DOI: 10.18372/2310-5461.43.13980

УДК 681.3.06

Л. П. Галата
Національний авіаційний університет
orcid.org/0000-0002-7978-3954
e-mail: galataliliya@gmail.com;

Б. Я. Корнієнко, д-р. техн. наук, доц.
Національний технічний університет України
«Київський політехнічний інститут імені І. Сікорського»
orcid.org/0000-0002-2521-0878
e-mail: bogdanko@gmx.net;

В. В. Заболотний
Національний технічний університет України
«Київський політехнічний інститут імені І. Сікорського»
orcid.org/0000-0002-6345-2069
e-mail: vladyslavzabolotny@gmail.com

МАТЕМАТИЧНА МОДЕЛЬ ПРОТИДІЇ ЗАГРОЗАМ У СИСТЕМІ ЗАХИСТУ КРИТИЧНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Вступ

Не дивлячись на велику кількість аварій з катастрофічними наслідками, проблема захисту критичних інформаційних ресурсів на промислових підприємствах хімічної та енергетичної галузей ніколи не стояла так гостро як останніми роками.

Загальний інтерес до безпеки промислових систем виник лише після інцидентів з комп'ютерними вірусами Stuxnet, Duqu, Flame, які атакували іранські атомні об'єкти, державні заклади та промислові об'єкти Індії, Китаю та інших країн. Окремо слід виділити атаки на підприємства енергетичної галузі та банківського сектору в Україні. До появи цих інцидентів вважалось, що скомпрометувати роботу системи захисту критичних інформаційних ресурсів було дуже важко. Такі уявлення будувались на таких постулатах: програмне забезпечення кожної системи захисту критичних інформаційних ресурсів унікальне і закрите; проникнення в систему пов'язане з великими витратами інтелектуальних ресурсів, а грошова винагорода для зловмисника не очевидна; локальна мережа системи захисту критичних інформаційних ресурсів вирішує проблеми обмеження доступу. Вивчення структури та програмно-апаратних засобів, що використовуються в системах захисту критичних інформаційних ресурсів, показало, що за останній час пройшли великі зміни. Майже всюди використовується широко розповсюджене програмне забезпечення як ОС Windows, TCP/IP протоколи тощо, які разом зі своїми перевагами стандартності, простоти та якості використання принесли також і недоліки – вразливості. У локальній мережі з'являються комп'ютери, підключені до мережі Інтернет, що також вносить велику кількість потенційних загроз до системи [1–3].

Постановка проблеми

Також нещодавно з'явився новий термін «кібервійна» (*cyberwarfare*), який часто згадується у засобах масової інформації у зв'язку з проблемою захисту систем критичних інформаційних ресурсів на інфраструктурних об'єктах та небезпечних виробництвах. Таким чином повсюдне використання комп'ютерного обладнання у керуванні промисловими підприємствами створює необхідність приділення все більшої уваги до проблем інформаційної безпеки таких систем.

Основні проблеми інформаційної безпеки критичних інформаційних ресурсів, які виділяють експерти, з'являються через:

– слабкий захист від несанкціонованого доступу (паролі);

– незадекларованих можливостей SCADA;

– відсутність контролю керуючих впливів;

– використання бездротових комунікацій (некрипостійке шифрування Wi-Fi);

– відсутність чітких меж між різними сегментами мережі;

– несвоєчасне чи некоректне оновлення програмного забезпечення;

– відмову від навіть мінімальних заходів безпеки (нерідко заради зручності чи продуктив-

ності, компанії відмовляються від встановлення не тільки, наприклад, антивірусного захисту, а навіть захисту паролем критично важливих активів);

– поширення Windows як операційної системи для робочих станцій та навіть серверів;

– розробку з розрахунком на використання у довіреному середовищі закритих індустріальних мереж;

– створення систем без врахування кращих практик розробки безпечного коду;

– людський фактор, слабку дисципліну персоналу.

