1. Tymoshchuk, D., Zagorodna, N., Klots, Y., Yatskiv, V., Petliak, N. AutoML and explainable AI-based approach to enhance the efficiency and interpretability of IDS. CEUR Workshop Proceedings, 2025, 4163, pp. 231-246
2. Tymoshchuk, D., Sverstiuk, A., Klots, Y., Petliak, N., Titova, V. An explainable artificial intelligence approach for detecting network attacks. CEUR Workshop Proceedings, 2025, 4141, pp. 38-51

Застосування нечітких продукційних правил для контекстно-довірчого оцінювання кіберризиків у середовищі Інтернету речей

УДК 621.395.7 (043.2)

Підлісний Юрій[1], Шелест Михайло[2]

Національний університет «Чернігівська політехніка», [1]ypodlesny@ukr.net

Стрімкий розвиток Інтернету речей (IoT) призвів до масового впровадження інтелектуальних пристроїв у різних сферах, що супроводжується зростанням кіберзагроз через обмежені ресурси та спрощені механізми захисту [1].

Традиційні методики оцінювання ризиків орієнтовані на класичні інформаційні системи та недостатньо ефективні в IoT через динамічність середовища, гетерогенність пристроїв та неповноту даних [2]. У таких умовах доцільним є застосування методів нечіткої логіки, які дозволяють працювати з експертними оцінками та невизначеними параметрами [3].

У роботі запропоновано підхід до оцінювання кіберризиків у середовищі IoT на основі нечітких продукційних правил типу IF–THEN (табл.1). Наведена база правил є фрагментом знань, який може бути розширений або адаптований залежно від специфіки IoT-середовища та моделі загроз.

Таблиця 1

Фрагмент бази нечітких продукційних правил

№	Правило	Результат
1	IF V = High AND T = High AND D = Low THEN R = Critical	Критичний
2	IF V = Medium AND T = High THEN R = High	Високий
3	IF V = Low AND T = Medium AND D = High THEN R = Medium	Середній
4	IF S = High AND V = Low THEN R = Low	Низький
5	IF A = High AND T = Medium THEN R = High	Високий
6	IF C = High AND V = Medium THEN R = High	Високий
7	IF S = Low AND T = High THEN R = Critical	Критичний

Запропонована модель враховує технічні характеристики вузлів, стан середовища та достовірність даних, що забезпечує її застосування як у статичних, так і в динамічних IoT-системах.

Вхідними параметрами моделі є: рівень вразливості (V), інтенсивність загроз (T), рівень захищеності (S), критичність активу (C), мережева аномальність (A) та довіра до джерела даних (D). Вихідною змінною є інтегральний показник ризику R, що характеризує ступінь небезпеки для конкретного вузла, підсистеми або сегмента мережі.

$$R = \Psi(V, T, C, S, A, D) \quad (1)$$

де Ψ – оператор нечіткого логічного виведення.

Для отримання числового значення ризику використовується процедура дефазифікації методом центру ваги [3]:

$$R = \frac{\sum_{i=1}^{n} \mu_i x_i}{\sum_{i=1}^{n} \mu_i} \quad (2)$$

де μ_i – ступінь належності вихідного терма, x_i – відповідне значення шкали ризику.

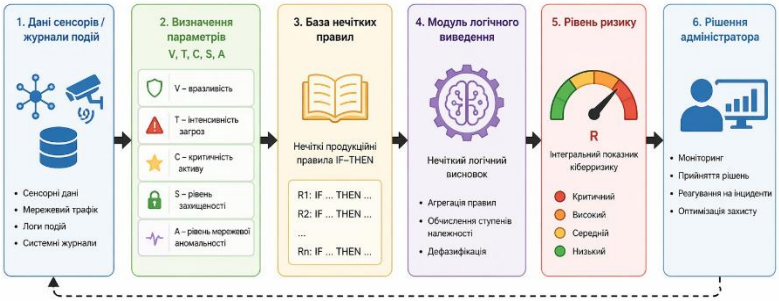

Рис.1 Структурна схема оцінювання кіберризику в IoT-середовищі

Наукова новизна. Полягає у переході від класичного оцінювання кіберризику на основі статичних параметрів до контекстно-залежної моделі, яка враховує не лише значення параметрів, але й ступінь довіри до джерел їх отримання. Запропонований підхід вводить мета-параметр довіри як фактор, що впливає на інтерпретацію вхідних даних, що дозволяє оцінювати ризик в умовах неповної, суперечливої або потенційно спотвореної інформації.

