УДК 004.056.5
DOI: 10.31891/CSIT-2020-2-8

ЛИСЕНКО С. М., КОНДРАТЮК А. С.
Хмельницький національний університет

МЕТОД ОЦІНКИ РИЗИКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КІБЕРФІЗИЧНИХ СИСТЕМ НА ОСНОВІ ВЗАЄМОЗАЛЕЖНОСТІ ВРАЗЛИВОСТЕЙ

Оцінка ризику - гарантія забезпечення безпечної та стабільної роботи кіберфізичної системи. В даній статті представлено новий метод оцінки ризику інформаційної безпеки кіберфізичних систем на основі взаємозалежності вразливостей. В роботі представлено метод оцінки ризику атак на кіберфізичні системи, який уможливлює кількісне визначення ризиків. Крім того, враховано рівень імовірності успішної атаки обчислюється з урахуванням взаємозалежного взаємозв'язку між вразливостями, а рівень впливу атаки враховує наслідки на кіберфізичну систему, що спричинюються в результаті кібератак.

Запропонований метод дозволяє розрахувати потенційний ризик системи та визначити оптимальну мету атаки. Крім того, він може бути розширений і до аналізу інвестицій в безпеку.

Ключові слова: кіберфізична система, інформаційна безпека, вразливість, атака.

LYSENKO S., KONDRATYUK A.
Khmelnytskyi National University, Khmelnytskyi, Ukraine

TECHNIQUE FOR THE RISK ASSESSING OF THE CYBERPHYSICAL SYSTEMS' INFORMATION SECURITY BASED ON THE VULNERABILITIES' INTERCONNECT

Information security has been growing steadily in recent times. Every organization depends on information technology and information security of cyberphysical systems to successfully perform its work. This has become not just a condition for the stability of doing business, but the most important strategic factor for its future development, even in the current, very turbulent environment. Cyberphysical systems can contain a wide variety of entities, ranging from office networks, financial and personnel systems to highly specialized systems.

The rapid development of cyber-physical systems has become due to the large number of cyberattacks, which have become one of the most powerful threats to the security of cyber-physical systems. Many studies have been conducted on the risk assessment method, and limited work has been published on quantifying the security risk of cyber-physical systems. In this paper, a technique for the risk assessing of the cyber-physical systems' information security based on the vulnerabilities' interconnect is proposed.

Technique operates with two indicators to quantify the risk: the probability of attack success and the index of the consequences of the attack based on the graph of the vulnerability. The first indicator - the index of the probability of a successful attack is calculated taking into account the interdependencies between vulnerabilities, the second indicator when calculating the index of the consequences of the attack takes into account the impact on the physical area resulting from cyberattack. A quantitative experimental example showed whether a system risk and an optimal attack target are possible. The proposed method can also be extended for security to investment analysis.

Keywords: cyber-physical system, cybersecurity, vulnerability inter-dependency graph, risk assessment

Вступ

Інформаційна безпека за останні часи безперервно росла. Кожна організація залежить від інформаційних технологій та інформаційної безпеки кіберфізичних систем для успішного виконання своєї роботи. Це стало не просто умовою стабільності ведення бізнесу, а найважливішим стратегічним чинником для його майбутнього розвитку, навіть в нинішніх, дуже турбулентних умовах. Кіберфізичні системи можуть містити дуже різноманітні суб'єкти, починаючи від офісних мереж, фінансових та кадрових систем до дуже спеціалізованих систем [1, 2].

Разом з тим рівень кіберфізичної безпеки в різних організаціях сильно відрізняється. Тільки 39% українських компаній відзначили, що вони підготовлені до кібератак, а 31% респондентів не змогли оцінити таку готовність. Це говорить про те, що кіберфізичій безпеці не приділяється належної уваги. У світі ж 68% керівників впевнені, що їхня компанія здатна впоратися з будь-якою кібератакою [3].

Кіберфізичні системи містять в собі взаємозалежні цифрові, аналогові, фізичні та людські компоненти, спроектовані для роботи за допомогою інтегрованої фізики та логіки. Кіберфізичні системи (Cyber-Physical System, CPS) – це інтелектуальні системи, до складу яких входять природні об'єкти та штучні підсистеми, що дозволяють визначати їх як єдине ціле. Вбудовані комп'ютери та мережі контролюють і керують фізичними процесами, впливають на обчислення і навпаки [4].

