of security requirements and configurations into software code, which in turn is considered an integral part of the full software development life cycle. By embedding security measures into code, scripts, templates, and automated workflows, an organization ensures that there are well-defined security controls that will be consistently and enforced across all operational phases of software creation (development, testing, implementation, support). This article examines the main problems of building security in cloud environments and their causes, also considers the components and principles of the "Security as code" approach, an implementation example with an explanation, the advantages of this approach, as well as the role of DevSecOps. This article aims to help readers understand the importance of the Security as Code approach as one of the most effective methods for managing security in cloud environments. As cloud environments continue to evolve and proliferate, and threats become more sophisticated, the Security as Code approach represents a core strategy for proactively protecting digital assets. This publication serves as a guide to understanding, implementing, and benefiting from a Security as Code approach, providing insight into the future cloud security landscape and the critical role of automation and integration in addressing today's security challenges. To support the research, an extensive review of literature and articles providing information on the Security as Code approach and its application was conducted.

Keywords: Security as code, Infrastructure as code, DevSecOps, DevOps, Cloud environments, software development cycle, security threats.

Вахула Олександр Петрович, асистент кафедри захисту інформації Національного університету «Львівська політехніка».

Oleksandr Vakhula, assistant at the Department of Information Security, National University "Lviv Polytechnic".
Email: oleksandr.p.vakhula@lpnu.ua.
Orcid ID: 0009-0008-5367-3344.

Опірський Іван Романович, д.т.н., професор, завідувач кафедри захисту інформації Національного університету «Львівська політехніка».

Ivan Opirskyy, Doctor of Technical Sciences, Professor, Head of the Department of Information Security, National University "Lviv Polytechnic".
E-mail: ivan.r.opirskyi@lpnu.ua.
Orcid ID: 0000-0002-8461-8996.

DOI: 10.18372/2410-7840.25.17937
УДК 004.056.53

ВПРОВАДЖЕННЯ НОВИХ ЗАСОБІВ І МЕТОДІВ ПІДВИЩЕННЯ РІВНЯ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Андрій Давидюк

Наявні методи та засоби забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури, розроблені на основі міжнародних стандартів та кращих практик, є досить ефективними в умовах мирного часу, проте не враховують гібридний характер війни, за якого з'являються нові загрози, зокрема такі як фізичне знищення, захоплення противником, відсутність можливості постійного моніторингу та контролю, обмеження в ресурсах захисту та наявному персоналі, проблеми в поставках обладнання для відновлення, перебої в процесах обміну інформацією, потреба у частій зміні умов функціонування, динамічне зростання кількості та якості кібератак тощо, через що їх ефективність значно спадає. З огляду на це виникає потреба у розробці нових та удосконалення існуючих методів та засобів кіберзахисту з метою підвищення рівня кібербезпеки критичної інфраструктури. Від забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури як невід'ємної частини об'єктів критичної інфраструктури залежить безпека населення, виконання бойових завдань військами.

***Ключові слова**: управління вразливостями, SCAP, опис кібератаки на основі шаблону з траєкторією поведінки керованої системи, оцінка ризиків, візуальна аналітика, антифішингова інфраструктура, система обміну знаннями та досвідом.*

ВСТУП

Забезпечення кібербезпеки є важливим завдання, визначеним Указом Президента України Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України», Законом України «Про основні засади забезпечення кібербезпеки України», Законом України «Про критичну інфра-

структуру». Значну роль кібербезпеці відводиться і в Законі України «Про національну безпеку України», що підтверджує залежність захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних кіберзагроз. Наявні методи та засоби забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури (далі – ОКІІ), розроблені на основі міжнародних стандартів та кращих практик, є досить ефективними в умовах мирного часу, проте не враховують гібридний характер війни, за якого з'являються нові загрози, зокрема такі як фізичне знищення, захоплення противником, відсутність можливості постійного моніторингу та контролю, обмеження в ресурсах захисту та наявному персоналі, проблеми в поставках обладнання для відновлення, перебої в процесах обміну інформацією, потреба у частій зміні умов функціонування, динамічне зростання кількості та якості кібератак тощо, через що їх ефективність значно спадає. З огляду на це виникає потреба у розробці нових та удосконалення існуючих методів та засобів кіберзахисту з метою підвищення рівня кібербезпеки критичної інфраструктури.

Актуальність дослідження також зумовлена тим, що під час війни різко збільшилась кількість кібератак на інформаційно-комунікаційні системи (далі – ІКС) ОКІІ, державних установ та приватного сектору. Причиною успішного проведення таких кібератак є наявність вразливостей в ІКС та технологічних мережах ОКІ, розробка нових інструментів для кібератак хактивістами та спецслужбами противника, швидка зміна тактик (методів) кібератак, недостатня кваліфікація фахівців з кіберзахисту, низький рівень кібергігієни співробітників. У рамках існуючої парадигми інформаційної безпеки (забезпечення конфіденційності, цілісності та доступності) захист інформації та кіберзахист повинен включати управління ризиками, менеджмент вразливостей, заходи з кібероборони держави.

ОСНОВНА ЧАСТИНА

Метод автоматизації управління вразливостями на основі технології SCAP

Управління вразливостями є одним з найважливіших процесів забезпечення кібербезпеки ІКС та АСУ ТП, який описаний в [1-3]. Водночас дані підходи лише вказують набори кроків для побудови процесу управління вразливостями, не пояснюючи особливостей їх реалізації в ІКС та АСУ ТП критичної інфраструктури. Як наслідок процес управління вразливостями реалізується несистематично і має досить сумнівну якість його результатів. З огляду на зазначене, доцільним є розробити метод автоматизації управління вразливостей на основі технології SCAP [4].

