© Horlichenko S. Methods of information security risk management: ISO/IEC 27001 and CIS Critical Secu-rity Controls // Ukrainian Scientific Journal of Information Security, 2024, vol. 30, issue 1, pp. 190-196. ©

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ/ INFORMATION SECURITY MANAGEMENT

DOI: 10.18372/2225-5036.30.18620

МЕТОДИ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: СТАНДАРТ ISO/IEC 27001 ТА CIS CRITICAL SECURITY CONTROLS

Сергій Горліченко

Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського"

ГОРЛІЧЕНКО Сергій Олександрович
Рік та місце народження: 1989 рік, м. Херсон, Україна.
Освіта: Військовий інститут телекомунікацій та інформатизації Національного технічного університету України Київський Політехнічний Інститут, 2011 рік.
Посада: науковий співробітник з 2019 року.
Наукові інтереси: інформаційна безпека.
Публікації: понад 15 друкованих публікацій, серед яких наукові статті, тези та матеріали доповідей на конференціях.
E-mail: serhii.horlichenko@gmail.com.
Orcid ID: 0000-0002-8999-7526.

Анотація. *Методи управління ризиками інформаційної безпеки, що ґрунтуються на двох стандартах – ISO/IEC 27001 та CIS Critical Security Controls, є важливою складовою сучасного підходу до забезпечення безпеки інформаційних систем. Аналіз та вивчення цих стандартів у контексті мінімізації ризиків для інформаційної безпеки є ключовим етапом в цифровому середовищі. Під час написання статті застосовано теоретичний метод, зокрема аналіз наукових досліджень та публікацій, що стосуються управління ризиками. Використання зазначеного методологічного підходу дозволило провести порівняльний аналіз стандартів ISO/IEC 27001 та CIS Critical Security Controls. CIS Critical Security Controls визначає 18 ключових контрольних заходів, орієнтованих на ефективний захист інформаційних ресурсів, включаючи моніторинг, захист від кіберзагроз, аутентифікацію та інші аспекти безпеки. ISO/IEC 27001 надає високорівневий фреймворк для управління ризиками, встановлюючи політику безпеки та процеси аудиту. З іншого боку, CIS Security Controls фокусується на конкретних діях та контрольних точках для забезпечення безпеки. Аналізуються переваги та недоліки обох стандартів, демонструючи їхню застосовність у різних контекстах та в умовах сучасних загроз інформаційної безпеки. Розглянуті аспекти допомагають прийняти обґрунтоване рішення щодо вибору стандарту для конкретної організації. Використання цих стандартів дозволяє ефективно управляти ризиками в умовах сучасних загроз і забезпечити надійність інформаційних систем. Широке застосування цих стандартів у комерційних компаніях та державних установах свідчить про їхню універсальність. Стаття розглядає переваги та недоліки обох підходів в контексті зростаючої кількості кіберзагроз і важливості інформаційної безпеки.*

Ключові слова: *управління ризиками, оцінювання ризиків безпеці інформації, реагування на ризик, кібербезпека, інформаційна безпека.*

Постановка проблеми

В сучасних умовах конфлікту між російською федерацією та Україною визначає актуальність вивчення та розвиток стратегій управління ризиками для захисту об'єктів критичної інфраструктури та стратегічних промислових об'єктів. IBM опублікували звіт про вартість витоку даних у 2023 році [1], в якому досліджували 550 витоків із даними. Середня глобальна вартість витоку даних у 2023 році становила 4,45 мільйона доларів США, що на 15% більше ніж за останні 3 роки [1]. Ризики інформаційної безпеки (ІБ) визнаються як одні з найбільш ймовірних та серйозних, рівень захисту об'єктів ІБ залежить від їхньої ефективної управлінської системи. У контексті цих викликів важливо розглядати управління ризиками ІБ як ключову функцію підприємства чи установи.

Створення ефективних систем захисту вимагає обрання засобів, які не тільки забезпечують зниження впливу потенційних ризиків, але і не обтяжують підприємство великими витратами на їх впровадження та підтримку. Результатом аналізу ризиків ІБ повинно бути визначення потрібних засобів захисту та рекомендацій з підтримки системи ІБ в робочому

стані. В умовах посилення загроз та зростання кількості реалізованих нападів управління ризиками ІБ стає двоетапним процесом. Перший етап - це ідентифікація та оцінка ризиків ІБ, а другий - ранжування ризиків для розроблення стратегії реагування.