Наведемо приклад основних загроз для систем захисту критичних інформаційних ресурсів, знайдених після аналізу справжніх інцидентів:

– атаки на SCADA;

– атаки на PLC, вразливості PLC (стандартний пароль, неавторизований доступ до оригінального програмного забезпечення);

– атаки на інфраструктуру та оперативну систему (віруси, троянські програми, черв'яки, DoS- і DDoS-атаки, ARP-спуфінг — перехват трафіку після оголошення себе маршрутизатором);

– атаки на протоколи, вразливість протоколів (несанкціонований доступ, SQL-ін'єкції);

– практичні атаки (переповнення буферу — Buffer Overflow, розкриття інформації — Information Disclose, відмова в доступі — Denial of Access, підміна представлення — Manipulation of View).

Серед усіх типів вразливих компонентів систем захисту критичних інформаційних ресурсів переважають SCADA — 87 %, системи, які забезпечують інтерфейси людина-машина — 49 %, програмовані контролери — 20 %, протоколи — 1 %.

Доля вразливостей по типах розділилась наступним чином: переповнення буферу — 36 %, аутентифікація/управління ключами — 22,86 %, вразливості Web-програм — сервер — 10,86%, клієнт — 9,14 %, віддалене виконання коду — 13,14 % [4–6].

Унаслідок експлуатації систем захисту критичних інформаційних ресурсів і суттєвої зміни складу і якості сучасних загроз, необхідно проектувати і реалізовувати інформаційну безпеку систем з врахуванням тенденцій розвитку кіберзагроз. З іншого боку необхідно проводити регулярну роботу з нейтралізації виникаючих чи потенційних загроз на працюючих системах. На цьому рівні реалізуються такі сервіси інформаційної безпеки: управління доступом, забезпечення цілісності, забезпечення безпечної міжмережевої взаємодії, антивірусний захист, аналіз захищеності, виявлення вторгнень, управління системою інформаційної безпеки (неперервний моніторинг станів, виявлення інцидентів, реагування).

Аналіз останніх досліджень і публікацій

Як об'єкт дослідження обрано систему захисту критичних інформаційних ресурсів виробництва мінеральних добрив [7]. Основу моделей забезпечення безпеки інформації складають такі теорії: формально-евристичний підхід; теорія ймовірностей і випадкових процесів; еволюційне моделювання; теорія графів, автоматів та мереж Петрі; теорії ігор та конфліктів; теорія катастроф; теорія нечітких множин; ентропійний підхід. Відмінності більшості моделей полягають у тому, які параметри вони використовують як вхідні, а які — наводять у вигляді вихідних після проведення розрахунків. Крім того, останнім часом широкого поширення набувають методи моделювання, засновані на неформальній теорії систем: методи структурування, методи оцінювання та методи пошуку оптимальних рішень [8]. Методи структурування є розвитком формального опису, що поширюється на організаційно-технічні системи. Використання цих методів дозволяє уявити архітектуру і процеси функціонування складної системи у вигляді, що задовольняє таким умовам: повнота відображення основних елементів і їх взаємозв'язків; простота організації елементів і їх взаємозв'язків; гнучкість — простота внесення змін до структури і т. д. Методи оцінювання дозволяють визначити значення характеристик системи, які не можуть бути виміряні або отримані з використанням аналітичних виразів, або в процесі статистичного аналізу — імовірності реалізації загроз, ефективність елемента системи захисту та ін., основа таких методів належить експертному оцінюванню — підхід, що полягає в залученні фахівців у відповідних галузях знань для отримання значень деяких характеристик.

Методи пошуку оптимальних рішень є узагальненням великої кількості самостійних, у більшості своїй математичній теорії з метою вирішення завдань оптимізації. У загальному випадку до цієї групи можна також віднести методи неформальної відомості складного завдання до формального опису з подальшим застосуванням формальних підходів. Комбінування методів цих трьох груп дозволяє розширити можливості застосування формальних теорій для проведення повноцінного моделювання систем захисту.

Мета статті — розроблення та дослідження математичної моделі протидії загрозам у системі захисту критичних інформаційних ресурсів, одержання перехідних характеристик для станів системи.

Виклад основного матеріалу дослідження

Запропонована математична модель протидії впливу внутрішніх та зовнішніх загроз на систему захисту критичних інформаційних ресурсів виробництва мінеральних добрив. Поетапно розписаний процес побудови математичної моделі протидії загрозам у системі захисту критичних інформаційних ресурсів за допомогою марковського ланцюга [9].

