Вісник Національного технічного університету "ХПІ", 2019, № 28 (1353)
ISSN 2079-0031 (Print) ISSN 2411-0558 (Online)

УДК 004.56 **DOI: 10.20998/2411-0558.2019.28.09**

О. В. МНУШКА, ас., ХНАДУ, Харків,
В. М. САВЧЕНКО, канд. техн. наук, ХНАДУ, Харків

МОДЕЛЬ БЕЗПЕКИ ІНФОРМАЦІЙНОЇ СИСТЕМИ НА БАЗІ ТЕХНОЛОГІЙ IOT

Проаналізовано моделі безпеки комп'ютерних та інформаційних систем, компоненти яких мають доступ до мережних ресурсів. Запропоновано математичну модель для оцінки безпеки інформаційної системи на основі технологій Інтернету речей (Internet of things, IoT) у вигляді атрибутивного метаграфу. На основі метрик Common Vulnerability Scoring System v. 3.0 проведено оцінку впливу кіберзагроз на компоненти веб-орієнтованої SCADA-системи. Іл.: 1. Бібліогр.: 14 назв.

Ключові слова: модель; безпека комп'ютерних та інформаційних систем; метаграф; IoT; Common Vulnerability Scoring System; SCADA-система.

Постановка проблеми. Поширення технологій IoT на промисловий сектор створює нові виклики щодо забезпечення інформаційної безпеки таких систем. Інформаційні системи на базі технологій IoT поступово витісняють традиційні рішення для SCADA (Supervisory Control And Data Acquisition) систем. Нові системи є веб-орієнтованими та використовують масові вироби для збирання та передавання даних. Розробник таких систем завжди стоїть перед вибором – забезпечити високу безпеку системи та отримати достатньо високу вартість та низьку конкурентну спроможність на ринку або за рахунок використання недорогих рішень забезпечити прийнятний рівень безпеки й вартості системи. Відсутність формального апарату оцінки безпеки таких систем, готового для інженерного застосування, є стримуючим фактором та не дозволяє отримати об'єктивну оцінку впливу різних загроз на кінцевий продукт.

Аналіз літератури. Архітектура SCADA-систем на основі технологій IoT в цілому відповідає традиційним системам автоматичного керування технологічними процесами (АСК ТП) з деякими обмеженнями [1 – 4]:

- дані в таких системах не локалізовані всередині технологічної комп'ютерної мережі підприємства;
- використовується більш просте та менш захищене апаратне забезпечення;
- для збирання даних використовується сервер в мережі Інтернет з

усіма перевагами та недоліками такого застосування;

- найбільш прийнятною формою використання таких систем є виключення функції керування та забезпечення наглядної візуалізації стану процесів;
- для забезпечення функції керування однією із основних проблем є проблема безпеки та доступності обладнання в режимі 24/7. Проблема в першу чергу пов'язана з тим, що дані часто передаються стандартними 2G/3G/4G каналами, що в загальному випадку не гарантують доступність каналу саме в режимі 24/7, особливо у віддалених районах.

У роботах [5 – 7] розглянуть питання забезпечення безпеки компонентів систем на основі технологій IoT, проаналізовано проблеми реалізації відповідних пристроїв та протоколів, показано основні тенденції розвитку "розумних речей" та розвиток загроз для інфраструктури "розумних речей", пов'язаних з конфіденційністю, через вразливості вбудованих систем та основних комунікаційних та embedded-технологій, наведено огляд нових технологій безпеки IoT та сучасних тенденцій досліджень IoT в галузі безпеки.

У роботі [8 – 9] наведено огляд математичних моделей, що описують безпеку комп'ютерних систем, показаний історичний розвиток різних підходів до опису безпеки, в т.ч. моделі The Bell and LaPadula, The Clark Wilson Model, The Roscoe-Woodcock-Wulf підхід, Communicating Sequential Processes (CSP) та ін., показані переваги та недоліки окремих підходів та моделей. В [9] описані підходи до математичного моделювання сучасних кіберзагроз, показано застосування імітаційного моделювання для розв'язання проблем розповсюдження вірусів у комп'ютерних мережах.

