є вдосконаленням електромагнітних радіохвиль, які використовуються у WI-FI. Однак воно не може проникати крізь стіни, на що здатні радіохвилі. Зазвичай це реалізується за допомогою білих світлодіодних ламп на передавачі низхідної лінії зв'язку [2]. Технологія Li-Fi працює подібно до оптоволоконної мережі, однак середовищем передачі є повітря/вільний простір. Сьогодні лазерне, інфрачервоне та ультрафіолетове випромінювання використовується для зв'язку по повітрю або у вільному просторі в різних системах. Для передачі даних в цій технології можуть використовуватися схеми модуляції OOK (On-Off Keying), OFDM. Для передачі даних за допомогою видимого світла необхідно увімкнути або вимкнути світлодіод. Коли світлодіод увімкнений, приймач розпізнає його як "1", а коли він вимкнений, приймач повинен розпізнати його як "0". Це не так просто, як надсилання та виявлення, для цього потрібно використовувати підсилювач/фільтр на стороні приймача. Найкраща частина комунікації видимого світла полягає в тому, що ми можемо скористатися перевагами високошвидкісної передачі даних і в той же час використовувати її для освітлення.[3], [4].

Література

1. HASANUDIN, Afif Hakim, et al. "From WI-FI to LI-FI: a comprehensive review of integration strategies." Przeglad Elektrotechniczny 2023.9 (2023).

2. Deval, Nimisha, et al. "Wireless Communication Using Light Fidelity Network." Techno-Societal 2020: Proceedings of the 3rd International Conference on Advanced Technologies for Societal Applications—Volume 1. Cham: Springer International Publishing, 2021.

3. Dahri, Faisal Ahmed, et al. "Design and implementation of LED–LED indoor visible light communication system." Physical communication 38 (2020): 100981.

4. Santosa, AA et. al. "An alternative dichromatic white LED light source for OOK-NRZ visible light communication system." Fourth International Seminar on Photonics, Optics, and Its Applications (ISPhOA 2020). Vol. 11789. SPIE, 2021.

УДК 681.6

А.А. Микитишин, Д.І. Ящишин, Р.З. Золотий, канд. техн. наук., доц.
Тернопільський національний технічний університет імені Івана Пулюя

РОЗВИТОК АВТОМАТИЗАЦІЇ КІБЕРБЕЗПЕКИ В ПРОТИДІЇ КІБЕРАТАКАМ В ЕНЕРГЕТИЦІ

A.A. Mykytyshyn, D.I. Yashchyshyn, R.Z. Zolotyi, Ph.D.
Ternopil Ivan Puluj National Technical University

DEVELOPMENT OF CYBER SECURITY AUTOMATION AGAINST CYBER ATTACKS IN THE ENERGY INDUSTRY

Автоматизація кібербезпеки згадується IT-фахівцями, а також у наукових статтях протягом багатьох років. Але її впровадження відбувалося повільніше, ніж очікувалося. IT-фахівці погоджуються, що для великих підприємств, які використовують багато різних операційних систем, додатків і пристроїв різних виробників, завдання перегляду стану безпеки широкого діапазону пристроїв і бізнес-сфер для відповідності вимогам безпеки, встановленим нормативними актами, або виявлення ризиків, таких як неправильно налаштовані пристрої, застаріле програмне забезпечення тощо, займає багато часу, є схильним до помилок і дорогим. Хоча люди відіграють важливу роль у процесі оцінки безпеки, вони не в змозі впоратися із завданням і можуть внести невідповідності, які можуть ще більше зробити організації вразливими до порушень безпеки. Автоматизація безпеки забезпечує вирішення цих проблем. Автоматизація може ефективно допомагати в протидії кібератакам кількома способами, деякі з них:

Автоматизоване виявлення загроз: системи кібербезпеки можуть швидко й точно ідентифікувати потенційні загрози, такі як зловмисне програмне забезпечення або спроби

несанкціонованого доступу, за допомогою алгоритмів машинного навчання та інших види автоматизації.

Автоматичне реагування: після виявлення загрози автоматизація кібербезпеки може бути використана для виконання заздалегідь визначених дій. Наприклад, автоматична відповідь може включати поміщення файлу в карантин або завершення роботи скомпрометованої системи.

Автоматизоване керування безпекою: без втручання людини автоматизацію кібербезпеки можна використовувати для керування та оновлення систем безпеки, таких як брандмауери та системи виявлення вторгнень.

Дефіцит IT-працівників: автоматизація кібербезпеки може допомогти заповнити прогалину, взявшись за виконання повторюваних і трудомістких завдань, які в іншому випадку мали б виконувати люди. Це може підвищити загальну ефективність і результативність заходів компанії з кібербезпеки, дозволяючи IT-персоналу зосередитися на більш складних і стратегічних завданнях.