Запропонована методика знаходження актуальних загроз безпеці даних при їх обробці. Наведені приклади розрахунків імовірностей знаходження математичної моделі інформаційної системи в одному з чотирьох станів (загроза не настала; загроза настала, але не була реалізована; загроза настала, була реалізована; загроза настала, але була відбита системою захисту).

Систему можна інтерпретувати як систему масового обслуговування, у яку надходять загрози.

Для початку розглянемо ситуацію, коли на вхід до системи надходять загрози одного типу, припускаючи, що загроза не може бути реалізована та надходити кілька разів в один і той самий період часу. Якщо ці умови виконуються, то система може знаходитися у одному з чотирьох станів (рис. 1):

1. Загроза не надходила і, відповідно, не була реалізована;
2. Загроза надійшла, але не була реалізована;
3. Загроза надійшла та була реалізована;
4. Загроза надійшла, але була відбита системою захисту.

Система, яка розглядається, є системою з відновленням, тобто система може переходити з будь-якого стану у початковий. Будемо розглядати систему з неперервним часом. Перехід зі стану у стан відбувається згідно з орієнтованим графом (рис. 1).

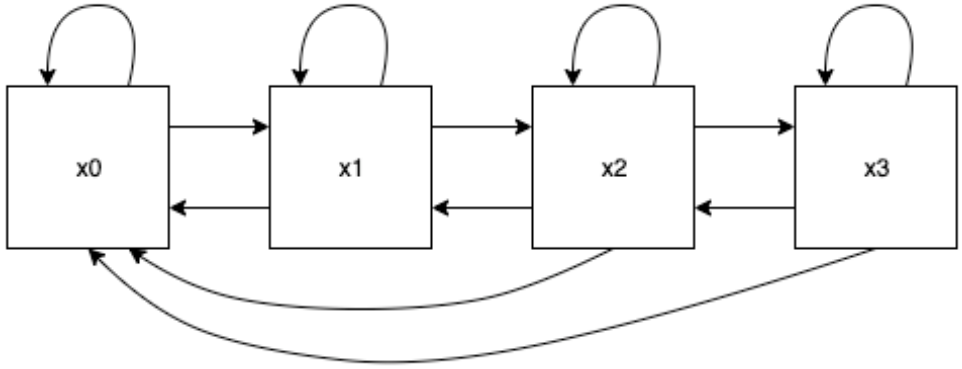

Рис. 1. Граф станів системи

Для опису процесу переходу зі стану у стан, побудуємо матрицю інтенсивностей переходу:

$$p_{ij} = \begin{vmatrix} \lambda_{11} & \lambda_{12} & \lambda_{11} & 0 \\ \lambda_{21} & \lambda_{22} & \lambda_{23} & \lambda_{24} \\ \lambda_{31} & \lambda_{32} & \lambda_{33} & \lambda_{34} \\ \lambda_{41} & \lambda_{42} & \lambda_{43} & \lambda_{44} \end{vmatrix}.$$

З попередніх погоджень випливає, що елементи цієї матриці мають такі властивості:

$$\lambda_{11} = -\lambda_{12} - \lambda_{13};$$
$$\lambda_{22} = -\lambda_{21} - \lambda_{23} - \lambda_{24};$$
$$\lambda_{33} = -\lambda_{31} - \lambda_{32} - \lambda_{34};$$
$$\lambda_{44} = -\lambda_{41} - \lambda_{42} - \lambda_{43}.$$

Для визначення ймовірностей перебування системи у станах x_0, x_1, x_2, x_3, побудуємо систему диференційних рівнянь:

$$\begin{cases} \dfrac{dp_0(t)}{dt} = p_0(t)\lambda_{11} + p_1(t)\lambda_{21} + p_2(t)\lambda_{31} + p_3(t)\lambda_{41}; \\ \dfrac{dp_0(t)}{dt} = p_0(t)\lambda_{11} + p_1(t)\lambda_{21} + p_2(t)\lambda_{31} + p_3(t)\lambda_{41}; \\ \dfrac{dp_2(t)}{dt} = p_0(t)\lambda_{13} + p_1(t)\lambda_{23} + p_2(t)\lambda_{33} + p_3(t)\lambda_{43}; \\ \dfrac{dp_3(t)}{dt} = p_1(t)\lambda_{24} + p_2(t)\lambda_{34} + p_3(t)\lambda_{44}. \end{cases}$$