Отже, для формалізації процесу управління вразливостями опишемо його математично з використанням теорії множин, визначивши як множини набори дій в рамках кожного етапу даного процесу. До таких наборів даних віднесемо набір ідентифікації (I), набір оцінювання (A), набір планування (P), набір впровадження (IM), набір перевірок (V), набір моніторингу (M). Таке математичне представлення забезпечує структуру для ідентифікації, оцінки, планування, реалізації, перевірки та моніторингу вразливостей для забезпечення проактивного та комплексного підходу до кібербезпеки.

Звісно, процес управління вразливостями нерозривно пов'язаний з процесами кібератаки, так як зловмисник безпосередньо використовує наявні в системах вразливості. Таким чином, доцільно є зіставити етапи моделі Cyber Kill Chain [5] з етапами процесу управління вразливостями в контексті вище визначених наборів даних моделі Cyber Kill Chain та процесу управління вразливостями, а саме з такими наборами Розвідувальний набір (R), Набір озброєнь (W), Набір доставки (D), Набір використання (E), Набір інсталяції (I), Набір команд і контролю (C), набору цілей (A). Таким чином можна констатувати, що проблеми з процесом управління вразливостями сприяють кібератакам згідно моделі Cyber Kill Chain.

Враховуючи вищезазначене, можна використати принципи теорії множин для представлення концепцій SCAP в рамках процесу управління вразливостями, а саме такими наборами даних як Набір вразливостей (V), Набір систем (S), Набір політик (P), Набір оцінки вразливості (A), Набір оцінки відповідності (C). Такий підхід передбачає і використання операцій над множинами, таких як перетин, об'єднання, різниця, підмножина. Вико-

ристовуючи ці набори та операції з наборами, стає можливим будувати математичні моделі для представлення зв'язків і взаємодій у SCAP, наприклад, аналізування вразливості, оцінювання вразливості, оцінювання відповідності системи політиці, оцінювання відповідності набору систем набору політик.

З метою математично представлення зв'язків та взаємодії в SCAP, ми можемо визначити наступні математичні моделі:

1. Модель аналізу вразливості.

Розглянемо систему S і вразливість V. Можливо визначити функцію $VA(S,V)$, яка представляє аналіз уразливості системи S проти вразливості V. Результатом цієї функції може бути двійкове значення, яке вказує, чи присутня вразливість у системі. Наприклад, $VA(S,V) = 1$, якщо вразливість V присутня в системі S, і $VA(S,V) = 0$ в іншому випадку;

2. Модель оцінки вразливості.

Розглянемо набір систем S і набір вразливостей V. Ми можемо визначити функцію $VAM(S,V)$, яка представляє оцінку вразливості систем S проти вразливостей V. Цю функцію можна визначити як перетин уразливості функції аналізу для кожної системи та пари вразливостей. Математично ми можемо представити це як (1):

$$VAM(S,V) = \{ (S,V) \mid VA(S,V) = 1 \}. \quad (1)$$

Результатом моделі оцінки вразливості VAM є набір пар (S,V), що вказує, які вразливості присутні в кожній системі;

3. Модель відповідності системи політиці.

Розглянемо систему S і політику P. Ми можемо визначити функцію $PC(S,P)$, яка представляє оцінку відповідності політики системи S щодо політики P. Результатом цієї функції може бути двійкове значення, яке вказує, чи система відповідає політиці чи ні. Наприклад, $PC(S,P) = 1$, якщо система S відповідає політиці P, і $PC(S,P) = 0$ в іншому випадку;

4. Модель оцінки відповідності набору систем набору потітик.

Розглянемо набір систем S і набір політик P. Ми можемо визначити функцію $CEM(S,P)$, яка представляє оцінку відповідності систем S політикам P. Цю функцію можна визначити як перетин функцій відповідностей політик для кожної системи та пари політики. Математично ми можемо представити це як:

$$CEM(S,P) = \{ (S,P) \mid PC(S,P) = 1 \}. \quad (2)$$

Результатом моделі оцінки відповідності $CEM(S,P)$ є набір пар (S,P), що вказує, які системи відповідають кожній політиці. Ці математичні моделі дозволяють аналізувати вразливості, оцінювати відповідність політикам у структурований спосіб. Визначивши функції VA, VAM, PC і CEM, можливо виконувати обчислення та отримувати корисні результати щодо стану безпеки систем і їх відповідності політикам. Ця модель забезпечує концептуальну основу для розуміння та аналізу SCAP з точки зору теорії множин.

На прикладі базової моделі інформаційного процесу управління [6] застосування SCAP може здійснюватися при формуванні інформації про виявлені вразливості (створенні звіту), передачі цієї інформації суб'єкту управління, прийнятті рішення про усунення (мінімізації) вразливостей, здійсненні команди для встановлення виправлення (патча) та реалізації встановлення патча.

З огляду на зазначене пропонується метод автоматизації управління вразливостей на основі технології SCAP, що полягає у виконанні наступних кроків:

1. Встановлення зв'язку з офіційним сайтом NVD [7];

2. Пошук посилань для завантаження потоків даних NVD (NVD data feeds);

3. Завантаження інформаційних потоків NVD data feeds у форматі *.json;

4. Вилучення вмісту *.json;

5. Зчитування даних з CVE_Items;

6. Аналіз даних з CVE_Items для їх використання у процесі менеджменту вразливостей організації.