Мета статті. Розробка моделі безпеки інформаційної системи на базі технологій IoT, що враховує одночасний вплив комплексу факторів – архітектуру, версії програмного забезпечення, конфігурацію мережі, операторів та ін.

Модель безпеки інформаційної системи на базі технологій IoT. Метаграф вкладеності n можна представити у вигляді впорядкованої пари [10 – 12]:

$$\boldsymbol{G} = (\boldsymbol{X}, \boldsymbol{E}), \tag{1}$$

де $\boldsymbol{X} = \{x_1, x_2, \ldots, x_n\}$ – множина усіх вершин графу; $\boldsymbol{E} = \{e_1, e_2, \ldots, e_m\}$ – множина ребер графу.

Кожне ребро метаграфу об'єднує дві підмножини вершин

$$\boldsymbol{e}_k=(\boldsymbol{V}_i, \boldsymbol{W}_i), \tag{2}$$

де $\boldsymbol{V}_i$, $\boldsymbol{W}_i$ належать до множини вершин $\boldsymbol{X}$, а об'єднання цих двох множин не є пустою множиною.

Для усіх вершин графу повинні існувати функції вигляду:

$$f_1^a : g_1^a(x_1^a, e_1^a) \to x_2^b,$$
$$f_2^b : g_2^b(x_2^b, e_2^b) \to x_3^c, \ldots, \quad (3)$$
$$f^j{}_{n-1} : g^j{}_{n-1}(x^j{}_{n-1}, e^j{}_{n-1}) \to x_n^j.$$

Верхні індекси у (3) визначають кількість вершин та ребер на відповідному рівні $i = 1, 2, \ldots, n$, що у (3) позначено нижніми індексами.

Кожна із вершин та кожне із ребер у метаграфі можуть мати необмежену кількість атрибутів, що є характеристиками реальних об'єктів та виражаються у вигляді рядків та чисел [11]:

$$x_i^j = \{a_1, a_2, \ldots, a_k\},\ i = 1, ..., n,\ \ j = 1, ..., m, \quad (4)$$

$$e_j^t = (x_i^S, x_i^F) = \{a_1, a_2, ..., a_q\}, \quad (5)$$

де x_i^S, x_i^F відповідно початкова та кінцева вершини ребра, t – номер ребра на відповідному рівні метаграфу.

Метаграф (1) – (3) у графічному вигляді можна представити відповідно до рис. 1. Зазначимо, що метаграф може вироджуватися у гіперграф або простий орієнтований граф в залежності від наявності елементарних вершин, тобто таких, для яких не існує функцій вигляду (3) на кожному із рівнів метаграфу. Зв'язки $e^j{}_i$ дозволені між вершинами будь-якого рівня (e_7, e_8, e_9, e_{10}). Якщо вершини $x^4{}_i$ та $x^3{}_i$ в свою чергу є також гіперребрами $g^j{}_{n-1}$ ($x^j{}_{n-1}$, $e^j{}_{n-1}$), то отримаємо метаграф вкладеності 4 і т.д.

Відома багаторівнева модель інформаційної системи на основі атрибутивних метаграфів [12], але вона не враховує особливості пристроїв Інтернету речей та архітектуру систем на їх основі.

