K0277, K0286, K0287, K0291, K0293, K0320, K0322, K0323, K0325, K0326, K0332, K0333, K0336, K0374, K0565
Навички	S0005, S0022, S0024, S0027, S0050, S0059, S0061, S0076, S0116, S0122, S0138, S0139, S0152, S0168, S0170, S367, S0374
Здатність	A0008, A0014, A0015, A0027, A0038, A0048, A0049, A0050, A0061, A0123, A0148, A0149, A0170, A0172

Робоча роль	**Спеціаліст з науково-дослідних робіт**
Ідентифікатор Робочої ролі	**SP-TRD-001**
Область спеціалізації	**Наукове дослідження технологій (TRD)**
Категорія	**Забезпечення безпеки (SP)**
Опис Робочої ролі	Досліджує інжиніринг програмного забезпечення та систем, а також досліджує програмні системи для розробки нових можливостей, забезпечуючи повне впровадження кібербезпеки. Проводить комплексне дослідження технологій для оцінки потенційних вразливостей в системах кіберпростору.
Завдання	T0064, T0249, T0250, T0283, T0284, T0327, T0329, T0409, T0410, T0411, T0413, T0547
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0019, K0059, K0090, K0126, K0169, K0170, K0171, K0172, K0174, K0175, K0176, K0179, K0202, K0209, K0267, K0268, K0269, K0271, K0272, K0288, K0296, K0310, K0314, K0321, K0342, K0499
Навички	S0005, S0017, S0072, S0140, S0148, S0172
Здатність	A0001, A0018, A0019, A0170

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Робоча роль	**Спеціаліст з планування вимог до систем**
Ідентифікатор Робочої ролі	**SP-SRP-001**
Область спеціалізації	**Планування системних вимог (SRP)**
Категорія	**Забезпечення безпеки (SP)**
Опис Робочої ролі	Консультується з клієнтами для оцінки функціональних вимог та переведення функціональних вимог у технічні рішення.
Завдання	T0033, T0039, T0045, T0052, T0062, T0127, T0156, T0174, T0191, T0235, T0273, T0300, T0313, T0325, T0334, T0454, T0463, T0497
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0008, K0012, K0018, K0019, K0032, K0035, K0038, K0043, K0044, K0045, K0047, K0055, K0056, K0059, K0060, K0061, K0063, K0066, K0067, K0073, K0074, K0086, K0087, K0090, K0091, K0093, K0101, K0102, K0126, K0163, K0164, K0168, K0169, K0170, K0180, K0200, K0267, K0287, K0325, K0332, K0333, K0622
Навички	S0005, S0006, S0008, S0010, S0050, S0134, S0367
Здатність	A0064, A0123, A0170

Робоча роль	**Спеціаліст з тестування та оцінки систем**
Ідентифікатор Робочої ролі	**SP-TST-001**
Область спеціалізації	**Тестування і оцінка (TST)**
Категорія	**Забезпечення безпеки (SP)**
Опис Робочої ролі	Планує, готує та проводить тестування систем для оцінки відповідності специфікаціям та вимогам, а також аналізує/звітує щодо результатів тестування.
Завдання	T0058, T0080, T0125, T0143, T0257, T0274, T0393, T0426, T0511, T0512, T0513, T0539, T0540
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0027, K0028, K0037, K0044, K0057, K0088, K0091, K0102, K0139, K0126, K0169, K0170, K0179, K0199, K0203, K0212, K0250, K0260, K0261, K0262, K0287, K0332
Навички	S0015, S0021, S0026, S0030, S0048, S0060, S0061, S0082, S0104, S0107, S0110, S0112, S0115, S0117, S0367
Здатність	A0026, A0030, A0040, A0123

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Робоча роль	**Розробник системи безпеки інформаційних систем**
Ідентифікатор Робочої ролі	**SP-SYS-001**
Область спеціалізації	**Розробка систем (SYS)**
Категорія	**Забезпечення безпеки (SP)**
Опис Робочої ролі	Проектує, розробляє, тестує та оцінює безпеку інформаційної системи протягом всього життєвого циклу розробки систем.
Завдання	T0012, T0015, T0018, T0019, T0021, T0032, T0053, T0055, T0056, T0061, T0069, T0070, T0076, T0078, T0105, T0107, T0109, T0119, T0122, T0124, T0181, T0201, T0205, T0228, T0231, T0242, T0269, T0270, T0271, T0272, T0304, T0326, T0359, T0446, T0449, T0466, T0509, T0518, T0527, T0541, T0544
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0015, K0018, K0024, K0027, K0028, K0030, K0032, K0035, K0036, K0044, K0045, K0049, K0050, K0052, K0055, K0056, K0060, K0061, K0063, K0065, K0066, K0067, K0073, K0081, K0082, K0084, K0086, K0087, K0090, K0091, K0093, K0102, K0126, K0139, K0169, K0170, K0179, K0180, K0200, K0203, K0260, K0261, K0262, K0276, K0287, K0297, K0308, K0322, K0325, K0332, K0333, K0336
Навички	S0001, S0022, S0023, S0024, S0031, S0034, S0036, S0085, S0145, S0160, S0367
Здатність	A0001, A0008, A0012, A0013, A0015, A0019, A0026, A0040, A0048, A0049, A0050, A0056, A0061, A0074, A0089, A0098, A0108, A0119, A0123, A0170

Робоча роль	**Розробник систем**
Ідентифікатор Робочої ролі	**SP-SYS-002**
Область спеціалізації	**Розробка систем (SYS)**
Категорія	**Забезпечення безпеки (SP)**
Опис Робочої ролі	Проектує, розробляє, тестує та оцінює інформаційну систему протягом всього життєвого циклу розробки систем.
Завдання	T0012, T0021, T0053, T0056, T0061, T0067, T0070, T0107, T0109, T0119, T0181, T0201, T0205, T0228, T0242, T0304, T0326, T0350, T0358, T0359, T0378, T0406, T0447, T0449, T0464, T0466, T0480, T0488, T0518, T0528, T0538, T0541, T0544, T0558, T0559, T0560
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0015, K0018, K0024, K0027, K0028, K0030, K0032, K0035, K0036, K0044, K0045, K0049, K0050, K0052, K0055, K0056, K0060, K0061, K0063, K0065, K0066, K0067, K0073, K0081, K0082, K0084, K0086, K0087, K0090, K0091, K0093, K0102, K0126, K0139, K0169, K0170, K0179, K0180, K0200, K0203, K0207, K0212, K0227, K0260, K0261, K0262, K0276, K0287, K0297, K0308, K0322, K0325, K0332, K0333, K0336
Навички	S0018, S0022, S0023, S0024, S0025, S0031, S0034, S0036, S0060, S0085, S0097, S0136, S0145, S0146, S0160, S0367
Здатність	A0123, A0170

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

B.2 Експлуатація і обслуговування (OM)

Робоча роль	**Адміністратор бази даних**
Ідентифікатор Робочої ролі	**OM-DTA-001**
Область спеціалізації	**Управління даними (DTA)**
Категорія	**Експлуатація і обслуговування (OM)**
Опис Робочої ролі	Адмініструє бази даних та/або системи управління даними, що дозволяють безпечно зберігати, запитувати, захищати та використовувати дані.
Завдання	T0008, T0137, T0139, T0140, T0146, T0152, T0162, T0210, T0305, T0306, T0330, T0422, T0459, T0490
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0020, K0021, K0022, K0023, K0025, K0031, K0056, K0060, K0065, K0069, K0083, K0097, K0197, K0260, K0261, K0262, K0277, K0278, K0287, K0420
Навички	S0002, S0013, S0037, S0042, S0045
Здатність	A0176

Робоча роль	**Спеціаліст з аналізу даних**
Ідентифікатор Робочої ролі	**OM-DTA-002**
Область спеціалізації	**Управління даними (DTA)**
Категорія	**Експлуатація і обслуговування (OM)**
Опис Робочої ролі	Досліджує дані з різних джерел з метою забезпечення обізнаності щодо безпеки та приватності. Проектує та впроваджує користувацькі алгоритми, робочі процеси та макети для складних корпоративних масивів даних, що використовуються для моделювання, пошуку даних та дослідницьких цілей.
Завдання	T0007, T0008, T0068, T0146, T0195, T0210, T0342, T0347, T0349, T0351, T0353, T0361, T0366, T0381, T0382, T0383, T0385, T0392, T0402, T0403, T0404, T0405, T0460
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0015, K0016, K0020, K0022, K0023, K0025, K0031, K0051, K0052, K0056, K0060, K0065, K0068, K0069, K0083, K0095, K0129, K0139, K0140, K0193, K0197, K0229, K0236, K0238, K0325, K0420
Навички	S0013, S0017, S0202, S0028, S0029, S0037, S0060, S0088, S0089, S0094, S0095, S0103, S0106, S0109, S0113, S0114, S0118, S0119, S0123, S0125, S0126, S0127, S0129, S0130, S0160, S0369
Здатність	A0029, A0035, A0036, A0041, A0066

Робоча роль	**Адміністратор бази знань**
Ідентифікатор Робочої ролі	**OM-KMG-001**
Область спеціалізації	**Управління знаннями (KMG)**
Категорія	**Експлуатація і обслуговування (OM)**
Опис Робочої ролі	Відповідальний за управління та адміністрування процесів та інструментів, які дозволяють організації ідентифікувати, документувати та отримувати доступ до інтелектуального капіталу та інформаційного контенту.
Завдання	T0037, T0060, T0154, T0185, T0209, T0339, T0421, T0452, T0524
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0013, K0094, K0095, K0096, K0146, K0194, K0195, K0228, K0260, K0261, K0262, K0283, K0287, K0315, K0338, K0420
Навички	S0011, S0012, S0049, S0055
Здатність	A0002

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Робоча роль	**Спеціаліст з технічної підтримки**
Ідентифікатор Робочої ролі	**OM-STS-001**
Область спеціалізації	**Робота з клієнтами та технічна підтримка (STS)**
Категорія	**Експлуатація і обслуговування (OM)**
Опис Робочої ролі	Надає технічну підтримку клієнтам, які потребують допомоги з використанням апаратного та програмного забезпечення на рівні клієнта відповідно до встановлених або затверджених компонентів організаційного процесу (наприклад, Плану управління інцидентами, якщо такий передбачений).
Завдання	T0125, T0237, T0308, T0315, T0331, T0468, T0482, T0491, T0494, T0496, T0502, T0530
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0053, K0088, K0109, K0114, K0116, K0194, K0224, K0237, K0242, K0247, K0260, K0261, K0262, K0287, K0292, K0294, K0302, K0317, K0330
Навички	S0039, S0058, S0142, S0159, S0365
Здатність	A0025, A0034, A0122