Вибір оптимальних та ефективних методів управління ризиками та їх оцінювання є ключовим завданням, оскільки це визначає успішність заходів забезпечення інформаційної безпеки. Аналіз відомих методів управління ризиками ІБ є важливою передумовою для розробки оптимальних стратегій управління ризиками в умовах сучасних геополітичних викликів та технологічних загроз.

Аналіз останніх досліджень та публікацій

Методи управління ризиками інформаційної безпеки досліджувалися в працях вітчизняних та закордонних науковців, таких як П. Складанний, В. Носов, С. Прокопченко, L. Johnson та ін.

У [5] детально описано ключові кроки при організації аудиту інформаційної безпеки в межах аудиту бізнесу, що представляється як сучасна концепція аудиту в цілому. Виділено особливості кожного етапу та надано конкретні рекомендації щодо їх впровадження.

Коллектив авторів [6] подав конкретний досвід оцінювання ризиків інформаційної безпеки в різноманітних організаціях, як комерційних, так і некомерційних. Вони розкривають використання набутих знань, зокрема у контексті державних установ, і пропонують вдосконалений підхід до процесу оцінювання ризиків. Зробили вдосконалення підходу, спрямованого на спрощення процесу оцінки ризиків для фахівця та отримання порівняльного та остаточного результату визначення ризиків інформаційної безпеки, використовуючи базові методики та враховуючи вимоги міжнародних стандартів.

У своєму дослідженні Носов В.В. [7] розглядає можливість впровадження класифікації інформації, включаючи технологічну інформацію, з відповідними мітками, в ресурси системи управління інформаційною безпекою. Це спрямовано на посилення адміністративної відповідальності користувачів інформаційно-комунікаційних систем в організації.

Прокопченко С.В. [8] досліджує можливості залагодження заходів з верифікації та стандартні методи проведення верифікації, приділяючи увагу процесам акредитації відповідно до вимог ДСТУ ISO/IEC 17025: 2017, ДСТУ ISO/IEC 17024:2012, ДСТУ EN ISO/IEC 17021-1:2015, а також сертифікації продукції оборонного призначення, послуг і персоналу в Службі безпеки України. Для цього використовуються стандарти, такі як ДСТУ ISO/IEC 27001:2015 "Методи захисту системи управління інформаційною безпекою" та ДСТУ STANAG 4107:2018 "Вимоги НАТО щодо проектування, розроблення та виготовлення". Пропонується механізм впровадження міжнародних стандартів та стандартів НАТО в Україні.

Робота [9] присвячена ключовим аспектам технологічного ланцюга, спрямованого на оцінку та усунення ризиків. Вона включає перегляд етапів, які описують процес виявлення вразливостей в компанії чи організації. Також розглядається отримання детального аналізу та впровадження контрольних заходів відповідно до найкращих практик з безпеки та сучасних фреймворків.

Група науковців [10] провела докладний аналіз вразливостей та атак, спрямованих на інформаційні ресурси державного рівня, які використовуються в інформаційно-комунікаційних системах. Метою було визначення набору параметрів для оцінки рівня захищеності цих інформаційних ресурсів.

Мета та постановка завдання

Метою статті є здійснення ретельного аналізу методів управління ризиками, зокрема стандарт ISO/IEC 27001 та CIS Critical Security Controls, з метою їхнього оптимального використання для мінімізації впливу ризиків на інформаційну безпеку підприємства, організації чи установ

Організації повинні стратегічно визначати пріоритети використання ресурсів для ефективного захисту від кібератак, з метою мінімізації потенційних ризиків для своїх мереж. Системи кібербезпеки відіграють ключову роль у визначенні пріоритетів, надаючи чіткі рекомендації щодо конкретних методів, програмного забезпечення та систем, необхідних для реалізації конкретних засобів контролю.

Відзначено, що зараз керівники з безпеки та корпоративні менеджери повинні приділяти особливу увагу виконанню вимог і ефективному управлінню ризиками, безпекою та використанням інформації у своїх системах [2].

Це стає особливо актуальним для закладів, які проводячи свою діяльність, повинні дотримуватися строгих мандатів щодо захисту від кібератак, в іншому випадку їм загрожує втрата критичної інформації, фінансування, своєї репутації та довіри. Зазначається, що ця необхідність стає важливою частиною відповідальності для установ, які працюють у високотехнологічних та інноваційних галузях, де зберігаються великі обсяги чутливої інформації.