Для аналізування отриманих даних пропонується математично формалізувати вразливості на основі потоків даних NVD наступним чином:

Нехай множина (3), що має вигляд:

$$C = \{n, t, i, c, w\}, \quad (3)$$

представляє опис деякої вразливості з потоку даних NVD, де n – ідентифікатор програмно-апа-

ратного продукту, що задовольняє специфікації CPE, і представлений у вигляді CPE-URI; t – дата останньої модифікації інформації про програмно-апаратний продукт; i – внутрішній ідентифікатор NVD; c – унікальний ідентифікатор вразливості CVE-ID; w – ідентифікатор опису виду помилки для програмно-апаратного продукту CWE-ID у відповідності до класифікатору Common Weakness Enumeration.

Тоді множина всіх вразливостей потоків даних NVD представляється множиною $I = \{C_i\}$, де $i \in Q$ – індексна множина записів потоків даних NVD в процесі аналізу.

Маючи таке представлення даних, фахівець з кібербезпеки зможе систематизувати дані про вразливості за наявними в нього продуктами, часом появи вразливостей, пріоритетом внесення виправлення. Варто зазначити, що можливість систематизації даних дасть можливість уникнути конфлікту версій і як наслідок некоректної роботи програмного забезпечення в середовищі операційної системи. У випадку адміністрування складних географічно рознесених систем дозволить налагодити спостережність та контроль версій програмного забезпечення. Також розроблено ПЗ для імпорту отриманих даних до платформи MISP (Malware Information Sharing Platform).

Метод опису кібератаки на основі шаблону з вектором кібератаки

Під час гібридної війни кібердомен починає відігравати важливу роль, впливаючи на національну безпеку держави. Відповідно зростає кількість кібератак. Більшість кібератак використовують однакові підходи та технології, мають одне і теж джерело походження. Враховуючи те, що ряд кібератак схожі за своїми властивостями розробляються шаблони кібератак. Проте опис кібератак в таких шаблонах може мати різну ступінь деталізацію і формат даних. З урахуванням критеріїв безпеки АСУ ТП в [7] та моделі інформаційних процесів управління в [6] в рамках опису кібератаки повинна бути включена інформація з різних елементів системи у визначений проміжок часу. Враховуючи гібридний характер загроз під час війни, кібератаки можуть бути комбінованими з фізичним впливом, що також повинно бути описано шаблоном. Враховуючи, що на роботу системи впливають не лише процеси в середині організації, а й інших систем, доцільно розглядати системи, поєднані між собою як єдину комплексну систему. Звісно, порушення функціонування однієї з функцій складової комплексної системи, може і не вплинути на всі елементи, але може порушити їх процеси. З огляду на це виникає питання розроблення шаблону з вектором кібератаки.

З використанням теорії множин такі відносини між системами на рівні їх властивостей можуть бути представлені у вигляді об'єднання, перетину та різниці множин. Для цього визначимо набір властивостей системи А (P_A) і набір властивостей системи В (P_B). Таким чином (4) відображає властивості системи В у поєднанні з можливими пошкодженнями системи А, тобто показує, як на систему В може вплинути пошкодження системи А:

$$P_B \cup P_A. \quad (4)$$

Перетин цих множин відображатиме у (5) властивості, які поділяють як система Б, так і пошкодження системи А. Підкреслюється, на які властивості системи В безпосередньо впливає пошкодження:

$$P_B \cap P_A. \quad (5)$$

Відповідно, різниця цих множин покаже властивості системи В, на які вплив пошкоджень системи А буде відсутнім або незначним.

Враховуючи, що ланцюгу пов'язаних систем впливи залежать від конкретного вузла в ланцюгу, відношення впливів можуть бути один до одного, один до багатьох, багато до одного. З огляду на це шаблон повинен містити інформацію про можливість впливу на інші системи. Це дасть змогу швидко локалізувати кіберінцидент, що виник в конкретній системи, зменшивши ризики для інших. Прикладом таких взаємопов'язаних систем може бути зокрема фінансовий сектор.

Таким чином процедура формування такого шаблону повинна включати такі процеси:

1. Ідентифікація загроз функціонування системи;
2. Ідентифікація ризиків функціонування системи;
3. Ідентифікація властивостей (функцій) системи;

4. Визначення пов'язаних з іншими системами функцій;

5. Визначення вражених кібератакою елементів;

6. Визначення вектору атаки;

7. Визначення можливих наслідків від здійснення кібератаки та/або фізичного ефекту.

Вищевказані процеси варто розглядати в рамках етапів кібератаки, відповідно до моделі «Cyber Kill Chain» [5].

З огляду на вищезазначене, на прикладі взаємодії систем A, B, C вектор кібератаки може бути визначена наступним чином $Q(A \cup B \cup C) \cap H$, де вектором певної атаки є перетин множини Q із множиною H, що являє собою множину елементів систем, які були атаковані.

Тому представимо подібний шаблон (табл. 1). Звісно, такий опис може містити неточності, так як не виключається вплив людського фактору, але водночас дозволяє описати процес кібератаки поза межами системи організації, швидко локалізувати кібератаку і сприяє попередженню можливих кібератак. В залежності від реалізації вектору кібератаки будуть змінюватися стани системи, що матиме такий вигляд $Q(A \cup B \cup C) \cap (H \cup S)$, де S є набором станів елементів системи. Це може забезпечити більш повне розуміння впливу атаки, включаючи як фізичні пошкодження, так і зміни в стані системи в результаті кібератак.