Робоча роль	**Спеціаліст з мережевих операцій**
Ідентифікатор Робочої ролі	**OM-NET-001**
Область спеціалізації	**Обслуговування мереж (NET)**
Категорія	**Експлуатація і обслуговування (OM)**
Опис Робочої ролі	Планує, реалізовує і експлуатує мережеві послуги /системи, включаючи апаратне та віртуальні середовища.
Завдання	T0035, T0065, T0081, T0121, T0125, T0126, T0129, T0153, T0160, T0200, T0232
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0010, K0011, K0029, K0038, K0049, K0050, K0053, K0061, K0071, K0076, K0093, K0104, K0108, K0111, K0113, K0135, K0136, K0137, K0138, K0159, K0160, K0179, K0180, K0200, K0201, K0203, K0260, K0261, K0262, K0274, K0287, K0332, K0622
Навички	S0004, S0035, S0040, S0041, S0056, S0077, S0079, S0084, S0150, S0162, S0170
Здатність	A0052, A0055, A0058, A0059, A0062, A0063, A0065, A0159

Робоча роль	**Системний адміністратор**
Ідентифікатор Робочої ролі	**OM-ADM-001**
Область спеціалізації	**Системне адміністрування (ADM)**
Категорія	**Експлуатація і обслуговування (OM)**
Опис Робочої ролі	Відповідає за встановлення та підтримку системи або конкретних компонентів системи (наприклад, встановлення, конфігурування та оновлення апаратного та програмного забезпечення, створення та управління обліковими записами користувачів, нагляд або виконання резервного копіювання та відновлення, впровадження оперативного та технічного контролів безпеки; і дотримання політик та процедур безпеки організації).
Завдання	T0029, T0054, T0063, T0136, T0144, T0186, T0207, T0418, T0431, T0435, T0458, T0461, T0498, T0501, T0507, T0514, T0515, T0531
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0049, K0050, K0053, K0064, K0077, K0088, K0100, K0103, K0104, K0117, K0130, K0158, K0167, K0179, K0260, K0261, K0262, K0274, K0280, K0289, K0318, K0332, K0346
Навички	S0016, S0033, S0043, S0073, S0076, S0111, S0143, S0144, S0151, S0153, S0154, S0155, S0157, S0158
Здатність	A0025, A0027, A0034, A0055, A0062, A0074, A0088, A0123, A0124

Робоча роль	**Аналітик з безпеки систем**
Ідентифікатор Робочої ролі	**OM-ANA-001**
Область спеціалізації	**Системний аналіз (ANA)**
Категорія	**Експлуатація і обслуговування (OM)**
Опис Робочої ролі	Відповідальний за аналіз та розвиток процесів інтеграції, тестування, експлуатації та підтримки систем безпеки.
Завдання	T0015, T0016, T0017, T0085, T0086, T0088, T0123, T0128, T0169, T0177, T0187, T0194, T0202, T0205, T0243, T0309, T0344, T0462, T0469, T0470, T0475, T0477, T0485, T0489, T0492, T0499, T0504, T0508, T0526, T0545, T0548
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0015, K0018, K0019, K0024, K0035, K0036, K0040, K0044, K0049, K0052, K0056, K0060, K0061, K0063, K0075, K0082, K0093, K0102, K0179, K0180, K0200, K0203, K0227, K0260, K0261, K0262, K0263, K0266, K0267, K0275, K0276, K0281, K0284, K0285, K0287, K0290, K0297, K0322, K0333, K0339
Навички	S0024, S0027, S0031, S0036, S0060, S0141, S0147, S0167, S0367
Здатність	A0015, A0123

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

B.3 Нагляд і корпоративне управління (OV)

Робоча роль	**Юрисконсульт з інформаційного права**
Ідентифікатор Робочої ролі	**OV-LGA-001**
Область спеціалізації	**Юридичний супровід та адвокатура (LGA)**
Категорія	**Нагляд і корпоративне управління (OV)**
Опис Робочої ролі	Надає юридичну консультацію та рекомендації з актуальних питань, пов’язаних з інформаційним правом.
Завдання	T0006, T0098, T0102, T0131, T0220, T0419, T0434, T0465, T0474, T0476, T0478, T0487, T0522
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0017, K0059, K0107, K0157, K0261, K0262, K0267, K0312, K0316, K0341, K0615
Навички	S0356
Здатність	A0046

Робоча роль	**Уповноважений з приватності /Менеджер із забезпечення комплаєнсу приватності**
Ідентифікатор Робочої ролі	**OV-LGA-002**
Область спеціалізації	**Юридичний супровід та адвокатура (LGA)**
Категорія	**Нагляд і корпоративне управління (OV)**
Опис Робочої ролі	Розробляє та здійснює нагляд за програмами забезпечення приватності та персоналом програми приватності, підтримуючи дотримання вимог приватності, умови корпоративного управління /політики, а також процеси управління інцидентами відповідно до потреб виконавчих керівників з приватності та безпеки, а також їхніх команд.
Завдання	T0003, T0004, T0029, T0930, T0032, T0066, T0098, T0099, T0131, T0133, T0188, T0381, T0384, T0478, T0861, T0862, T0863, T0864, T0865, T0866, T0867, T0868, T0869, T0870, T0871, T0872, T0873, T0874, T0875, T0876, T0877, T0878, T0879, T0880, T0881, T0882, T0883, T0884, T0885, T0886, T0887, T0888, T0889, T0890, T0891, T0892, T0893, T0894, T0895, T0896, T0897, T0898, T0899, T0900, T0901, T0902, T0903, T0904, T0905, T0906, T0907, T0908, T0909, T0910, T0911, T0912, T0913, T0914, T0915, T0916, T0917, T0918, T0919
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0008, K0066, K0168, K0612, K0613, K0614, K0615
Навички	S0354, S0355, S0356
Здатності	A0024, A0033, A0034, A0104, A0105, A0110, A0111, A0112, A0113, A0114, A0115, A0125

Робоча роль	Розробник навчальної програми з кібербезпеки
Ідентифікатор Робочої ролі	OV-TEA-001
Область спеціалізації	Підготовка, освіта та обізнаність (TEA)
Категорія	Нагляд і корпоративне управління (OV)
Опис Робочої ролі	Розробляє, планує, координує та оцінює навчальні\тренінгові курси, методи та методики навчання з кібербезпеки відповідно до навчальних потреб.
Завдання	T0230, T0247, T0248, T0249, T0345, T0352, T0357, T0365, T0367, T0380, T0437, T0442, T0450, T0451, T0534, T0536, T0926
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0059, K0124, K0146, K0147, K0204, K0208, K0213, K0216, K0217, K0220, K0243, K0239, K0245, K0246, K0250, K0252, K0287, K0628
Навички	S0064, S0066, S0070, S0102, S0166, S0296
Здатність	A0004, A0013, A0015, A0018, A0019, A0022, A0024, A0032, A0054, A0057, A0055, A0057, A0058, A0063, A0070, A0083, A0089, A0105, A0106, A0112, A0114, A0118, A0119, A0171

Робоча роль	Викладач з кібербезпеки
Ідентифікатор Робочої ролі	OV-TEA-002
Область спеціалізації	Підготовка, освіта та обізнаність (TEA)
Категорія	Нагляд і корпоративне управління (OV)
Опис Робочої ролі	Розробляє програму та проводить тренінги або навчання персоналу з кібербезпеки.
Завдання	T0030, T0073, T0101, T0224, T0230, T0247, T0316, T0317, T0318, T0319, T0320, T0321, T0322, T0323, T0352, T0365, T0367, T0381, T0382, T0395, T0443, T0444, T0450, T0451, T0467, T0519, T0520, T0535, T0536, T0926
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0059, K0115, K0124, K0130, K0146, K0147, K0204, K0208, K0213, K0215, K0216, K0217, K0218, K0220, K0226, K0239, K0245, K0246, K0250, K0252, K0287, K0313, K0319, K0628
Навички	S0001, S0004, S0006, S0051, S0052, S0053, S0055, S0056, S0057, S0060, S0064, S0070, S0073, S0075, S0076, S0081, S0084, S0097, S0098, S0100, S0101, S0121, S0131, S0156, S0184, S0270, S0271, S0281, S0293, S0301, S0356, S0358
Здатність	A0006, A0011, A0012, A0013, A0014, A0015, A0016, A0017, A0018, A0019, A0020, A0022, A0023, A0024, A0032, A0055, A0057, A0057, A0058, A0063, A0066, A0070, A0083, A0089, A0105, A0106, A0112, A0114, A0118, A0119, A0171

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Робоча роль	**Менеджер з безпеки інформаційних систем**
Ідентифікатор Робочої ролі	**OV-MGT-001**
Область спеціалізації	**Управління кібербезпекою (MGT)**
Категорія	**Нагляд і корпоративне управління (OV)**
Опис Робочої ролі	Відповідальний за кібербезпеку програми, організації, системи або замкнутої групи.
Завдання	T0001, T0002, T0003, T0004, T0005, T0024, T0025, T0044, T0089, T0091, T0092, T0093, T0095, T0097, T0099, T0106, T0115, T0130, T0132, T0133, T0134, T0135, T0147, T0148, T0149, T0151, T0157, T0158, T0159, T0192, T0199, T0206, T0211, T0213, T0215, T0219, T0227, T0229, T0234, T0239, T0248, T0254, T0255, T0256, T0263, T0264, T0265, T0275, T0276, T0277, T0280, T0281, T0282
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0008, K0018, K0021, K0026, K0033, K0038, K0040, K0042, K0043, K0046, K0048, K0053, K0054, K0058, K0059, K0061, K0070, K0072, K0076, K0077, K0087, K0090, K0092, K0101, K0106, K0121, K0126, K0149, K0150, K0151, K0163, K0167, K0168, K0169, K0170, K0179, K0180, K0199, K0260, K0261, K0262, K0267, K0287, K0332, K0342, K0622, K0624
Навички	S0018, S0027, S0086
Здатність	A0128, A0161, A0170

Робоча роль	**Менеджер з безпеки комунікацій (COMSEC)**
Ідентифікатор Робочої ролі	**OV-MGT-002**
Область спеціалізації	**Управління кібербезпекою (MGT)**
Категорія	**Нагляд і корпоративне управління (OV)**
Опис Робочої ролі	Особа, яка керує ресурсами безпеки комунікацій (COMSEC) в організації (CNSSI 4009) або ключовий розпорядник Системи управління криптографічним ключем (CKMS).
Завдання	T0003, T0004, T0025, T0044, T0089, T0095, T0099, T0215, T0229
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0018, K0026, K0038, K0042, K0090, K0101, K0121, K0126, K0163, K0267, K0285, K0287, K0622
Навички	S0027, S0059, S0138
Здатність	A0162, A0163, A0164, A0165, A0166, A0167, A0168