Виклад основного матеріалу дослідження

Оцінка ризиків є ключовим, а водночас найбільш складним етапом створення систем управління інформаційною безпекою. Це випливає, насамперед, з того, що існує широкий спектр методик, таких як Austrian IT Security Handbook, AS/NZS 4360, BSI 100-3, CRISAM, EBIOS, HB 167, ISF IRAM, ISO 27005, ISO 31000, ISO 31100, ISO 31010, MAGERIT, MARION, MEHARI, COBIT, MSF NIST SP 800 – 39, NIST SP 800 – 37, NIST SP 80 – 30, OCTAVE, OSSTMM RAV, SOMAP. Втім, в підходах до оцінювання ризиків інформаційної безпеки між ними відсутні значущі відмінності. Тому для наших досліджень ми виберемо найбільш актуальну на даний момент методику.

Стандарт ISO/IEC 27001 [14] з початку 1995 року, як був заснований, безперервно вдосконалюється та адаптується до сучасних викликів. Навіть з введенням останнього оновлення у жовтні 2022 року його основа лишається на трьох основних принципах (рис.1):

- конфіденційність передбачає, що лише особи з належними повноваженнями мають можливість отримувати доступ до інформації;
- цілісність означає, що право на зміну інформації мають лише ті, хто має відповідні повноваження;
- доступність гарантує, що інформація доступна уповноваженим особам в необхідний момент.

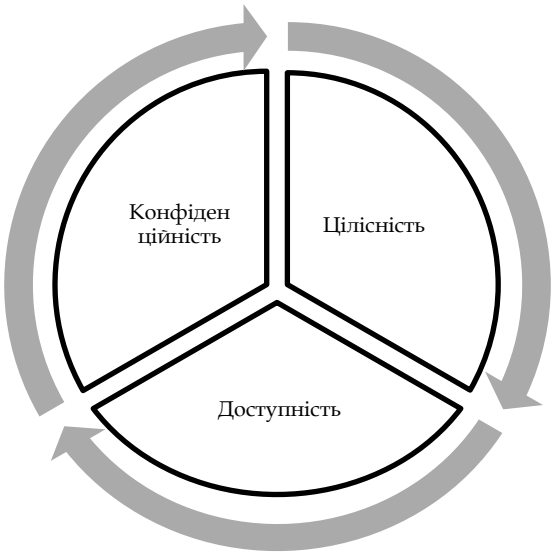

Рис. 1. Головні принципи стандарту ISO/IEC 27001

Засоби контролю в рамках стандарту ISO/IEC 27001 [14] представляють собою методи, спрямовані на зниження ризиків до прийнятного рівня. У додатку А до останньої редакції стандарту (2022 рік) перераховано 93 таких засоби, які можна розділити на чотири секції:

1. Організаційний контроль. Цей вид контролю реалізується шляхом визначення правил, які має дотримуватися персонал, а також очікуваної поведінки користувачів, обладнання, програмного забезпечення та систем;

2. Контроль людей. Застосовується шляхом надання особам необхідних знань, освіти, навичок або досвіду, щоб вони могли безпечно виконувати свої обов'язки;

3. Фізичні засоби контролю. Вони реалізуються через використання обладнання або пристроїв, які фізично взаємодіють з людьми та об'єктами;

4. Технологічні засоби контролю. Такі засоби впроваджуються в інформаційних системах за допомогою програмних, апаратних і мікропрограмних компонентів, які додаються до системи.

Також, стандарт ISO/IEC 27001 [16] рекомендує, щоб при розробці Системи Управління Інформаційною Безпекою (СУІБ) були виконані наступні завдання:

1. Визначити підхід організації до оцінки ризиків і обрати або розробити власний метод;

2. Здійснити аналіз та оцінку ризиків, включаючи оцінку ймовірності виникнення порушень безпеки в контексті домінуючих загроз, та провести кількісну оцінку ризиків.

Перш за все, акцентуємо увагу на двох важливих аспектах, які характерні для другого завдання. В першу чергу, це одночасне використання трьох термінів: "Assessment", "Estimation", "Evaluation". Таким чином, при їх перекладі українською мовою слід належним чином ураховувати використання дієслова "оцінити", іменника "оцінка", а також відповідних дієслівних іменників "оцінювання" та "оцінення". Щоб уникнути цього, ми можемо побудувати модель сутності "Assessment". Використання цієї моделі дозволить подолати когнітивний дисонанс, пов'язаний із наявністю неоднозначностей у розумінні англомовних термінів "Risk Assessment", "Risk Estimation" та "Risk Evaluation" українською мовою (рис. 2).