Оскільки

$$p(0) = (1, 0, 0, 0),$$

заданий, то вектор абсолютних імовірностей

$$p(n) = \left(p_0(n), p_1(n), p_2(n), p_3(n)\right),$$

визначається відношенням:

$$p(n) = p(0)\left\| p_{ij}(n) \right\|.$$

Після проведення дослідження на імітаційній моделі було визначено два результати знаходження коефіцієнтів λ_{ij}, які будуть наведені нижче [10–18].

Варіант 1. Нехай матриця інтенсивностей переходів λ_{ij} має вигляд:

$$\begin{vmatrix} -0,040 & 0,015 & 0,010 & 0,015 \\ 0,225 & -0,250 & -0,025 & 0,050 \\ 0,625 & -0,160 & -0,855 & 0,390 \\ -0,000 & 0,075 & 0,200 & -0,275 \end{vmatrix}.$$

Отримаємо розв'язок системи рівнянь методом Рунге–Кутти четвертого порядку для моменту часу $t = 50$ с.

Для реалізації розв'язку системи рівнянь розроблено програмний модуль на мові програмування Piton.

У результаті проведених обчислень були знайдені значення імовірності знаходження системи у кожному зі станів (рис. 2).

Варіант 2. Зробимо аналогічні до варіанту 1 обчислення із значеннями матриці інтенсивностей переходів λ_{ij}:

$$\begin{vmatrix} -0,040 & 0,015 & 0,010 & 0,015 \\ 0,225 & -0,250 & -0,025 & 0,050 \\ 0,575 & -0,200 & -0,875 & 0,500 \\ -0,125 & 0,145 & 0,180 & -0,200 \end{vmatrix}.$$

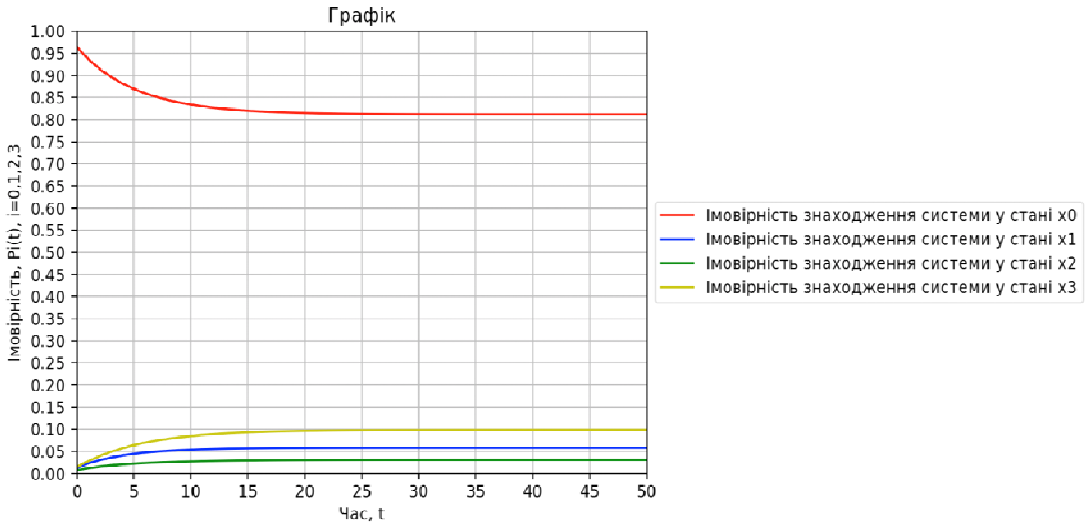

Рис. 2. Імовірність знаходження системи у кожному зі станів

У результаті отримаємо такий графік (рис. 3):