Кіберфізичні системи тепер широко використовується в найважливіших інфраструктурах, таких як зв'язок, електроенергетика, транспорт та нафтова промисловість. У міру наближення до масштабного впровадження IT-технологій у цих секторах та автоматичного управління, будь-які цифрові загрози, які можуть виникнути, матимуть відчутний вплив на реальний світ та його процес [5].

Потенційне вторгнення в мережу з боку противників може призвести до різних серйозних наслідків в інтелектуальній мережі, від витоку інформації про клієнта до каскаду збоїв [6]. Таким чином, вирішення питань безпеки кіберфізичних систем є дуже важливим. Оцінка та аналіз ризиків мають високий потенціал для вирішення цих проблем.

Пов'язані роботи

На сьогодні в кіберфізичній системі практикуються кількісні методи оцінки ризиків, такі як оцінка ризику ймовірності, дерева атак, графік атак та сітка Петрі. Метод оцінки ризику, заснований на оцінці

ймовірнісних ризиків для систем інтелектуальних мереж, запропонованих у роботі [7]. У оцінці ризику ймовірностей рівні ризику для безпеки обчислюються ймовірністю виникнення подій кібербезпеки, ймовірністю інцидентів, викликаних подіями, та пов'язаними з ними втрат потужності. Але оцінка ризику ймовірностей має труднощі з визначенням ймовірностей потенційних інцидентів із безпекою, яких немає в базі даних історії.

Метод, запропоновий в роботі [8], забезпечує ефективний спосіб моделювання сценаріїв атак та кількісного визначення оцінки ризику кібербезпеки кіберфізичних систем за допомогою дерева атак.

У роботі [9] автор представляє дерево контрзаходів, що дозволяє провести імовірнісний аналіз на основі комбінаторної моделі. Але формулювання дерев атаки не показує послідовність, в якій листя атаки проникають в сценарій.

У [10] запропоновано ігрово-теоретичну основу для моделювання кіберфізичної безпеки з точки зору узгодженої кібератаки. Але за допомогою цього методу важко визначити кінцеву мету нападника. Забезпечення кіберфізичних систем виходить за рамки забезпечення окремих компонентів системи. Вмотивовані супротивники часто використовують взаємозалежність вразливостей для проведення багатоступеневих атак. Кожен аспект атаки може не становити серйозної загрози для відповідного компонента, однак комбінований ефект може бути катастрофічним. Більшість наявних методів розглядають лише атомну атаку (тобто атаку на одній стадії), але не враховують взаємозалежних зв’язків між вразливими місцями.

Для розв’язання цієї проблеми в цій роботі пропонується метод кількісної оцінки ризику кібербезпеки кіберфізичних систем з урахуванням взаємозалежності вразливих місць. Для кількісного виміру ризику було залучено дві показника: індекс імовірності успішної атаки та індекс впливу атаки. Крім того, метод враховує також вплив на фізичну область, спричинену кібератаками.

Метод оцінки ризику інформаційної безпеки кіберфізичних систем на основі взаємозалежності вразливостей

Вразливості - неспроможність системи протистояти спричиненій певній загрозі або сукупності загроз. Якщо вразливість знаходиться в хості, це створює серйозні загрози безпеці, оскільки супротивник може використовувати її для отримання несанкціонованого доступу до системи. Деякі вразливості взаємозалежні. Це означає, що противник може атакувати інші хости, використовуючи взаємозалежність між вразливими місцями.

Мережа, базується на основі залежності вразливості, являє собою граф залежності вразливості. На графі вразливості розглядаються як вузли, а ребра представляють односторонні залежності між вразливими місцями. Для кожного ребра вузол призначення залежить від його вихідного вузла. Граф залежностей уразливості може бути заданий як спрямований ациклічний граф

$VG = (S_i, \tau_i, P_i, L_i)$,

де S - це набір вершин, що представляють уразливості системи, τ - це набір ребер (дуг), які представляють зв'язки між вразливими місцями.