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Робоча роль	**Відповідальний за розвиток та управління персоналом з кібербезпеки**
Ідентифікатор Робочої ролі	**OV-SPP-001**
Область спеціалізації	**Стратегічне планування та політика (SPP)**
Категорія	**Нагляд і корпоративне управління (OV)**
Опис Робочої ролі	Розробляє плани, стратегії та методологію з кібербезпеки для підтримки особового складу робочої сили, персоналу, вимог до навчання та освіти та врахування змін в політиці, доктрині, матчастині, структурі з сил та вимогах щодо освіти та навчання кадрів.
Завдання	T0001, T0004, T0025, T0044, T0074, T0094, T0099, T0116, T0222, T0226, T0341, T0352, T0355, T0356, T0362, T0363, T0364, T0365, T0368, T0369, T0372, T0373, T0374, T0375, T0376, T0384, T0387, T0388, T0390, T0391, T0408, T0425, T0429, T0437, T0441, T0445, T0472, T0481, T0505, T0506, T0529, T0533, T0536, T0537, T0552
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0072, K0101, K0127, K0146, K0147, K0168, K0169, K0204, K0215, K0233, K0234, K0241, K0243, K0309, K0311, K0313, K0335
Навички	S0108, S0128
Здатність	A0023, A0028, A0033, A0037, A0042, A0053

Робоча роль	**Спеціаліст зі стратегічного планування та кіберполітики**
Ідентифікатор Робочої ролі	**OV-SPP-002**
Область спеціалізації	**Стратегічне планування та розробка політики (SPP)**
Категорія	**Нагляд і корпоративне управління (OV)**
Опис Робочої ролі	Розробляє та підтримує плани, стратегії та політики з і кібербезпеки для підтримки та узгодження з організаційними ініціативами з кібербезпеки та законодавством.
Завдання	T0074, T0094, T0222, T0226, T0341, T0369, T0384, T0390, T0408, T0425, T0429, T0441, T0445, T0472, T0505, T0506, T0529, T0533, T0537
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0070, K0127, K0146, K0168, K0234, K0248, K0309, K0311, K0313, K0335, K0624
Навички	S0176, S0250
Здатність	A0003, A0033, A0037

Робоча роль	**Виконавчий керівник з кібербезпеки**
Ідентифікатор Робочої ролі	**OV-EXL-001**
Область спеціалізації	**Виконавчий керівник з кібербезпеки (EXL)**
Категорія	**Нагляд і корпоративне управління (OV)**
Опис Робочої ролі	Виконує повноваження щодо прийняття рішень і визначає перспективи та напрямки для кіберресурсів і ресурсів, пов’язаних з кібербезпекою та/або операційною діяльністю.
Завдання	T0001, T0002, T0004, T0006, T0025, T0066, T0130, T0134, T0135, T0148, T0151, T0227, T0229, T0229, T0248, T0254, T0263, T0264, T0282, T0337, T0356, T0429, T0445, T0509, T0763, T0871, T0872, T0927, T0928
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0070, K0106, K0314, K0296, K0147, K0624, K0628
Навички	S0018, S0356, S0357, S0358, S0359
Здатність	A0033, A0070, A0085, A0094, A0105, A0106, A0116, A0117, A0118, A0119, A0129, A0130, A0130

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Робоча роль	**Менеджер програм**
Ідентифікатор Робочої ролі	**OV-PMA-001**
Область спеціалізації	**Управління проектами/програмами (PMA) та закупівля**
Категорія	**Нагляд і корпоративне управління (OV)**
Опис Робочої ролі	Керує, координує, спілкується, інтегрує та відповідає за загальний успіх програми, забезпечуючи її узгодження з пріоритетами агентства чи підприємства.
Завдання	T0066, T0072, T0174, T0199, T0220, T0223, T0256, T0273, T0277, T0302, T0340, T0354, T0377, T0379, T0407, T0412, T0414, T0415, T0481, T0493, T0551
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0047, K0048, K0072, K0090, K0101, K0120, K0126, K0146, K0148, K0154, K0164, K0165, K0169, K0194, K0196, K0198, K0200, K0235, K0257, K0270
Навички	S0038, S0372
Здатність	A0009, A0039, A0045, A0056,

Робоча роль	**Менеджер IT проектів**
Ідентифікатор Робочої ролі	**OV-PMA-002**
Область спеціалізації	**Управління проектами/програмами (PMA) та закупівля**
Категорія	**Нагляд і корпоративне управління (OV)**
Опис Робочої ролі	Безпосередньо керує проектами інформаційних технологій.
Завдання	T0072, T0174, T0196, T0199, T0207, T0208, T0220, T0223, T0256, T0273, T0277, T0340, T0354, T0370, T0377, T0379, T0389, T0394, T0407, T0412, T0414, T0415, T0481, T0493, T0551
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0012, K0043, K0047, K0048, K0059, K0072, K0090, K0101, K0120, K0126, K0146, K0148, K0154, K0164, K0165, K0169, K0194, K0196, K0198, K0200, K0235, K0257, K0270
Навички	S0038, S0372
Здатність	A0009, A0039, A0045, A0056

Робоча роль	**Менеджер з підтримки продукту**
Ідентифікатор Робочої ролі	**OV-PMA-003**
Область спеціалізації	**Управління проектами/програмами (PMA) та закупівля**
Категорія	**Нагляд і корпоративне управління (OV)**
Опис Робочої ролі	Керує набором функцій підтримки, необхідних для роботи та забезпечення готовності та операційної спроможності систем та компонентів.
Завдання	T0072, T0174, T0196, T0204, T0207, T0208, T0220, T0223, T0256, T0273, T0277, T0302, T0340, T0354, T0370, T0377, T0389, T0394, T0412, T0414, T0493, T0525, T0551, T0553
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0043, K0048, K0059, K0072, K0090, K0120, K0126, K0148, K0150, K0154, K0164, K0165, K0169, K0194, K0196, K0198, K0200, K0235, K0249, K0257, K0270
Навички	S0038, S0372
Здатність	A0009, A0031, A0039, A0045, A0056

Робоча роль	**Керівник портфелю IT-інвестицій**
Ідентифікатор Робочої ролі	**OV-PMA-004**
Область спеціалізації	**Управління проектами/програмами (PMA) та закупівля**
Категорія	**Нагляд і корпоративне управління (OV)**
Опис Робочої ролі	Управляє портфелем IT-інвестицій, який узгоджуються з загальними потребами місії та пріоритетами підприємства.
Завдання	T0220, T0223, T0277, T0302, T0377, T0415, T0493, T0551
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0048, K0072, K0120, K0126, K0146, K0154, K0165, K0169, K0235, K0257, K0270
Навички	S0372
Здатність	A0039

Робоча роль	**Аудитор програми IT**
Ідентифікатор Робочої ролі	**OV-PMA-005**
Область спеціалізації	**Управління проектами/програмами (PMA) та закупівля**
Категорія	**Нагляд і корпоративне управління (OV)**
Опис Робочої ролі	Здійснює оцінку програми IT або її окремих компонентів для визначення відповідності опублікованим стандартам.
Завдання	T0072, T0207, T0208, T0223, T0256, T0389, T0412, T0415
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0043, K0047, K0048, K0072, K0090, K0120, K0126, K0148, K0154, K0165, K0169, K0198, K0200, K0235, K0257, K0270
Навички	S0038, S0085, S0372
Здатність	A0056

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

B.4 Захист і охорона (PR)

Робоча роль	**Аналітик системи захисту кіберпростору**
Ідентифікатор Робочої ролі	**PR-CDA-001**
Область спеціалізації	**Аналіз захисту кіберпростору (CDA)**
Категорія	**Захист і охорона (PR)**
Опис Робочої ролі	Використовує дані, зібрані за допомогою різних інструментів кіберзахисту (наприклад, сповіщення системи виявлення атак, брандмауери, логи мережевого трафіку) для аналізу подій, що відбуваються в середовищах з метою пом'якшення загроз.
Завдання	T0020, T0023, T0043, T0088, T0155, T0164, T0166, T0178, T0187, T0198, T0214, T0258, T0259, T0260, T0290, T0291, T0292, T0293, T0294, T0295, T0296, T0297, T0298, T0299, T0310, T0332, T0469, T0470, T0475, T0503, T0504, T0526, T0545, T0548
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0013, K0015, K0018, K0019, K0024, K0033, K0040, K0042, K0044, K0046, K0049, K0056, K0058, K0059, K0060, K0061, K0065, K0070, K0074, K0075, K0093, K0098, K0104, K0106, K0107, K0110, K0111, K0112, K0113, K0116, K0139, K0142, K0143, K0157, K0160, K0161, K0162, K0167, K0168, K0177, K0179, K0180, K0190, K0191, K0192, K0203, K0221, K0222, K0260, K0261, K0262, K0290, K0297, K0300, K0301, K0303, K0318, K0322, K0324, K0332, K0339, K0342, K0624
Навички	S0020, S0025, S0027, S0036, S0054, S0057, S0063, S0078, S0096, S0147, S0156, S0167, S0169, S0367, S0370
Здатність	A0010, A0015, A0066, A0123, A0128, A0159

Робоча роль	**Спеціаліст з підтримки інфраструктури захисту кіберпростору**
Ідентифікатор Робочої ролі	**PR-INF-001**
Область спеціалізації	**Підтримка інфраструктури кіберзахисту (INF)**
Категорія	**Захист і охорона (PR)**
Опис Робочої ролі	Тестує, впроваджує, розгортає, підтримує та адмініструє інфраструктурне обладнання та програмне забезпечення.
Завдання	T0042, T0180, T0261, T0335, T0348, T0420, T0438, T0483, T0486
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0021, K0033, K0042, K0044, K0058. K0061, K0062, K0104, K0106, K0135, K0157, K0179, K0205, K0258, K0274, K0324, K0332, K0334
Навички	S0007, S0053, S0054, S0059, S0077, S0079, S0121, S0124, S0367
Здатність	A0123

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Робоча роль	**Спеціаліст з управління інцидентами з кібербезпеки**
Ідентифікатор Робочої ролі	**PR-CIR-001**
Область спеціалізації	**Управління інцидентами (IR)**
Категорія	**Захист і охорона (PR)**
Опис Робочої ролі	Досліджує, аналізує та реагує на кіберінциденти в рамках мережевого середовища або замкненої групи.
Завдання	T0041, T0047, T0161, T0163, T0164, T0170, T0175, T0214, T0233, T0246, T0262, T0278, T0279, T0312, T0395, T0503, T0510
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0021, K0026, K0033, K0034, K0041, K0042, K0046, K0058, K0062, K0070, K0106, K0157, K0161, K0162, K0167, K0177, K0179, K0221, K0230, K0259, K0287, K0332, K0565, K0624
Навички	S0003, S0047, S0077, S0078, S0079, S0080, S0173, S0365
Здатність	A0121, A0128

Робоча роль	**Аналітик з оцінки вразливостей**
Ідентифікатор Робочої ролі	**PR-VAM-001**
Область спеціалізації	**Оцінка та управління вразливостями (VAM)**
Категорія	**Захист і охорона (PR)**
Опис Робочої ролі	Виконує оцінки систем та мереж у межах NE або замкненої групи та визначає, де ці системи/мережі відхиляються від прийнятних конфігурацій, політик замкненої групи чи локальних політик. Вимірює результативність ешелонованого захисту щодо відомих вразливостей.
Завдання	T0010, T0028, T0138, T0142, T0188, T0252, T0549, T0550
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0019, K0021, K0033, K0044, K0056, K0061, K0068, K0070, K0089, K0106, K0139, K0161, K0162, K0167, K0177, K0179, K0203, K0206, K0210, K0224, K0265, K0287, K0301, K0308, K0332, K0342, K0344, K0624
Навички	S0001, S0009, S0025, S0044, S0051, S0052, S0081, S0120, S0137, S0171, S0364, S0367
Здатність	A0001, A0044, A0120, A0123