Перейдемо до розгляду моделі для опису безпеки на основі пристроїв та технологій IoT для типового застосування – веб-орієнтованої SCADA-системи. Елементами даної моделі є:

- множина всіх пристроїв та $\boldsymbol{X_1} = \{x_1, x_2, \ldots, x_k\}$ та зв'язків між ними $\boldsymbol{E_1} = \{e_1^1, e_1^2, \ldots, e_1^K\}$;
- множина системного програмного забезпечення $\boldsymbol{X_2} = \{x_1, x_2, \ldots, x_m\}$ та зв'язків між компонентами ПЗ $\boldsymbol{E_2} = \{e_2^1, e_2^2, \ldots, e_2^M\}$;
- множина прикладного програмного забезпечення $\boldsymbol{X_3} = \{x_1, x_2, \ldots, x_n\}$ та зв'язків між компонентами ПЗ $\boldsymbol{E_3} = \{e_3^1, e_3^2, \ldots, e_3^N\}$;
- множина протоколів обміну даними $\boldsymbol{X_4} = \{x_1, x_2, \ldots, x_p\}$ та зв'язків між ними $\boldsymbol{E_4} = \{e_4^1, e_4^2, \ldots, e_4^P\}$;
- множина ліній зв'язку (мереж) $\boldsymbol{X_5} = \{x_1, x_2, \ldots, x_r\}$ та зв'язків між

ISSN 2079-0031 (Print) ISSN 2411-0558 (Online)

ними $\boldsymbol{E_5} = \{e_5^1, e_5^2, \ldots, e_5^R\}$;

- множина клієнтів (персоналу) системи $\boldsymbol{X_6} = \{x_1, x_2, \ldots, x_s\}$ та зв'язків між ними $\boldsymbol{E_6} = \{e_6^1, e_6^2, \ldots, e_6^R\}$.

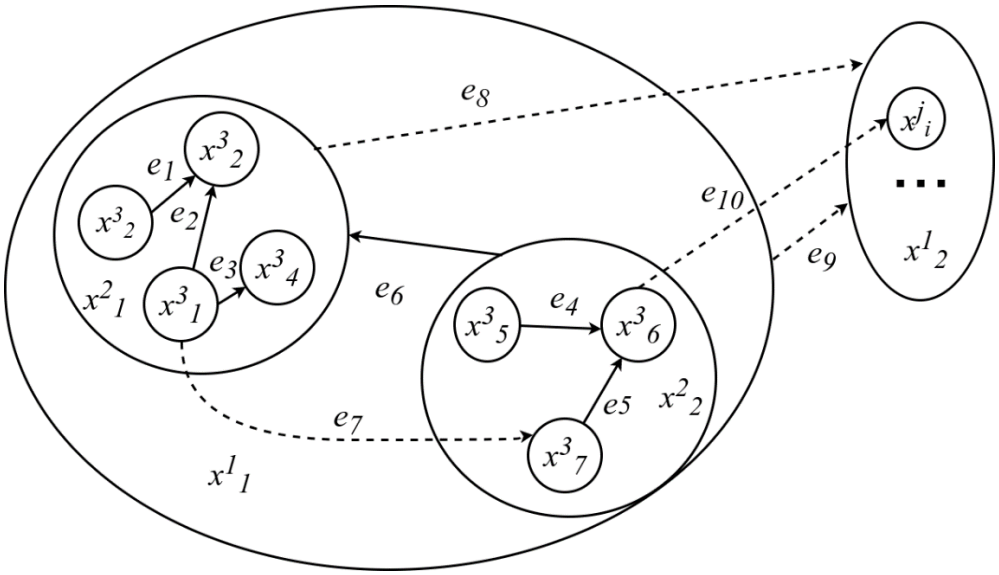

Рис. 1 Метаграф вкладеності 3

Таким чином можемо записати (1) у вигляді

$$\boldsymbol{G} = (\boldsymbol{X_1}, \boldsymbol{X_2}, \boldsymbol{X_3}, \boldsymbol{X_4}, \boldsymbol{X_5}, \boldsymbol{X_6}, \boldsymbol{E_1}, \boldsymbol{E_2}, \boldsymbol{E_3}, \boldsymbol{E_4}, \boldsymbol{E_5}, \boldsymbol{E_6}). \quad (6)$$

Зв'язок між елементами на деякому рівні існує тільки у тому випадку, коли існує відповідний зв'язок між усіма елементами верхніх рівнів.