Існує ймовірність P_i, пов'язана з кожною вершиною, що представляє ймовірність успішної атаки. Існує вплив атаки L_i, пов'язаний з кожною вершиною, який представляє значення втрат у грошових одиницях, коли вершина була успішно атакована. Один перехід від вузла S_j до вузла S_{j+1}, являє собою перехід стану, як правило, викликаний діями супротивника. Кожен шлях в графі атак призводить до небажаного стану, наприклад, той, який представляє зловмисника, який отримує доступ адміністратора до компонента управління. Послідовність переходу $S_0, S_1, \dots, S_n$, що складає $(S_i, S_{i+1}) \in \tau,\ 0 \le i \le n-1$ та $S_0 \in S_s \in S_0$ являє собою шлях атаки.

Таким чином, ризики шляхів атаки можуть бути обчислені з ймовірностей і очікуваних втрат, пов'язаних з кожною вершиною в графі атаки. Отже ризик системи можна обчислити наступним чином:

$$R_v = (\prod_{i=1}^{n} P_i) \times C_i \quad (1)$$

$$\overline{R_v} = R_v \,/\, p = [(\prod_{i=1}^{n} P_i) \times C_i]/p \quad (2)$$

де, R_v, - ризик атаки шляху *v;* $\overline{R_v}$, - одиничний ризик шляху атаки *v*. P_i, - ймовірність успішної атаки від вузла S_j до вузла S_{j+1}, C_i - наслідок, спричинений успішною атакою. *n* - кількість вразливостей на шляху атаки. *p* - кроки на шляху атаки.

Обчислення ймовірності успіху атаки

Ймовірність успіху атаки - це ймовірність успішного використання вразливостей. Вона може бути оцінена сприйнятливістю вразливості, яка залежить від таких елементів, як складність, експлуатація та рівень відновлення. Загальна система оцінювання вразливості (CVSS) забезпечує спосіб обліку основних характеристик вразливостей та отримання числової оцінки, що зображає її сприйнятливість [11]. Імовірність успішної атаки можна розрахувати наступним чином:

$$P_i = \frac{Ac_i \times Av_i \times PR_i / RE_i}{\sum_{i=1}^{m} (Ac_i \times Av_i \times PR_i / RE_i)} \quad (3)$$

де, *Ac* позначає складність атаки, описує умови поза контролем зловмисника, які повинні існувати для того, щоб використовувати вразливість.

Значення показника є найбільшим для найменш складних атак. *Av* позначає вектор атаки, він

зображає контекст, за допомогою якого можлива експлуатація вразливості. Це значення показника буде тим більшим, чим віддаленішим може бути зловмисник, щоб скористатися вразливістю. *PR* позначає необхідні привілеї, описує рівень привілеїв, якими повинен володіти зловмисник, перш ніж успішно використовувати вразливість. Цей показник найбільший, якщо не потрібні привілеї. *RE* позначає рівень відновлення. Імовірність успішної атаки вразливості визначається не лише фундаментальними характеристиками самої уразливості, але і ймовірністю її джерела вразливості.

Кількість та ймовірність успішної атаки її вразливих джерел сприяють успішності атаки вразливості цілі. Алгоритм *Pagerank* - це алгоритм сортування веб-важливості, його основна ідея полягає в тому, що веб-сайти з більш важливими посиланнями важливіші за інші [9]. Важливість веб-сторіноки пов'язана з кількістю та якістю пов'язаних веб-сторінок. На основі застосування алгоритму pagerank, ймовірність успішних атак можна оцінити за формулою (4).

$$P_j` = P_j + \lambda(\frac{P_1(j)}{L_{out}(1)} + \cdots + \frac{P_n(n)}{L_{out}(n)}) \quad (4)$$

де P_j - ймовірність успішної атаки вразливості j; $P_1(j), P_2(j), \dots, P_n(n)$ є ймовірністю успішної атаки вихідних вразливостей, які пов'язані з уразливістю *j*. $L_{out}(n)$ - кількість посилань із вразливості джерела *n*; *n* - загальна кількість вразливих місць, λ - регулюючий фактор, який використовується для регулювання ефекту вразливості джерела.

