УДК 004.056.5:338.49-021.412.1(043.2)

Єрмак Д. М., здобувач вищої освіти;
Загоруйко Л. В., канд. техн. наук, доцент,
доцент кафедри прикладної математики та кібербезпеки,
Донецький національний університет імені Василя Стуса

ОГЛЯД МЕТОДІВ ТА СПОСОБІВ ПІДВИЩЕННЯ БЕЗПЕКИ ЕКСПЛУАТАЦІЇ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ВІД КІБЕРАТАК

Ключові слова: критична інфраструктура, кібератака, захист від кібератак, інформаційні технології.

Вступ. Широке використання інформаційних технологій породило проблему захисту від протиправних процесів у віртуальному просторі. Кількість кіберінцидентів у всьому світі зростає щороку у півтора-два рази, зокрема комп'ютерних атак на системи управління процесами виробництва та забезпечення життєдіяльності.

Актуальність. Оскільки з огляду на умови експлуатації критична інформаційна інфраструктура є відкритою системою, яка здійснює взаємодію з пов'язаними інформаційними системами, то не виключена реалізація віддаленого деструктивного інформаційного впливу з боку зловмисників. Водночас тривалість підготовки та реалізації деструктивного інформаційного впливу на критичну інфраструктуру може здійснюватися протягом тривалого часу. Втрата працездатності критичної інфраструктури не проявляється миттєво у вигляді стрибкоподібного процесу, а є наслідком зниження якості основних показників її функціонування та їх виходу за межі допусків. Процес зміни показників, що характеризують якість функціонування, займає деякий проміжок часу, який визначається вихідними значеннями показників, а також різними факторами, що впливають на цей процес. Отже, постає завдання підтримки критичної інфраструктури у працездатному стані протягом деякого часу, необхідного для проведення заходів щодо нейтралізації негативних наслідків впливу [1, 2, 3].

Основним джерелом інформації для виявлення цільових атак є аналіз процесу функціонування критичної інфраструктури, а саме мережевого трафіку, подій безпеки, споживаних ресурсів, цілісності об'єктів файлової системи. Деяка частина ресурсів системи критичної інфраструктури виділяється для запису та аналізу трафіку, що дає змогу накопичувати статистичну інформацію для формування еталонної моделі поведінки критичної інфраструктури. Це допомагає контролювати динаміку зміни трафіку та шляхом його моніторингу виявляти ознаки атак. Аналіз мережевого трафіку дає змогу виявляти відправку невизначених пакетів, наявність у мережі комп'ютерів або програм, які не повинні там бути. Події безпеки фіксуються в журналах подій, куди записуються значні події, зокрема помилки та збої в роботі критичної інфраструктури, спроби

некоректного введення даних під час входу в систему, а також усі операції, що здійснюються під обліковим записом [3,4].

Основними ресурсами, що споживаються у процесі функціонування критичної інфраструктури, є процесорний час, пам'ять, канали введення-виведення, периферійні пристрої. Їх моніторинг дає змогу ідентифікувати загрозу в загальному вигляді. Контроль цілісності об'єктів файлової системи дає змогу визначити зміни у використовуваних програмах. Обчислення контрольних сум для всіх важливих бінарних і конфігураційних файлів у системі та порівняння їх з попередніми записами, що зберігаються у базі даних, може попередити про наявність невідповідностей або модифікацій. Організатори цільових атак змінюють файли або об'єкти з метою розміщення шкідливих програм або створення *«back door»,* які дають змогу непомітно здійснювати вхід до системи або підключатися до інших комп'ютерів, а також маскування деструктивного впливу [4].

Також доцільно проводити кібернавчання. Суть кібернавчань полягає в перевірці реагування на загрози, що моделюються. Для аналізу застосування методу моделювання під час проведення масштабних кібернавчань доцільно розглянути та узагальнити досвід США. У процесі стратегічних навчань у створюваній обстановці з дотриманням заходів безпеки розробниками пропонувалися сценарії кібератак, максимально наближені до реальних та потенційних ризиків. На основі підсумків навчань *DHS* розробляються національні кібернавчання та програма підтримки планів реагування на кіберзагрози [5].

Висновки

Вразливість критичної інфраструктури для зовнішніх і внутрішніх кібератак зростає у міру посилення її залежності від інформаційних технологій. Серед таких атак можуть бути і кібертерористичні, що створюють загрози економіці країни, системам зв'язку, комп'ютерним мережам та іншій критично важливій інфраструктурі. Тому питання захисту критичної інфраструктури є важливим для кожної держави.

Список використаних джерел

1. Інформаційна та кібербезпека / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа. Львів: «Магнолія 2006», 2018. 320 с.

2. S. P. Leblanc, A. Partington, I. M. Chapman, M. Bernier. An overview of cyberattack and computer network operations simulation. *Spring Simulation Multi-conference*, Boston, MA, USA, April 03-07, 2011. Vol. 7: Proceedings of the 2011 Military Modeling & Simulation Symposium. URL: https://www.researchgate.net/publication/220953920_An_overview_of_cyber_attack_and_computer_network_operations_simulation

3. Cyber attack modeling and simulation for network security analysis / M. E. Kuhl, J. Kistner, K. Costantini, M. Sudit. 2007 *Winter Simulation Conference.* 2007. P. 1180–1188.

4. Gore R., Padilla J., Diallo S. Markov Chain modeling of cyber threats. *The Journal of Defense Modeling and Simulation*. 2017. № 14(3). P. 233-244. DOI: 10.1177/1548512916683451.

5. Cyber Storm VI: National Cyber Exercise, D.o.H. Security, Editor, 2020. URL: https://www.cisa.gov/cyber-storm-vi-national-cyber-exercise