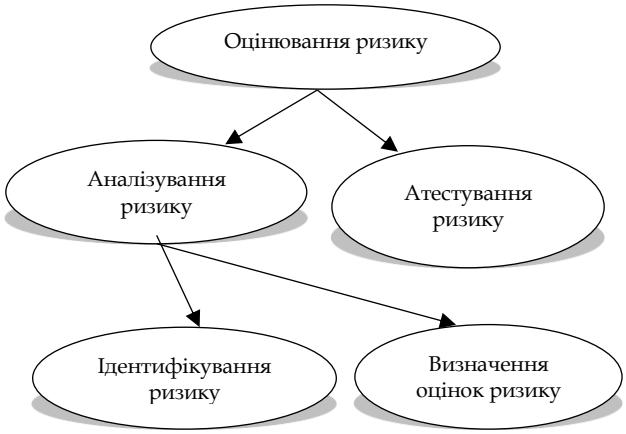

Рис. 2. Модель сутності "Risk Assessment"

Вдруге, можна відзначити, що при визначенні ризикових оцінок у стандарті ISO/IEC 27001 акцент зроблено на визначенні переважаючих загроз.

При цьому організація вільна обирати свій підхід до оцінювання ризику, тобто використовувати будь-який метод для визначення якісних або кількісних оцінок. Важливо щоб обраний метод в організації мав обґрунтовану довіру і його результати відповідали наступним вимогам [16]:

1. Порівнюваність ("Comparability") визначає можливість порівняти оцінки ризику з іншими результатами їх визначення, встановлюючи ступінь відмінності між ними;

2. Відтворюваність ("Reproducibility") характеризує ступінь близькості результатів визначення кількісних оцінок ризику, отриманих різними оцінювачами при використанні одного й того ж методу для однакових початкових даних.

Для ефективного функціонування систем управління інформаційною безпекою необхідно забезпечити безпеку державних інформаційних ресурсів шляхом вибору та впровадження заходів оброблення ризиків на основі порівнюваних і відтворюваних оцінок.

Тим часом, при використанні методів визначення якісних оцінок ризику, виконання цих вимог ускладнюється, передусім, через неможливість порівнювання отриманих результатів. Це пов'язано з тим, що вони, в основному, виражаються в балах ("1", "2", "3") або словесно ("низький", "середній", "високий"). В цьому випадку можливе лише їх ранжування без визначення ступеня відмінності між ними, і складність відтворюваності якісних оцінок пов'язана з їх суб'єктивністю, тобто залежністю від суджень експертів. Ці обмеження менш помітні для методів визначення кількісних оцінок ризику, але на практиці їх важко отримати через недостатній обсяг статистик втрат внаслідок реалізації загроз. Кожен негативний прояв ризику в сфері безпеки має бути оброблений для унеможливлення його повторення в майбутньому. Отже, системи управління інформаційною безпекою пості-

йно розвиваються, що ускладнює виконання умов стаціонарності спостережень для накопичення статистик втрат внаслідок реалізації загроз. Визначення кількісних оцінок ризику здійснюється в умовах невизначеності, обумовленої недостатнім обсягом статистик втрат.

У той же час, для визначення кількісних оцінок ризику в умовах невизначеності можна скористатися експертними методами. Однак їх характерним обмеженням є ускладненість отримання відтворюваних результатів через їх суб'єктивність, а також викликані проблеми відбору експертів, формування їх груп, збирання, обробка та аналіз експертних оцінок.

CIS Critical Security Controls представляють собою компіляцію практичних порад та рекомендацій у галузі комп'ютерної безпеки. Ініційована Інститутом SANS у 2008 році в США, цю ініціативу було передано до Ради з кібербезпеки США у 2013 році та потім до Центру Інтернет-безпеки (CIS) у 2015 році. Початково відомий як Рекомендації з аудиту ІБ та SANS Critical Security Controls, цей фреймворк надає комплексні настанови для забезпечення кібербезпеки.

CIS є некомерційною організацією, яка зосереджена на підвищенні рівня готовності та реагування на кібернетичні загрози в області державного та приватного секторів [3]. Критичні елементи управління безпекою CIS виступають як фундаментальна основа для допомоги організаціям в удосконаленні їхніх стратегій інформаційної безпеки. Експерти з різних організацій, які об'єднали свій значний досвід у сфері захисту від реальних кібератак, спільно розробили консенсусний перелік елементів управління. Цей перелік втілює найкращі практики у сфері захисту, спрямовані на запобігання або виявлення кібератак [4].

Такий підхід дозволяє забезпечити ефективний захист, враховуючи реальний досвід та консолідацію експертної ерудиції для створення надійних засобів захисту від кіберзагроз.