Обчислення значення пливу атаки

В кіберфізичних системах оператори контролюють стан роботи системи за допомогою сигналів монітора та змінюють алгоритми та параметри керування через віддалені сигнали. У фізичній області контрольні компоненти отримують сенсорні сигнали та посилають керуючі сигнали на основі віддалених сигналів, які безпосередньо впливають на керований процес.

Управління та сигнали передачі (сенсорні сигнали, сигнали управління, сигнали монітора та віддалені сигнали) працюють разом, щоб забезпечити загальні функціональні можливості системи. Різні атаки призводять до різного роду наслідків.

Деякі результати призводять до зловживань доступом, які заважають операторам контролювати пристрої. Деякі з них призводять до порушення цілісності, наприклад зміна даних з давачів, що передаються в центр управління. Інші пов'язані зі зловживанням конфіденційністю, наприклад з розголошенням пароля користувача. Кібератаки проти CPS можна класифікувати на чотири типи:

1. Кібератаки, спрямовані на наявність фізичних компонентів.
2. Кібератаки, націлені на наявні компоненти системи.
3. Кібератаки, спрямовані на порушення цілісності переданих в системі даних
4. Кібератаки, націлені на конфіденційність компонентів.

Під впливом атаки вважатимемо значення від 1 до 10, яке вказує на вплив успішної атаки на систему. Загалом, три атрибути параметрів, що допомагають визначити атаку-вплив: ймовірність успішного виявлення, тип режиму використання і вартість активу. Атака-вплив можна обчислити так:

$$L_i = (1 - \rho_i) \cdot Value_i \cdot \delta$$

де p_i є успішною ймовірністю виявлення. $Value_i$- вартість активів хостів, яким належить використовувана уразливість. δ - вага різних режимів використання.

На відміну від IT-систем, інциденти безпеки CPS можуть спричинити жертви або завдати шкоди навколишньому середовищу [8]. Тим часом пошкоджені пристрої потребують великої кількості робочої сили та матеріальних ресурсів. Тому, крім врахування економічних втрат, кількісна оцінка вартості активів повинна враховувати також жертви, екологічні збитки та витрати на ремонт.

Експерименти

З метою оцінки здатності оцінки ризиків атак було проведено ряд експериментальних досліджень. З цією метою було залучено систему тестів [11]. Тестове середовище включало в себе компоненти: три підмережі, підключені до мережі Інтернет, сервер та брандмауер. Системи можуть отримати доступ лише до сервера баз даних у підмережі 1 та до файлового сервера в підмережі 3. Керуючий компонент 1 у підмережі 2 може отримати доступ до файлового сервера в підмережі 3.

Хости тієї ж підмережі можуть оцінювати один одного. Інформація про вразливість в системі може бути отримана за допомогою інструментів сканера вразливостей, а взаємозалежні зв’язки між вразливостями визначаються відповідно до досвіду експертів.

Граф залежності вразливості може бути створений на основі вищевказаної імітаційної мережі. Він має дев'ять вузлів і дванадцять ребер. Використавши формулу обчислення ймовірності успішної атаки було одержано результати , подані в таблиці 1 та таблиці 2.

В якості мети атаки в цій модельованої мережі передбачається використовувати уразливості 3187, 3886 і 4032 бази [11-14]. Таким чином, існує десять можливих шляхів атаки. У реальній ситуації кожен крок атаки має свою ціну. Таким чином, атака припиниться, якщо крок перевищить певне число.

В експериментальних дослідженнях було визначено шляхи здійснення атаки. В результаті можливим є здійснення атаки шістьома шляхами. Ризик шляху та ризик одиничного шляху можна обчислити за формулами (1)-(4), а результати показані в таблиці 2.

Результати експериментів продемонстрували, що найбільш імовірною та успішною атакою може бути атака експлойтом, що використовує вразливість 4173, а також атаки, що ґрунтуються на застосуванні вразливостей 3271 та 3187 в IP2.

Таблиця 1.

Рівень впливу атаки на кіберфізичну систему та ймовірність здійснення успішної атаки на основі застосування вразливостей

Вразливість	Рівень впливу атаки на кіберфізичну систему	Ймовірність здійснення успішної атаки
1299	8	0,54
3271	9	0,43
5409	5	0,32
4173	9	0,69
2231	4	0,34
3187	10	0,33
1219	6	0,22

Таблиця 2.