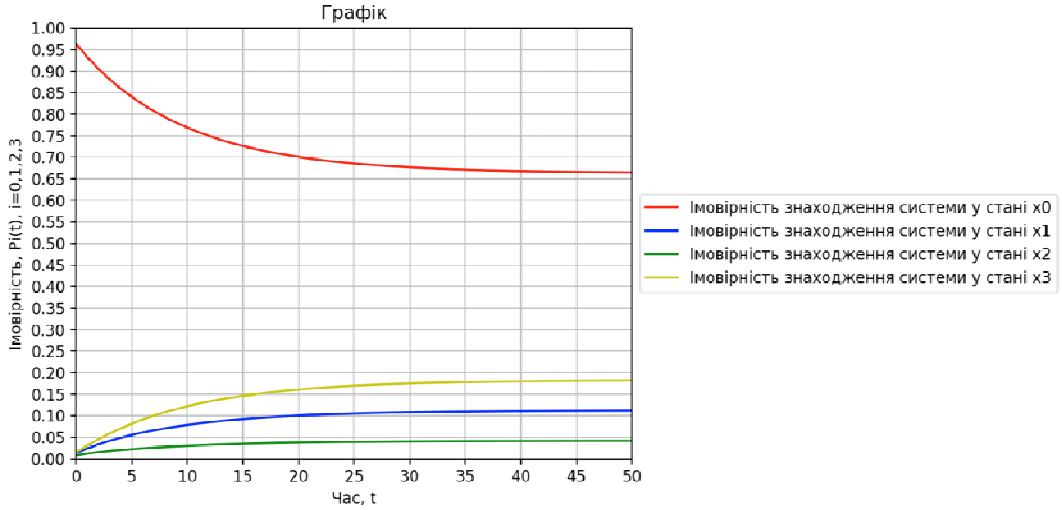

Рис. 3. Імовірність знаходження системи у кожному зі станів

Висновки

На основі отриманих результатів можна сказати, що у варіанті 2 більша ймовірність знаходження системи у стані, викликаним отриманням загрози, хоча також велика вірогідність успішного відбиття загрози системою захисту.

Запропонована математична модель протидії загрозам у системі захисту критичних інформаційних ресурсів виробництва мінеральних добрив. Також розроблена та наведена на основі цієї моделі методика виявлення актуальних загроз безпеки.

Приклади аналізу числових результатів за допомогою запропонованої методики наочно показують, що їх використання допомагає з визначенням загроз, які є актуальними для досліджуваної системи та можуть використовуватись на практиці. Недоліком запропонованої методики є необхідність розгляду поведінки системи при дії на неї кожного типу загроз окремо і неможливість визначення поведінки про одночасній дії кількох загроз. Але з іншого боку вивчення впливу кожної загрози окремо дозволяє більш детально вивчити кожен її тип та визначити ті, вірогідність появи яких є найбільшою.

ЛІТЕРАТУРА

1. Корнієнко Б. Я. Безпека інформаційно-комунікаційних систем та мереж. Навчальний посібник для студентів спеціальності 125 «Кібербезпека». К.: НАУ, 2018. 226 с.

2. Корниенко Б. Я. Информационная безопасность и технологии компьютерных сетей : монография. ISBN 978-3-330-02028-3, LAMBERT Academic Publishing, Saarbrucken, Deutschland. 2016. 102 с.

3. Корниенко Б. Я. Кибернетическая безопасность — операционные системы и протоколы. ISBN 978-3-330-08397-4, LAMBERT Academic Publishing, Saarbrucken, Deutschland. 2017. 122 с.

4. Корнієнко Б. Я. Дослідження моделі взаємодії відкритих систем з погляду інформаційної безпеки. *Наукоємні технології*. 2012. № 3 (15). С. 83 — 89. doi.org/10.18372/2310-5461.15.5120 (ukr).

5. Korniyenko B., Yudin O., Novizkij E. Open systems interconnection model investigation from the viewpoint of information security. *The Advanced Science Journal*. 2013. issue 8. P. 53–56.

6. Корнієнко Б. Я., Юдін О. К. Реалізація інформаційної безпеки у моделі взаємодії відкритих систем. Збірник тез VI Міжнародної науково-технічної конференції «*Комп'ютерні системи та мережні технології*» CSNT-2013 (11-13 червня 2013 р., Київ, Україна). С. 73.

