COMPUTER SYSTEMS AND NETWORKS

Vol. 6, No. 1, 2024

DOI: https://doi.org/10.23939/csn2024.01.089

УДК 004.057.2

ВИКОРИСТАННЯ ШАБЛОНІВ CIS БЕНЧМАРК ДЛЯ ВИКОНАННЯ ВИМОГ МІЖНАРОДНОГО СТАНДАРТУ ISO/IEC 27001:2022

Є. О. Курій, І. Р. Опірський

Національний університет "Львівська політехніка",
кафедра захисту інформації
E-mail: yevhenii.o.kurii@lpnu.ua, ivan.r.opirskyi@lpnu.ua

Розглянуто проблему розвитку нових методів і векторів атак на критичну інфраструктуру і відповіді на загрози, які виникають через впровадження визнаних стандартів у галузі інформаційної безпеки, таких як ISO 27001. Проведено аналіз оновленої редакції міжнародного стандарту ISO/IEC 27001 2022 року і, зокрема, основних змін у контролях управління. Здійснено детальний аналіз нового контролю безпеки з Додатку А – А.8.9 – Управління налаштуваннями (Configuration management) і можливих способів його ефективного впровадження в організаціях.

Запропоновано використання конфігураційних стандартів від Центру інтернет-безпеки (CIS – Center for Internet Security) CIS Бенчмарк (Benchmark) як одного з найефективніших способів забезпечення захисту активів організації і впровадження найкращих галузевих практик безпеки.

Внаслідок проведеного аналізу і дослідження виявлено чіткий зв'язок і залежність між використанням CIS Бенчмарків і задоволенням вимог пункту А.8.9 – Управління налаштуваннями стандарту ISO/IEC 27001:2022. Наведено класифікацію CIS Бенчмарків та описано перелік основних моментів впровадження на прикладі серверної інфраструктури.

Ключові слова: інформаційна безпека, кібербезпека, фреймворк інформаційної безпеки, фреймворк кібербезпеки, ISO 27001, Центр інтернет-безпеки, об'єкт критичної інфраструктури, інформаційний актив, управління налаштуваннями, CIS Бенчмарк.

Вступ

У цій статті автори розглянули оновлену версію найпопулярнішого стандарту в галузі інформаційної безпеки – ISO/IEC 27001:2022. Проведено дослідження основних змін порівняно з попередньою редакцією стандарту 2013 року. Зокрема, основний фокус дослідження спрямовано на детальний аналіз нового контролю безпеки з Додатку А – А.8.9 – Управління налаштуваннями (Configuration management).

Управління налаштуваннями – це процес систематичного керування конфігураціями інформаційних систем. Він містить ідентифікацію та контроль змін до програмного забезпечення, апаратних засобів, мережевих пристроїв, даних та інших компонентів інформаційної системи впродовж їх життєвого циклу.

Управління налаштуваннями є важливим аспектом забезпечення інформаційної безпеки, оскільки воно дає можливість забезпечити стабільність та надійність системи, уникнути несанкціонованих змін і забезпечити відновлення роботи системи в разі аварійних ситуацій. Крім того,

належне управління налаштуваннями допомагає зменшити ризики збоїв у роботі системи, забезпечити відповідність вимогам законодавства та стандартів щодо захисту інформації, а також підвищити довіру користувачів до системи.

1. Огляд літературних джерел

У зв'язку із виходом нової версії міжнародного стандарту ISO/IEC 27001:2022 [1], важливим стало визначення й аналіз основних змін порівняно з попередньою редакцією стандарту 2013 року [2].

З огляду на появу індустріалізованих кібератак, пристосування до ризиків інформаційної безпеки, що постійно змінюються, потребує своєчасного та гнучкого підходу до будівництва стійкої і захищеної інфраструктури підприємства [3]. З урахуванням постійної еволюції кіберзагроз та їх стрімкого збільшення стає очевидним оновлення практик інформаційної безпеки. Потреба адаптації до найновіших викликів цифрового середовища стала критичною [4].

Міжнародні стандарти ISO/IEC 27001/02 [1, 5] допомагають організаціям різних галузей забезпечити конфіденційність, цілісність та доступність інформації через впровадження системи управління ризиками. Це надає впевненість зацікавленим сторонам у тому, що ризики інформаційної безпеки адекватно оцінюються та керуються [6].

