впливає на вхідний імпеданс. Рівняння, що зв'язує глибину вставки, імпеданс антени та імпеданс фідерної лінії, має вигляд:

$$D = \frac{L}{\pi}\cos^{-1}\left(\sqrt[4]{\frac{Z_{Feedline}}{Z_{Antenna}}}\right)$$

Дослідний взірець антени пройшов натурні випробування на літаючому швидкісному об’єкті.

Література

1. Mbinack, Clement, E. Tonye and D. Bajon. Microstrip-line theory and experimental study for the characterization of the inset-fed rectangular microstrip- patch antenna impedance. Microwave and Aptical Technology Letters, #2, 2015.
2. Kumar Girish. Broadband microstrip antennas/Girish Kumar and K.P. Ray. Artech House antennas and propagation library. ISBN 1-58053-244-6, 2003.

УДК 004.056

В.Г. Хомишин, Н.В. Загородна, к.т.н., доц., М.А. Стадник, к.т.н., доц.
Тернопільський національний технічний університет імені Івана Пулюя, Україна

БЕЗПЕКА SCADA СИСТЕМ НА ОБ’ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

V.H. Khomyshyn, N.V. Zagorodna, Ph.D., Assoc. Prof., M.A. Stadnyk, Ph.D., Assoc. Prof.

SCADA SYSTEM SECURITY AT CRITICAL INFRASTRUCTURE FACILITIES

Системи диспетчерського управління та збору даних (SCADA) є основними компонентами моніторингу та управління на об’єктах критичної інфраструктури, такими як енергетика, телекомунікації, транспорт, тощо. Застарілі SCADA-системи працювали в ізольованих мережах й були менш вразливими до інтернет-загроз. Проте все частіше підключення корпоративних мереж, включаючи SCADA-системи, до мережі Інтернет створює серйозні проблеми з безпекою. При цьому спостерігається зростання кількості інцидентів безпеки щодо цих критичних інфраструктур. Кібератака на систему SCADA може мати руйнівні наслідки. Зловмисник, скомпрометувавши таку систему, може відключити послуги електропостачання, газу та водопостачання або знищити критично важливу військову інфраструктуру [1].

У 2015-2016 роках серія кібератак на українську енергосистему спричинила перебої в електропостачанні. Атаки проводило хакерське угруповання Sandworm. Зловмисники надіслали документ Microsoft Excel, у якому було шкідливе програмне забезпечення, що здійснювало атаки типу «відмова в обслуговуванні» на контролери SCADA й призвело до виведення з ладу підстанцій, відключення електроенергії та видалення інформації на жорстких дисках заражених систем.

Існують певні вразливості, які зловмисник використовує, щоб скомпрометувати SCADA системи. Такі системи часто побудовані на загальних комп'ютерних протоколах та функціях, таких як передача файлів по мережі або віддалений доступ. Незашифрований обмін даними може бути скомпрометований зловмисником з метою отримання конфіденційної інформації. Крім того, системні програми та служби вимагають певних відкритих мережевих портів. Зловмисник може використовувати ці порти для отримання доступу до системи SCADA, збору інформації про неї та отримання адміністративних привілеїв. Крім того, зловмисник може завантажити шкідливий код, який експлуатує вразливу програму, й отримати несанкціонований доступ. Таким чином, атака на мережі зв'язку може перерости в атаку на всю систему.

Однією з основних проблем захисту таких систем є відсутність зрілих інструментів для аналізу безпеки, адаптованих до вимог SCADA-систем. На відміну від традиційних

комп'ютерних систем, SCADA-системи мають інші вимоги до безпеки та низькі обчислювальні можливості. Крім того, механізми безпеки не завжди враховуються в специфікаціях пристрою або протоколу, потенційно через високу вартість реалізації або низьку обчислювальну здатність пристрою. Ще одним важливим фактором безпеки є те, що життєвий цикл SCADA-систем набагато довший, ніж стандартних комп'ютерних систем. Забезпечення безпеки для величезної кількості мережевих пристроїв, які часто розгорнуті в широких географічних зонах, є складним завданням, яке потребує вивчення та розробки сценарію реагування на кіберінциденти в SCADA системах. Крім того, фізичний доступ до цих пристроїв може бути необмеженим, що може дозволити зловмиснику скомпрометувати всю мережу.

Література

1. Pliatsios, D., Sarigiannidis, P., Lagkas, T. and Sarigiannidis, A.G. (2020) A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics. Communications Surveys and Tutorials, 22, pp. 1942-1976.

УДК 004.41

В.Ю.Шевчук, Є.Б.Яворська, к.т.н., доц..
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ПРЕДМЕТНО-ОРІЄНТОВАНИЙ ПІДХІД ЯК ОПТИМАЛЬНИЙ ДЛЯ РОЗРОБКИ СУЧАСНИХ, МОБІЛЬНИХ ОБ'ЄКТНО-ОРІЄНТОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

V.Yu.Shevchuk, Ye.B.Yavorska, Ph.D., Assoc. Prof.

OBJECT-ORIENTED APPROACH AS OPTIMAL FOR DEVELOPING MODERN, MOBILE OBJECT-ORIENTED INFORMATION SYSTEMS

Кожне покоління інше, всі більше зусиль прикладається на автоматизацію та зменшення фізичної праці, натомість вже почалась ера роботизованої «розумної» техніки. Моє покоління за цифровою обізнаністю та можливостями далеко перевершує вже навіть попереднє, натомість тут я бачу і проблему, коли людина не має можливості скористуватись телефоном чи іншим ґаджетом вона стає безпомічною. Не дивлячись ні на що в цьому я вважаю і один з моментів прогресу, і на часі нові винаходи, коли вже не потрібно буде мати фізично навіть телефон чи інший ґаджет. Проте, якого б рівня техніка не була, як би тісно штучний інтелект не зайшов в наше життя, я вважаю, що ІТ спеціальності як і всі, де, окрім знань, потрібна креативністсь, кмітливість, винахідливість, тобто навики притаманні саме інженерам, ще довго будуть актуальними і роботонезамінними в повній мірі.

Все що я роблю завжди пов'язано з розробками, що дають змогу економити один із основних ресурсів – час, адже то є важко, а подекуди не відновлюваний ресурс і його заощадження – це в першу чергу можливість дослідити щось нове, чи просунутись вперед, розвиватись.

Розробники інформаційних систем, доволі часто, на початку своєї роботи, вагаються який підхід обрати, і з різних міркувань, буває, що приймають рішення не на користь об'єктно-орієнтованого підходу, зумовлюючи свій вибір відповідною складністю в тому числі при моделюванні. Однак, реалізації механізмів з врахуванням парадигм об'єктно-орієнтованого підходу має значно більше переваг ніж недоліків, важливими з яких є швидкість і надійність, а також можливість для гнучкої модифікації. І саме це і стало вирішальним при побудові систем інформаційного типу вже як окремого напрямку, який виділився та інтенсивно розвивається.