Рівень впливу атаки на кіберфізичну систему та ймовірність здійснення успішної атаки на основі застосування вразливостей

Номер шляху атаки на основі застосування вразливостей	Послідовність застосування вразливостей	Оцінка ризику атаки
1	1299->3271->4173->1219	0,54
2	1299->3271->3187->1219	0,43
3	1299->4173->2231->1219	0,32
4	1299->5409->4173->2231	0,69
5	1299->3271->5409->1219	0,34
6	1299->5409->4173->3187	0,33
7	1299->4173->2231->3187	0,22

Висновок. Оцінка ризику - гарантія забезпечення безпечної та постійної роботи кіберфізичної системи. В роботі представлено новий метод оцінки ризику атак на кіберфізичні системи, який уможливлює кількісне визначення ризиків. Крім того, індекс імовірності успішної атаки обчислюється з урахуванням взаємозалежного взаємозв'язку між вразливостями, а індекс впливу атаки враховує вплив на фізичну область, що виникає в результаті кібератак.

Запропонований метод дозволяє розрахувати потенційний ризик системи та визначити оптимальну мету атаки. Крім того, він може бути розширений і до аналізу інвестицій в безпеку. Для подальших досліджень відкриті кілька напрямків. Оптимальна схема посилення буде запропонована на основі визначення ключової уразливості.

Література

1. Лисенко С.М., Бобровнікова К.Ю., Харченко В.С. Методи виявлення бот-мереж в комп'ютерних системах. Сучасні інформаційні системи. 2019. Т.3. №4. С.87-95.

2. Agyepong, Enoch & Buchanan, William & Jones, Kevin. (2018). Detection of Algorithmically Generated Malicious Domain Using Frequency Analysis. International Journal of Computer Science and Information Technology. 10. 91-111. 10.5121/ijcsit.2018.10306.

3. B. Craggs and A. Rashid, "Smart Cyber-Physical Systems: Beyond Usable Security to Security Ergonomics by Design," 2017 IEEE/ACM 3rd International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS), Buenos Aires, 2017, pp. 22-25, doi: 10.1109/SEsCPS.2017.5.

4. H W. Wu, R. Kang and Z. Li, "Risk assessment method for cyber security of cyber physical systems," 2015 First International Conference on Reliability Systems Engineering (ICRSE), Beijing, 2015, pp. 1-5, doi: 10.1109/ICRSE.2015.7366430.

5. Chen, Thomas M., and Saeed Abu-Nimeh. "Lessons from stuxnet." Computer, vol. 49, no. 4, pp. 91-93,2017.

6. Han C., Zhang Y. CODDULM: an approach for detecting C&C domains of DGA on passive DNS traffic. 6-th International Conference on Computer Science and Network Technology, Dalian, China, Oct 2017. P. 385–388.

7. X. Chu, M. Tang, H. Huang and L. Zhang, "A security assessment scheme for interdependent cyber-physical power systems," 2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS), Beijing, 2017, pp. 816-819, doi: 10.1109/ICSESS.2017.8343036.

8. Xie, Feng, et al. "Security Analysis on Cyber-physical System Using Attack Tree." In Intelligent Information Hiding and Multimedia Signal Processing, 2013 Ninth International Conference on. IEEE, pp. 429-432.

9. Xin XU, Huiqun Yu, Junhu Huang. " Petri net based security quantitative analysis model for cyber-physical system. " Computer Engineering and Applications,vol.50,no.3, pp.82-88. 2014.

10. Frei, Stefan, et al. "Large-scale vulnerability analysis."In Proceedings of the 2006 SIGCOMM workshop on Largescale attack defense. ACM, pp. 131-138.

11. E. Pavlenko and D. Zegzhda, "Sustainability of cyber-physical systems in the context of targeted destructive influences," 2018 IEEE Industrial Cyber-Physical Systems (ICPS), St. Petersburg, 2018, pp. 830-834, doi: 10.1109/ICPHYS.2018.8390814.

