УДК 004.056.5:004.738.5

Черкас С.А., здобувач,
Ящук В.І., к.екон.н., доцент,
Пановик У.П., к.т.н., доцент
Львівський державний університет безпеки життєдіяльності

ІНТЕГРАЦІЯ ТЕХНОЛОГІЙ БЕЗПЕКИ ДЛЯ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ IOT-СИСТЕМ У ПОБУТОВОМУ СЕРЕДОВИЩІ

Стрімке зростання кількості IoT-пристроїв у побутових мережах створює нові вектори кібератак і підвищує ризики несанкціонованого доступу до персональних даних користувачів. Існуючі стандарти безпеки, зокрема ENISA, NIST та OWASP, здебільшого орієнтовані на корпоративний сектор, що ускладнює їх застосування в умовах обмежених ресурсів побутових систем. Автори сформували інтегровану модель кіберзахисту, яка враховує специфіку домашнього середовища, динамічність підключень та економічні аспекти реалізації безпечного життєвого циклу пристроїв.

Методологічна основа дослідження включає системний підхід до оцінки кіберстійкості IoT-систем, моделювання тестових середовищ (honeypots, sandbox, digital twins), використання емпіричних методів перевірки захисних механізмів і побудову кількісних метрик за п'ятьма доменами: апаратна безпека, мережевий захист, життєвий цикл, приватність і операційна стійкість**.** Вагові коефіцієнти для кожного домену дозволяють адаптувати оцінку під конкретні сценарії – критичні або комфортні пристрої.

Запропонована модель підтримує уніфікований процес тестування: інвентаризація пристроїв, базове сканування вразливостей, функціональні та атакуючі тести, вимірювання показників відновлення (MTTR), детекції інцидентів та ефективності контрзаходів. Верифікація здійснюється через повторні експерименти та кореляцію результатів. Особливу увагу приділено етичним аспектам проведення експериментів, забезпеченню конфіденційності даних і дотриманню принципів відповідального розкриття вразливостей (responsible disclosure).

Економічна складова дослідження базується на поєднанні моделей Total Cost of Ownership (TCO) і Cost–Benefit Analysis, що дає змогу оцінити економічну доцільність заходів кіберзахисту. Передбачено впровадження маркування рівня безпеки («security label»), яке стимулює виробників до пролонгованої підтримки продуктів і підвищення довіри користувачів. Пілотне дослідження включає 20–30

пристроїв п’яти типів, охоплює типові топології домашніх мереж та різні сценарії атак (brute-force, MITM, експлуатація CVE, DDoS тощо).

Результати валідації підтверджують відтворюваність запропонованої методології та її ефективність у кількісній оцінці безпеки IoT-екосистем. Формування стандартизованих рейтингів безпеки пристроїв створює передумови для розвитку регуляторних вимог, а відкритий науковий репозиторій результатів забезпечує прозорість і доступність методики для подальших досліджень.

Запропонована комплексна модель захисту IoT-пристроїв у побутовому середовищі поєднує технічні, поведінкові та економічні підходи до забезпечення кіберстійкості. Її основою є кількісно-орієнтована методологія оцінки безпеки, що дозволяє уніфікувати процес тестування, формувати порівняльні рейтинги пристроїв і розробляти практичні рекомендації для виробників, користувачів і регуляторних органів. Впровадження запропонованої моделі сприятиме підвищенню конфіденційності, цілісності та доступності даних у побутових IoT-мережах, а також розвитку стандартів і політик кіберзахисту споживчих технологій.

Список використаних джерел:

1. ENISA – Guidelines for Securing the Internet of Things (2020) doi: 10.2824/314452.

2. NIST – Cybersecurity for IoT / Consumer IoT Cybersecurity (SP-серія, 2022 і суміжні документи). Електронне видання. Режим доступу: https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program.

3. OWASP – Internet of Things Project / IoT Top 10 Електронне видання. Режим доступу: https://owasp.org/www-project-internet-of-things/

4. Пановик У. П., Кутас С.А. Інтернет речей для інтелектуального поліграфічного виробництва. Поліграфія і видавнича справа, № 1(87),2024, С. 61–74. URL: https://doi.org/10.32403/0554-4866-2024-1-87-61-74.

5. Пановик У. П. Кібербезпека в телекомунікаційних мережах та системах. Наукові записки, № 1(68), 2024, С. 122–135. URL: https://doi.org/10.32403/1998-6912-2024-1-68-122-135

7. Пановик У. П. Стандартизація інтернету речей: сучасний стан та перспективи розвитку. Поліграфія і видавнича справа. 2023. № 1 (85). С. 51–64. URL: https://doi.org/10.32403/0554-4866-2023-1-85-51-64.