Незважаючи на те, що рух шляхом автоматизації здається очевидним, існує багато факторів, які уповільнюють автоматизацію у сфері кібербезпеки. Впровадження автоматизованих систем може означати додаткові витрати та персонал. Відсутність кваліфікованих і досвідчених фахівців у сфері автоматизації, кібербезпеки та ШІ/машинного навчання ускладнює впровадження та підтримку систем. Керівники та співробітники можуть бути стійкими до використання нових технологій і процесів. Відсутність стандартизації в індустрії кібербезпеки ускладнює взаємодію та ефективну співпрацю автоматизованих систем. Складність може ускладнити розробку та впровадження автоматизованих систем, здатних ефективно протистояти всім потенційним загрозам. Багато організацій навіть не мають даних, необхідних для ефективного навчання та вдосконалення автоматизованих систем. Ця проблема пов’язана з проблемами конфіденційності, особливо якщо автоматизовані системи збирають, зберігають або обробляють конфіденційні дані.

Як запровадити автоматизацію кібербезпеки? Ми зосередимося на факторах, які перешкоджають реалізації автоматизації, розглянемо додаткові дані, що підтверджують основну ідею, що автоматизація кібербезпеки є відповідним інструментом для вирішення сучасних викликів у сфері кібербезпеки, і ми дамо рекомендації щодо процесу впровадження автоматизації у сфері кібербезпеки.

Вартість автоматизації. Впровадження автоматизованих систем є складним завданням, але це не обов’язково робити за один крок. Зазвичай найкращим способом є використання поступових кроків до автоматизації. Вартість витоку даних щороку зростає, але зменшується відповідно до рівня автоматизації. Ті, хто повністю розгорнув автоматизацію, змогли зменшити негативний вплив витоку даних до менш ніж 50%.

Кваліфікована робоча сила. Виділення частини наявних IT-спеціалістів для сприяння автоматизації спочатку може здатися нелогічним. Але вони можуть заощадити багато годин роботи щотижня завдяки автоматизації безпеки з низьким кодом, а аналітики можуть завчасно реагувати на майже на 80% більше даних телеметрії безпеки.

Опір змінам. Інертність є природною. Кожна людина має свої пріоритети, через які вона оцінює можливі зміни. Деякі навіть розуміють, що зміни неминучі, але відкладають оновлення, сподіваючись вижити на поточних системах, перш ніж покинуть бізнес. Ефективна автоматизація може автоматично фільтрувати, сортувати та впорядковувати дані та автоматично реагувати на різні загрози. Це забезпечує економію робочого часу, тому IT-спеціалісти можуть мати більше часу, щоб зосередитися на стратегічних пріоритетах і скоротити додаткові години, реагуючи на загрози вручну. Також можна запровадити програми управління змінами, щоб допомогти співробітникам зрозуміти переваги автоматизації та те, як її можна використовувати для покращення їхньої роботи.

Відсутність стандартизації та інтеграції. Робота з різними системами та технологіями, які були впроваджені або оновлені в різний час, з різною якістю та різними варіантами інтеграції, є фактом, який ми повинні прийняти.

Комплексність має справу з багатьма проблемами стандартизації та інтеграції. Різноманітні системи та технології, розподілені між різними рівнями та часто різними фізичними розташуваннями, кількість яких зростає з кожним десятиліттям. Кожна компанія повинна оцінити основні виклики, з якими вона стикається, і з цього починати роботу.

Штучний інтелект і машинне навчання. На відміну від факторів, які перешкоджають автоматизації, штучний інтелект є каталізатором змін. Методи штучного інтелекту дуже добре нам допомагають, а також можуть використовуватися для вирішення проблем кібербезпеки. Під егідою штучного інтелекту входять різні методи, такі як аналіз даних, нейронні мережі, нечітка логіка, які можна інтегрувати з традиційними практичними та статистичними механізмами для аналізу даних. Машинне навчання — це галузь інформатики (точніше, штучного інтелекту), яка займається розробкою методів і алгоритмів, які вивчають характеристики та шаблони з доступних даних, щоб робити прогнози.

Аутсорсинг є ще одним важливим каталізатором змін. Якщо ви працюєте зі старими системами або недосвідченим персоналом, пам’ятаючи про можливі втрати після зламу або поломки системи, можливо, буде дешевше передати кібербезпеку аутсорсингу, поки компанія не знайде ресурси та людей, які підходять для цілей.

Виходячи з аналізу можна надати наступні рекомендації, що стосуються впровадження автоматизації в процеси кібербезпеки, включаючи використання штучного інтелекту та машинного навчання.

Почніть із підручників, у яких задокументовано кроки, процеси та найкращі практики, які ваші команди використовують сьогодні для ефективного вирішення інциденту. Переконайтеся, що команди дотримуються послідовного та повторюваного процесу щоразу, коли трапляється інцидент. Потім визначте найбільш трудомісткі, повторювані процеси та використовуйте їх для визначення ваших перших автоматизованих ігор.