З урахуванням специфіки роботи системи на основі експертної оцінки визначимо набори можливих атрибутів для компонентів системи:

- $\boldsymbol{A}_{X1}$ = {"ідентифікатор", "координати розташування", "режим роботи", "фізична адреса", "автономність"};
- $\boldsymbol{A}_{X2}$ = {"назва", "тип", "логічна адреса в мережі"};
- $\boldsymbol{A}_{X3}$ = {"назва", "протокол обміну", "ідентифікатор хоста"};
- $\boldsymbol{A}_{X4}$ = {"назва", "протокол обміну", "адреса/ідентифікатор"};
- $\boldsymbol{A}_{X5}$ = {"назва", "тип лінії", "протокол обміну", "адреса/ідентифікатор", "таблиці маршрутизації"};
- $\boldsymbol{A}_{X6}$ = {"ідентифікатор", "права доступу", "закріплене обладнання"}.

ISSN 2079-0031 (Print) ISSN 2411-0558 (Online)

В нашому випадку під протоколами обміну ми маємо на увазі модель стеку TCP/IP та її відповідні рівні [13].

Під час роботи система знаходиться під впливом різних факторів, що визначають безпечність її роботи. Основною проблемою систем на базі IoT є різна обчислювальна можливість пристроїв (constrained devices, smart dust та ін.), що, наприклад, не дозволяє використовувати потужні та добре захищені протоколи або операційні системи. Проблемою є фізична доступність пристроїв, які часто розташовані за межами охоронних зон або безпосередньо використовуються клієнтом у змінних середовищах, що можуть бути скомпрометованими з точки зору безпеки. Наявність оператора (чи будь-якого іншого обслуговуючого персоналу) або клієнта в системі також є додатковим фактором небезпеки.

Основні типи загроз можна розділити на три основні групи:

- *підміна* елемента системи (метаграфа), у запропонованій моделі (6) виражається підміною вершини або ребра $(\boldsymbol{X}_1 \setminus x^j_1) \vee x_1^{k+1}$;
- *додавання* елемента метаграфа виражається у додаванні нового елементу $\boldsymbol{X}_1 \vee x_1^{k+1}$ та зміни структури вихідного графа за рахунок порушення зв'язків між ребрами або вершинами;
- *видалення* елемента метаграфа також порушує визначені зв'язки між елементами метаграфу $\boldsymbol{X}_1 \setminus x^j_1$;

Відповідні перетворення можна записати для ребер **E**. Заміна атрибутів змінює інформацію про стан системи, але не впливає на характеристики метаграфа.

Для оцінки безпеки конкретного елемента метаграфа використаємо модифіковані підходи та методики CVSS3 [14].

$$BaseScore = (0{,}6\times Impact) + (0{,}4\times Exploitability) - 1{,}5\times \mathrm{f}(Impact), \quad (7)$$

$$Impact = 10{,}41\times(1 - (1 - ConfIm)\times(1 - IntegIm)\times(1 - AvailIm), \quad (8)$$

$$Exploitability = 20\times AccessVect\times AccessComplex\times Auth. \quad (9)$$

Параметри, що входять у (7) – (9) мають наступний смисл та кількісну експертну оцінку:

- $f(Impact) = 0$ для $Impact = 0$; 0,176 для $Impact \neq 0$ є характеристикою безпеки для компонентів метаграфу.
- $ConfIm = \{0; 0{,}275; 0{,}67\}$ визначає ступінь впливу загрози на конфіденційність даних, цей параметр є важливим з точки зору забезпечення актуальності та адекватності даних, що передаються між вузлами метаграфу.

