3. Соколов А. В., Жданов О. Н. Криптографические конструкции на основе функций многозначной логики. Монография. М. : Научная мысль, 2020. 192 с.
4. Бакунина Е. В. О существовании класса s-блоков, удовлетворяющих корреляционному иммунитету компонентных булевых функций и 4-функций. Наука та суспільне життя України в епоху глобальних викликів людства у цифрову еру: у 2 т. : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 21 трав. 2021 р.) / за загальною редакцією С. В. Ківалова. Одеса : Видавничий дім «Гельветика», 2021. Т. 1. С. 603–606.
5. Яковлєв С. В. Збалансовані критерії якості довгострокових ключових елементів алгоритму ГОСТ 28147-89. Київ: Міжнародний науково-технічний журнал «Інформаційні технології та комп'ютерна інженерія». 2009. С. 5–12.

Ключові слова: криптографія, кореляційний імунітет, булева функція, функція багатозначної логіки.
Key words: cryptography, correlation immunity, Boolean function, many-valued logic function.

БОЙКО ВІКТОР ДМИТРОВИЧ

Національний університет «Одеська юридична академія», доцент кафедри кібербезпеки, кандидат технічних наук

ОЦІНКА ЖИВУЧОСТІ ТА СТІЙКОСТІ КОМПОНЕНТІВ ІНФОРМАЦІЙНИХ СИСТЕМ ЗА ДОПОМОГОЮ КОГНІТИВНО-ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ

Питання стійкості та живучості інформаційних систем в даний час набуває все більшої актуальності. Більшість існуючих інформаційних систем після введення в експлуатацію піддається різноманітним атакам, та з великою ймовірністю можуть бути зламані, або виведені з ладу. При цьому, якщо злому піддаються інформаційні системи, що обслуговують індустріальні та промислові комплекси (industrial control system – ICS) ризики та масштаби збитків багаторазово збільшуються.

В аналітичному звіті компанії Dragos [1] вказується, що експлойти для ICS систем існують (і активно використовуються) вже більше десяти років, при цьому загальнодоступні експлойти потрапляють до баз даних (наприклад бази даних уразливостей CVE (cve.mitre.org)) протягом приблизно місяца. В цілому, експерти з інформаційної безпеки вказують, що на злом ICS в даний час з'явився попит і в найближчому майбутньому очікується значне збільшення пропозиції ([2]). Найбільш відомими прикладами атак в Україні можуть бути епідемії WannaCry, Petya збої української енергосистеми у 2015 році.

Типово, що розробники промислових та інфраструктурних інформаційних систем, на відміну розробників ПО «загального призначен-

ня», часто запізнюються з реакцією на нові загрози. Наприклад, при аналізі безпеки ICS багато фахівців схильні покладатися на «air gap» – «повітряний зазор», що ізолює ICS від глобальних інформаційно-комунікаційних систем. Простіше кажучи – якщо система, що управляє, не підключена до інтернету – звідти не може здійснюватися атак. При цьому один з перших прикладів атаки – вірус Stuxnet, якраз був побудований на подоланні «повітряного зазору» ([3]). Таким чином на ризик та небезпеку наражаються навіть ICS, які не підключені до глобальних інформаційно-комунікаційних систем.

Для систем ICS характерна складність і різнорідність компонентів – навіть однакові за номенклатурою системи ICS, реалізовані на різних підприємствах будуть нести специфіку роботи і контексту експлуатації і таким чином не буває двох ідентичних ICS. Наприклад, часто має місце практика інтеграції систем ICS у загальну інформаційну систему підприємства (наприклад, інтеграція з ERP – корпоративно-інформаційною системою). При цьому при всіх перевагах, які дає така інтеграція (ефективніше управління, прийняття рішень з урахуванням більшого обсягу інформації, підвищення швидкості реагування на складні ситуації тощо) така інтеграція збільшує поверхню атаки («attack surface») для зловмисників. Кожен елемент, що додається в систему, потенційно має свої власні вразливості, при цьому його інтеграція в загальний простір ICS означає, що зловмисник, використовуючи ці вразливості, може отримати через них доступ до загальної інфраструктури ICS ([4]). Крім цього, загальна складність системи може призводити до того, що відбита, або частково купована атака викличе «ланцюгові реакції» в системі, при яких вихід з ладу одного сегмента може вплинути, або вивести з ладу суміжні сегменти та обрушити систему за рахунок вторинних ефектів.

Виділити ще кілька вразливостей, притаманних сучасним ICS: недостатній пентестинг (тестування на можливість атаки, або несанкціонованого проникнення в систему) або його повна відсутність для впроваджуваних рішень (розробники віддають перевагу простоті та легкості розгортання безпеки системи). Наявність великого відсотка бездротових рішень у керуючих технологіях, що відкриває для потенційних зловмисників можливість атаки навіть без заходу на територію підприємства. Наявність застарілих систем в ICS – промислові системи взагалі виявляють максимальну інерцію щодо модернізації обладнання, відкладаючи її до моменту, коли окупляться початкові інвестиції в інформаційну систему, інколи ж просто до моменту, коли в бюджеті з'являться кошти. Це призводить до парадоксальних ситуацій, коли технологічні компоненти ICS, а часто і проектну документацію неможливо знайти, оскільки розробники вже давно зняли системи з обслуговування – і добре, якщо компанії, що обслуговують, взагалі не пішли з ринку.