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

B.5. Аналіз (AN)

Робоча роль	**Аналітик загроз/попереджень**
Ідентифікатор Робочої ролі	**AN-TWA-001**
Область спеціалізації	**Аналіз загроз (TWA)**
Категорія	**Аналіз (AN)**
Опис Робочої ролі	Розробляє кіберпоказники для забезпечення обізнаності щодо стану високодинамічного операційного середовища. Збирає, обробляє, аналізує та поширює оцінки кіберзагрози/попереджень.
Завдання	T0569, T0583, T0584, T0585, T0586, T0589, T0593, T0597, T0615, T0617, T0660, T0685, T0687, T0707, T0708, T0718, T0748, T0749, T0751, T0752, T0758, T0761, T0783, T0785, T0786, T0792, T0800, T0805, T0834
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0108, K0109, K0177, K0349, K0362, K0377, K0392, K0395, K0405, K0409, K0415, K0417, K0427, K0431, K0436, K0437, K0440, K0444, K0445, K0446, K0449, K0458, K0460, K0464, K0469, K0471, K0480, K0499, K0511, K0516, K0556, K0560, K0561, K0565, K0603, K0604, K0610, K0612, K0614
Навички	S0194, S0196, S0203, S0211, S0218, S0227, S0228, S0229, S0249, S0256, S0278, S0285, S0288, S0289, S0296, S0297, S0303
Здатність	A0013, A0066, A0072, A0080, A0082, A0083, A0084, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0107, A0109

Робоча роль	**Аналітик з експлуатації**
Ідентифікатор Робочої ролі	**AN-EXP-001**
Область спеціалізації	**Аналіз експлуатації (EXP)**
Категорія	**Аналіз (AN)**
Опис Робочої ролі	Співпрацює над виявленням пробілів у доступі та зборі даних, які можна заповнити за допомогою заходів зі збору та/або підготовки в кіберпросторі. Використовує всі дозволені ресурси та методи аналізу для проникнення в мережі цілі.
Завдання	T0028, T0266, T0570, T0572, T0574, T0591, T0600, T0603, T0608, T0614, T0641, T0695, T0701, T0720, T0727, T0736, T0738, T0754, T0775, T0777
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0108, K0109, K0131, K0142, K0143, K0177, K0224, K0349, K0362, K0417, K0444, K0471, K0560, K0351, K0354, K0368, K0371, K0376, K0379, K0388, K0393, K0394, K0397, K0418, K0430, K0443, K0447, K0451, K0470, K0473, K0484, K0487, K0489, K0509, K0510, K0523, K0529, K0535, K0544, K0557, K0559, K0608
Навички	S0066, S0184, S0199, S0200, S0201, S0204, S0207, S0214, S0223, S0236, S0237, S0239, S0240, S0245, S0247, S0258, S0260, S0264, S0269, S0279, S0286, S0290, S0294, S0300
Здатність	A0013, A0066, A0080, A0084, A0074, A0086, A0092, A0093, A0104

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Робоча роль	**Аналітик даних з різних джерел**
Ідентифікатор Робочої ролі	**AN-ASA-001**
Область спеціалізації	**Аналіз даних з різних джерел (ASA)**
Категорія	**Аналіз (AN)**
Опис Робочої ролі	Аналізує дані/ інформацію з одного або декількох джерел для підготовки середовища, відповідає на запити щодо інформації та подає на розгляд вимоги щодо збору та добування розвідданих для забезпечення планування і здійснення операцій.
Завдання	T0569, T0582, T0583, T0584, T0585, T0586, T0589, T0593, T0597, T0615, T0617, T0642, T0660, T0678, T0685, T0686, T0687, T0707, T0708, T0710, T0713, T0718, T0748, T0749, T0751, T0752, T0758, T0761, T0771, T0782, T0783, T0785, T0786, T0788, T0789, T0792, T0797, T0800, T0805, T0834
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0108, K0109, K0177, K0221, K0349, K0362, K0444, K0471, K0560, K0377, K0392, K0395, K0405, K0409, K0427, K0431, K0436, K0437, K0440, K0445, K0446, K0449, K0458, K0460, K0464, K0469, K0480, K0511, K0516, K0556, K0561, K0565, K0603, K0604, K0610, K0612, K0614, K0357, K0410, K0457, K0465, K0507, K0533, K0542, K0549, K0551, K0577, K0598
Навички	S0194, S0203, S0211, S0218, S0227, S0229, S0249, S0256, S0278, S0285, S0288, S0289, S0296, S0297, S0303, S0189, S0254, S0360
Здатність	A0013, A0066, A0080, A0084, A0072, A0082, A0083, A0085, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0107, A0108, A0109

Робоча роль	Спеціаліст з оцінки місії
Ідентифікатор Робочої ролі	AN-ASA-002
Область спеціалізації	Аналіз даних з різних джерел (ASA)
Категорія	Аналіз (AN)
Опис Робочої ролі	Розробляє плани оцінки та показники продуктивності /ефективності. Проводить стратегічну та операційну оцінки ефективності кіберподій. Визначає чи працюють системи належним чином та забезпечу\ вхідні дані для визначення операційної ефективності очікуванням.
Завдання	T0582, T0583, T0585, T0586, T0588, T0589, T0593, T0597, T0611, T0615, T0617, T0624, T0660, T0661, T0663, T0678, T0684, T0685, T0686, T0707, T0718, T0748, T0749, T0752, T0758, T0761, T0782, T0783, T0785, T0786, T0788, T0789, T0793, T0797, T0834
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0108, K0109, K0177, K0349, K0362, K0377, K0392, K0395, K0405, K0409, K0410, K0414, K0417, K0427, K0431, K0436, K0437, K0440, K0444, K0445, K0446, K0449, K0457, K0460, K0464, K0465, K0469, K0471, K0480, K0507, K0511, K0516, K0549, K0551, K0556, K0560, K0561, K0565, K0598, K0603, K0604, K0610, K0612, K0614
Навички	S0189, S0194, S0203, S0211, S0216, S0218, S0227, S0228, S0229, S0249, S0254, S0256, S0271, S0278, S0285, S0288, S0289, S0292, S0296, S0297, S0303, S0360
Здатність	A0013, A0066, A0080, A0084, A0072, A0082, A0083, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0107, A0109, A0085, A0108

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Робоча роль	**Розробник цілі**
Ідентифікатор Робочої ролі	**AN-TGT-001**
Область спеціалізації	**Аналіз цілей (TGT)**
Категорія	**Аналіз (AN)**
Опис Робочої ролі	Виконує аналіз цільової системи, створює та/або підтримує електронні папки цілі для включення вхідних даних з підготовки середовища та/або джерел внутрішньої або зовнішньої розвідки. Координує свої дії з партнерською діяльністю по цілі та розвідувальними організаціями та пропонує на затвердження і перевірку потенційні цілі.
Завдання	T0597, T0617, T0707, T0582, T0782, T0797, T0588, T0624, T0661, T0663, T0684, T0642, T0710, T0561, T0594, T0599, T0633, T0650, T0652, T0688, T0717, T0731, T0744, T0769, T0770, T0776, T0781, T0790, T0794, T0798, T0799, T0802, T0815, T0824, T0835
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0108, K0109, K0177, K0142, K0349, K0362, K0444, K0471, K0560, K0392, K0395, K0409, K0427, K0431, K0436, K0437, K0440, K0445, K0446, K0449, K0460, K0464, K0516, K0556, K0561, K0565, K0603, K0604, K0614, K0457, K0465, K0507, K0549, K0551, K0598, K0417, K0458, K0357, K0533, K0542, K0351, K0379, K0473, K0381, K0402, K0413, K0426, K0439, K0461, K0466, K0478, K0479, K0497, K0499, K0543, K0546, K0547, K0555
Навички	S0194, S0203, S0218, S0227, S0229, S0249, S0256, S0278, S0285, S0288, S0289, S0296, S0297, S0189, S0228, S0216, S0292, S0196, S0187, S0205, S0208, S0222, S0248, S0274, S0287, S0302, S0360, S0361
Здатність	A0013, A0066, A0080, A0084, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0109, A0085, A0073

Робоча роль	**Аналітик мережі цілі**
Ідентифікатор Робочої ролі	**AN-TGT-002**
Область спеціалізації	**Аналіз цілей (TGT)**
Категорія	**Аналіз (AN)**
Опис Робочої ролі	Здійснює поглиблений аналіз збору даних та даних з відкритих джерел для забезпечення безперервності цілей, для профілювання цілей та їх діяльності; і розробляє методи отримати більше інформації про цілі. Визначає, як цілі спілкуються, рухаються, діють і живуть, базуючись на знаннях технологій, цифрових мереж та програм цілей.
Завдання	T0617, T0707, T0582, T0797, T0624, T0710, T0599, T0650, T0802, T0595, T0606, T0607, T0621, T0653, T0692, T0706, T0715, T0722, T0745, T0765, T0767, T0778, T0803, T0807
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0108, K0109, K0177, K0349, K0362, K0444, K0471, K0392, K0395, K0431, K0436, K0440, K0445, K0449, K0516, K0379, K0473, K0413, K0439, K0479, K0547, K0487, K0544, K0559, K0389, K0403, K0424, K0442, K0462, K0472, K0483, K0499, K0500, K0520, K0550, K0567, K0592, K0599, K0600
Навички	S0194, S0203, S0229, S0256, S0228, S0196, S0187, S0205, S0208, S0222, S0248, S0274, S0287, S0177, S0178, S0181, S0183, S0191, S0197, S0217, S0219, S0220, S0225, S0231, S0234, S0244, S0246, S0259, S0261, S0262, S0263, S0268, S0277, S0280, S0291, S0301
Здатність	A0013, A0066, A0080, A0084, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0109, A0085, A0073

