Секція 2

ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ДЛЯ ОЦІНКИ КІБЕРБЕЗПЕКИ ПРОМИСЛОВИХ РОБОТИЗОВАНИХ СИСТЕМ: ВИКЛИКИ ТА РІШЕННЯ

Абакумов А.І.
Національний аерокосмічний університет ім. М.Є Жуковського «Харківський авіаційний інститут»
Науковий керівник Харченко В.С.

Актуальність. Інциденти, спричинені атаками на промислові роботизовані системи (РС) впровдовж останніх років [1,2], свідчать про зростання кіберзагроз і відповідних відмов компонентів РС. Затримки в розробленні та впровадженні стандартів і інструментів для оцінювання та пом'якшення загроз, а також забезпечення кібербезпеки (КБ) РС в цілому, посилюють їх вразливість до кібератак, особливо з огляду на інтеграції з інтернетом речей і хмарними сервісами [3] через великі ризики вторгнення. Брак методів та інструментів оцінювання КБ РС обумовлює наступне [1]:

- відмовлення від впровадження тестування на проникнення (ТнП) може призвести до порушення кібербезпеки розгорнутих програм, включаючи різні компоненти РС;
- відсутність патчів безпеки збільшує ймовірність зловмисних атак, зокрема, викрадення конфіденційних даних, віддалений доступ і руткіт.

Таким чином, для забезпечення ринкової конкурентоспроможності впроваджуваних послуг з урахуванням принципу «нульового інжинірингу» та мінімізації ризиків безпеки, які є невід'ємною частиною впровадження «нульового бізнес-ризику», необхідно надати надійні та зрозумілі гарантії безпеки під час експлуатації систем. Це вимагає поєднання аналітичних та формальних методів, зокрема, IMECA-аналізу (Intrusion Modes and Criticality Analysis) та ТнП з урахуванням специфіки архітектури РС.

Аналіз інформаційних джерел. Автори [1-3] аналізують загрози, вразливості та атаки РС, але не формулють системні вимоги щодо впровадження ТнП спільно з іншими методами. У [4] розроблено метод ТнП, адаптований для інтернету речей шляхом поєднання методоів ТнП та IMECA-аналізу. З огляду на аналіз публікацій, об'єктивними є висновки: по-перше, про відсутність методу ТнП з урахуванням специфікі промислових РС і його недосконаліть для індустріального інтеренту речей; по-друге, необхідності більш системного погляду на задачі ТнП у поєднанні з іншими методами задля обєктивного оцінювання кібербезпеки і функційної безпечності РС.

Метою досліджень є підвищення достовірної оцінки ризиків і надання надійних гарантій функційної та кібербезпеки впродовж експлуатації РС шляхом поєднання методів IMECA та ТнП.

Задачі, які розвязуються задля досягненя мети досліджень**,** полягають у проведенні аналізу інформації про вразливості РС та напрями атак, описі процесу ТнП та IMECA за допомогою функціональної моделі IDEF, наданні прикладу використання IMECA для аналізу вразливостей РС та оцінки ризику атак, а також обґрунтуванні напрямів майбутніх досліджень.

Висновки. У даній роботі зроблений перший крок вирішення проблеми відсутності методів ТнП, адаптованих до специфіки РС, а саме розроблена дворівнева IDEF модель процесу проведення ТнП та детально розглянуто етап впровадження IMECA для аналізу вразливостей РС та оцінювання ризиків успішних кібератак. Подальші дослідження необхідно проводити за напрямом практичного підтвердження дієвості запропонованого методу за допомогою використання реальної РС або її емулятора. Цей процес пропонується розділити на етапи, які дозволяють розглянути окремі компоненти РС, її інфраструктурну частину та зробити наступний крок щодо аналізу КБ і функційної безпечності коботів.

Список літератури

1. *Yaacoub P.A., Noura H.N., Salman O.* Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations // International Journal of Information Security, Vol. 21, PP. 115–158, Режим доступу: https://doi.org/10.1007/s10207-021-00545-8

2. *Pu H., He L., Cheng P., Sun M., Chen J.* Security of Industrial Robots: Vulnerabilities, Attacks, and Mitigations // IEEE Network, Режим доступу: https://doi.org/10.1109/MNET.116.2200034

3. *Bhardwaj A., Avasthi V., Goundar S.* Cyber security attacks on robotic platforms // Network Security, Vol. 2019, No. 10, PP. 13–19, Режим доступу: https://doi.org/10.1016/S1353-4858(19)30122-9

4. *Абакумов А.І., Харченко В.С.* Тестування на проникнення систем Інтернету речей: кіберзагрози, методи та етапи // Electronic Modeling, Vol. 44, No. 4, PP. 79–104, Режим доступу: https://doi.org/10.15407/emodel.44.04.079

Відомості про авторів

Абакумов Артем Ігорович, аспірант кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 095-024-79-98, a.i.abakumov@csn.khai.edu

Харченко Вячеслав Сергійович, завідувач кафедри комп'ютерних систем, мереж і кібербезпеки, д.т.н., професор, v.kharchenko@csn.khai.edu