7. Корнієнко Б. Я. Інформаційні технології оптимального управління виробництвом мінеральних добрив : монографія. К. : Вид-во Аграр Медіа Груп, 2014. 288 с.

8. Курилов Ф. М. Моделирование систем защиты информации. Приложение теории графов. Материалы III Междунар. науч. конф. «*Технические науки: теория и практика*». Чита: Издательство Молодой ученый, 2016. С. 6–9.

9. Росенко А. П. Теоретические основы анализа и оценки влияния внутренних угроз на безопасность конфиденциальной информации: монография. М.: Гелиос АРВ, 2008. 154 с.

10. Korniyenko B. Y., Galata L.P. Design and research of mathematical model for information security system in computer network. *Наукоємні технології*. 2017. № 2. Вип. 34. С. 114–118. doi.org/10.18372/2310-5461.34.11608 (eng).

11. Korniyenko B., Galata L., Kozuberda O. Modeling of security and risk assessment in information and communication system. *Sciences of Europe*. 2016. V. 2. No 2 (2). P. 61–63.

12. Korniyenko B. The classification of information technologies and control systems. *International scientific journal*. 2016. № 2. P. 78–81.

13. Korniyenko B., Yudin A., Galata L. Risk estimation of information system. *Wschodnio europejskie Czasopismo Naukowe*. 2016. Vol. 5. P. 35–40.

14. Корнієнко Б. Я., Юдін О. К., Снігур О. С. Безпека аутентифікації у web-ресурсах. *Захист інформації*. 2012. № 1 (54). С. 20–25. doi.org/10.18372/2410-7840.14.2056 (ukr).

15. Корнієнко Б. Я., Максімов Ю. О., Марутовська Н. М. Прикладні програми управління інформаційними ризиками. *Захист інформації*. 2012. № 4 (57). С. 60 — 64. doi.org/10.18372/2410-7840.14.3493 (ukr).

16. Korniyenko B., Galata L., Ladieva L. Security Estimation of the Simulation Polygon for the Protection of Critical Information Resources. CEUR Workshop Proceedings, Selected Papers of the XVIII International Scientific and Practical Conference "*Information Technologies and Security*" – ITS 2018 (27 November 2018, Kyiv, Ukraine). Vol 2318. P. 176–187.

17. Корнієнко Б. Я., Галата Л. П. Дослідження імітаційного полігону захисту критичних інформаційних ресурсів методом IRISK. *Моделювання та інформаційні технології*. 2018. Вип. 83. С. 34–41.

18. Корнієнко Б. Я., Галата Л. П. Побудова та тестування імітаційного полігону захисту критичних інформаційних ресурсів. *Наукоємні технології*. 2017. № 4 (36). С. 316–322. doi.org/10.18372/2310-5461.36.12229.

Галата Л. П., Корнієнко Б. Я., Заболотний В. В.

МАТЕМАТИЧНА МОДЕЛЬ ПРОТИДІЇ ЗАГРОЗАМ У СИСТЕМІ ЗАХИСТУ КРИТИЧНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

У статті наведені основні проблеми інформаційної безпеки критичних інформаційних ресурсів та причини їх виникнення. Розглянуто приклади основних загроз для систем захисту критичних інформаційних ресурсів, знайдених після аналізу справжніх інцидентів. Здійснено аналіз основних підходів до побудови математичних моделей систем захисту інформації. Запропонована математична модель протидії впливу внутрішніх та зовнішніх загроз на систему захисту критичних інформаційних ресурсів виробництва мінеральних добрив. Поетапно розписаний процес побудови математичної моделі протидії загрозам у системі захисту критичних інформаційних ресурсів за допомогою Марківського ланцюга. Запропонована методика знаходження актуальних загроз безпеці даних при їх обробці. Розроблено програмний модуль на мові програмування Python. Проведено дослідження на імітаційній моделі захисту критичних інформаційних ресурсів. Наведені приклади розрахунків імовірностей знаходження математичної моделі інформаційної системи захисту критичних інформаційних ресурсів в одному з чотирьох станів (загроза не настала; загроза настала, але не була реалізована; загроза настала, була реалізована; загроза настала, але була відбита системою захисту). Приклади аналізу числових результатів за допомогою запропонованої методики наочно показують, що їх використання допомагає з визначенням загроз, які є актуальними для досліджуваної системи та можуть використовуватись на практиці. Недоліком запропонованої методики є необхідність розгляду поведінки системи захисту критичних інформаційних ресурсів при дії на неї кожного типу загроз окремо і неможливість визначення поведінки при одночасній дії кількох загроз. Але з іншого боку вивчення впливу кожної загрози окремо дозволяє більш детально вивчити кожен її тип та визначити ті, вірогідність появи яких є найбільшою.