- *AvailIm* = {0; 0,275; 0,67} визначає ступінь загрози для доступності даних, цей параметр є критичним для систем реального часу, таких як АСК ТП – загроза не впливає, впливає при певних умовах, безумовно впливає.
- *AccessVect* = {0,395; 0,46; 1} визначає ступінь доступу до компонентів, що описуються метаграфом системи. Значення відповідають наступним станам – загроза реалізується тільки при локальному доступі, в середині мережі передачі даних та ззовні по відношенню до об'єкта атаки.
- *AccessComplex* = {0,35; 0,61; 0,71} є характеристикою протидії загрозам та атакам зі сторони SCADA – протидія достатня для більшості загроз, протидія недостатня та протидія відсутня.
- *Auth* = {0,45; 0,56; 0,7} є оцінкою небезпеки несанкціонованого доступу для реалізації загрози – при постійному доступі, при однократному (тимчасовому) доступі, без доступу у внутрішню мережу передачі даних.

Для SCADA систем із можливістю керування технологічними процесами визначимо наступні рівні загроз для безпеки функціонування системи:

- низький, коли $BaseScore \leq 4{,}0$;
- середній для $4{,}1 \leq BaseScore \leq 6{,}5$;
- високий для $6{,}6 \leq BaseScore \leq 8{,}9$;
- критичний $9{,}0 \leq BaseScore \leq 10$.

Для систем, орієнтованих на збирання та візуалізацію даних, потрібний більш низький рівень безпеки, тому порогові значення збільшують на 15 – 20 відсотків.

Висновки. Запропоновано математичну модель інформаційної безпеки для систем на основі технологій IoT, яка на відміну від відомих моделей враховує особливості архітектури веб-орієнтованих SCADA-систем та апаратно-програмні обмеження таких систем. Отримана модель є атрибутивним метаграфом вкладеності 6, та забезпечує зручний інструмент для подальшого аналізу в т. ч. візуалізації потоків даних в системі, станів системи з плином часу тощо. Показано, що вплив загроз на стан метагарфу виражається стандартними операціями над множиною. Для оцінки впливу загроз на конкретні елементи метаграфу запропоновано використовувати оцінку у відповідності до CVSS, отримано інтегральну оцінку для систем, орієнтованих на керування

процесами, та для систем, орієнтованих на збирання та візуалізацію даних.

Список літератури:

1. *Unde M.D.* Web based control and data acquisition system for industrial application monitoring / *M.D. Unde, P.S. Kurhe* // International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), Chennai, 2017. – P. 246-249.
2. *Liu Y.* The Application of Digital Flexible Intelligent Manufacturing System in Machine Manufacturing Industry / *Y. Liu, Y. Zhao, L. Tao, K. Zhao, K. Li* // 2018 IEEE 8th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER), Tianjin, China, 2018. – P. 664-668.
3. *Мнушка О.В*. SCADA на основі промислового Інтернету речей: архітектура системи / *О.В*. *Мнушка* // Технічний сервіс агропромислового, лісового та транспортного комплексів. – Харків, 2018. – № 12. – С. 117-124.
4. *Мнушка О.В*. Архітектура веб-орієнтованої SCADA-системи / *О.В*. *Мнушка* // Вісник Національного технічного університету "Харківський політехнічний інститут". Збірник наукових праць. Серія: Інформатика та моделювання. – Харків: НТУ "ХПІ", 2018. – № 24 (1300). – С. 117-128.
5. *Sezer S.* T1C: IoT Security: Threats, Security Challenges and IoT Security Research and Technology Trends / *S. Sezer* // 31st IEEE International System-on-Chip Conference (SOCC), Arlington, VA, 2018. – P. 1-2.
6. *Garg H*. Securing IoT Devices and Securely Connecting the Dots Using REST API and Middleware / *H. Garg, M. Dave* // 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 2019. – P. 1-6.
7. *Chung B*. On-demand security configuration for IoT devices / *B*. *Chung*, *J. Kim, Y. Jeon* // International Conference on Information and Communication Technology Convergence (ICTC), Jeju, 2016. – P. 1082-1084.
8. *Ryan P*. Mathematical Models of Computer Security / *P*. *Ryan* – LNCS. 2171. – 2000. – 62 p.
9. *Dinesh K.S.* Cyber Defense: Mathematical Modeling and Simulation / *K.S. Dinesh* // International Journal of Applied Physics and Mathematic. – 2012. – Vol. 2. – No. 5. – P. 312-315.
10. *Basu A.* Metagraphs and their applications / *A. Basu*, *R.W. Blanning*. – Springer, 2007. – 174 p.
11. *Астанин С.В.* Вложенные метаграфы как модели сложных объектов / *С.В. Астанин*, *Н.В. Драгныш, Н.В. Жуковская* // Инженерный вестник Дона, 2012. – Том. 23. – Вып. 4-2. – С. 74-78.
12. *Новохрестов А.К.* Многоуровневая модель информационной системы на основе атрибутивных метаграфов / *А.К. Новохрестов*, *А.А. Конев* // Электронные средства и системы управления: Материалы докладов XI Международной научно-практической конференции (25–27 ноября 2015 г.). В 2 ч. – Ч. 2. – Томск: В-Спектр, 2015. – С. 182-188.
13. *Forouzan*, *Behrouz A.* TCP/IP Protocol Suite (2nd ed.) / *A. Behrouz Forouzan*. – McGraw-Hill, 2003. – 976 p.
14. Common Vulnerability Scoring System Version 3.0 Calculator URL: https://www.first.org/cvss/calculator/3.0.