Робоча роль	**Багатопрофільний мовний аналітик**
Ідентифікатор Робочої ролі	**AN-LNG-001**
Область спеціалізації	**Мовний аналіз (LNG)**
Категорія	**Аналіз (AN)**
Опис Робочої ролі	Застосовує експертизу щодо мови та культури цілей/загроз та технічні знання для обробки, аналізу та/або розповсюдження розвідувальної інформації, отриманої з мовних, голосових та/або графічних матеріалів. Створює та підтримує лінгвоспецифічні бази даних та допоміжні засоби для підтримки виконання діяльності з кібербезпеки та забезпечення обміну критичними знаннями. Забезпечує предметну експертизу у інтенсивах проектах з іноземною мовою або міждисциплінарних проектах.
Завдання	T0650, T0606, T0715, T0745, T0761, T0837, T0838, T0839, T0840, T0841, T0842, T0843, T0844, T0845, T0846, T0847, T0848, T0849, T0850, T0851, T0852, T0853, T0854, T0855, T0856, T0857, T0858, T0859, T0860
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0108, K0143, K0177, K0431, K0449, K0413, K0487, K0462, K0520, K0550, K0567, K0599, K0600, K0417, K0377, K0356, K0359, K0391, K0396, K0398, K0407, K0416, K0476, K0488, K0491, K0493, K0499, K0524, K0532, K0539, K0540, K0541, K0545, K0548, K0564, K0571, K0574, K0579, K0596, K0606, K0607
Навички	S0187, S0217, S0244, S0259, S0262, S0277, S0218, S0184, S0290, S0179, S0188, S0193, S0195, S0198, S0210, S0212, S0215, S0224, S0226, S0232, S0233, S0235, S0241, S0251, S0253, S0265, S0283, S0284
Здатність	A0013, A0089, A0071, A0103

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

B.6 Збір і обробка (CO)

Робоча роль	**Менеджер зі збору даних з різних джерел**
Ідентифікатор Робочої ролі	**CO-CLO-001**
Область спеціалізації	**Збір інформації (CLO)**
Категорія	**Збір і обробка (CO)**
Опис Робочої ролі	Визначає відомства зі збору даних та середовище; включає пріоритетні вимоги до інформації в систему управління збором даних; розробляє концепції для задоволення намірів керівництва. Визначає можливості наявних засобів розвідки, нові можливості збору даних; та будує і поширює плани зі збору даних. Контролює виконання завдання зі збору даних та забезпечує ефективне виконання плану зі збору даних.
Завдання	T0562, T0564, T0568, T0573, T0578, T0604, T0605, T0625, T0626, T0631, T0632, T0634, T0645, T0646, T0647, T0649, T0651, T0657, T0662, T0674, T0681, T0683, T0698, T0702, T0714, T0716, T0721, T0723, T0725, T0734, T0737, T0750, T0753, T0755, T0757, T0773, T0779, T0806, T0809, T0810, T0811, T0812, T0814, T0820, T0821, T0827
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0109, K0177, K0431, K0449, K0417, K0579, K0596, K0444, K0471, K0392, K0395, K0440, K0445, K0516, K0560, K0427, K0446, K0561, K0565, K0405, K0480, K0610, K0612, K0353, K0361, K0364, K0380, K0382, K0383, K0386, K0387, K0390, K0401, K0404, K0412, K0419, K0425, K0435, K0448, K0453, K0454, K0467, K0474, K0475, K0477, K0482, K0492, K0495, K0496, K0498, K0503, K0505, K0513, K0521, K0522, K0526, K0527, K0552, K0553, K0554, K0558, K0562, K0563, K0569, K0570, K0580, K0581, K0583, K0584, K0587, K0588, K0601, K0605, K0613
Навички	S0238, S0304, S0305, S0311, S0313, S0316, S0317, S0324, S0325, S0327, S0328, S0330, S0332, S0334, S0335, S0336, S0339, S0342, S0344, S0347, S0351, S0352, S0362
Здатність	A0069, A0070, A0076, A0078, A0079

Робоча роль	**Менеджер з розробки вимог до збору даних з різних джерел**
Ідентифікатор Робочої ролі	**CO-CLO-002**
Область спеціалізації	**Збір інформації (CLO)**
Категорія	**Збір і обробка (CO)**
Опис Робочої ролі	Оцінює операції зі збору даних та розробляє стратегії вимог до збору даних з точки зору їхнього результату з використанням доступних ресурсів та методів покращення збору. Розробляє, підтримує, затверджує та координує подання вимог до збору даних. Оцінює продуктивність активів збору даних та операційну діяльність зі збору даних.
Завдання	T0564, T0568, T0578, T0605, T0651, T0714, T0725, T0734, T0809, T0810, T0811, T0565, T0577, T0580, T0596, T0602, T0613, T0668, T0673, T0675, T0682, T0689, T0693, T0694, T0730, T0746, T0780, T0819, T0822, T0830, T0831, T0832, T0833
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0109, K0177, K0353, K0361, K0364, K0380, K0382, K0383, K0384, K0386, K0387, K0390, K0395, K0401, K0404, K0412, K0417, K0419, K0421, K0425, K0427, K0431, K0435, K0444, K0445, K0446, K0448, K0453, K0454, K0467, K0474, K0475, K0477, K0480, K0482, K0492, K0495, K0496, K0498, K0505, K0513, K0516, K0521, K0526, K0527, K0552, K0554, K0558, K0560, K0561, K0562, K0563, K0565, K0568, K0569, K0570, K0579, K0580, K0581, K0584, K0587, K0588, K0596, K0605, K0610, K0612
Навички	S0304, S0305, S0316, S0317, S0327, S0330, S0334, S0335, S0336, S0339, S0344, S0347, S0352, S0329 S0337, S0346, S0348, S0353, S0362
Здатність	A0069, A0070, A0078

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Робоча роль	**Спеціаліст з планування кіберрозвідки**
Ідентифікатор Робочої ролі	**CO-OPL-001**
Область спеціалізації	**Планування кібероперацій (OPL)**
Категорія	**Збір і обробка (CO)**
Опис Робочої ролі	Розробляє детальні плани розвідки для задоволення вимог кібероперацій. Співпрацює зі спеціалістами з планування кібероперацій з метою визначення, затвердження та застосування вимог до збору та аналізу. Бере участь у виборі цілей, затвердженні, синхронізації та виконанні кібердій. Синхронізує заходи розвідки для підтримки цілей організації в кіберпросторі.
Завдання	T0734, T0563, T0575, T0576, T0579, T0581, T0587, T0590, T0592, T0601, T0627, T0628, T0630, T0636, T0637, T0638, T0639, T0640, T0648, T0656, T0659, T0667, T0670, T0676, T0680, T0690, T0691, T0705, T0709, T0711, T0719, T0726, T0728, T0733, T0735, T0739, T0743, T0760, T0763, T0772, T0784, T0801, T0808, T0816, T0836
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0108, K0109, K0120, K0431, K0417, K0444, K0395, K0445, K0560, K0427, K0446, K0561, K0565, K0480, K0610, K0612, K0435, K0471, K0392, K0440, K0405, K0377, K0349, K0362, K0436, K0379, K0403, K0460, K0464, K0556, K0603, K0614, K0465, K0507, K0598, K0511, K0414, K0577, K0347, K0350, K0352, K0355, K0358, K0399, K0400, K0408, K0411, K0422, K0432, K0455, K0456, K0459, K0463, K0494, K0499, K0501, K0502, K0504, K0506, K0508, K0512, K0514, K0517, K0518, K0519, K0525, K0538, K0566, K0572, K0575, K0578, K0582, K0585, K0586, K0589, K0590, K0591, K0593, K0594, K0595, K0599, K0602
Навички	S0218, S0203, S0249, S0278, S0296, S0297, S0176, S0185, S0186, S0213, S0250, S0272, S0273, S0306, S0307, S0308, S0309, S0310, S0312, S0314, S0315, S0318, S0319, S0320, S0321, S0322, S0323, S0331, S0333, S0338, S0340, S0341, S0343, S0345, S0350, S0360
Здатність	A0013, A0066, A0070, A0089, A0085, A0082, A0074, A0067, A0068, A0077, A0081, A0090, A0094, A0096, A0098, A0105, A0160

Робоча роль	**Спеціаліст з планування кібероперацій**
Ідентифікатор Робочої ролі	**CO-OPL-002**
Область спеціалізації	**Планування кібероперацій (OPL)**
Категорія	**Збір і обробка (CO)**
Опис Робочої ролі	Розробляє детальні плани проведення або підтримки відповідного діапазону кібероперацій за допомогою співпраці з іншими спеціалістами з планування, операторами та/або аналітиками. Бере участь у виборі цілей, затвердженні, синхронізації та інтеграції під час виконання кіберзаходів.
Завдання	T0734, T0563, T0579, T0581, T0592, T0627, T0628, T0640, T0648, T0667, T0670, T0680, T0690, T0719, T0733, T0739, T0743, T0763, T0772, T0801, T0836, T0571, T0622, T0635, T0654, T0655, T0658, T0665, T0672, T0679, T0699, T0703, T0704, T0732, T0741, T0742, T0747, T0764, T0787, T0791, T0795, T0813, T0823
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0108, K0109, K0347, K0349, K0350, K0352, K0362, K0377, K0379, K0392, K0395, K0399, K0400, K0403, K0408, K0411, K0414, K0417, K0422, K0431, K0432, K0435, K0436, K0444, K0445, K0446, K0455, K0464, K0465, K0471, K0480, K0494, K0497, K0499, K0501, K0502, K0504, K0506, K0507, K0508, K0511, K0512, K0514, K0516, K0518, K0519, K0525, K0534, K0538, K0556, K0560, K0561, K0565 K0566, K0572, K0576, K0582, K0585, K0586, K0589, K0590, K0593, K0594, K0597, K0598, K0599, K0603, K0610, K0612, K0614
Навички	S0218, S0249, S0296, S0297, S0176, S0185, S0186, S0213, S0250, S0273, S0309, S0312, S0322, S0333, S0209, S0326, S0349, S0360
Здатність	A0013, A0066, A0070, A0089, A0085, A0082, A0074, A0067, A0068, A0077, A0081, A0090, A0094, A0096, A0098, A0105

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Робоча роль	**Спеціаліст з планування партнерської інтеграції**
Ідентифікатор Робочої ролі	**CO-OPL-003**
Область спеціалізації	**Планування кібероперацій (OPL)**
Категорія	**Збір і обробка (CO)**
Опис Робочої ролі	Працює над поглибленням співпраці між партнерами з кібероперацій через організаційні або національні кордони. Сприяє інтеграції партнерських кібергруп, надаючи настанови, ресурси, допомогу у розробці кращих практик та сприяння організаційної підтримки для досягнення цілей у інтегрованих кібердіях
Завдання	T0581, T0582, T0627, T0670, T0739, T0763, T0772, T0836, T0571, T0635, T0665, T0699, T0732, T0747, T0764, T0787, T0795, T0823, T0601, T0760, T0784, T0629, T0666, T0669, T0671, T0700, T0712, T0729, T0759, T0766, T0817, T0818, T0825, T0826
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0108, K0109, K0431, K0417, K0444, K0395, K0435, K0392, K0377, K0362, K0436, K0379, K0403, K0465, K0507, K0598, K0511, K0414, K0350, K0400, K0408, K0411, K0422, K0432, K0455, K0499, K0501, K0504, K0506, K0508, K0512, K0514, K0538, K0585, K0599
Навички	S0218, S0249, S0296, S0297, S0185, S0186, S0213, S0250, S0326, S0360
Здатність	A0013, A0066, A0070, A0089, A0085, A0082, A0074, A0067, A0068, A0077, A0081, A0090, A0094, A0096, A0098, A0105

