УДК 004.057.4:355.451]:004.75

ОГЛЯД БАЗ ДАНИХ ВРАЗЛИВОСТЕЙ ДЛЯ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Назаров Байрамалі Аріф
Науковий керівник – д.т.н., проф. Євдокименко М.О.
Харківський національний університет радіоелектроніки,
каф. ІКІ ім. В.В. Поповського
Харків, Україна
тел. +38(068) 420-39-29

The importance of ensuring the protection of infocommunication networks is due to the need to ensure their stability in the conditions of constant cyber attacks. One of the effective method of ensuring the cyber protection of ICM is a preliminary assessment of information security risk, which can be calculated using the criticality metrics of vulnerabilities specified in the recommendations of the National Institute of Standards and Technology. Criticality metrics of vulnerabilities collected in databases are used to quantify the information security risks of any ICM vulnerabilities. Using these metrics, it is possible to make an accurate assessment of risks, the degree of criticality of vulnerabilities present in ICM, and possible damage due to the use of identified vulnerabilities.

Важливість забезпечення захисту інфокомунікаційних мереж (ІКМ) обумовлена необхідністю забезпечення їх стійкості в умовах здійснення постійних кібератак. Захист будь-якої інфокомунікаційної мережі починається ще на етапі проектування та продовжується під час функціонування. Одним з ефективних засобів забезпечення захисту ІКМ є попередня оцінка ризику інформаційної безпеки, який може розраховуватись за допомогою використання зазначених в рекомендації National Institute of Standards and Technology (NIST) метрик критичності вразливостей [1].

Для оцінки ризику інформаційної безпеки та рівня захищеності ІКМ в цілому можуть використовуватися організаційні стандарти та моніторинг мережі за допомогою мережних сканерів, SIEM-систем та систем виявлення та протидії атакам тощо. Приведені інструменти дозволяють отримати кількісні оцінки безпеки, що базуються на метриках безпеки з прогнозуванням та вимірюванням вразливостей мережі.

На сьогодні існує велика кількість баз даних із вразливостями та пропозиціями щодо їх усунення. Найбільш відомими є 10 баз даних вразливостей, якими користуються для аналізу та оцінці ризику інформаційної безпеки та які представлені нижче [2]:

1. Open Sourced Vulnerability Database є базою із детальну інформацію про всі наявні вразливості та постійним оновленням шляхом реєстрації та валідації нових вразливостей.

2. Vulnerability Intelligence є базою, що пропонує безпеку на основі ризиків для комплексного аналізу вразливостей за допомогою постійного моніторингу в режимі реального часу.

3. Open Vulnerability and Assessment Language є системою звітів про стан інформаційної системи.

4. Exploit Database представляє собою каталог із сценаріями використання вразливостей в інформаційній системи із їх детальним описом.

5. IBM X-Force Exchange представляє собою хмарну платформа обміну розвідувальними даними, що використовується для дослідження останніх загроз, співпраці та консультації з експертами.

6. CXSecurity представляє собою базу даних про вразливості для інформування користувачів про різні помилки в веб додатках.

7. VFeed є базою даних вразливостей, яка використовує специфічну методологію для автоматизованого збору та відстеження та оцінки вразливості для вчасного виявлення, реагування та захисту від кібератак.

8. Secunia Advisory and Vulnerability Database Database представляє собою базу даних з інформаційними бюлетенями, які сформовані експертами Secunia Research та містять відомості про виявлені загрози і вразливості програмного забезпечення.

9. Vulnerability Notes Database (VND) представляє собою базу даних вразливостей мережного обладнання, програмного забезпечення, посилаючись на безліч відповідних CVE ідентифікаторів.

10. Common Vulnerabilities and Exposures – це база даних вразливостей, що містить відомі вразливості обладнання, програмного забезпечення або прошивки, яка допомагає уиувати вразливості, виявляти вторгнення, та управляти інцидентами тощо.

Висновок: Для кількісної оцінки ризиків інформаційної безпеки будь-якої ІКМ використовуються метрики критичності вразливостей, зібраних в бази даних вразливостей у відкритому доступі. Користуючись даними метриками з різних баз можна здійснити точну оцінку ризиків, ступінь критичності наявних в ІКМ вразливостей та можливий збиток внаслідок використання ідентифікованих вразливостей.

Список використаних джерел

1. Hu C. Guidelines for Access Control System Evaluation Metrics [Електронний ресурс] / C. Hu, K. Scarfone // NIST Interagency/Internal Report (NISTIR), National Institute of Standards and T3echnology, Gaithersburg, MD. – 2012. – Режим доступу до ресурсу: https://doi.org/10.6028/NIST.IR.7874 (Accessed March 26, 2021).

2. National Vulnerability Database [Електронний ресурс] – Режим доступу до ресурсу: https://nvd.nist.gov/vuln/data-feeds.