References:

1. Unde, M.D., and Kurhe, P.S. (2017), "Web based control and data acquisition system for industrial application monitoring", *2017 International Conference on Energy,*

Communication, Data Analytics and Soft Computing (ICECDS), Chennai, pp. 246-249.
2. Liu, Y., Zhao, Y., Tao, L., Zhao, K., and K. Li. (2018), "The Application of Digital Flexible Intelligent Manufacturing System in Machine Manufacturing Industry", *2018 IEEE 8th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER)*, Tianjin, China, pp. 664-668.
3. Mnushka, O.V. (2018), "SCADA based on the industrial Internet of Things: architecture of the system", *Technical service of agriculture, forestry and transport systems,* Kharkiv, № 12, pp.117-124.
4. Mnushka, O.V. (2018), "The architecture of a web-based SCADA system", *Herald of NTU "KhPI". Series: Informatics and modeling. – Kharkov: NTU "KhPI". –* № 24 (1300), pp. 117-128.
5. Sezer, S. (2018), "T1C: IoT Security: Threats, Security Challenges and IoT Security Research and Technology Trends", *31st IEEE International System-on-Chip Conference (SOCC)*, Arlington, VA, pp. 1-2.
6. Garg, H., and Dave, M. (2019), "Securing IoT Devices and SecurelyConnecting the Dots Using REST API and Middleware", *4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, Ghaziabad, India, pp. 1-6.
7. Chung, B., Kim, J., and Jeon, Y. (2016), "On-demand security configuration for IoT devices", *International Conference on Information and Communication Technology Convergence (ICTC)*, Jeju, pp. 1082-1084.
8. Ryan, P. (2000), *Mathematical Models of Computer Security,* LNCS. 2171, 62 p.
9. Dinesh, K.S. (2012), *"*Cyber Defense: Mathematical Modeling and Simulation", *International Journal of Applied Physics and Mathematic*, Vol. 2, No. 5, pp. 312-315.
10. Basu, A., and Blanning, R.W. (2007), *Metagraphs and their applications,* Springer, 174 p.
11. Astanin, S.V., Dragnysh, N.V., and Zhukovskaya, N.V. (2012), "Nested Metrographs as Models of Complex Objects", *Engineering Bulletin of the Don*, Vol. 23, No. 4-2, pp. 74-78.
12. Novokrestov, A.K., and Konev, A.A. (2015), "A multilevel model of an information system based on attributive metgraphs", *Electronic tools and control systems: Proceedings of the XI International Scientific and Practical Conference* (November 25-27, 2015), Tomsk, *V*-Spectrum, pp. 182-188.
13. Forouzan, Behrouz A. (2003), *TCP/IP Protocol Suite (2nd ed.),* McGraw-Hill, 976 p.
14. Common Vulnerability Scoring System Version 3.0 Calculator, available at: https://www.first.org/cvss/calculator/3.0.