Надайте пріоритет автоматизації для областей високого ризику, таких як безпека мережі, безпека даних, реагування на інциденти та управління відповідністю. Майте на увазі, що існує зворотна залежність між ступенем автоматизації та розміром втрат від кібератаки.

Працюйте поетапно. Почніть з автоматизації простих, повторюваних завдань і поступово переходьте до більш складних завдань. Це допоможе вам краще керувати наявною робочою силою, витратами та ресурсами. Крім того, якщо під час процесу виникнуть деякі перешкоди, ви все одно зможете повернутися до працездатної системи, перш ніж виправити проблему.

Інвестуйте в інструменти, які можна інтегрувати з існуючими системами. Інструменти автоматизації повинні бути сумісні з існуючими системами та процесами, щоб мінімізувати перебої та підвищити ефективність. Якщо ваші поточні системи застаріли, шукайте рішення, які можуть замінити завдання, які виконуються вашими поточними системами.

Використовуйте автоматизацію для покращення керування безпекою та реагування на інциденти. Автоматизацію можна використовувати для покращення керування системами безпеки, такими як брандмауери та системи виявлення вторгнень, зменшуючи потребу в ручному налаштуванні та управлінні. Автоматизація безпеки дуже корисна для команди інформаційних технологій. Якщо з’являється сповіщення, він миттєво визначає, чи потрібна дія на основі попередніх відповідей на подібні інциденти, і якщо так, вона може автоматично усунути проблему.

Приєднайтеся до всіх. Включіть навчання для керівництва та співробітників у план впровадження. Вкажіть позитиви, які приносить співробітникам впровадження нових заходів автоматизації. Заохочуйте їх прийняти процес автоматизації та дайте їм необхідні інструменти для цього. Збирайте дані для керівництва, щоб продемонструвати підвищення ефективності та скорочення витрат.

Дивіться в майбутнє. Слідкуйте за новими тенденціями в автоматизації кібербезпеки та будьте готові прийняти нові технології, коли вони стануть доступними. Нові рішення можуть підвищити ефективність, зменшити навантаження на співробітників і скоротити витрати.

Література.

1. AlSadhan, T., Park, J. S. Enhancing Risk-Based Decisions by Leveraging Cyber Security Automation. European Intelligence and Security Informatics Conference (EISIC), Uppsala, 2016, p. 164-167.
2. Barak, E. Explaining security automation and its evolving definitions, IDG Communications, Inc, New York, NY. 2022. Режим доступу : www.networkworld.com/article/3121275/explaining-securityautomation-and-its-evolving-definitions.html.
3. Cynet. What is Security Automation? Tools, Process and Best Practices. 2022. Режим доступу : https://www.cynet.com/incident-response/securityautomation-tools-process-and-best-practices.

УДК 004.9+621.3

Р.І. Королюк, І.В. Булич, М.В. Гаврилюк, І.С. Дідич докт. філ.
Тернопільський національний технічний університет імені Івана Пулюя, Україна

СТЕНД УПРАВЛІННЯ АСИНХРОННИМ ДВИГУНОМ З ДОПОМОГОЮ ОДНОПЛАТНОГО КОМП’ЮТЕРА RASPBERRY PI

R.I. Koroliuk, I.V. Bulych, M.V. Havryliuk, I.S. Didych Ph. D

ASYNCHRONOUS MOTOR CONTROL STAND USING A SINGLE BOARD COMPUTER RASPBERRY PI

Асинхронні двигуни найбільш часто використовують в електроприводі різноманітного технологічного обладнання, виконавчих механізмах різних пристроїв в широкому спектрі потужностей. Для управління асинхронними двигунами використовуються кілька базових систем, але найбільш ефективна на базі частотного перетворювача [1]. Управління самим частотним перетворювачем здійснюється як в ручному режимі так і з допомогою промислових контролерів. Тому важливе місце в підготовці спеціалістів технічних спеціальностей займає набуття навиків управління асинхронними двигунами. Набуття практичних навиків ефективніше на лабораторних стендах.

Метою даної роботи є розробка та виготовлення стенду управління асинхронним двигуном. Стенд складається з наступних компонентів:

1) пари гвинт-гайка довжиною 2000мм;
2) пасової передачі, захищеної кожухом;
3) асинхронного двигуна AIP80B4;
4) частотного перетворювача Simphoenix 500;
5) адаптера USB to RS485;
6) одноплатного комп’ютера Rasberry Pi 4;
7) монітор з підтримкою HDMI.

Для керування частотним перетворювачем Simphoenix 500 використано одноплатний комп’ютер Rasberry Pi 4 [2, 3. 4], який дозволяє писати керуючі програми на мові високого рівня Python.

На рис. 1 показано схему управління асинхронним двигуном з допомогою одноплатного комп’ютера Raspberry Pi.