

УДК 004.942
Давидюк А.В.
асп. ПІМЕ ім. Г.Є. Пухова НАН України

ПОКАЗНИКИ НЕФУНКЦІОНАЛЬНИХ ХАРАКТЕРИСТИК СИСТЕМИ КРИТИЧНОГО ПРИЗНАЧЕННЯ ЯК СКЛАДОВА МОНІТОРИНГУ СТАНУ КІБЕРЗАХИСТУ

З початком активних бойових дій російської федерації на території України у лютому 2022 року, значно збільшилась кількість та потужність атак на об'єкти критичної інформаційної інфраструктури [1]. Метою цих атак є порушення функціонування систем критичного призначення. Безпека таких систем в цей час, окрім стандартних процедур кіберзахисту, потребує підвищеної уваги власних нефункціональних характеристик.

Для уникнення невизначеностей, під терміном нефункціональні характеристика в контексті кіберзахисту будемо розуміти наявність функцій та показників, що не визначені технічною документацією на систему та її складові.

Такі нефункціональні характеристики можуть виникати як внаслідок порушення персоналом правил експлуатації системи, так і внаслідок програмних та апаратних закладок на етапі ланцюгів постачання такого обладнання. Загрози порушення вимог до безпеки експлуатації персоналом мають виключно фізичну природу. Водночас атаки на ланцюги постачання є дуже небезпечними [2].

Попередження виникнення таких загроз здійснюється шляхом експертних випробувань такого технічного забезпечення систем критичного призначення [3]. Проблемами таких випробувань є невідповідність компетенцій експерта розробникам, гарантійні обмеження обладнання тощо. Саме тому важливою складовою кібербезпеки є постійний моніторинг стану систем і виявлення аномалій в їх поведінці: зокрема підвищення аномалії в трафіку, сповільнення в роботі, підвищення температури складових також можуть бути поверхневими ознаками наявності шкідливих програмно-апаратних закладок.

Таким чином, є необхідним розроблення стандартних операційних процедур для моніторингу роботи систем критичного призначення, основою яких стане механізм порівняння елементів множини відмов роботи, визначених технічною документацією, з елементами множини показників нефункціональних характеристик даних систем. Додання статистичного аналізу співпадінь результатів такого порівняння дасть можливість швидше виявляти можливі проблеми кіберзахисту та попереджувати їх появу.

Розроблення математичної моделі з використанням теорії множин [4] дасть можливість створювати вибірки даних для подальшого аналізу їх з використанням технологій штучного інтелекту.

Дослідження проведено згідно планів науково-дослідної роботи, що виконується Інститутом проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України: «Розроблення методів та засобів верифікації артефактів

процесу проектування систем критичного призначення» (Державний реєстраційний номер: 0121U110615; 2021-2022).

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Кібератака групи UAC-0010 (Armageddon) на державні організації України (CERT-UA#4378) [Електронний ресурс]. / 2022. – Режим доступу: <https://cert.gov.ua/article/39138>.

2. Атаки на ланцюг постачання: хто під прицілом та як протистояти [Електронний ресурс]. / 2021. – Режим доступу: <https://cybercalm.org/novyny/ataky-na-lantsyug-postachannya-hto-pid-prytsilom-ta-yak-protystoyaty/>.

3. Наказ № 93 "Про затвердження Положення про державну експертизу в сфері технічного захисту інформації" [Електронний ресурс] / 2007. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/z0820-07#Text>.

4. Михалін Г.О., Елементи теорії множин і теорії чисел / Г.О.Михалін, Л.І.Дюженкова – Київ : НПУ імені М.П. Драгоманова, 2003. – 128 с. – ISBN 966-660-105-2.