Таблиця 1

Шаблон APT атаки з вектором кібератаки

Системи	Розвідка	Озброєння	Доставка	Експлуатація	Інсталяція	Управління та контроль	Здійснення негативного впливу
Система A	Загрози та ризики, що існують на кожному етапі, з урахуванням властивостей системи, що можуть бути порушені						
$A \cup B$							
Система B	Загрози та ризики, що існують на кожному етапі, з урахуванням властивостей системи, що можуть бути порушені						
$B \cup C$							
Система C	Загрози та ризики, що існують на кожному етапі, з урахуванням властивостей системи, що можуть бути порушені						
H	Набір елементів, що були атаковані на кожному етапі.						
$Q(A \cup B \cup C) \cap H$							
Наслідки	Для кожної системи, з урахуванням траєкторії кібератаки						

Даний шаблон може бути використаний як доповнення до шаблонів кібератак, що описують кібератаки на рівні конкретних елементів ІКС чи АСУ ТП в рамках організації. Водночас до переваг розробленого шаблону можна віднести можливість верхнерівневого аналізу подій. Зокрема, наявна можливість оцінити ризики для інших пов'язаних систем. Оцінка таких ризиків є досить актуальною, так як зловмисники не рідко використовують сторонні системи для отримання чутливих даних на етапі розвідки або використовують їх мережі як довірені для доступу до інших систем в ланцюгу. Яскравим прикладом подібних ситуацій можуть зламані системи сервісів підтримки клієнтів, систем розробників програмного забезпечення з метою підміни оновлень тощо.

Метод управління ризиками на основі аналізу причин, факторів впливу і можливих наслідків

Під час проєктування систем критичного призначення значна увага приділяється виконанню вимог до надійності та якості на кожній стадії. Водночас вплив внутрішнього та зовнішнього факторів на функціонування таких систем та їх імовірнісні характеристики іноді залишаються без належної уваги.

Щоб представити процес управління ризиками математично на основі теорії множин, включаючи зв'язки між причинами, наслідками та фак-

торами впливу, можна визначити такі набори даних набір причин (C), набір наслідків (C_n), набір факторів впливу (F), набір подій ризику (R).

Причинно-наслідковий зв'язок (CC) відображає зв'язок між причиною та наслідком. Можемо визначити функцію $CC(C, C_n)$, яка відображає кожну причину C та набір асоційованих з нею наслідків C_n. Математично можемо представити це як (6):

$$CC(C) = \{C_n \mid C_n \text{ є наслідком, пов'язаним з причиною } C\}. \quad (6)$$

Відношення причинно-впливаючих факторів (CF) – представляє фактори впливу, пов'язані з кожною причиною. Можемо визначити функцію $CF(C)$, яка відображає кожну причину C на набір факторів впливу F, пов'язаних із нею. Математично можемо представити це як (7):

$$CF(C) = \{F \mid F - \text{фактор впливу, пов'язаний із причиною } C\}. \quad (7)$$

Відношення факторів, що впливають наслідки (C_nF): це співвідношення представляє фактори впливу, пов'язані з кожним наслідком. Можемо визначити функцію $C_nF(C_n)$, яка відображає кожен наслідок C_n на набір факторів впливу F, пов'язаних із ним. Математично можемо представити це як (8):

$$C_nF(C_n) = \{F \mid F - \text{фактор впливу, пов'язаний із наслідком } Cn\}. \quad (8)$$

Склад подій ризику (RC) представляє склад причин, наслідків і факторів, що впливають на кожну подію ризику. Можемо визначити функцію $RC(C, C_n, F)$, яка відображає кожну комбінацію причини C, наслідку C_n і фактора впливу F на подію ризику R. Математично можемо представити це як (9):

$$RC(C, C_n, F) = R. \quad (9)$$

Використовуючи ці набори та зв'язки, можемо побудувати математичні моделі для представлення взаємозв'язків і взаємодій у процесі управління ризиками, наприклад визначення причин, наслідків, факторів впливу та складання переліку подій ризику. Ця модель забезпечує концептуальну основу для розуміння та аналізу процесів управління ризиками з точки зору теорії множин.

Математичний опис такого підходу з використанням теорії множин може бути використаний для розробки нейронних мереж, що можуть навчатися як самостійно, так і з учителем. Автоматизація процесу управління ризиками ІБ сприятиме оперативному прийняттю рішень з забезпечення кіберзахисту, обґрунтуванню підрозділу з кібербезпеки керівництву організації щодо потреб для ефективного захисту інформації [8].

Метод оцінки ризиків інформаційної безпеки на основі репутації вендора, рівня впровадження заходів кіберзахисту та рівня знань зловмисника

Для зменшення об'єму статистичних даних, що використовуються у кількісних методах оцінки ризику ІБ доцільним є розробити систему «коефіцієнт репутації вендора» Kr, що відображатиме рівень довіри до певного програмного чи апаратного продукту у сфері ІБ, що являє собою оцінку вразливостей виявлених у продуктах даного вендора. Дану оцінку можна розрахувати як відношення кількості вразливостей V_n до кількості типів P_t продукту (засоби захисту, мережеве обладнання, програмне забезпечення тощо) за певний проміжок часу t (10):

$$K_r = \frac{V_n}{P_t} * t. \quad (10)$$

Оцінку рівня кваліфікації потенційного зловмисника доцільно буде здійснювати за правилом (11).

$$L_k = L_s + 1, \quad (11)$$

де L_k – рівень кваліфікації зловмисника; L_s – рівень кваліфікації фахівця з ІБ.

