УДК 004.056

С.П. Мурза
Л.О. Нікіфорова
А.А. Шиян
О.М. Хошаба

Використання рольової моделі управління доступом для запобігання витоку інформації через співробітників підприємства

Вінницький національний технічний університет

Анотація

В статті визначено важливість захисту підприємства від витоку інформації, розглянуто види загроз щодо безпеки інформації та комплекс заходів захисту підприємства від витоку інформації, визначено специфіку використання рольової моделі управління доступом для запобігання витоку інформації через робітників підприємства.

Ключові слова: *інформація, захист інформації, рольова модель управління доступом.*

Abstract

The article defines the importance of protecting the enterprise from information leakage, examines the types of information security threats and a set of measures to protect the enterprise from information leakage, specifies the use of the role model of access control to prevent the leakage of information through employees of the enterprise.

Key words: *information, information protection, access control role model.*

Ефективність бізнесу в багатьох випадках залежить від збереження конфіденційності, цілісності та доступності інформації. В даний час однією з найбільш актуальних загроз у сфері інформаційної безпеки є витік конфіденційних даних від несанкціонованих дій користувачів [1].

Серед загроз безпеки інформації підприємства виділяють загрози випадкові та ненавмисні. Їх джерелом можуть бути вихід з ладу апаратних засобів, неправильні дії працівників автоматизованих інформаційних систем або її користувачів, ненавмисне допущення помилок у програмному забезпеченні та ін [2]. Проте більше всього уваги необхідно приділяти загрозам навмисним, які на відміну від випадкових переслідують ціль нанесення збитку деякій системі, технології або користувачам. Основним джерелом витоку інформації з підприємства є її персонал [3].

Необхідний комплекс заходів захисту підприємства від витоку інформації включає [4]:

- використання особливого режиму конфіденційності;
- використання організаційних заходів захисту інформації;
- обмежений доступ персоналу до конфіденційної інформації;
- використання технічних засобів захисту інформації;
- систематичний контролю за дотриманням встановленого режиму конфіденційності.

Зазначені заходи можуть відрізнятись масштабами та формами для кожного окремо взятого підприємства, це в першу чергу залежить від фінансових, виробничих та інших можливостей підприємства, а також безпосередньо від обсягів конфіденційної інформації та ступеню її значимості для підприємства [5]. Важливо зазначити що весь перелік зазначених заходів обов'язково необхідно планувати і використовувати з урахуванням особливостей функціонування інформаційної системи підприємства [6].

При великій кількості користувачів традиційні підсистеми управління доступом стають вкрай складними для адміністрування. Число зв'язків у них пропорційне добутку кількості користувачів на кількість об'єктів. Необхідні рішення в об'єктно-орієнтованому стилі, здатні цю складність знизити [7]. Для мінімізації загрози витоку конфіденційної інформації доцільно застосувати рольову модель управління доступом, тобто розмежування доступу в інформаційній системі, яка автоматизує організаційно-технологічні й організаційно-управлінські процеси, буде будуватися на основі функціонально-рольових відносин. Система є безпечною, якщо будь-який користувач системи, який працює в певному сеансі, зможе здійснити дії, які вимагають певних повноважень тільки в тому випадку, коли ці повноваження належать відповідно до сукупності усіх ролей, що беруть участь у цьому сеансі [8].

Рольова модель безпеки сформувалася внаслідок розвитку дискреційної моделі [9]. Проте, на відміну від вихідної моделі вона має нові властивості: управління доступом в ній здійснюється як на

основі визначення характеру доступу для ролей, так і шляхом зіставлення ролей користувачам і установки правил, що регламентують використання ролей під час сеансів.

У рольовій моделі поняття «суб'єкт» замінюється поняттями «користувач» і «роль» [10]. Користувач -це людина, яка працює з системою та виконує певні службові обов'язки. Роль - це активно діюча в системі абстрактна сутність, з якою пов'язаний набір повноважень, необхідних для виконання певних завдань. Подібний поділ добре відображає особливості діяльності різних організацій, що призвело до поширення рольових політик безпеки [11]. При цьому як один користувач може бути авторизований адміністратором на виконання однієї або кількох ролей, так і одна роль може бути присвоєна одному або декільком користувачам [12].

Розмежування доступу для кожної ролі потребує виокремлення набору повноважень, які являють собою набір прав доступу до об'єктів системи [13]. Призначення повноваження ролям здійснюється у відповідності до принципу найменших привілеїв, тобто кожному користувачеві відводиться лише мінімально необхідні для виконання його роботи повноваження [14]. Повноваження – це право здійснювати певні функціонально-логічні процедури над всією сукупністю об'єктів системи або ж над певною їх групою[15].

Використання рольової політики управління доступом здійснюється в дві стадії [16]:

- кожній ролі вказується набір повноважень (дозволів на доступ до окремих об'єктів системи);
- кожному користувачеві формується список доступних йому ролей.

Відповідно формальні специфікації рольових моделей повинні регламентуватись тим або ж іншим способом, а точніше в рамках тієї чи іншої політики, і визначення повноважень ролям і призначення ролей користувачам [17].