Робоча роль	**Спеціаліст з кібероперацій**
Ідентифікатор Робочої ролі	**CO-OPS-001**
Область спеціалізації	**Кібероперації (OPS)**
Категорія	**Збір і обробка (CO)**
Опис Робочої ролі	Здійснює збір, обробку та/або геолокацію систем для експлуатації, пошуку та/або відстеження цілей, що представляють інтерес. Виконує мережеву навігацію, тактичний криміналістичний аналіз і, у випадку поставленої задачі, виконує операції в мережі.
Завдання	T0566, T0567, T0598, T0609, T0610, T0612, T0616, T0618, T0619, T0620, T0623, T0643, T0644, T0664, T0677, T0696, T0697, T0724, T0740, T0756, T0768, T0774, T0796, T0804, T0828, T0829
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0021, K0051, K0109, K0142, K0224, K0363, K0372, K0373, K0375, K0379, K0403, K0406, K0420, K0423, K0428, K0427, K0429, K0430, K0433, K0438, K0440, K0452, K0468, K0481, K0485, K0486, K0480, K0516, K0528, K0530, K0531, K0536, K0560, K0565, K0573, K0608, K0609
Навички	S0062, S0183, S0236, S0182, S0190, S0192, S0202, S0206, S0221, S0242, S0243, S0252, S0255, S0257, S0266, S0267, S0270, S0275, S0276, S0281, S0282, S0293, S0295, S0298, S0299, S0363
Здатність	A0095, A0097, A0099, A0100

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

B.7 Розслідування (IN)

Робоча роль	**Слідчий кіберзлочинів**
Ідентифікатор Робочої ролі	**IN-INV-001**
Область спеціалізації	**Кіберрозслідування (INV)**
Категорія	**Розслідування (IN)**
Опис Робочої ролі	Визначає, збирає, аналізує та зберігає докази, використовуючи контрольовані та документально підтверджені аналітичні та слідчі методики.
Завдання	[Примітка: Деякі з цих заходів можуть проводитись лише працівниками правоохоронних органів чи контррозвідувального органу.] T0031, T0059, T0096, T0103, T0104, T0110, T0112, T0113, T0114, T0120, T0193, T0225, T0241, T0343, T0346, T0360, T0386, T0423, T0430, T0433, T0453, T0471, T0479, T0523
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0046, K0070, K0107, K0110, K0114, K0118, K0123, K0125, K0128, K0144, K0155, K0156, K0168, K0209, K0231, K0244, K0251, K0351, K0624
Навички	S0047, S0068, S0072, S0086
Здатність	A0174, A0175

Робоча роль	**Експерт-криміналіст судової експертизи/контррозвідки**
Ідентифікатор Робочої ролі	**IN-FOR-001**
Область спеціалізації	**Цифрова криміналістика (FOR)**
Категорія	**Розслідування (IN)**
Опис Робочої ролі	Проводить детальні розслідування комп’ютерних злочинів, встановлює документальні чи фізичні докази, включаючи цифрові носії та лог-журнали, пов’язані з інцидентами вторгнення в кіберпростір.
Завдання	T0059, T0096, T0220, T0308, T0398, T0419, T0401, T0403, T0411, T0425
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0017, K0021, K0042, K0060, K0070, K0077, K0078, K0107, K0109, K0117, K0118, K0119, K0122, K0123, K0125, K0128, K0131, K0132, K0133, K0134, K0145, K0155, K0156, K0167, K0168, K0179, K0182, K0183, K0184, K0185, K0186, K0187, K0188, K0189, K0305, K0624
Навички	S0032, S0046, S0047, S0062, S0065, S0067, S0068, S0069, S0071, S0073, S0074, S0075, S0087, S0088, S0089, S0090, S0091, S0092, S0093
Здатність	A0005, A0175

Робоча роль	**Експерт-криміналіст з кібербезпеки**
Ідентифікатор Робочої ролі	**IN-FOR-002**
Область спеціалізації	**Цифрова криміналістика (FOR)**
Категорія	**Розслідування (IN)**
Опис Робочої ролі	Аналізує цифрові докази та досліджує інциденти, пов'язані з безпекою комп'ютерів, для отримання корисної інформації з метою зменшення системної/ мережевої уразливості.
Завдання	T0027, T0036, T0048, T0049, T0075, T0087, T0103, T0113, T0165, T0167, T0168, T0172, T0173, T0175, T0179, T0182, T0190, T0212, T0216, T0238, T0240, T0241, T0253, T0279, T0285, T0286, T0287, T0288, T0289, T0312, T0396, T0397, T0398, T0399, T0400, T0401, T0432, T0532, T0546
Знання	K0001, K0002, K0003, K0004, K0005, K0006, K0018, K0021, K0042, K0060, K0070, K0077, K0078, K0109, K0117, K0118, K0119, K0122, K0123, K0125, K0128, K0131, K0132, K0133, K0134, K0145, K0155, K0156, K0167, K0168, K0179, K0182, K0183, K0184, K0185, K0186, K0187, K0188, K0189, K0224, K0254, K0255, K0301, K0304, K0347, K0624
Навички	S0032, S0047, S0062, S0065, S0067, S0068, S0069, S0071, S0073, S0074, S0075, S0087, S0088, S0089, S0090, S0091, S0092, S0093, S0131, S0132, S0133, S0156
Здатність	A0005, A0043

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Додаток С – Інструменти розвитку персоналу

С.1 Набір засобів підготовки персоналу з кібербезпеки Департамента внутрішньої безпеки (DHS)

Набір засобів підготовки персоналу з Департамента внутрішньої безпеки (CWDT) [8] допомагає організаціям усвідомити свій персонал з кібербезпеки та потреби у кадрах з кібербезпеки для захисту інформації, клієнтів та мереж організації. Цей інструментарій містить шаблони кар'єрного шляху з питань кібербезпеки та ресурси для підбору персоналу для найму та утримання талантів з кібербезпеки. CWDT пропонує інструменти, які допомагають зрозуміти ризики організації та провести інвентаризацію персоналу в організації. Інструменти CWDT охоплюють Області спеціалізації, KSA та Завдання в Загальних принципах NICE. CWDT зазначає, що першим кроком в підготовці до створення кібербезпеки є спільне бачення персоналу з кібербезпеки в організації. Спільне бачення передбачає підтримку керівників, оскільки вони реагують на зміни у середовищах і забезпечують дані для кращого спрямування ресурсів, бачення закономірності робіт та виділення сфер потенційного ризику. Розуміння цього факту є особливо важливим в мінливому середовищі кібербезпеки. CWDT включає Модель зрілості спроможності планування персоналу з кібербезпеки (CMM) та інструмент самооцінки, який допомагає організації оцінити свою готовність до планування персоналу з кібербезпеки.

CWDT пропонує профілі як орієнтир для зосередження на збереженні персоналу на всіх рівнях: будь то початківці, середні чи досвідчені фахівці з кібербезпеки.

С.1.1 Рівні кваліфікації та кар'єрний ріст

Розвиток кар'єри та обмін досвідом з працівниками допоможе їм визначити рівень їхньої кваліфікації та розвинути шляхи розвитку кар'єри з кібербезпеки.

CWDT включає в себе три етапи процесу розробки кар'єрних шляхів з кібербезпеки в рамках організації.

- 1 Етап – Ознайомлення з рівнями кваліфікації та перегляд еталонних схем просування по службі.
- 2 Етап – Розробка індивідуальних кар'єрних шляхів для конкретної організації за допомогою еталонних схем CWDT, заповнюючи форми «*Рекомендований досвід та повноваження»,* «*Компетенції і типові навички/ KSA* та «*Рекомендовані заходи професійної підготовки та розвитку».*
- 3 Етап – Подання зразків кар'єрних шляхів на розгляд керівникам та персоналу з кібербезпеки.

С.2 Інструмент Болдріджа для досягнення досконалості з кібербезпеки

Як тільки організація визначила свої вимоги щодо кібербезпеки (наприклад, за допомогою аудиту кібербезпеки або внутрішньої самооцінки), вона може за допомогою Загальних принципів NICE визначити робочі ролі та завдання для виконання таких вимог. Незважаючи на те, що загальні терміни, такі як «кіберпрофесіонали», історично використовувались для вимірювання потреб, специфіка, надана Загальними принципами NICE, забезпечує кращий підхід до опису десятків необхідних окремих робочих функцій. Визначивши необхідні та наявні компетенції, а також визначаючи пробіли між необхідними та наявними навичками, організація може визначити критичні потреби. Загальні принципи NICE допомагають організації відповісти на наступні питання, взяті з Інструмента Болдріджа для досягнення досконалості з [9], щодо підтримки ефективного та сприятливого середовища персоналу для досягнення цілей в сфері кібербезпеки:

- Як ви оцінюєте можливості та потенціал персоналу з кібербезпеки у вашій організації?
- Як ви організуєте та управляєте персоналом з кібербезпеки у вашій організації і як визначаєте робочі ролі та обов’язки?
- Як ви готуєте персонал вашої організації до змін у потребах щодо можливостей та потенціалу системи кібербезпеки?

Якщо все більше організацій будуть оцінювати свій персонал з кібербезпеки відповідно до Загальних принципів NICE, загальна лексика Загальних принципів NICE відкриє можливість здійснювати оцінку спроможностей та можливостей різних організацій, галузей та регіонів.

C.3 Інструмент шаблонного опису штатної посади

Інструмент шаблонного опису штатної посади в рамках Ініціативи з управління навичками з кібербезпеки Департамента внутрішньої безпеки [10] дозволяє менеджерам, відповідальним керівникам та спеціалістам з персоналу швидко формувати опис посади (PD) федеральних службовців без необхідності проведення масштабної підготовки або попередньої обізнаності про класифікації посад. Інструмент містить дані різних авторитетних джерел та стандартів про обов'язки, завдання та KSA, охоплює вимоги щодо найму працівників та представляє їх у якості надійного пакета, що може легко інтегруватись в існуючі процеси управління персоналом організації. Будь-яка організація може проекспериментувати з інструментом PushbuttonPD, щоб дізнатися, як він включає матеріал Загальних принципів NICE в опис посади.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Додаток D – Перехресні посилання на методології та настанови з кібербезпеки

Настанова з кар'єрного розвитку та планування персоналу NICE Strategic Goal #3 Guide Career Development and Workforce Planning спрямована на підтримку роботодавців у задоволенні потреб ринку та покращення підбору, найму, розвиток та збереження талантів з кібербезпеки. Однією з цілей цієї стратегічної мети є публікація та підвищення обізнаності про Загальні принципи NICE та заохочення їх впровадження. Впровадження в даному випадку означає використання Загальних принципів NICE у якості довідкового ресурсу для дій, пов'язаних із персоналом з кібербезпеки, тренінгами та освітою.
Один із способів заохотити впровадження Загальних принципів NICE - заохотити авторів настанов з кібербезпеки або директивних документів посилатись на Загальні принципи NICE. Три приклади публікацій досліджуються у Додатку D.