Наприкінці 2022 року вийшла оновлена та поліпшена версія стандарту ISO/IEC 27001. Цей стандарт, який посідає визначне місце у світі управління інформаційною безпекою, відіграє критичну роль у допомозі організаціям у захисті їхніх інформаційних активів [7]. Враховуючи життєву важливість цього завдання у сучасному цифровому середовищі, оновлення стандарту відображає постійні зусилля вдосконалення та адаптації до щораз вищих вимог і загроз. Це спрямовано на створення більш надійних і ефективних механізмів захисту інформації та збільшення довіри у цифровому просторі [8].

2. Постановка завдання

Майже всі сучасні бізнес-процеси визначаються і стимулюються інформацією та даними. В нашій цифровій економіці ніщо не функціонує без обміну інформацією. Наші основні послуги ґрунтуються на критичних інфраструктурах, чия функціональність сильно залежить від обміну інформацією та даними. Інформаційна безпека проникає глибоко в реальність нашої роботи та життя. Тому для підприємств будь-якого розміру обов'язковим є і захист щоденних інформаційних операцій, критичних даних та інтелектуальної власності від кіберзагроз.

Для ефективного захисту об'єктів критичної інфраструктури потрібно використовувати передові технології та методики кібербезпеки. Такі фреймворки і стандарти інформаційної безпеки, як ISO 27001 і CIS Бенчмарки надають систематичний підхід до забезпечення захисту основних активів організації і допомагають організувати процес забезпечення безпеки, встановлюючи загальноприйняті межі та вимоги.

Водночас у процесі впровадження інформаційної безпеки організації часто нехтують процесом правильного управління налаштуваннями активів, зокрема налаштуваннями безпеки. Дуже часто цей процес відбувається ситуативно і не є систематичним. Саме тому у новій редакції міжнародного стандарту ISO 27001:2022 процесу управління налаштуваннями відведено окремий контроль, який з'являється у редакції стандарту вперше. Відповідно важливим стає розроблення практичних рекомендацій для успішного впровадження цього пункту стандарту у різноманітних організаціях, і, зокрема, на об'єктах критичної інфраструктури. CIS Бенчмарки, розглянуті в цій статті, слугують спеціалізованими шаблонами для безпечного налаштування різних категорій активів організації.

Мета статті. Метою статті є розроблення практичних рекомендацій відповідно до стандарту ISO/IEC 27001:2022 для впровадження процесу безпечного управління налаштуваннями активів через застосування конфігураційних шаблонів CIS Бенчмарк.

Завдання. Ця наукова стаття має такі завдання:

1) дослідити зміни в оновленій редакції стандарту ISO/IEC 27001 2022 року порівняно з версією 2013 року;

2) розглянути способи впровадження нового контролю безпеки із Додатку А стандарту ISO/IEC 27001:2022 – A.8.9 – Управління налаштуваннями;

3) провести огляд і класифікацію шаблонів для налаштування інформаційних активів конфігураційних стандартів від Центру інтернет-безпеки CIS Бенчмарк;

4) обґрунтувати важливість використання CIS Бенчмарк як засобів забезпечення контролю A.8.9 – Управління налаштуваннями;

5) навести приклад використання CIS Бенчмарк для безпечного налаштування інформаційних активів.

3. Основна частина

3.1 . Огляд оновленої редакції стандарту ISO/IEC 27001:2022. Опис нових контролів безпеки

На кінець 2022 року оприлюднено оновлену та покращену версію стандарту ISO/IEC 27001, який є одним з найвідоміших у світі стандартів управління інформаційною безпекою. Цей стандарт допомагає організаціям захистити свої цифрові активи, що є надзвичайно важливим у сучасному цифровому середовищі, де зростають глобальні проблеми кібербезпеки та підвищується значення цифрової довіри [8].

Багато змін у новій версії стандарту є редакційними, наприклад, зміна формулювання “міжнародний стандарт” на “документ”, чи зміна порядку фраз для забезпечення кращого міжнародного перекладу [9].

Проте найбільшої уваги потребують нові контролі безпеки в додатку А. Всього в оновленій версії стандарту ISO/IEC 27001:2022 їх 11, а саме:

1) дані про загрози;
2) інформаційна безпека під час використання хмарних сервісів;
3) готовність інформаційних і телекомунікаційних технологій для забезпечення безперервності бізнесу;
4) моніторинг фізичної безпеки;
5) управління налаштуваннями;
6) видалення інформації;
7) маскування даних;
8) запобігання витокам даних;
9) моніторингова діяльність;
10) вебфільтрація;
11) безпечне кодування [1].