Контролі є "пріоритетним, чітко спрямованим набором заходів, які мають підтримку спільноти, забезпечуючи їх реалістичність, використовуваність, масштабованість та відповідність всім вимогам безпеки галузі або урядових вимог" [4]. Каркас CIS Control розроблено для того, щоб вказати організації ключові області, на які вона повинна спрямувати свої зусилля. Кожен Контроль пропонує конкретні технології, які можна впроваджувати для досягнення основної мети - зменшення ризиків. Оскільки немає жодного важливого заходу, що гарантує запобігання інцидентам кібербезпеки, рекомендується впроваджувати всі Контролі, створюючи стратегію всебічного захисту.

На сьогодні є актуальною версія CIS Controls v8, яка об’єднує та консолідує 18 Контролів з кібербезпеки (рис. 3) [4].

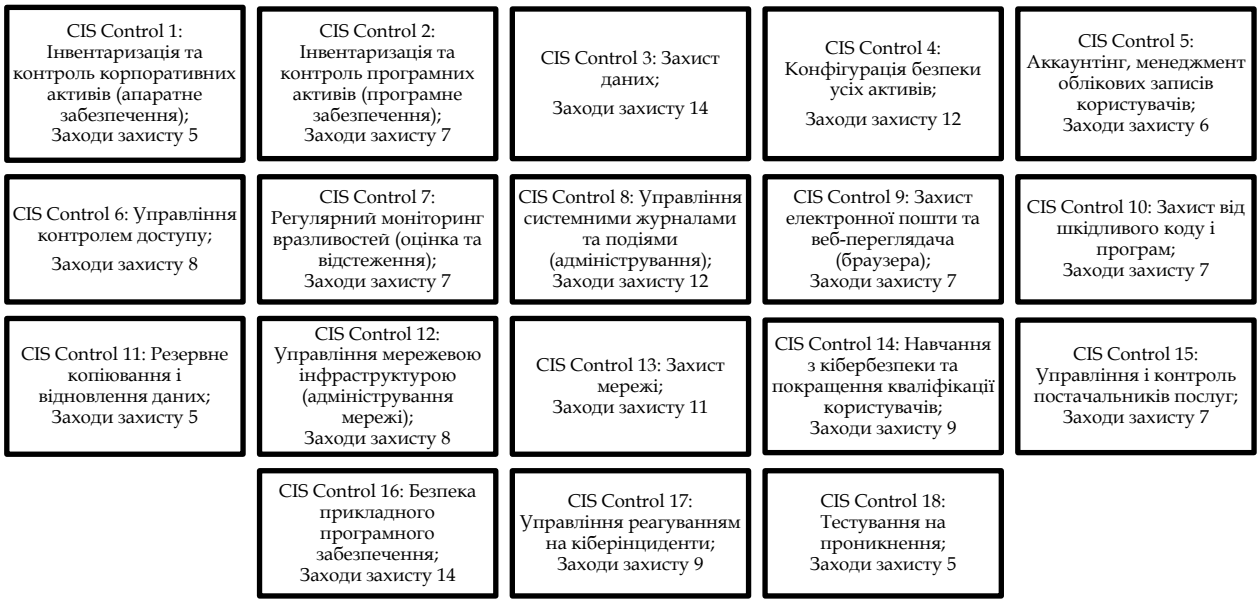

Рис. 3. CIS Security Controls v8

Також CIS Security Controls вводить Групи впровадження (IG - Implementation Groups) які є рекомендованим інструментом для визначення пріоритетності впровадження засобів контролю системи безпеки мережі (СБМ). З метою надання допомоги підприємствам різних розмірів, IG розділяються на три категорії, що грунтуються на профілі ризику та наявних ресурсах для впровадження засобів контролю СБМ. Кожна IG визначає конкретний набір заходів безпеки (раніше відомих як підконтрольні CIS), які необхідно впроваджувати.

В CIS Controls v8 налічується 153 заходи безпеки. Початковим етапом для будь-якого підприємства є IG1, який представляє собою "основну кібергігієну" - базовий набір заходів захисту від кіберзагроз, які слід застосовувати для захисту від найпоширеніших атак. IG2 будується на основі IG1, а IG3 включає всі аспекти управління та заходи безпеки [9].

CIS Control v8 — це комплексна версія v7, яка містить захисні оновлення для покращення безпеки даних і зниження ризиків злому. Деякі зміни включають:

– контроль керування постачальником послуг: новий засіб керування, який вирішує конфіденційність даних на платформах SaaS, включаючи їх зберігання та обробку;

– переміщення Контролю захисту даних з 13 місця на 3 і додавання п'яти нових заходів безпеки до цього контролю. Ці п'ять нових заходів захисту зосереджені на управлінні та ідентифікації даних із більш безпечним підходом для мінімізації вразливостей.