Таким чином злом будь-якої ICS системи – лише питання часу. Враховуючи це, а також загальну складність і динамічність факторів впливу на функціонувальну систему ICS, можна зробити висновок, що

живучість та забезпечення стійкості функціонування ICS в умовах зовнішніх атак, загроз та впливу несприятливих факторів, так само як і при «частковому пробої захисту» та ситуації Коли окремі компоненти системи виведені зловмисниками з ладу потрібно, щоб система підтримки прийняття рішень (Decision Support System, DSS), дозволяла оцінювати рівень загрози ризику як для окремих складових ICS, так і для системи в цілому.

На живучість і роботу ICS впливає функціональний стан (справність, надійність, працездатність) агрегатів, що входять до їх складу, структурні аспекти системи – надмірність структура, топологія, склад контекстної «обв'язки», а також керуючі компоненти (здатність системи реагувати на зовнішні керуючі імпульси) та передавати достовірну інформацію про стан системи). При розробці методів оцінки живучості ICS можна виділити три основні категорії, пов'язані з живучістю: структурний, функціональний та керуючий.

Хоча між поняттями «надійність» і «живучість» багато спільного, в даний час прийнято розділяти ці поняття за умовами, в яких функціонує система, що розглядається. Моделі дослідження надійності припускають штатні режими функціонування, моделі дослідження живучості – функціонування системи у позаштатних режимах, що передбачають нерозрахункові зовнішні впливи, що призводять до відмови окремих частин системи, внаслідок їх пошкодження, що характеризує їхню проектну «міцність», захист та стійкість до зовнішніх впливів. У таких граничних умовах моделі відмов елементів, прийнятих у теорії надійності та відмовостійкості не дають необхідних результатів.

Запропонована методика оцінки ризиків та загроз використовує поняття загроз та ризиків у додатку до окремих частин системи.

Загрозою є безрозмірна позамасштабна оцінка вразливості елемента з погляду структурної живучості системи загалом. Вона відображає частку елементів, які залишаться функціонувати після виходу з ладу аналізованого елемента – чим більша ця частка, тим більше елементів торкнеться виходу з ладу даного елемента. Така оцінка спирається на критерій Бірнбаума [5] і використовує як базові поняття про потенційні структурні, функціональні та кібернетичні (керуючі) загрози.

Основою когнітивно-імітаційної моделі системи ICS є орієнтований граф (орграф). Вузли орграфа моделюють компоненти ICS, спрямовані на ребра (дуги) – зв'язки між компонентами.

Залежно від рівня моделювання, така модель карта з різною точністю та достовірністю відображає взаємодію складових системи, при цьому дуги розглядаються як зв'язок її компонентів за ресурсом, що відповідає категоріям живучості системи («енергія» – «інформація» – «речовина»).

На узагальненому рівні оцінюється лише топологія та структура системи загалом – без урахування реальних характеристик її елементів. Така оцінка є свідомо надмірною і моделює «найгірший сценарій» розвитку подій, задаючи «стелю» у системній оцінці ролі та важливості елемента. На рівні оцінки критичності вводиться поняття критичності

– елементам на основі експертної оцінки може бути присвоєно значення, що визначає важливість та критичність функціонування цього елемента у загальній системі ICS. Залежно від зміни критичності елементів з'являється можливість отримати оцінку загрози не за узагальненою, а за реальною системою – з урахуванням ролі та важливості кожного з її елементів. На рівні оцінки надійності, враховується як становище і роль елемента у системі, а й його надійність. Підсумковою інтегральною оцінкою вкладу елемента в живучість системи є ризик – математичне очікування шкоди, який може завдати системі вихід із ладу даного елемента. На реальному рівні моделюється вплив несприятливих факторів на систему, що максимально близько відображає реальність, внаслідок чого з'являється можливість оцінити можливі наслідки ураження тих чи інших елементів комплексу та сценарії розвитку негативних наслідків.

Використання когнітивно-імітаційної моделі системи ICS та методик оцінки структурного, функціонального та керуючого компонентів живучості для розширення існуючих DSS ICS дозволить суттєво підвищити живучість та стійкість експлуатації ICS в умовах впливу зовнішніх атак, помилок персоналу та впливу несприятливих факторів.

Список використаних джерел:

1. Baines J. EXAMINING ICS/OT EXPLOITS: Findings from more than a decade of data: White Paper. – Dragos, Inc., 2021.
2. Friis K., Muller L. P., Gjesvik L. Cyber-weapons in international politics: Possible sabotage against the norwegian petroleum sector // NUPI Report. – NUPI, 2018.
3. Barzashka I. Are cyber-weapons effective? Assessing stuxnet's impact on the iranian enrichment programme // The RUSI Journal. – Taylor & Francis, 2013. – Vol. 158, no. 2. – P. 48–56.
4. Staggs J., Ferlemann D., Shenoi S. Wind farm security: Attack surface, targets, scenarios and mitigation // International Journal of Critical Infrastructure Protection. – 2017. – Vol. 17. – P. 3–14.
5. Rausand M., Høyland A. System reliability theory: Models, statistical methods, and applications, second edition / 2nd ed. – Wiley-Interscience, 2003.

Ключові слова: живучість, ризики, загрози, кібератаки, ICS, industrial control systems, надійність.

Key words: survivability, risks, threats, cyber attacks, ICS, industrial control systems, reliability.