3.2 . Детальний огляд контролю A.8.9 – Управління налаштуваннями

Метою цієї статті є детальніший огляд нового контролю стандарту – A.8.9 – Управління налаштуваннями.

Налаштування або конфігурації, як окремий конфігураційний файл чи група пов’язаних між собою конфігурацій, є базовими параметрами, які визначають, як управляється апаратне забезпечення, програмне забезпечення і навіть цілі мережі в організації.

Наприклад, файл конфігурації мережевого екрану міститиме основні атрибути, які пристрій використовує для управління трафіком від і до мережі організації, зокрема списки блокування, перенаправлення портів, віртуальні локальні мережі та інформація щодо віртуальної приватної мережі (VPN).

Управління налаштуваннями є невід'ємною частиною загального управління активами організації. Налаштування є основним елементом для забезпечення того, щоб активи компанії, такі як мережа, робочі станції чи інформаційні системи не лише працювали належно, а й були захищені від несанкціонованих чи некоректних змін з боку технічного персоналу та/або постачальників [10].

Рекомендації щодо безпечного управління налаштуваннями мають різні інтерпретації в різноманітних фреймворках інформаційної безпеки, таких як SOC2, HIPAA, PCI DSS, CIS Critical Security Controls та інших [11].

Таблиця ілюструє мапінг (взаємну відповідність) між контролями CIS Critical Security Controls (CIS Controls) та ISO/IEC 27001:2022 щодо безпечного управління налаштуваннями [12].

Мапінг між контролями CIS Controls та ISO/IEC 27001:2022 щодо безпечного управління налаштуваннями

Ідентифікатор CIS Control	Назва контролю	Опис контролю	Ідентифікатор ISO 27001	Назва контролю
1	2	3	4	5
4.1	Встановіть та підтримуйте процес безпечного налаштування	Встановіть та підтримуйте процес безпечного налаштування корпоративних активів (пристроїв кінцевих користувачів, зокрема портативних і мобільних, некомп'ютерних пристроїв/пристроїв Інтернету речей і серверів) і програмного забезпечення (операційних систем і програм). Переглядайте та оновлюйте документацію щороку або коли відбуваються значні зміни на підприємстві, які можуть вплинути на цей контроль	A8.9	Управління налаштуваннями
4.2	Встановіть та підтримуйте процес безпечного налаштування мережевої інфраструктури	Встановіть та підтримуйте процес безпечного налаштування мережевих пристроїв. Переглядайте та оновлюйте документацію щороку або коли відбуваються значні зміни на підприємстві, які можуть вплинути на цей контроль		
4.3	Налаштуйте автоматичне блокування сесії на корпоративних активах	Налаштуйте автоматичне блокування сесії на корпоративних активах після певного періоду бездіяльності. Для операційних систем загального призначення період не має перевищувати 15 хвилин. Для мобільних пристроїв кінцевих користувачів період не має перевищувати 2 хвилини	A8.9	Управління налаштуваннями

Продовження таблиці

1	2	3	4	5
4.7	Управляйте обліковими записами за замовчуванням на корпоративних активах і програмному забезпеченні	Управляйте обліковими записами за замовчуванням на корпоративних активах і програмному забезпеченні, таких як облікові записи root, адміністратора та інших попередньо налаштованих облікових записах постачальників. Приклади реалізацій можуть містити: вимкнення облікових записів за замовчуванням або налаштування їх невикористовуваними	A8.9	Управління налаштуваннями
4.8	Видаляйте або вимикайте непотрібні/зайві сервіси на корпоративних активах і програмному забезпеченні	Видаляйте або вимикайте непотрібні/зайві сервіси на корпоративних активах і програмному забезпеченні, наприклад невикористовувані служби обміну файлами, модулі вебдодатків або службові функції	A8.9	Управління налаштуваннями

Отже, важливо створити та впровадити політики управління налаштуваннями для забезпечення належного контролю як над новим обладнанням і системами, так і над тими, які вже використовують в організації. Внутрішні механізми контролю мають охоплювати всі елементи, які критичні для бізнесу, зокрема, налаштування безпеки, апаратне забезпечення з файлами конфігурації та відповідні програмні додатки чи системи.