З офіційних змін у Контролях, що показані нижче (табл. 1), ми бачимо інші зміни які стосуються елементів керування, таких як 4, 5, 6, 14 та ін. Таким чином ми бачимо корегування та оптимізацію фокусу захисту безпеки.

Таблиця 1

Відмінності CIS Security Controls v7 від CIS Security Controls v8

Номер Контролю	CIS Security Controls v7	CIS Security Controls v8
1	Інвентаризація авторизованих і неавторизованих пристроїв	Інвентаризація та контроль корпоративних активів (апаратне забезпечення)
2	Інвентаризація авторизованого і неавторизованого програмного забезпечення	Інвентаризація та контроль програмних активів (програмне забезпечення)
3	Засоби управління вразливостями	Захист даних
4	Використання адміністративних привілеїв	Конфігурація безпеки усіх активів
5	Захищені конфігурації для мобільних пристроїв, ноутбуків, робочих станцій і серверів	Аккаунтінг, менеджмент облікових записів користувачів
6	Обслуговування, моніторинг та аналіз журналів аудиту	Управління контролем доступу
7	Захист електронної пошти та веб-браузера	Регулярний моніторинг вразливостей (оцінка та відстеження)
8	Захист від шкідливих програм	Управління системними журналами та подіями (адміністрування)
9	Обмеження і контроль мережевих портів	Захист електронної пошти та веб-переглядача (браузера)
10	Можливість відновлення даних	Захист від шкідливого коду і програм
11	Захищені конфігурації для мережевих пристроїв (файерволи, роутери, комутатори)	Резервне копіювання і відновлення даних
12	Захист периметра	Управління мережевою інфраструктурою (адміністрування мережі)
13	Захист даних	Захист мережі
14	Контроль доступу	Навчання з кібербезпеки та покращення кваліфікації користувачів
15	Контроль доступу бездротових мереж	Управління і контроль постачальників послуг
16	Контроль облікових записів	Безпека прикладного програмного забезпечення
17	Контроль рівня обізнаності персоналу	Управління реагуванням на кіберінциденти
18	Контроль прикладного програмного забезпечення	Тестування на проникнення
19	Реагування на інциденти	-
20	Тестування на проникнення	-

У цій статті ми приділимо увагу першому Контролю визначеному в CIS Control 1: інвентаризації дозволених та недозволених пристроїв. Підконтроль CIS Control 1.1, який визначає: " створіть і ведіть детальну інвентаризацію активів підприємства" [4], має загальне застосування для мереж Інтернет-протоколу версії 4 (IPv4). Організації можуть проводити сканування свого мережевого адресного простору для ідентифікації хостів і навіть намагатися визначити операційну систему. Деякі інструменти, такі як Nmap та інші, можуть допомагати у цьому [7]. На жаль, сканування мережі Інтернет-протоколу версії 6 (IPv6) є менш простим завдяки великому адресному простору і тривалому часу, необхідному для обходу кожного адреси для відправлення запитів та очікування відповіді [12]. У останні роки пасивне сканування, або прослуховування активних хостів у мережі, стало більш розповсюдженим. Цей метод включає "процес моніторингу мережевого трафіку на рівні пакетів для визначення топології, надання інформації про сервіси та виявлення вразливостей" [13].

CIS Control 1.2, "вести інвентаризацію активів усіх систем, підключених до мережі..." [4], описує всебічне ведення інвентаризації. Здавалося б, це завдання можна вирішити за допомогою додатків на основі бази даних для відстеження цієї інформації. Це поширене в багатьох організаціях, як і електронні таблиці. Однак точність таких ручних процесів зазви-

чай зменшується з часом через значні зусилля, які потрібно витратити на введення та оновлення даних для кожного комп'ютера. Цей метод також не ефективний для мереж з десятками і сотнями тисяч хостів.

CIS Control 1.3, " Використовуйте інструмент активного виявлення, щоб ідентифікувати активи, підключені до мережі підприємства. " [4], фактично є бізнес-процесом. Для відповідності цьому вимоги, організації повинні автоматизувати оновлення інвентаризації, враховуючи нові придбання. Це можна забезпечити шляхом інтеграції програми планування ресурсів підприємства з системою інвентаризації. Для багатьох організацій вручну виконувати такі оновлення стає проблематичним, оскільки це вимагає введення даних у бізнес- та фінансові системи, які є специфічними для IT. У деяких організаціях відбувається важливе розчленування бізнес-операцій від мережевих операцій.