Оцінку рівня кваліфікації фахівця з ІБ, доцільно здійснювати за наступною шкалою: 1 – низький (фахівець володіє термінологією з ІБ, але не має практичного досвіду); 2 – середній (фахівець володіє термінологією з ІБ, має практичний досвід з конфігурування та встановлення засобів захисту); 3 – високий (фахівець володіє термінологією з ІБ, має практичний досвід з конфігурування та встановлення засобів захисту, здатен розробляти власні проектні рішення).

При оцінюванні рівня кваліфікації зловмисника додаємо 1 бал, так як зловмисник на відміну

від розробника (фахівця з ІБ) на початковому етапі володіє меншою кількістю інформації про систему і її захист. Тому щоб здійснити успішну атаку кваліфікація зловмисника має бути вищою за кваліфікацію фахівця з ІБ. Рівень впровадження заходів кіберзахисту визначається відповідно до [9].

Залишається відкритим питання яким чином визначити та формалізувати оцінку ризику ІБ з урахуванням просторово-часових характеристик ризику та рівня кваліфікації зловмисника.

Таким чином, ризик ІБ можна обчислити, враховуючи вище зазначені фактори, за наступною формулою (12):

$$R = \frac{K_r + \text{СЦ}_{\text{кат}} + L_k}{100}, \qquad (12)$$

де K_r – коефіцієнт репутації вендора; $\text{СЦ}_{\text{кат}}$ – мінімальний середній рівень впровадження; L_k – рівень кваліфікації зловмисника.

Одиницею виміру R буде імовірність можливих втрат інформаційних активів.

Система обміну знаннями та досвідом між фахівцями з кібербезпеки

Незважаючи на розвиток інформаційних технологій та технологій кібербезпеки, людина залишається найуразливішим місцем будь-якої інформаційно-комунікаційної або технологічної системи ОКІ. Причинами такої вразливості людини є недостатність знань, досвіду, відсутність відповідних інструкцій, мотивації тощо. Зосередимось на проблемі знань та досвіду. Природньо склалося так, що з підвищенням рівня знань та досвіду фахівця, фахівець отримує більш вигідні пропозиції роботи і змінює своє місце роботи. В умовах війни з рф існує дефіцит фахівців для критичної інфраструктури, який зумовлений підвищеними ризиками для життя таких фахівців та їх загибеллю від ракетних ударів. Саме в цей момент часу система залишається найбільш вразливою. Новий спеціаліст який прийшов працювати потребує часу для ознайомлення з системою, визначення її слабких місць, аналізування наявних ризиків. Кіберінциденти та нештатні ситуації, які можуть виникнути в цей проміжок часу також зазвичай потребуватимуть більше часу для їх усунення, що може мати значні негативні наслідки для ОКІ, в тому числі і на безпеку життя громадян. Таким чином постає проблема зменшення часу для опанування новим фахівцем своєї сфери відповідальності. Ця проблема може бути вирішена шляхом передачі знань і досвіду від попередника. Однак передати такі знання та досвід з урахуванням частої зміни персоналу та інших факторів не можливим без використання засобів інформатизації. З огляду на це пропонується створення та впровадження системи обміну знаннями та досвідом між фахівцями (далі – платформа) з інформаційних технологій та кібербезпеки.

Основними критеріями такої платформи повинно бути довірене середовище, ефективна взаємодія, обмін знаннями та досвідом, можливість пошуку ефективних рішень. Зокрема довірене середовище, забезпечене підтвердженням приналежності фахівця до організації його роботодавцем дасть змогу створення статистичних даних про проблеми кіберзахисту в галузі та підвищить ефективність взаємодії в галузі та фахівцями з інших галузей. Обмін знаннями та досвідом може бути забезпечений профілем користувача, де користувач може додати перелік програмного та програмно-апаратного забезпечення, що його оточує, переглянути історію чатів з інформацією про виявлені проблеми іншими фахівцями, в тому числі виявлені попередником та їх варіанти рішень. Водночас є можливість і задати питання, де учасники системи можуть допомогти, підвищивши власний рейтинг, якщо порада буде оцінена іншими фахівцями. Така платформа стане предметом зацікавленості вендорів, так як вони безпосередньо зацікавлені у виявлені та вирішенні проблем з їх продуктами, які не були виявлені в процесі тестування перед виходом в продаж.

Цілями такої системи повинні бути накопичення знань та досвіду, забезпечення швидкого пошуку інформації, створення рейтингів вразливостей, рекомендацій користувачів, надійності вендорів, генерація ретроспективного аналізу, прогнозування. Такі цілі можуть бути досягнені шляхом залучення до платформи фахівців з АСУ ТП, інформаційних технологій та кібербезпеки, вендорів, представників (CERT/CSIRT), менеджерського складу (CIO, CTDO, CISO), аудиторів інформаційної безпеки та аудиторів систем управління інформаційною безпекою. Таким чином основними цінностями системи стануть спільні цілі, довіра, бажання прогресу, мотивація. Звісно, для того

щоб впровадження системи набуло поширення, вона повинна бути простою у користуванні, адаптивною, інтерактивною, сприяти стратегічним комунікаціям та бути ефективною.