Крім того, під час впровадження політики конфігурацій треба розглядати всі релевантні ролі та відповідальності, зокрема делеговане володіння конфігураціями для окремих пристроїв чи застосунків.

Де можливо, організації мають використовувати стандартизовані шаблони для налаштування всього обладнання, програмного забезпечення та систем. Ці шаблони мають:

1) за змогою використовувати загальнодоступні, визначені специфічним підрядником, та/або відкриті джерела для забезпечення оптимальної конфігурації апаратного та програмного забезпечення;

2) відповідати мінімальним вимогам безпеки для пристрою, застосунку чи системи, до яких вони застосовуються;

3) гармонізуватися із зусиллями організації в галузі інформаційної безпеки, також всі відповідні контролі стандарту ISO;

4) враховувати унікальні бізнес-вимоги організації, зокрема щодо конфігурацій безпеки, і визначати, наскільки реально застосовувати або управляти шаблоном в будь-який конкретний момент;

5) переглядатися з відповідними інтервалами для врахування оновлень системи або апаратного забезпечення та актуальних загроз безпеці [10].

3.3 . Використання CIS Бенчмарків для забезпечення ефективного і безпечного управління налаштуваннями

Коли мовиться про захист і безпеку активів, одним з найбільш поширених і надійних способів забезпечити захист активів організації і впровадити найкращі галузеві практики є використання конфігураційних стандартів від Центру інтернет-безпеки (CIS – Center for Internet Security), відомі як CIS Бенчмарк.

Стандарти CIS Бенчмарк є набором глобально визнаних та консенсус-орієнтованих найкращих практик, які допомагають спеціалістам з інформаційної безпеки реалізувати та управляти захистом від кіберзагроз. Розроблені спільнотою світових експертів з безпеки, ці рекомендації допомагають організаціям протидіяти ризикам, що активно виникають у цифровому світі. Компанії впроваджують стандарти CIS Бенчмарк, щоб уникнути вразливостей, що виникають внаслідок неправильного налаштування систем і активів.

Інструменти, такі як Стандарти CIS Бенчмарк, є важливими, оскільки вони дають рекомендації щодо найкращих практик у сфері безпеки, розроблені фахівцями з безпеки та експертами з предметної галузі, для розгортання понад 25 різних продуктів від різних виробників. Ці найкращі практики є доброю основою для створення плану розгортання нового продукту чи послуги або для перевірки того, чи є наявні розгортання безпечними [13].

Ці стандарти створюються спільними зусиллями фахівців із безпеки з урахуванням найбільш актуальних загроз і ризиків для інформаційної безпеки. Вони надають конкретні поради щодо конфігурації систем, зокрема налаштування безпеки, вимоги до паролів, керування доступом та інші аспекти, які допомагають зменшити ризики вразливості системи перед потенційними атаками.

Застосування CIS Бенчмарк допомагає організаціям забезпечити належний рівень безпеки своїх інформаційних систем, відповідаючи вимогам стандартів безпеки та регулятивних вимог.

Незважаючи на те, що CIS Бенчмарк багато вважає галузевим стандартом для зміцнення (hardening) систем, дослідження свідчать, що більша частина організацій не в змозі забезпечити виконання понад 50 % перевірок на відповідність, викладених у CIS Бенчмарк. Більше половини цих невідповідностей визначені як невідповідності високого (high-severity) рівня критичності. Водночас безпечне налаштування систем є обов'язковою вимогою в багатьох стандартах і нормативних актах, що підкреслює важливість впровадження суворих заходів безпеки. CIS Бенчмарк пропонує детальний набір інструкцій, які забезпечують високий ступінь охоплення. Однак саме через їх деталізованість, організації можуть сприймати дотримання цих контрольних показників як обтяжливе і складне завдання.

CIS Бенчмарк охоплює перелік рекомендованих політик з безпечного налаштування (hardening) різноманітних активів, додатків і операційних систем. Кожна платформа має специфічні правила для кожної версії, що робить CIS Бенчмарк найбільш низькорівневим і деталізованим фреймворком із забезпечення захисту систем. Вони містять докладні рекомендації щодо конфігурації системи, параметрів безпеки та інших заходів, які можуть допомогти організаціям захистити свою IT-інфраструктуру від широкого спектру кіберзагроз. Бенчмарки охоплюють різноманітні платформи та технології, такі як операційні системи, хмарні середовища, бази даних, веббраузери та мобільні пристрої. Водночас вони регулярно переглядаються і оновлюються, щоб запобігати новим вразливостям та загрозам.