Статтю представив д-р техн. наук, проф. ХНАДУ, зав каф. комп'ютерних технологій і мехатроніки Ніконов О.Я.

Надійшла (received) 12.11.2019.

Mnushka Oksana, Assistant Lecturer, M.S.
Kharkiv National Automobile and Highway University,
Str. 25, Yaroslava Mudrogo, Kharkiv, Ukraine, 61002
Tel.:(+38057)707-37-47, e-mail: mnushka.ov@gmail.com
ORCID ID: 0000-0001-7756-9260

Savchenko Volodymyr, Candidate of Science (Engineering), M.S.,
Kharkiv National Automobile and Highway University,
Str. 25, Yaroslava Mudrogo, Kharkiv, Ukraine, 61002
Tel.:(+38057)707-37-47, e-mail: savchenko@live.com
ORCID ID: 0000-0001-6548-0891

УДК 004.56

Модель безпеки інформаційної системи на базі технологій IoT / Мнушка О.В., Савченко В.М. // Вісник НТУ "ХПІ". Серія: Інформатика та моделювання. – Харків: НТУ "ХПІ". – 2019. – № 28 (1353). – С. 108 – 116.

Проаналізовано моделі безпеки комп'ютерних та інформаційних систем, компоненти яких мають доступ до мережних ресурсів. Запропоновано математичну модель для оцінки безпеки інформаційної системи на основі технологій Інтернету речей (Internet of things, IoT) у вигляді атрибутивного метаграфу. На основі метрик Common Vulnerability Scoring System v. 3.0 проведено оцінку впливу кіберзагроз на компоненти веб-орієнтованої SCADA-системи. Іл.: 1. Бібліогр.: 14 назв.

Ключові слова: модель; безпека комп'ютерних та інформаційних систем; метаграф; IoT; Common Vulnerability Scoring System; SCADA-система.

УДК 004.56

Модель безопасности информационной системы на базе технологий IoT / Мнушка О.В., Савченко В.Н. // Вестник НТУ "ХПИ". Серия: Информатика и моделирование. – Харьков: НТУ "ХПИ". – 2019. – № 28 (1353). – С. 108 – 116.

Проанализированы модели безопасности компьютерных и информационных систем, компоненты которых имеют доступ к сетевым ресурсам. Предложена математическая модель для оценки безопасности информационной системы на основе технологий Интернета вещей (Internet of things, IoT) в виде атрибутивного метаграфа. На основе метрик Common Vulnerability Scoring System v. 3.0 проведена оценка влияния киберугроз на компоненты веб-ориентированной SCADA-системы. Ил.: 1. Библиогр.: 14 назв.

Ключевые слова: модель; безопасность компьютерных и информационных систем; метаграф; IoT; Common Vulnerability Scoring System; SCADA-система.

UDC 004.56

Security model of an information system based on IoT technologies / Mnushka O.V., Savchenko V.M. // Herald of the National Technical University "KhPI". Series of "Informatics and Modeling". – Kharkov: NTU "KhPI". – 2019. – № 28 (1353). – P. 108 – 116.

The security models of computer and information systems, the components of which have access to network resources, are analyzed. A mathematical model is proposed for assessing the security of an information system based on the Internet of things (IoT) technologies in the form of an attribute metagraph. Based on the Common Vulnerability Scoring System v. 3.0, the impact of cyber threats on the components of a web-based SCADA-system was assessed. Figs.: 1. Refs.: 14 titles.

Keywords: model; security of computer and information systems; metagraph; IoT; Common Vulnerability Scoring System; SCADA-system.