Концепція такої системи поєднує професійний форум, маркетплейс та спортивні змагання. Концепція професійного форуму реалізується через обмін повідомленнями (коментарями), маркетплейс представлений можливістю користувача обрати програмне забезпечення та додати його з інформацією про нього до власного профілю, спортивні змагання – рейтингуванням фахівців відповідно до їх участі в наповненні баз даних платформи. Таким чином реалізується принцип «використовуй знання та поширюй їх». Важливо також відмітити, що локалізація фахівців спростить обмеження в знанні англійської мови, та можливі неточності перекладу при використанні автоматизованих засобів перекладу технічного тексту. За своєю суттю кабінет користувача стане його віртуальним портфелем, яким зможе користуватися його наступник, а на новому місці роботи у випадку однакових програмних та апаратних засобів при їх додаванні фахівцем у свій новий електронний кабінет він зможе знов використовувати свій попередній досвід. Наявність рейтингу дасть можливість оцінити фахівцю свій внесок, роботодавцю рейтинг стане додатковим аргументом щодо заохочень фахівця. Представлене рішення призначене для збору, обробки, аналізування та обміну даними кібербезпеки з метою підвищення ефективності засобів кіберзахисту. Також доцільним є інтеграція в платформу існуючих сервісів зі збору, обробки та візуалізації інформації з відкритих джерел. Така штучно сформована спільнота фахівців з урахуванням наявного розподілу ролей (категорій фахівців) наявними процесами буде мати перспективи до саморозвитку. Також до перспектив розвитку самої системи можна віднести можливість впровадження технологій штучного інтелекту, створення механізмів ретроспективного аналізу для оцінювання правильності прийнятих рішень, впровадження механізмів швидкого пошуку даних, розробка і додавання інших рейтингів для бізнес аналітиків, інтеграція систем оповіщення у випадку появи нових проблем (месенджери, електронна пошта).

Антифішингова інфраструктура як засіб протидії загрозам функціонування систем критичного призначення

У зв'язку з війною між рф та Україною, в рф зросла активність груп хактивістів, діяльність яких спрямована проти України та наших громадян. Постійно фіксуються DDoS та інші кібератаки на державні органи та ОКІ. Зокрема, хактивісти противника використовують фішинг для викрадення персональних даних, грошей громадян, які і так перебувають у скрутному фінансовому становищі, кібератаки на ІТ-інфраструктуру бізнесу, APT-атаки на критичну інфраструктуру України. Таким чином протидія фішингу є надзвичайно важливим завданням для кібербезпеки та національної безпеки України. Наслідками фішингу є втрачені гроші громадян, враження комп'ютерних систем шкідливим програмним забезпеченням та недоступність ряду сервісів порушення функціонування систем критичного призначення тощо. В сьогоденні противником розроблюється фішинг після будь якого інформаційного приводу, що стосується масової кількості людей, зокрема на популярні в нинішніх реаліях теми «Збір для ЗСУ», «Графіки відключень електроенергії», «Соціальні виплати», «Нова пошта» тощо. Це створює підвищену небезпеку для наших громадян. Для мінімізації загрози фішингу необхідним є зменшення його ефективності. Ефективність фішингу визначається кількістю успішних його застосувань. Кількість успішних застосувань залежить від часу існування фішингу, який визначається швидкістю реагування на таку загрозу і вжиттям відповідних заходів.

Іншою не менш важливою проблемою залишається протидія пропаганді противника, поширення ним фейків та дезінформації. Пропаганда противника спрямована на диверсифікацію громадської думки, підрив державного ладу, розпалювання ворожнечі всередині держави з метою досягнення власних злочинних цілей. Пропаганда і дезінформація можуть становити реальну небезпеку національній безпеці держави.

З огляду на зазначене та за результатом аналізу поширення інформації засобами інформаційних технологій постала необхідність розробки та впровадження інфраструктурних ІТ-рішень для ефективній протидії фішингу і пропаганді (далі –

система). Вимогами до системи є надання можливості користувачу оперативно перевірити посилання на вебресурс, адресу електронної пошти, посилання на групу чи телеграм канал, номер мобільного телефону, номер банківської карти (далі – об'єкти перевірки), створення автоматизованих перевірок вебресурсу та швидке поширення інформації про фішинг і пропаганду серед користувачів системи. Таким чином було розроблено IT архітектуру, яка складається з Telegram бота, мобільного застосунку, вебсайту, розширення для браузера (далі – плагін), загальної бази даних та DNS серверу (рис. 1).

Рис. 1. Структурна схема антифішингової інфраструктури

Система може бути використана також для раннього виявлення масових розсилок. Таке виявлення базується на оцінці кількості переходів з однієї мережі за одним посиланням в одиницю часу.

ВИСНОВКИ

Розроблено метод автоматизації управління вразливостями на основі технології SCAP. Для аналізування отриманих даних після реалізації методу запропоновано математичну формалізацію вразливості на основі потоків даних NVD.

Застосування розробленого методу дозволяє в рази пришвидшити процедуру збору та аналізу даних про вразливості, поширення цієї інформації в рамках організації, створює можливості для ретроспективного аналізу процесу управління виправленнями (патчами), контролю версій програмного та програмно-апаратного забезпечення, що значно зменшує імовірність наявності в системі вразливостей та помилок версійності програмного забезпечення. Відповідно значно зростає рівень кібербезпеки та стійкості ІКС та АСУ ТП.