CIS Бенчмарки розробляються за допомогою унікального процесу, заснованого на консенсусі, який очолює група IT-експертів і фахівців з кібербезпеки, а також галузевих експертів з усього світу, кожен з яких постійно визначає, удосконалює та валідує найкращі практики безпеки в межах своєї сфери знань. Загалом понад 12 000 професіоналів з CIS Benchmark Communities [14] співпрацюють над кожним Бенчмарком.

3.4 Класифікація CIS Бенчмарків

Більша частина CIS Бенчмарків містить декілька конфігураційних профілів, які описують налаштування, призначені для рекомендацій Бенчмарка. Вони відомі як Рівень 1, Рівень 2 і Профіль STIG, який замінив Рівень 3. Кожна рекомендація в межах конкретного CIS Бенчмарка пов'язана принаймні з одним рівнем.

1. **Профіль CIS Рівень 1** визначає базові вимоги безпеки, які можна запровадити в будь-якій системі з невеликим чи навіть без впливу на продуктивність чи функціональність. Метою Рівня 1 є зменшення поверхні атаки (attack surface), даючи змогу активам залишатися в робочому стані та не перешкоджати функціональності бізнесу.
2. **Профіль CIS Рівень 2** визначає суворіші параметри безпеки та вважається "поглибленим захистом" ("defense in depth") і призначений для середовищ, де безпека має першочергове значення. Рекомендації, пов'язані з Рівнем 2, можуть спричинити зниження функціональності системи та мати негативні наслідки, якщо їх не впровадити належно.
3. **Профіль STIG** (заміна Рівня 3) рекомендує конфігурації безпеки, специфічні для Security Technical Implementation Guides (STIG). Перекриття рекомендацій з інших профілів, тобто Рівня 1 і Рівня 2, часто наявні в цих профілях STIG.

Є **вісім** технологічних **категорій**, також відомих як Список CIS Benchmarks [15], на які можна розділити Бенчмарки:

1. **Бенчмарки операційних систем.** Бенчмарки операційної системи містять інструкції щодо безпечного налаштування різноманітних операційних систем. Вони охоплюють широкий спектр налаштувань, пов'язаних із безпекою, а також керування доступом, установку драйверів і налаштування браузера.
2. **Бенчмарки програмного забезпечення серверів.** Бенчмарки програмного забезпечення серверів містять базові параметри конфігурації та рекомендації щодо налаштувань серверів, контролів адміністратора сервера, налаштувань зберігання та безпечної конфігурації Microsoft Windows Server, Kubernetes, SQL Server та іншого серверного програмного забезпечення.
3. **Бенчмарки хмарної інфраструктури та хмарних сервісів.** Бенчмарки хмарної інфраструктури та хмарних сервісів містять найкращі практики безпеки та стандарти для хмарних інфраструктур, таких як Amazon Web Services (AWS), Microsoft Azure та Google Cloud Platform. Рекомендації містять найкращі практики щодо налаштувань віртуальної мережі, ідентифікації та керування доступом, журналювання подій, відповідності нормативним вимогам, контролів безпеки тощо.
4. **Бенчмарки мобільних пристроїв.** Бенчмарки мобільних пристроїв містять конфігурації безпеки для операційних систем, які працюють на мобільних телефонах, планшетах та інших портативних пристроях. Передові практики охоплюють налаштування розробника, дозволи програм, налаштування конфіденційності тощо.
5. **Бенчмарки мережевих пристроїв.** Бенчмарки мережевих пристроїв описують, як безпечно налаштувати мережеві пристрої, такі як брандмауери, маршрутизатори, комутатори та віртуальні приватні мережі (VPN). Інструкції надаються як для нейтральних постачальників, так і для конкретних постачальників, щоб гарантувати безпечне налаштування та керування цими мережевими пристроями.
6. **Бенчмарки програмного забезпечення для настільних ПК**. Бенчмарки програмного забезпечення для настільних ПК охоплюють більшу частину програмного забезпечення для настільних ПК, яке зазвичай використовують організації. Інструкції містять найкращі методи керування такими функціями програмного забезпечення настільного комп'ютера, як налаштування браузера, права доступу, облікові записи користувачів, керування мобільними пристроями (MDM) тощо.
7. **Бенчмарки багатофункціональних пристроїв друку.** Бенчмарки багатофункціональних пристроїв друку охоплюють найкращі методи безпечної конфігурації для багатофункціональних принтерів, такі як оновлення програмного забезпечення, доступ до бездротової мережі, налаштування спільного доступу до файлів тощо.
8. **Бенчмарки інструментів DevSecOps.** Бенчмарки інструментів DevSecOps містять нормативні вказівки щодо створення безпечної конфігурації для захисту ланцюжка поставок програмного забезпечення.