CIS Control 1.4, "Використовуйте протоколювання протоколу динамічної конфігурації хоста (DHCP) для оновлення інвентаризації активів підприємства" [4], є завданням, яке більшість організацій можуть легко впровадити. Просто записуючи події сервера DHCP, ми можемо ефективніше відстежувати пристрої в мережі. Зазвичай це використовується в мережах IPv4; однак, залежно від конфігурації IPv6, може не використовуватися протокол DHCP. Мережі IPv6 можуть використовувати автоконфігурацію адрес без статусу (SLAAC), DHCPv6 або статично призначені адреси [14], [15].

Наприклад, для дослідницьких установ загальним є можливість принести власні пристрої та підключити їх до мережі. Хоча багато корпоративних мереж можуть справлятися з BYOD (Bring Your Own Device). Це означає, що CIS Control 1.3 не застосовується в цьому випадку, оскільки власник пристрою не є власником мережі.

CIS Control 1.5 "Використовуйте інструмент пасивного виявлення для ідентифікації активів…" [4], вимагає впроваджувати процеси для тестування на наявність бездротових точок доступу, а також циклічно виявляти та ідентифікувати всі авторизовані та неавторизовані бездротові точки доступу.

Також це вимагає запровадити процедури реагування на інциденти у випадку виявлення неавторизованих точок бездротового доступу.

CIS Controls виникли як спроба знайти просте рішення, яке вирішило б більшість проблем безпеки для всіх. Початково метою було мати рішення "plug and play", або, в крайньому випадку, "next next finish". Протягом певного часу воно впроваджувалося саме так, навіть не дивлячись на попередження про необхідність знати свою систему перед виконанням будь-яких дій. Однак з часом, із розвитком ідеї наявності готових контролів для впровадження, це стало ще одним інструментом управління ризиками, із супровідним каталогом контролів, з якого можна було обирати, хоча, можливо, трошки обмеженим.

Підкреслимо той факт, що кібербезпека та інформаційна безпека є складними сферами, незалежно від того, наскільки ми намагаємося спростити їх. Це, частково, пов'язано з їхньою сильною залежністю від контексту, що кидає сумнів на можливість існування універсального рішення. Популярність CIS Controls на ринку обумовлена, зокрема, великим впливом CIS і SANS, а їхня просування включає певні маркетингові заяви.

Висновки. Таким чином однією з ключових задач забезпечення безпеки інформаційних ресурсів, є розробка систем управління інформаційною безпекою. Ефективність функціонування таких систем визначається вибором заходів для обробки ризиків, що базуються на порівнюваних та відтворюваних оцінках. Проте реалізація цих вимог ускладнена існуючими методами через виявлені обмеження їхнього використання в умовах невизначеності. Ці обмеження свідчать про наявність протиріччя між потребами практики у підвищенні продуктивності функціонування систем управління інформаційною безпекою, з одного боку, і відсутністю методів для визначення кількісних оцінок ризиків в умовах невизначеності, з іншого. Такий висновок ставить завдання перед нами – розробити методи визначення кількісних оцінок ризиків в умовах невизначеності.

Список літератури

[1]. Cost of a data breach report 2023. IBM. URL: https://www.ibm.com/es-es/reports/data-breach (date of access: 28.01.2024).

[2]. Johnson L. Security controls evaluation, testing, and assessment handbook (second edition). Elsevier Science, 2019. 788 p. URL: https://doi.org/10.1016/C2018-0-03706-8 (date of access: 24.01.2024).

[3]. About us. CIS The Center for Internet Security. URL: https://www.cisecurity.org/about-us (date of access: 24.01.2024).

[4]. CIS critical security controls. CIS The Center for Internet Security. URL: https: // www.cisecurity.org/ controls (date of access: 24.01.2024).

[5]. Рой Я. В., Мазур Н. П., Складанний П. М. Аудит інформаційної безпеки – основа ефективного захисту підприємства. Кібербезпека: освіта, наука, техніка. 2018. Т. 1 № 1. С. 86-93. URL: https: // elibrary. kubg. edu.ua/ id/eprint / 25663 / 1 / Я_Рой_Н_Мазур_П_Складанний_ КБ1(1)2018.pdf (дата звернення: 16.01.2024).

[6]. Підхід до оцінювання ризиків інформаційної безпеки для автоматизованої системи класу "1" / І. С. Літвінчук та ін. Кібербезпека: освіта, наука, техніка. 2020. Т. 2, № 10. С. 98–112. URL: https://doi.org/10.28925/2663-4023.2020.10.98112 (дата звернення: 24.01.2024).

