УДК 004.056:621.396

СУЧАСНІ СИСТЕМИ АВТОМАТИЗАЦІЇ УПРАВЛІННЯ МЕРЕЖНОЮ БЕЗПЕКОЮ

Фролов Д.І., Дягілєва М.С.
e-mail: denys.frolov@nure.ua, e-mail: mila.diahilieva@nure.ua
Харківський національний університет радіоелектроніки,
каф. ІКІ ім.В.В. Поповського
м. Харків, Україна

The dynamic threat landscape necessitates the automation of network security management (especially in telecommunications). Modern challenges include the increase in targeted attacks, stricter regulations, and the expansion of the attack surface due to network evolution. The main vendors of security management automation solutions in 5G networks are Ericsson, Nokia, and Huawei. Ericsson Security Manager provides a holistic approach. Systems from Nokia NetGuard and Huawei are its main competitors. Investments in security management automation reduce risks and financial losses.

За останні кілька років було зафіксовано широкий спектр атак на системи GSM, UMTS та LTE, які загрожували конфіденційності користувачів, секретності даних та цілісності бізнесу [1]. Мережі 5G є динамічними та стикаються з постійно змінюваним ландшафтом загроз, тому критично важливо забезпечити їх безпеку для бізнесу та суспільства.

Так, до найбільш відомих випадків кіберінцидентів у телекомунікаційній мережі, які виникли протягом останніх років, відносяться наступні:

- T-Mobile (США): прямі збитки становили 500 млн. долл. США після втрати особистої інформації 76 млн. підписників;
- Vodafon (Португалія): 5 днів масштабного відключення 4G/5G мережі;
- Київстар (Україна): 7 днів масштабного відключення мережі, прямі збитки: 100 млн. долл. США.

Рішення з автоматизації управління мережною безпекою забезпечують захист, виявлення загроз та активну відповідь, а також, уможливлюють ефективний захист мереж з боку операційного центра безпеки (SOC). Перелік таких систем включає (але не обмежується):

- Cisco, Fortinet, PaloAlto, Tufin - зосереджені на рішеннях для мережної безпеки, таких як ngFW, IDS, IPS тощо;
- CrowdStrike - виявлення та реагування на загрози на кінцевих точках (EDR);
- Splunk, Elastic, HP ArcSight - SIEM рішення;
- AWS, Google Cloud, Azure – відповідно, безпека публічної (та гібридної) хмари;

- PaloAlto Prisma, Checkpoint Dome9, AquaSec, StackRox - загальна безпека у хмарі;

- Tenable та Qualys - забезпечують управління вразливостями.

Основні виклики в безпеці мобільних мереж включають зростання тяжкості цілеспрямованих атак, суворіші регуляторні вимоги для захисту критичної інфраструктури та розширення поверхні атаки через еволюцію програмованих відкритих мереж. Це призводить до підвищення ризиків з боку бізнесу та керівників вищої ланки (їхньої особистої відповідальності).

Побудова безпечної мережі 5G вимагає цілісного підходу для захисту кінцевих користувачів, а не зосередження на окремих технічних частинах в ізоляції [2]. До основних вендорів рішень з автоматизації управління безпекою телекомунікаційних 5G мереж відносяться Ericsson, Nokia, Huawei.

Ericsson Security Manager (ESM) є сучасною платформою автоматизації управління кібербезпекою в 5G мережах, що забезпечує потрібний холістичний підхід з автоматизації управління сертифікатами, політиками безпеки, виявлення загроз та швидке реагування на потенційні інциденти. Як результат, ESM, в тому числі, вирішує основне завдання 3GPP для забезпечення наскрізної безпеки в комунікаційній мережі. ESM зосереджується на управлінні безпекою телекомунікаційних додатків або специфічній для телекомунікаційної індустрії безпеці. ESM розроблений з використанням сучасної хмарної архітектури та технологій автоматизації, які краще адаптуються до нових сценаріїв, таких як нарізка (slicing) мереж 5G, multitenancy, багатопостачальницькі мережі, хмарні VNF тощо. Разом з цим, ESM не забезпечує контроль розвинених сталих загроз (APT) [3], що є особливо актуальним в сучасному напруженому світовому контексті.

Nokia NetGuard [4] пропонує набір рішень, що охоплюють подібні випадки використання (але не об'єднані в один продукт, як ESM). Він включає додаткові продукти, що пропонують управління життєвим циклом сертифікатів, віртуальний брандмауер, рішення для захисту від DDoS та IdAM.

Huawei [5] не є прямим конкурентом рішень від Ericsson та Nokia, оскільки не вважається надійним постачальником рішень безпеки в західних країнах. Разом з цим, Huawei пропонує портфель рішень, що включає брандмауери, захист від DDoS та APT, а також, рішення для управління безпекою, що зосереджені в основному на продуктах Huawei.

На стан безпеки постачальника телекомунікаційних послуг (CSP), а також, на рівень потенційних матеріальних та нематеріальних втрат з його боку внаслідок кіберінцидентів (особливо, розвинутих сталих загроз) впливають такі критерії як ринкова капіталізація, річний дохід та кількість клієнтів CSP, кількість та кваліфікація працівників, які залучені до моніторингу та інженерії безпеки, а також, до реагування на інциденти (SOC).

Інвестиції в системи управління кібербезпекою (такі як ESM та Nokia NetGuard для телекомунікаційних мереж) здатні значно знизити ризики загроз, що, в свою чергу, зменшує потенційні фінансові втрати від атак.

Список використаних джерел:

1. The Wiley 5G REF: Security / Editors-in-Chief Rahim Tafazolli, Chin-Liang Wang, Periklis Chatzimisios ; Section Editor Madhusanka Liyanage. – 1st ed. – John Wiley & Sons, Ltd, 2021.

2. Securing 5G networks in an evolving threat landscape / Securing today's 5G networks – Mobility Report - Ericsson. – Ericsson, 2021. – URL: https://www.ericsson.com/en/reports-and-papers/mobility-report/articles/securing-5g-networks (дата звернення: 04.03.2025).

3. Розвинена стала загроза. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Розвинена_стала_загроза (дата звернення: 04.03.2025).

4. NetGuard Cybersecurity Dome / Nokia. – URL: https://www.nokia.com/cybersecurity/xdr/netguard-cybersecurity-dome/ (дата звернення: 04.03.2025).

5. Network Security Products / Huawei. – URL: https://e.huawei.com/hk/products/security (дата звернення: 04.03.2025).