3.5 . CIS Бенчмарки і досягнення відповідності нормативним актам

Нині постійно зростає кількість нормативних і регуляторних актів, відповідність яким організації мають впроваджувати і підтримувати. Тож організаціям, які прагнуть відповідати всім вимогам, стає важко орієнтуватися в складному нормативному ландшафті.

CIS Бенчмарки є цінним ресурсом для досягнення цієї відповідності, представляючи найкращі практики, які відповідають основним регуляторним нормам і стандартам. Примітно, що Бенчмарки добре узгоджені з такими фреймворками, як NIST Cybersecurity Framework, PCI DSS, HIPAA та ISO 27001.

На додаток до рекомендацій щодо найкращих методів посилення системи CIS надає CIS Controls і CIS Hardened Images, які є попередньо налаштованими образами безпечно налаштованих систем.

У більшій частині випадків програмне забезпечення, випущене виробником за замовчуванням, насамперед спрямоване на зручність використання, а не на інформаційну безпеку. Отже, без вжиття спеціальних заходів захисту, системи можуть бути досить вразливими до кіберзагроз. Часто зловмисники використовують поверхню атаки організації, проникаючи в мережу організації, поширюючи шкідливе програмне забезпечення та завдаючи великої шкоди. Щоб пом'якшити ці ризики та забезпечити відповідність стандартам IT безпеки і відповідності, дуже важливо дотримуватися CIS Бенчмарків, які містять конкретні параметри налаштувань для захисту систем від потенційних загроз.

Окрім очевидної потреби зменшити площу атаки (attack surfaces) організації, під час прийняття рішення слідувати CIS Бенчмарк треба також враховувати застосовні до організації регуляторні і нормативно-правові акти. Справедливо сказати, що майже всі основні нормативні акти прямо чи опосередковано потребують дотримання CIS Бенчмарк [16].

3.6. Приклад впровадження CIS Бенчмарка

Як описано вище, метою CIS Бенчмарків є допомогти організаціям із завданням посилення безпеки її активів, наприклад, серверів, впровадженням налаштувань безпеки.

Впровадження CIS Бенчмарків, хоч і є досить складним і комплексним завданням, є значним кроком на шляху до створення безпечної інфраструктури організації.

Для прикладу нижче наведено перелік контролів, які треба впровадити для безпечного налаштування сервера:

1) **застосування оновлень безпеки:** регулярне оновлення серверів відповідно до останніх оновлень безпеки для усунення вразливостей і захисту проти відомих загроз і експлойтів (exploits);

2) **впровадження суворого контролю доступу:** застосування надійних механізмів автентифікації, таких як складні паролі або багатофакторна автентифікація, для запобігання несанкціонованому доступу до серверів.

3) **регулярні перегляди рівнів доступів користувачів:** регулярний перегляд прав користувачів сприяє забезпеченню того, що привілеї доступу актуальні та відповідають вимогам організації та найкращим практикам безпеки;

4) **вимкнення непотрібних служб:** вимкнення будь-яких непотрібних служб чи протоколів на серверах, щоб мінімізувати потенційні вектори атак;

5) **використання автоматизованого моніторингу налаштувань:** такий моніторинг дає змогу автоматично перевіряти налаштування серверів і за потреби сигналізувати про відхилення від конфігураційного профілю чи будь-які несанкціоновані зміни (нові порти прослуховування, нові користувачі з правами адміністраторів, зміни в об'єктах групової та локальної політики та нові служби, запущені в системі);

6) **розгортання інструментів керування конфігураціями системи:** такі інструменти автоматично забезпечують прийнятні налаштування системи (на періодичній основі або в режимі реального часу). Використовуючи їх, ви зможете повторно розгортати або контролювати параметри конфігурації в режимі реального часу за розкладом, вручну або на основі подій.