Ключові слова: математична модель; загроза; система захисту; критичні інформаційні ресурси.

Galata L. P., Korniyenko B. Y., Zabolotny V. V.

MATHEMATICAL MODEL OF COUNTERACTION TO THREATS IN PROTECTION SYSTEM OF CRITICAL INFORMATION RESOURCES

The article presents the main problems of information security of critical information resources and the reasons for their occurrence. Examples of the main threats to critical information resource protection systems found after the analysis of these incidents are considered. The analysis of the main approaches to the construction of mathematical models of information security systems is carried out. The mathematical model of counteraction to the influence of internal and external threats on the system of protection of critical informative resources of production of mineral fertilizers is proposed. The process of constructing a mathematical model for counteracting threats in the system of protection of critical information resources with the help of the Markov chain is gradually presented. The method of finding actual threats to data security during processing has been proposed. The program module has been developed by programming language Python. The research on the simulation model of the protection of critical information resources was conducted. Examples of calculations of the probability of finding a mathematical model of an information security system of critical information resources in one of the four states are presented (the threat did not occur, the threat came, but was not realized; the threat came, it was realized; the threat came, but was reflected by the system of protection). Examples of analyzing numerical results using the proposed methodology clearly show that their use helps to identify threats that are relevant to the system under study and can be used in practice. The disadvantage of the proposed method is the need to consider the behavior of the critical information resource protection systems under the influence of each type of threat separately and the impossibility of determining the behavior of the simultaneous action of several threats. But on the other hand, the study of the impact of each threat individually allows one to study in more detail each of its types and identify those whose likelihood of occurrence is greatest.

Key words: mathematical model; threat; system of protection; critical information resources.

Галата Л. П., Корниенко Б. Я., Заболотный В. В.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ В СИСТЕМЕ ЗАЩИТЫ КРИТИЧЕСКИХ ИНФОРМАЦИОННЫХ РЕСУРСОВ

В статье приведены основные проблемы информационной безопасности критических информационных ресурсов и причины их возникновения. Рассмотрены примеры основных угроз для систем критических информационных ресурсов, найденных после анализа настоящих инцидентов. Осуществлен анализ основных подходов к построению математических моделей систем защиты информации. Предложенная математическая модель противодействия влиянию внутренних и внешних угроз на систему защиты критических информационных ресурсов производства минеральных удобрений. Поэтапно расписан процесс построения математической модели противодействия угрозам в системе защиты критических информационных ресурсов с помощью марковской цепи. Предложенная методика нахождения актуальных

угроз безопасности данных при их обработке. Разработан программный модуль на языке программирования Python. Проведено исследование на имитационной модели защиты критических информационных ресурсов. Приведены примеры расчетов вероятностей нахождения математической модели информационной системы критических информационных ресурсов в одном из четырех состояний (угроза не наступила, угроза наступила, но не была реализована, угроза наступила, была реализована, угроза наступила, но была отбита системой защиты). Примеры анализа числовых результатов с помощью предложенной методики наглядно показывают, что их использование помогает с определением угроз, которые актуальны для исследуемой системы и могут использоваться на практике. Недостатком предложенной методики является необходимость рассмотрения поведения системы защиты критических информационных ресурсов при воздействии на нее каждого типа угроз отдельно и невозможность определения поведения при одновременном действии нескольких угроз. Но, с другой стороны, изучение влияния каждой угрозы отдельно позволяет более детально изучить каждый ее тип и определить те, вероятность появления которых является наибольшей.

Ключевые слова: математическая модель; угроза; система защиты; критические информационные ресурсы.

Стаття надійшла до редакції 10.06.2019 р.
Прийнято до друку 20.09.2019 р.