D.1 Загальні принципи кібербезпеки

У 2014 році NIST випустив Загальні принципи для посилення кібербезпеки критичної інфраструктури (Framework for Improving Critical Infrastructure Cybersecurity) [11], які зазвичай називають Cybersecurity Framework (Загальними принципами кібербезпеки). Розроблені у відповідності до Executive Order (EO) 13636 [12], Загальні принципи кібербезпеки пропонують ефективний та економічний підхід, який допомагає організаціям ідентифікувати, оцінювати та управляти ризиками кібербезпеки. Цей підхід був сформований за допомогою низки громадських семінарів, проведеними NIST для кращого розуміння того, які стандарти та методології допомагають досягненню ефективного управління ризиками, і як добровільні існуючі кращі практики можуть біти впроваджені для покращення кібербезпеки.
Допоміжний документ до Загальних принципів кібербезпеки *Дорожня карта NIST для посилення кібербезпеки критичної інфраструктури* (*NIST Roadmap for Improving Critical Infrastructure Cybersecurity) [13]* вказує на необхідність формування кваліфікованого персоналу з кібербезпеки для задоволення унікальних потреб кібербезпеки в критичній інфраструктурі. В документі відзначається, що з розвитком загрози безпеці та технологічного середовища, персонал повинен продовжувати адаптуватися і проектувати, розробляти, впроваджувати, підтримувати та постійно вдосконалювати необхідні практики кібербезпеки.
Загальні принципи кібербезпеки складаються з трьох частин: Framework Core, Framework Implementation Tiers та Framework Profiles Кожен компонент Загальних принципів кібербезпеки посилює зв'язок між драйверами бізнесу та діяльністю з кібербезпеки. Елементи Framework Core пов'язані наступним чином:

- **Функції** організовують основні заходи кібербезпеки на найвищому рівні. Ці функції - ідентифікація, захист, виявлення, реагування та відновлення - детально описані нижче.
- **Категорії** поділяють Функцію на підгрупи результатів кібербезпеки, тісно пов'язані з програмними потребами та діяльністю.
- **Підкатегорії** розділяють Категорію на специфічні результати технічної та/або управлінської діяльності. Вони надають сукупність результатів, які, хоч і не є вичерпними, але допомагають підтримувати досягнення результатів у кожній категорії.
- **Інформаційні посилання** це окремі розділи стандартів, настанов та практик, що є загальними для секторів критичної інфраструктури та ілюструють метод досягнення результатів, пов'язаних з кожною підкатегорією. Інформаційні посилання, представлені в Framework Core, є ілюстративними, а не є вичерпними. Вони представляють міжгалузеві настанови, на які найчастіше посилаються під час процесу розробки Загальних принципів.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Основні функції допомагають досягти високого рівня розуміння потреб кібербезпеки в організації :

- **Ідентифікація (ID)** – розробляти організаційне розуміння управління ризиками кібербезпеки для систем, активів, даних та спроможностей.
- **Захист (PR)** – розробляти та впроваджувати відповідні засоби захисту для надання послуг критичної інфраструктури.
- **Виявлення (DE)** - розробляти та впроваджувати відповідні заходи ідентифікації події кібербезпеки.
- **Реагування (RS)** - розробляти та впроваджувати відповідні дії для вжиття заходів щодо виявленої події кібербезпеки.
- **Відновлення (RC)** - розробляти та впроваджувати відповідні дії для підтримки планів стійкості та відновлення будь-яких спроможностей або послуг, які були порушені через подію кібербезпеки.

Багато в чому ці Функції співвідносяться з категоріями в Загальних принципах NICE. У таблиці 8 описаний взаємозв'язок між функціями в Загальних принципах кібербезпеки та Категоріями в Загальних принципах NICE

Таблиця 8 - Відповідність категорій в Загальних принципах NICE функціям в Загальних принципах кібербезпеки

Категорія в Загальних принципах NICE	Опис категорії	Відповідні функції в Загальних принципах кібербезпеки
Забезпечення безпеки (SP)	Концептуалізує, розробляє, та/або створює безпечні системи інформаційних технологій (IT), з відповідальністю за аспекти розвитку системи та/або мережі.	Ідентифікація (ID), Захист (PR)
Експлуатація і обслуговування (OM)	Забезпечує підтримку, адміністрування та технічне обслуговування, необхідне для забезпечення ефективної та продуктивної роботи та безпеки системи інформаційних технологій (IT).	Захист (PR), Виявлення (DE)
Нагляд і корпоративне управління (OV)	Забезпечує керування, управління, спрямування або розвиток та захист, щоб організація могла ефективно проводити заходи з кібербезпеки.	Ідентифікація (ID), Захист (PR), Виявлення (DE), Відновлення (RC)
Захист та охорона (PR)	Визначає, аналізує та пом'якшує загрози внутрішнім системам інформаційних технологій (IT) та/або мережам.	Захист (PR), Виявлення (DE), Реагування (RS)
Аналіз (AN)	Виконує високо спеціалізований перегляд та оцінку вхідної інформації про кібербезпеку, щоб визначити її корисність для розвідки.	Ідентифікація (ID), Виявлення (DE), Реагування (RS)
Збір і обробка (CO)	Забезпечує спеціалізовані операції з заборони та дезінформації і збір інформації про кібербезпеку, яка може бути використана для розвитку розвідки.	Виявлення (DE), Захист (PR), Реагування (RS)
Розслідування (IN)	Розслідує події кібербезпеки або злочини, пов'язані з системами інформаційних технологій (IT), мережами та цифровими доказами.	Виявлення (DE), Реагування (RS), Відновлення (RC)

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

D.1.2 Приклад інтеграції Загальних принципів кібербезпеки із Загальними принципами NICE

Хоча документи Загальних принципів кібербезпеки та Загальних принципів NICE розроблялись окремо, вони доповнюють один одного, описуючи ієрархічний підхід до досягнення цілей кібербезпеки. Розглянемо наступний приклад:
Функція **Реагування** в Загальних принципах кібербезпеки включає категорію **Пом'якшення (RS.MI)**. Ця категорія має субкатегорію **RS.MI-2,** що вказує на результат «подолання інцидентів». В Загальних принципах кібербезпеки описується цей результат і міститься декілька інформаційних посилань щодо контролів безпеки для досягнення такого результату і, при цьому, не надається інформація стосовно того, хто повинен відповідати за досягнення результату або які KSA потрібно застосовувати.

У Загальних принципах NICE ми визначаємо роль «**Спеціаліста з управління інцидентами кібербезпеки» (PR-IR-001)** в категорії **«Захист та охорона (PR)»**, область спеціалізації **«Управління інцидентами (IR)»**. Ми можемо переглянути опис цієї ролі, щоб переконатися, що вона узгоджується з результатами Загальних принципах кібербезпеки в підкатегорії **RS.MI-2:** :

> Реагує на перебої у відповідному домені для пом'якшення безпосередніх та потенційних загроз. Використовує підходи щодо пом'якшення, готовності, реагування та відновлення для максимального збереження системи, власності та інформаційної безпеки. Досліджує та аналізує відповідні заходи реагування та оцінює ефективність та покращення існуючих практик.
>
> Досліджує, аналізує та реагує на кіберінциденти в рамках мережевого середовища або замкненої групи.

З Додатку А цього документу ми визначили, що особа, посада якої включає дану Робочу роль, можна очікувати виконання багатьох із наведених нижче завдань, що узгоджуються з бажаними результатами в Загальних принципах кібербезпеки:

- **T0041** - Координувати та надавати експертну технічну підтримку технічним спеціалістам з кіберзахисту в масштабах усієї організації для управління інцидентами у сфері кіберзахисту.
- **T0047** - Зіставляти дані про інциденти для виявлення конкретних вразливостей та надання рекомендацій для якомога швидшого відновлення роботи.
- **T0161** - Виконувати аналіз лог-файлів з різних джерел (наприклад, лог-файлів окремих хостів, лог-журналів мережевого трафіку, лог-журналів мережевих екранів і систем виявлення вторгнень (IDS лог-журнали) з метою визначення можливих загроз безпеці мережі.
- **T0163** - Виконувати сортування кіберінцидентів для визначення обсягу, терміновості та потенційного впливу, ідентифікації специфічної вразливості та надання рекомендації, які дозволяють оперативно усунути проблему.
- **T0170** - Виконувати первинне накопичення і криміналістичну перевірку зображень з метою визначення можливих заходів щодо зниження/усунення несправностей в системах підприємства.
- **T0175** - Виконувати в масштабі реального часу аналіз кіберінцидентів (наприклад, збір криміналістичних матеріалів, зіставлення і відстеження вторгнень, аналіз загроз і пряме відновлення системи) з метою підтримки створюваних груп реагування на інциденти (IRT).
- **T0214** - Отримувати і аналізувати сигнали сповіщення про мережу від різних джерел всередині організації та визначати можливі причини появи таких сигналів.
- **T0233** - Відстежувати та документувати інциденти кібербезпеки з моменту їх виявлення до остаточного вирішення.

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

- **T0246** - Писати та публікувати методики та настанови з кіберзахисту, а також звіти про виявлення інцидентів для відповідної аудиторії.
- **T0262** - Застосовувати затверджені принципи і практики «ешелонованого» захисту (наприклад, багатоточкову систему, багаторівневу систему, відмовостійкість системи безпеки).
- **T0278** - Збирати докази вторгнень (наприклад, програмний код, шкідливе програмне забезпечення, трояни) і використовувати здобуті дані щоб уникнути потенційних інцидентів кіберзахисту в організації.
- **T0279** - Слугувати технічним експертом, взаємодіяти з представниками правоохоронних органів та роз'яснювати деталі інцидентів за необхідності.
- **T0312** - Співпрацювати з аналітиками розвідки з метою кореляції даних при оцінці загроз.
- **T0164** - Виконувати аналіз тенденцій в області кіберзахисту та звітування.
- **T0395** - Писати і публікувати звіти проведених заходів.
- **T0503** - Моніторити зовнішні джерела даних (наприклад, сайти постачальників засобів кіберзахисту, груп реагування на надзвичайні комп'ютерні події, центр безпеки) для підтримки поточного стану загроз кіберзахисту, та визначення того, які проблеми безпеки можуть вплинути на підприємство.
- **T0510** - Координувати функції реагування на інциденти.

Більше того, в Додатку В описані KSA, які можуть знадобитись особі, посада якої включає цю робочу роль.

Озброєна цією інформацією організація, яка хоче досягти результатів, описаних в категорії **RS.MI-2** Загальних принципів кібербезпеки, може визначити, чи володіє один чи кілька працівників необхідними навичками для виконання описаних завдань. Якщо одного чи кількох визначених KSA не вистачає, працівник, який бажає виконувати цю робочу роль, буде знати, які сфери потребують вдосконалення, і зможе звернутися до академічних класів або тренінгових курсів для здобуття необхідних знань. Якщо в організації взагалі не знайдено такого персоналу, роботодавець має конкретні описи завдань та KSA зможе розмістити оголошення про вакантну посаду, або які можуть бути використані для персоналу підрядників для збільшення наявного персоналу.