Цілком імовірно, що вам буде потрібно підтримувати різноманітні стандартизовані образи (images) налаштувань безпеки через складність організації та діапазон підтримуваних функцій. Кіль-

кість варіацій цих образів має бути мінімальною, щоб краще розуміти та керувати властивостями безпеки кожного, але організація має мати можливість керувати кількома базовими рівнями.

Зрозуміло, що в процесі виконання такого складного завдання, як налаштування інфраструктури часто можуть виникати труднощі, які ведуть до збоїв у системах. Тому перед впровадженням будь-яких змін у налаштуваннях треба проводити ретельне тестування цих змін у контрольованому тестовому середовищі, і тільки після задовільних результатів тестування впроваджувати зміну на операційному середовищі.

4. Результати дослідження

Внаслідок дослідження встановлено чіткий зв'язок між використанням CIS Бенчмарк і задоволенням вимог стандарту ISO/IEC 27001:2022. Використання CIS Бенчмарк дає змогу організаціям ефективно впроваджувати та вдосконалювати свої системи безпеки інформації, гарантуючи безпечне налаштування активів відповідно до вимог стандарту ISO/IEC 27001:2022. Використання CIS Бенчмарк допомагає зменшити ризики порушення безпеки інформації за допомогою визначення конкретних налаштувань та процедур, які треба застосовувати до активів і систем. Це сприяє підвищенню впевненості зацікавлених сторін у тому, що активи організації належно захищені від потенційних загроз та атак. Такий підхід допомагає забезпечити відповідність найвищим міжнародним стандартам безпеки інформації та збільшує рівень довіри до організації клієнтів, партнерів та інших зацікавлених сторін.

Висновки

Після аналізу та дослідження актуального стану ландшафту кіберзагроз було встановлено, що впровадження визнаних стандартів інформаційної безпеки, таких як ISO/IEC 27001, може ефективно забезпечити захист критичної інфраструктури від нових методів та векторів атак. Також унаслідок дослідження було визначено основні відмінності оновленої редакції стандарту ISO/IEC 27001:2022 порівняно з версією 2013 року.

Особливу увагу присвячено аналізу нового контролю безпеки з Додатку А стандарту ISO/IEC 27001:2022 – А.8.9 – Управління налаштуваннями. Розглянуто основні способи впровадження цього контролю в організації. Визначено, що цей контроль є важливим елементом для надання безпеки організацій, що підтверджується численними інтерпретаціями вимог контролю безпеки в інших популярних фреймворках інформаційної безпеки.

Додатково було запропоновано використання конфігураційних стандартів від Центру інтернет-безпеки (CIS) як ефективного способу захисту активів організації та впровадження найкращих галузевих практик безпеки. Цей підхід дає змогу забезпечити вимоги стандарту ISO/IEC 27001:2022, зокрема пункту А.8.9 – Управління налаштуваннями.

Ввнаслідок дослідження встановлено чіткий зв'язок між використанням CIS Бенчмарк і задоволенням вимог стандарту ISO/IEC 27001:2022. Наведено класифікацію шаблонів CIS Бенчмарк та описано основні моменти їх впровадження на прикладі серверної інфраструктури, що демонструє їхню практичну придатність та ефективність у гарантуванні безпеки IT-інфраструктури організацій.

Список літератури

1. (2022) ISO/IEC 27001: Information security, cybersecurity and privacy protection – Information security management systems – Requirements. URL: https://www.iso.org/standard/82875.html (Accessed: 15 March 2024).

2. (2013) ISO/IEC 27001: Information Technology – Security Techniques – Information Security Management Systems – Requirements. URL: https://www.iso.org/standard/54534.html (Accessed: 15 March 2024).

3. Susukailo V., Opirsky I., Yaremko O. (2022). Methodology of ISMS Establishment Against Modern Cybersecurity Threats. In: Klymash M., Beshley M., Luntovskyy A. (eds.) Future Intent-Based Networking. Lecture Notes in Electrical Engineering, vol. 831. Springer, Cham. DOI: 10.1007/978-3-030-92435-5_15

4. Kurii Y., Opirskyy I. (2021). Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001:2013. Paper presented at the CEUR Workshop Proceedings, 3288, 21–32.