Розроблено метод опису кібератаки на основі шаблону з траєкторією поведінки керованої кіберсистеми. Метод опису кібератаки на основі шаблону з траєкторією поведінки керованої кіберсистеми базується на тому, що завданням шаблона є вказати ті події на пристроях ІКС та АСУ ТП, за якими можна визначити факт проведення атаки. Застосування даного методу дає можливість постійної актуалізації моделі загроз та моделі порушника безпеки інформації, пришвидшує процеси побудови вектора атаки і ідентифікації її джерела, створення правил та політик розмежування доступу, моделей для поведінкових аналізаторів засобів захисту, створює основу для розробки методик стрестестування, розробки сценаріїв для проведення навчань з метою підвищення обізнаності та набуття практичних навичок з кіберзахисту відповідального за кібербезпеку персоналу, що значно підвищує рівень кібербезпеки ОКІ.

Розроблено метод управління ризиками на основі аналізування причин, факторів впливу і можливих наслідків. З використанням теорії множин представлено такі множини як набір причин, набір наслідків, набір факторів впливу, набір подій ризику та визначено зв'язки між цими наборами, які представлені у вигляді відповідних функцій. Застосування даного методу дає можливість зменшення впливу невизначеності на цілі організації в умовах постійно змінюваного навколишнього середовища в умовах гібридної війни, в тому числі – ідентифікації непрямих ризиків пов'язаних з діяльністю організації, що значно мінімізує потенційні збитки від настання несприятливих умов і зменшує витрати ресурсів на оброблення ризиків в умовах обмежених ресурсів.

Також математичний опис такого підходу з використанням теорії множин може бути використаний для розробки нейронних мереж, що забезпечує можливість прогнозування можливих ризиків та є основою для інтегрування наявного досвіду, що значно підвищить рівень кібербезпеки ОКІ і зможе компенсувати проблеми компетентності персоналу.

Розроблено метод оцінки ризиків інформаційної безпеки на основі репутації вендора, рівня впровадження заходів кіберзахисту та рівня знань зловмисника. Зокрема, запропоновано введення

коефіцієнту репутації вендора, рівня кваліфікації потенційного зловмисника та рівня впровадження заходів кіберзахисту для оцінювання ризиків. Даний метод дасть можливість враховувати показники якості використовуваних засобів і кваліфікацію зловмисника, що зменшить імовірність впливу суб'єктивізму на прийняття рішень з кібербезпеки, водночас сприятиме підвищенню якості постійного моніторингу появи нових вразливостей як складової коефіцієнту репутації вендора та оцінювання зрілості процесів інформаційної безпеки з метою уникнення надлишковості при використанні активів для забезпечення кіберзахисту.

Розроблено систему обміну знаннями та досвідом між фахівцями з кібербезпеки. Дана система вирішує проблему накопичення та збереження знань і досвіду персоналу в межах організації, що значно зменшує час на опанування обов'язків з кіберзахисту новим співробітником СЗІ при зміні персоналу в умовах швидкої плинності кадрів в сфері ІТ та кібербезпеки, при чому мінімізуючи час функціонування системи без належно моніторингу із-за обмежених знань нового працівника про ІКС та АСУ ТП в перші дні роботи на новому місці. Також перевагою даної системи є підвищення швидкості та якості інформаційного обміну за рахунок наявності в одному інформаційному середовищі представників різних спеціальностей з ІТ, кібербезпеки та представників розробників, що відповідно впливає на швидкість виявлення вразливостей (проблем функціонування) і їх усунення. Система підвищує спроможності з оцінювання персоналу виявляючи глобальні та локальні проблеми з персоналом та забезпеченням кіберзахисту як в рамках галузі, так і в межах організації, що зменшує імовірність помилок при прийнятті управлінських рішень різного рівня в сфері кібербезпеки і дасть змогу зменшити вплив несприятливих подій на кібербезпеку ОКІ.

Розроблено антифішингову інфраструктуру як засіб протидії загрозам функціонування систем критичного призначення. Використання даної інфраструктури дає змогу зменшити час для масового поширення інформації про фішинг від моменту першого його виявлення до декількох секунд, що зробить фішинг неефективним і відповідно нерентабельним з точки зору затрачених на його розробку ресурсів. Таким чином це мінімізує значимі ризики пов'язані з використанням мережі Інтернет, потенційні збитки, знизить наявну кількість кіберінцидентів і об'єм затрачених ресурсів на відповідне реагування.

ЛІТЕРАТУРА

[1] OWASP Top Ten | OWASP Foundation. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. URL: https://owasp.org/www-project-top-ten/ (date of access: 31.07.2023).

[2] Souppaya M., Scarfone K. Guide to enterprise patch management technologies. National Institute of Standards and Technology, 2013. URL: https://doi.org/10.6028/ nist.sp.800-40r3 (дата звернення: 26.02.2023).

[3] Palmaers T. Implementing a vulnerability management process. Egnyte. URL: https://sansorg.egnyte.com/dl/2IL7fioFhM (date of access: 31.07.2023).

[4] The technical specification for the security content automation protocol (SCAP) version 1.3 / D. Waltermire et al. Gaithersburg, MD : National Institute of Standards and Technology, 2018. URL: https://doi.org/10.6028/nist.sp.800-126r3 (date of access: 10.09.2023).