Контекст безпеки моделі. Особливу увагу слід приділити сценаріям навмисного спотворення вхідних параметрів, коли атакуючий впливає не безпосередньо на систему, а на дані, що використовуються для оцінювання ризику. У таких умовах параметр довіри до джерела інформації дозволяє враховувати можливість компрометації сенсорів, каналів передачі або систем моніторингу, що забезпечує більш стійке оцінювання ризику в умовах інформаційного впливу.

Практична цінність. Полягає у можливості використання запропонованої моделі в системах моніторингу безпеки та підтримки прийняття рішень у середовищах Інтернету речей. Модель дозволяє адаптивно оцінювати ризики з урахуванням динамічних змін середовища, неповноти даних та рівня довіри до джерел інформації, що особливо важливо для систем із розподіленою архітектурою та обмеженими ресурсами. Перспективним напрямом є дослідження атак, спрямованих на спотворення параметрів оцінювання ризику.

Висновки. Запропонований підхід дозволяє перейти від статичних моделей оцінювання вразливостей до адаптивного аналізу кіберризиків, який враховує як технічні характеристики системи, так і контекст її функціонування.

Введення параметра довіри до джерел даних розширює можливості моделі в умовах невизначеності та потенційного інформаційного впливу, що робить її придатною для застосування в сучасних кіберфізичних системах.

1. Roman R., Lopez J. Security in the Internet of Things: Current status and future challenges // Computer Networks. 2021.
2. Information security, cybersecurity and privacy protection — Guidance on managing information security risks : ISO/IEC 27005:2022. Geneva, 2022.
3. Zadeh L. Fuzzy sets // Information and Control. 1965. Vol. 8 / 3. P. 338–353.

Модифікація шифру Present

УДК:004.056.55

Володимир Лужецький[1], Тетяна Кирилащук[2]

Вінницький національний технічний університет,
[1]lva.kzi2002@gmail.com, [2]kgt0998@gmail.com

Алгоритм PRESENT є легковаговим блоковим шифром [1, 2], що базується на SP-мережі та складається з операцій підстановки та перестановки бітів. Операції підстановки реалізуються з використанням 16-ти однакових S-блоків, що складаються з логічних елементів, а перестановки бітів реалізуються фізичним розташуванням зв'язків. Крім того, для розгортання ключа використовується ще один S-блок. Оскільки S-блоки є необоротними, то для розшифрування використовуються інші S-блоки. Разом із перевагами алгоритму PRESENT існують і певні недоліки, пов'язані зі структурою S-блоків та кількістю раундів шифрування. У стандартній реалізації в кожному раунді використовуються однакові S-блоки, що значно спрощує апаратну реалізацію алгоритму, однак створює повторювану криптографічну структуру. Така регулярність може негативно впливати на стійкість алгоритму до окремих видів криптоаналізу, зокрема лінійного та диференціального. Ще одним недоліком є необхідність використання окремих інверсних S-блоків для процесу розшифрування. Для досягнення достатнього рівня нелінійності та дифузії даних використовується 31 раунд перетворень щоб компенсувати використання однакових S-блоків у всіх раундах.

З метою підвищення ефективності алгоритму шифрування у доповіді пропонується використовувати різні S-блоки, побудовані на основі латинських квадратів та перестановки змінних для S-блоків. Використання різних нелінійних перетворень у різних раундах дозволяє ускладнити криптоаналітичні залежності між ними та потенційно забезпечити необхідну криптографічну стійкість при меншій кількості раундів. Такий підхід може сприяти пришвидшенню процесу шифрування, зменшенню затримок обробки даних та підвищенню продуктивності алгоритму в ресурсно-обмежених системах, зокрема в IoT-пристроях та вбудованих інформаційних системах.

Пропонується для реалізації S-блоків використовувати латинські квадрати 4-го порядку. Оскільки, існує 576 таких латинських квадратів [3], то є можливість вибрати з них 16, які забезпечать побудову оборотних S-блоків. Як