D.2 Інженерія безпеки систем

Спеціальне видання NIST (SP) 800-160 «*Розробка захисту системи – Розгляд міждисциплінарного підходу для розробки надійних захищених систем»* (NIST Special Publication (SP) 800-160, Systems Security Engineering - Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems) [14] описує інженерно-орієнтовані дії, необхідні для розробки більш захищених та стійких систем, включаючи компоненти, з яких складається така система, і послуги, які від них залежать. Публікація містить і посилається на відомі міжнародні стандарти для інженерії систем та програмного забезпечення, та пропонує впровадження методики інженерії безпеки, методів та практик в діяльність з інженерії таких систем та програмних продуктів. Кінцевою метою є вирішення проблем безпеки з точки зору вимог зацікавлених сторін і потреб захисту та використання визнаних інженерних процесів, щоб забезпечити якісне дотримання таких вимог і потреб протягом всього життєвого циклу системи. Підвищення надійності систем є істотним зобов’язанням, яке потребує значних інвестицій у вимоги, архітектуру, проектування та розвиток систем, компонентів, прикладних програм та мереж, а також докорінну культурну зміну в нинішньому підході до ведення справ «як завжди».

Впровадження упорядкованого, структурованого набору заходів та завдань інженерії захищених систем, що основується на стандартах, забезпечує важливу відправну точку та змушує функцію ініціювати необхідні зміни. Кінцевою метою є отримання надійних безпечних систем, які цілком можуть підтримувати критичні місії та операційну діяльність

бізнесу, захищаючи активи зацікавлених сторін та робити це з рівнем впевненості, що відповідає толерантності до ризику для таких зацікавлених сторін.
Відповідність компонентів в Загальних принципів NICE напрямку спеціалізації, описана в NIST SP 800-160, буде слугувати обґрунтуванням для таких компонентів. Практикуючі фахівці -розробники захищених систем ймовірно стануть експертами, які зможуть обґрунтувати встановлення додаткових KSA та завдань, які будуть додані до Загальних принципів NICE.

D.3 Коди кібербезпеки, встановлені Федеральним офісом управлінням персоналом США

4 січня 2017 р. Федеральний офіс управління персоналом США (OPM) випустив меморандум [15] під назвою «Керівництво для федеральних агентств щодо присвоєння нових кодів кібербезпеки посадам, що передбачають виконання функцій, пов'язаних з кіберпростором, інформаційними технологіями, та кібербезпекою» ("Guidance for federal agencies assigning new cybersecurity codes to positions with information technology, cybersecurity, and cyber-related functions"). У меморандумі зазначається, що Федеральний закон про охорону праці в сфері кібербезпеки від 2015 року [16] вимагає від OPM виконання процедур для впровадження структури кодування NICE та визначення всіх цивільних посад, що передбачають виконання функцій, пов'язаних з кіберпростором, інформаційними технологіями, та кібербезпекою. Таблиця 9 показує співставлення ідентифікаторів Робочих ролей в Загальних принципах NICE, що представляє міждисциплінарний характер діяльності в сфері кібербезпеки, з кодами кібербезпеки OPM, сумісними з системою інтеграції персоналу OPM.

Таблиця 9 - Відповідність ідентифікаторів робочих ролей кодам кібербезпеки OPM

Ідентифікатор робочої ролі	Код OPM	Ідентифікатор робочої ролі	Код OPM	Ідентифікатор робочої ролі	Код OPM
SP-RSK-001	611	OV-LGA-001	731	AN-TWA-001	141
SP-RSK-002	612	OV-LGA-002	732	AN-EXP-001	121
SP-DEV-001	621	OV-TEA-001	711	AN-ASA-001	111
SP-DEV-002	622	OV-TEA-002	712	AN-ASA-002	112
SP-ARC-001	651	OV-MGT-001	722	AN-TGT-001	131
SP-ARC-002	652	OV-MGT-002	723	AN-TGT-002	132
SP-TRD-001	661	OV-SPP-001	751	AN-LNG-001	151
SP-SRP-001	641	OV-SPP-002	752	CO-CLO-001	311
SP-TST-001	671	OV-EXL-001	901	CO-CLO-002	312
SP-SYS-001	631	OV-PMA-001	801	CO-OPL-001	331
SP-SYS-002	632	OV-PMA-002	802	CO-OPL-002	332
OM-DTA-001	421	OV-PMA-003	803	CO-OPL-003	333
OM-DTA-002	422	OV-PMA-004	804	CO-OPS-001	321
OM-KMG-001	431	OV-PMA-005	805	IN-INV-001	221
OM-STS-001	411	PR-CDA-001	511	IN-F0R-001	211
OM-NET-001	441	PR-INF-001	521	IN-F0R-002	212
OM-ADM-001	451	PR-CIR-001	531		
OM-ANA-001	461	PR-VAM-001	541		

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181

Додаток E – Скорочення

Нижче наведені окремі скорочення та абревіатури, що використовувались в цьому документі:

API	Application programming interface	Інтерфейс прикладних програм
CDM	Continuous Diagnostics and Mitigation	Безперервна діагностика і пом’якшення
CDS	Cross-Domain Solutions	Міждоменні рішення
CIO	Chief Information Officer	Директор з інформаційних технологій
CKMS	Crypto Key Management System	Система управління криптографічним ключем
CMMI	Capability Maturity Model Integration	Інтеграція моделі зрілості спроможностей
CMS	Content Management System	Система управління контентом
CNSSI	Committee on National Security Systems Instruction	Інструкція Комітету з систем національної безпеки
COMSEC	Communications Security	Безпека комунікацій
COTR	Contracting Officer's Technical Representative	Технічний представник офіцера по контрактам
DNS	Domain Name System	Система доменних імен
EISA	Enterprise Information Security Architecture	Архітектура інформаційної безпеки підприємства
FISMA	Federal Information Security Modernization Act	Федеральний акт про модернізацію інформаційної безпеки
FOIA	Freedom of Information Act	Акт про свободу інформації
HR	Human Resource	Людські ресурси
IDS	Intrusion detection system	Система виявлення вторгнень
IP	Internet Protocol	Інтернет-протокол
IPS	Intrusion Prevention System	Система запобігання вторгнень
IR	Incident Response	Реагування на інциденти
IRT	Incident Response Teams	Групи реагування на інциденти
ISD	Instructional System Design	Дизайн освітнього середовища
ITL	Information Technology Laboratory	Лабораторія інформаційних технологій
KSA	Knowledge, Skills, and Abilities	Знання, навички та здатність
LAN	Local area network	Мережа локального доступу
NICE	National Initiative for Cybersecurity Education	Національна освітня ініціатива з кібербезпеки
OLA	Operating-Level Agreement	Угода про операційний рівень
OMB	Office of Management and Budget	Офіс управління та бюджету
OPM	Office of Personnel Management	Офіс управління персоналом
OS	Operating system	Операційна система
OSI	Open System Interconnection	Взаємодія відкритих систем
P.L.	Public Law	Публічний закон
PCI	Payment Card Industry	Галузь платіжних карт
PHI	Personal Health Information	Персональні дані про здоров’я
PIA	Privacy Impact Assessments	Оцінка впливу на приватність
PII	Personally Identifiable Information	Персональні ідентифікаційні дані
PKI	Public key infrastructure	Інфраструктура відкритих ключів
R&D	Research and Design	Дослідження і проектування
RFID	Radio Frequency Identification	Радіочастотна ідентифікація
RMF	Risk Management Framework	Загальні принципи управління ризиками
SA&A	Security Assessment and Authorization	Оцінка та авторизація безпеки
SDLC	System development life cycle	Життєвий цикл розробки програмного забезпечення
SLA	Service-Level Agreements	Угода про рівень обслуговування
SOP	Standard operating procedures	Стандартні операційні процедури
SQL	Structured query language	Мова структурованих запитів
TCP	Transmission Control Protocol	Протокол управління передачею
TTP	Tactics, techniques, and procedures	Тактика, методики та процедури
URL	Uniform Resource Locator	Уніфікований покажчик ресурсу
VPN	Virtual Private Network	Віртуальна приватна мережа
WAN	Wide Area Network	Мережа широкого доступу

Додаток F- Посилання

[1] National Initiative for Cybersecurity Education, *National Cybersecurity Workforce Framework, ver. 1.0,* https://www.nist.gov/file/359276

[2] National Initiative for Cybersecurity Education, *National Cybersecurity Workforce Framework, ver. 2.0,* https://www.nist.gov/file/359261

[3] Reference Spreadsheet for NIST Special Publication 800-181 https://www.nist.gov/file/372581

[4] NICE Framework, National Institute of Standards and Technology [Website], https:// www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce- framework

[5] Department of Labor, Employment and Training Administration (ETA) [Website]. https://www.doleta.gov

[6] Competency Model Clearinghouse, Cybersecurity Competency Model, https://www.careeronestop.org/competencymodel/competency- models/cybersecurity. aspx

[7] U.S. Department of Homeland Security, Cybersecurity Workforce Development Toolkit (CWDT), https://niccs.us-cert.gov/workforce-development/cybersecurity- workforce-development-toolkit

[8] Baldrige Cybersecurity Excellence Program, National Institute of Standards and Technology [Website], https://www.nist.gov/baldrige/products-services/baldrige- cybersecurity-initiative

[9] U.S. Department of Homeland Security, CMSI PushButtonPD™ Tool Website, https://niccs.us-cert.gov/workforce-development/dhs-cmsi-pushbuttonpd-tool

[10] *Framework for Improving Critical Infrastructure Cybersecurity Version 1.0,* National Institute of Standards and Technology February 12, 2014, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[11] Executive Order no. 13636, *Improving Critical Infrastructure Cybersecurity,* DCPD-201300091, February 12, 2013. http://www.gpo.gov/fdsys/pkg/FR-2013-02- 19/pdf/2013-03915.pdf

[12] *NIST Roadmap for Improving Critical Infrastructure Cybersecurity,* National Institute of Standards and Technology, February 12, 2014, https://www.nist.gov/sites/default/files/documents/cyberframework/ roadmap-021214.pdf

[13] NIST Special Publication (SP) 800-160, *Systems Security Engineering - Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems,* National Institute of Standards and Technology, November 2016, https://doi.org/10.6028/NIST.SP.800-160

[14] Memorandum on Guidance for Assigning New Cybersecurity Codes to Positions with Information Technology, Cybersecurity, and Cyber-Related Functions, January 2017, https://www.chcoc.gov/content/guidance-assigning-new-cybersecurity-codes- positions-information-technology-cybersecurity

[15] H.R.2029 - Consolidated Appropriations Act, 2016 which contains Division N- Cybersecurity Act of 2015, https://www.congress.gov/114/plaws/publ113/PLAW- 114publ113.pdf

Ця публікація доступна безкоштовно за посиланням: https://doi.org/10.6028/NIST.SP.800-181