[5] The cyber kill chain. www.lockheedmartin.com. URL: https:// www.lockheedmartin.com / en-us / capabilities/cyber/cyber-kill-chain.html (date of access: 25.02.2023).

[6] Yakoviv I. The base model of informational processes of management and safety criteria for cybernetic systems. Collection "Information technology and security". 2015. Vol. 3, no. 1. P. 68–74. URL: https://doi.org/10.20535/2411-1031.2015.3.1.57735 (date of access: 10.09.2023).

[7] Davydiuk A., Yakoviv I. Criteria of cybernetic systems safety. Наука і молодь в XXI сторіччі : Збірник тез доповідей, Полтава, 1 Грудня 2016. Полтава, 2016. С. 356-357.

[8] Давидюк А. Модель управління ризиками як артефакт процесу проєктування систем критичного призначення. XII Міжнародна науково-практична конференція молодих вчених Інформаційні технології: економіка, техніка, освіта '2021 : Зб. тез конф., м. Київ, 2021 р. Київ, 2021. С. 162–163.

[9] Зубок В., Давидюк А. Використання топологічного простору для оцінювання рівня забезпечення функцій кібербезпеки в критичній інфраструктурі. Інформаційні технології та безпека матеріали XXII міжнародної науково-практичної конференції : Зб. тез доп., Київ, 2022. С. 22–30.

IMPLEMENTATION OF NEW TOOLS AND METHODS FOR INCREASING THE LEVEL OF CYBER SECURITY OF CRITICAL INFRASTRUCTURE OBJECTS

Existing methods and means of ensuring cyber security of critical information infrastructure objects, developed on the basis of international standards and best practices, are quite effective in peacetime conditions, but do not take into account the hybrid nature of war, in which new threats appear, in particular, such as physical destruction , capture by the enemy, the lack of possibility of constant monitoring and control, limitations in defense resources and available personnel, problems in the supply of recovery equipment, interruptions in information exchange processes, the need for frequent changes in operating conditions, dynamic growth in the number and quality of cyber-attacks, etc., due to which their efficiency drops significantly. In view of this, there is a need to develop new and improve existing methods and means of cyber protection in order to increase the level of cyber security of critical infrastructure. The safety of the population and the performance of combat tasks by the troops depend on ensuring the cyber security of critical information infrastructure facilities as an integral part of critical infrastructure facilities.

Keywords: vulnerability management, SCAP, description of a pattern-based cyber-attack with a managed system behavior trajectory, risk assessment, visual analytics, anti-phishing infrastructure, knowledge and experience sharing system.

Давидюк Андрій Вікторович, аспірант кафедри Безпеки інформаційних технологій НАУ, молодший науковий співробітник ІПМЕ ім. Г.Є. Пухова НАН України, Technical researcher NATO CCDCOE.

Andrii Davydiuk, Phd student of the Department of information technology security of NAU, junior scientific researcher G.E. Pukhov IMEE NAS of Ukraine, Technical researcher NATO CCDCOE.
E-mail: andrey19941904@gmail.com.
Orcid ID: 0000-0003-1238-2598.

DOI: 10.18372/2410-7840.25.17938
УДК 004.056:061.68

РОЗРОБКА МЕТОДОЛОГІЇ ОЦІНКИ ВІДПОВІДНОСТІ СТАНДАРТУ ISO 27001

Євгеній Курій, Віталій Сусукайло, Іван Опірський

Даний науковий документ пропонує розробку методології оцінки відповідності організацій новій версії стандарту ISO 27001, яка була представлена в кінці 2022 року. Висока значущість інформаційної безпеки в сучасному світі вимагає від компаній адаптувати свої практики та політики до нових вимог стандарту. Автори аналізують останні дослідження у галузі впровадження стандарту ISO 27001 та недоліки релевантних матеріалів для оцінки відповідності. Методологія включає аналіз нових вимог стандарту, порівняння їх із зіставленням існуючих практик організацій, визначення «гепів» (розривів/невідповідностей) між ними, розробку плану впровадження змін та моніторингу відповідності. Запропоновані рекомендації допоможуть організаціям забезпечити ефективний перехід на новий стандарт, мінімізувати ризики і зберегти високий рівень інформаційної безпеки. Ця методологія є актуальним інструментом для організацій, що прагнуть адаптувати свої практики і політики до нової версії стандарту ISO 27001 та підтримувати безпеку своєї інформації на високому рівні. Дана розробка враховує унікальні потреби організацій та сприяє їхньому успішному впровадженню нових практик і вимог інформаційної безпеки. Ця стаття має на меті допомогти читачам зрозуміти складність та важливість проведення початкової оцінки на невідповідність перед впровадженням стандарту та висвітлити ефективність застосування детального чекліста під час проведення аналізу на невідповідності. Для підтримки дослідження був проведений детальний аналіз літератури та статей, що стосуються впровадження стандарту ISO 27001 в організаціях.

Ключові слова: *інформаційна безпека, кібербезпека, ISO 27001, фреймворк інформаційної безпеки, система управління інформаційною безпекою, оцінка на невідповідність, аналіз на невідповідність.*

ВСТУП

В сучасному цифровому світі збільшується значення інформації та даних, що обробляються, зберігаються та передаються організаціями. Відповідно, зростає і загроза порушення цілісності, конфіденційності та доступності цих даних. Саме тому організації мають звертати особливу увагу на забезпечення високого рівня інформаційної безпеки. Один із способів досягнення цієї мети - впровадження стандарту ISO 27001.