5. (2022) ISO/IEC 27002: Information security, cybersecurity and privacy protection – Information security controls. URL: https://www.iso.org/standard/75652.html (Accessed: 15 March 2024).

6. Alrehili Afnan A., Alhazmi Omar. (2024). ISO/IEC 27001 Standard: Analytical and Comparative Overview. In: Advances in Data-Driven Computing and Intelligent Systems. DOI: 10.1007/978-981-99-9524-0_12

7. Which ISO standards are the most popular – Analysis of ISO 2019 survey. [Електронний ресурс]. Resource Access Mode: https://advisera.com/articles/which-iso-standards-are-the-most-popular-analysis-of-iso-2019-survey/ (Accessed: 15 March 2024).

8. Kurii Y., Opirskyy I., Bortnik L. ISO/IEC 27001:2022 – Analysis of Changes and Compliance Features of The New Version Of The Standard // Materials of IXth International Scientific and Technical Conference Information Protection and Information Systems Security, May 25–26, 2023. Lviv, Ukraine, pp. 15–17, ISBN 978- 966-941-829-6 Resource Access Mode: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/37567/127406.pdf?sequence=2&isAllowed=y (Accessed: 16 March 2024).

9. What Are The ISO 27001 Changes In 2022. [Електронний ресурс]. Resource Access Mode: https://bestpractice.biz/what-are-the-iso-27001-changes-in-2022/ (Accessed: 15 March 2024).

10. ISO 27002:2022, Control 8.9 – Configuration Management. [Електронний ресурс]. Resource Access Mode: https://www.isms.online/iso-27002/control-8-9-configuration-management/ (Accessed: 15 March 2024).

11. CIS Critical Security Controls Version 8 [Електронний ресурс]. Resource Access Mode: https://www.cisecurity.org/controls/v8 (Accessed: 15 March 2024).

12. CIS Controls v8 Mapping to ISO/IEC 27001:2022. [Електронний ресурс]. Resource Access Mode: https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mapping-to-iso-iec-27001-2022 (Accessed: 15 March 2024).

13. What are CIS Benchmarks? [Електронний ресурс]. Resource Access Mode: https://aws.amazon.com/what-is/cis-benchmarks/#:~:text=CIS%20Benchmarks%20from%20the%20Center,and%20manage%20their%20cybersecurity%20defenses (Accessed: 15 March 2024).

14. CIS Benchmarks Community [Електронний ресурс]. Resource Access Mode: https://www.cisecurity.org/communities/benchmarks (Accessed: 15 March 2024).

15. CIS Benchmarks List [Електронний ресурс]. Resource Access Mode: https://www.cisecurity.org/cis-benchmarks (Accessed: 15 March 2024).

16. What is CIS Compliance?(and How to Apply CIS Benchmarks) [Електронний ресурс]. Resource Access Mode: https://www.algosec.com/resources/cis-compliance/ (Accessed: 15 March 2024).

OVERVIEW OF THE CIS BENCHMARKS USAGE FOR FULFILLING THE REQUIREMENTS FROM INTERNATIONAL STANDARD ISO/IEC 27001:2022

Y. Kurii, I. Opirskyy

Lviv Polytechnic National University,
Information Security Department

The problem of developing new methods and vectors of attacks on critical infrastructure and responding to emerging threats through the implementation of recognized standards in the field of information security, such as ISO 27001, was considered. The updated edition of the international standard ISO/IEC 27001 of 2022 and, in particular, the main changes in the structure of controls were analyzed. A detailed analysis of the new security control from Appendix A – A.8.9 – Configuration Management and possible ways of its effective implementation in organizations were carried out.

The use of configuration standards CIS Benchmark from the Center for Internet Security (CIS) is proposed as an effective way to ensure the protection of the organization's assets and the implementation of the best industry security practices.

As a result of the conducted analysis and research, a clear connection and dependence between the use of the CIS Benchmark and compliance with the requirements of clause A.8.9 – Configuration Management of the ISO/IEC 27001:2022 standard was revealed. The classification of CIS Benchmark is presented and the list of key implementation points is described using the example of server infrastructure.

Keywords: information security, cybersecurity, information security framework, cybersecurity framework, ISO 27001, Center for Internet Security, critical infrastructure, information asset, configuration management, CIS Benchmark.