[7]. Носов В. В. Деякі аспекти управління ресурсами СУІБ. Протидія кіберзлочинності та торгівлі людьми : зб. матеріалів Міжнар. наук.-практ. конф. (м. Харків, 27 трав. 2022 р.), м. Харків, 27 трав. 2022 р. Харків, 2022. С. 57-58. URL: http://dspace.univd.edu.ua/xmlui/ handle/123456789/13115 (дата звернення: 09.01.2024).

[8]. Прокопченко С. В. Акредитація та сертифікація як типові методи верифікації в Службі безпеки України. Збірник наукових праць Харківського національного університету Повітряних Сил. 2021. № 4(70). С. 114-117. URL: https: // doi.org / 10.30748 / zhups.2021.70.16. (дата звернення: 10.01.2024).

[9]. Таченко І., Коробейнікова Т., Захарченко С. Огляд сучасного стану питання в галузі оцінювання ризиків мережевої безпеки. THEORY AND PRACTICE OF SCIENCE: KEY ASPECTS (November 7-8, 2021) : Scientific Collection «InterConf», Rome, 7–8 November 2021 p. 2021.

С. 417-432. URL: https://doi.org/10.51582/interconf.7-8.11.2021 (дата звернення: 23.01.2024).

[10]. Сальник С.В., Сторчак А.С., Крамський А.Є. Аналіз вразливостей та атак на державні інформаційні ресурси, що обробляються в інформаційно-телекомунікаційних системах. Системи обробки інформації. 2019. № 2(157). С. 121-128. DOI: 10.30748/soi.2019.157.17.

[11]. Information technology. Security techniques. Information security management systems. Requirements [ISO/IEC 27001:2022].

[12]. Chown T. IPv6 implications for network scanning. RFC Editor, 2008. URL: https://doi.org/10.17487/rfc5157 (date of access: 21.01.2024).

[13]. Deraison R., Gula R., Hayton T. Passive vulnerability scanning introduction to nevo. 9th ed. Tenable Network Security Inc., 2003. 13 p. URL: https://markowsky.us/papers/net-papers/gula_passive_scanning_tenable.pdf (date of access: 09.01.2024)

[14]. Dynamic host configuration protocol (dhcpv6). Understanding IPv6. New York. pp. 85-113. URL: https://doi.org/10.1007/0-387-25614-8_7 (date of access: 21.01.2024).

[15]. Thomson S., Narten T., Jinmei T. IPv6 stateless address autoconfiguration. RFC Editor, 2007. 30 p. URL: https: // doi.org / 10.17487 / RFC4862 (date of access: 02.01.2024).

[16]. Information technology. Security techniques. Information security management systems. Requirements [ISO/IEC 27001:2013].

УДК 004.056.53

Horlichenko S. Methods of information security risk management: ISO/IEC 27001 and CIS Critical Security Controls

Abstract. *Information security risk management methods based on two key standards, namely CIS Critical Security Controls and ISO/IEC 27001, are an essential part of a modern approach to ensuring the security of information systems. The analysis and study of these standards in the context of minimizing information security risks are crucial stages in the digital environment. During the writing of the article, a theoretical method was used, specifically the analysis of scientific research and publications related to risk management. The use of this methodological approach allowed a comparative analysis of ISO/IEC 27001 and CIS Critical Security Controls. CIS Critical Security Controls define 18 key control measures for the effective protection of information resources, covering aspects such as monitoring, protection against cyber threats, authentication and other security aspects. ISO/IEC 27001 provides a high-level framework for risk management, establishing security policies and audit procedures. CIS Security Controls, on the other hand, focus on specific actions and control points to ensure security. The pros and cons of both standards are analyzed, demonstrating their applicability in different contexts and in the face of modern information security threats. The use of these standards enables effective risk management under the conditions of modern threats and ensures the reliability of information systems. Their widespread use in commercial enterprises and government institutions demonstrates their universality. This article examines the pros and cons of both approaches. In the context of the increasing number of cyber threats and the importance of information security, both standards prove to be valuable tools, but have their limitations.*

Keywords*: risk management, information security risk assessment, risk response, cybersecurity, information security.*

Горліченко Сергій Олександрович, науковий співробітник Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський Політехнічний Інститут імені Ігоря Сікорського".

Serhii Horlichenko, researcher of the Institute of special communication and information protection of the National technical university of Ukraine "Ihor Sikorsky Kyiv polytechnic institute".

Отримано *18 березня 2024 року*, затверджено редколегією *1 квітня 2024 року*