12. Лисенко С. М. Метод забезпечення резильєнтності комп'ютерних систем в умовах кібер-загроз на основі самоадаптивності. Радіоелектронні і комп'ютерні системи. 2019. №4. С. 4–16.

13. Лисенко С. М., Харченко В.С., Бобровнікова К.Ю., Щука Р. Резильєнтність комп'ютерних систем в умовах кіберзагроз: Онтологія та таксономії. Радіоелектронні і комп'ютерні системи. 2020. №1. С. 17-28.

14. Лисенко С. М. Моделі кібератак мережного та хостового типу. Вимірювальна та обчислювальна техніка в технологічних процесах. 2019. №2. С. 58-63.

References

1. Lysenko S.M., Bobrovnikova K.Iu., Kharchenko V.S. Metody vyiavlennia bot-merezh v kompiuternykh systemakh. Suchasni informatsiini systemy. 2019. T.3. №4. S.87-95.

2. Agyepong, Enoch & Buchanan, William & Jones, Kevin. (2018). Detection of Algorithmically Generated Malicious Domain Using Frequency Analysis. International Journal of Computer Science and Information Technology. 10. 91-111. 10.5121/ijcsit.2018.10306.

3. B. Craggs and A. Rashid, "Smart Cyber-Physical Systems: Beyond Usable Security to Security Ergonomics by Design," 2017 IEEE/ACM 3rd International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS), Buenos Aires, 2017, pp. 22-25, doi: 10.1109/SEsCPS.2017.5.

4. H W. Wu, R. Kang and Z. Li, "Risk assessment method for cyber security of cyber physical systems," 2015 First International Conference on Reliability Systems Engineering (ICRSE), Beijing, 2015, pp. 1-5, doi: 10.1109/ICRSE.2015.7366430.

5. Chen, Thomas M., and Saeed Abu-Nimeh. "Lessons from stuxnet." Computer, vol. 49, no. 4, pp. 91-93,2017.

6. Han C., Zhang Y. CODDULM: an approach for detecting C&C domains of DGA on passive DNS traffic. 6-th International Conference on Computer Science and Network Technology, Dalian, China, Oct 2017. P. 385–388.

7. X. Chu, M. Tang, H. Huang and L. Zhang, "A security assessment scheme for interdependent cyber-physical power systems," 2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS), Beijing, 2017, pp. 816-819, doi: 10.1109/ICSESS.2017.8343036.

8. Xie, Feng, et al. "Security Analysis on Cyber-physical System Using Attack Tree." In Intelligent Information Hiding and Multimedia Signal Processing, 2013 Ninth International Conference on. IEEE, pp. 429-432.

9. Xin XU, Huiqun Yu, Junhu Huang. " Petri net based security quantitative analysis model for cyber-physical system. " Computer Engineering and Applications,vol.50,no.3, pp.82-88. 2014.

10. Frei, Stefan, et al. "Large-scale vulnerability analysis."In Proceedings of the 2006 SIGCOMM workshop on Largescale attack defense. ACM, pp. 131-138.

11. E. Pavlenko and D. Zegzhda, "Sustainability of cyber-physical systems in the context of targeted destructive influences," 2018 IEEE Industrial Cyber-Physical Systems (ICPS), St. Petersburg, 2018, pp. 830-834, doi: 10.1109/ICPHYS.2018.8390814.

12. Lysenko S. M. Metod zabezpechennia rezylientnosti kompiuternykh system v umovakh kiber-zahroz na osnovi samoadaptyvnosti. Radioelektronni i kompiuterni systemy. 2019. №4. S. 4–16.

13. Lysenko S. M., Kharchenko V.S., Bobrovnikova K.Iu., Shchuka R. Rezylientnist kompiuternykh system v umovakh kiberzahroz: Ontolohiia ta taksonomii. Radioelektronni i kompiuterni systemy. 2020. №1. S. 17-28.

14. Lysenko S. M. Modeli kiberatak merezhnoho ta khostovoho typu. Vymiriuvalna ta obchysliuvalna tekhnika v tekhnolohichnykh protsesakh. 2019. №2. S. 58-63.

Надійшла / Paper received: 23.09.2020
Надрукована / Paper Printed : 03.11.2020