Рольова модель буде ефективною у використанні при умові правильного розподілення повноважень і роботи вцілому [18]. Звичайно ж, для забезпечення інформаційної безпеки одного застосування рольової моделі управління доступом недостатньо [19]. Необхідні програмні, технічні засоби захисту, забезпечення адекватної документації, її виконання й актуалізація [20].

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Матвієнко О.В. Основи інформаційного менеджменту: Навчальний посібник.- К.: Центр навчальної літератури, 2004.- 128 с.
2. Голубченко О.Л. Політика інформаційної безпеки / О.Л. Голубченко. – Луганськ : Вид-во СНК ім. В. Даля, 2009. – 300 с.
3. Грайворонський М.В. Безпека інформаційно-комунікаційних систем / Грайворонський М.В., Новіков О.М. – К. : Вид. група BHV, 2009. – 608 с.
4. Політика інформаційної безпеки. [Електронний ресурс]. – Доступний з http://uk.wikipedia.org/wiki/Політика_інформаційної_безпеки.
5. Галатенко В. А. Основи інформаційної безпеки. - М: ІнтернетУніверситет Інформаційних Технологій - Інтуїт. РУ, 2003.
6. Грязнов Є., Панасенко С. Безпека локальних мереж - Електрон. журнал "Мир і безпека" № 2, 2003. - Режим доступу до журн.: www.daily.sec.ru.
7. Азарова А.О. Розроблення принципів побудови раціонального методу формалізації процесу оцінювання конкурентоспроможності вітчизняних підприємств / А.О. Азарова, О.В. Житкевич // Інноваційна економіка. - № (41). – 2013. – С. 93-96
8. Азарова А.О. Управління конкурентоспроможністю вітчизняних підприємств як базовий важіль забезпечення інноваційного розвитку економіки / А.О. Азарова, О.В. Житкевич // Колективна монографія: Sosio economic problems of management Collevtive monograph: - Thorpe-Bowker:registered: Melbourne, Australia, 2015. – С. 209-218.
9. Азарова, А. О. Математичні моделі та методи оцінювання фінансового стану підприємства [Текст] : монографія / А. О. Азарова, О. В. Рузакова. — Вінниця : ВНТУ, 2010. — 172 с.
10. Азарова А. О. Розробка методики визначення компетентності експертів при побудові СППР щодо оцінювання фінансового стану підприємства [Текст] / А. О. Азарова, О. В. Рузакова, Л. В. Воронюк // Механізми регулювання економіки. – 2006. –№ 2. – С.133–138.
11. Азарова А. О. Математичні моделі та методи управління мотивацією персоналу [Текст] / А . О. Азарова, О. А. Ковальчук . — Вінниця : ВНТУ, 2014. – 140 с.
12. Ткачук Л. М. Оцінка ефективності роботи консолідованого інформаційного ресурсу аналізу діяльності банків [Текст] / Л. М. Ткачук А.П.Ткачук // Materials of the XIII International scientific and practical Conference «SCIENCE AND CIVILIZATION- 2017»,Volume 9 : Modern information technology . Agriculture . Mathematics . Construction and architecture . Sheffield. Science and education LTD - P.28-30.

13. Азарова А. О. Математична модель та метод оцінки рівня ризику структури капіталу засобами нейронної мережі Хопфілда [Текст] / А. О. Азарова, О. М. Роїк, Л. А. Кілимник // Актуальні проблеми економіки. - 2010. –№ 1(103). – С. 245–253.

14. Методичні вказівки до проведення практичних занять та до виконання самостійної й індивідуальної роботи з дисципліни «Основи науково-дослідної роботи» для студентів напрямів підготовки 6.030601 – «Менеджмент» та 6.170103 – «Управління інформаційною безпекою» / Укладачі: А. О. Азарова, В. В. Карпінець. – Вінниця: ВНТУ, 2013. – 44 с.

15. Ткачук Л. М. Організаційно-правові аспекти державного управління регіональним розвитком / Л. М. Ткачук, Т. К. Калугаряну // Ефективна економіка. – 2012. – № 12. – [Електронний ресурс]. – URL: http: //www.economy. nayka.com.ua

16. Небава М. І. Управління регіональним розвитком : Ел. навч. посібник / М. І. Небава, Л. М. Ткачук [Електронний ресурс]. – URL : https://web.posibnyky.vntu.edu.ua/fmib/ 25nebava_upravlinnya_regionalnym_rozvytkom/

17. Ткачук Л. М. Впровадження системи RAROC для оцінки ефективності консолідованого інформаційного ресурсу аналізу діяльності банків / Л. М. Ткачук , А. П. Ткачук, В. О. Романець // Materials of the XIII International scientific and practical Conference «Cutting-edge science-2017»,Volume 5 : Modern information technology . Agriculture . Mathematics. Construction and architecture . Sheffield. Science and education LTD - P.14-16.

18. Ткачук Л. М. Інформаційна безпека України / Л. М. Ткачук, К. В. Волчаста // Матеріали VIII науково-практичної конференції «Актуальні проблеми управління інформаційною безпекою держави (Київ, 24 травня 2017 р.)» - Київ : Нац. Акад. СБУ, 2017 . - С. 138-140.

19. Фурик В. Г. Самофінансування підприємства:механізм реалізації в умовах відкритої та прихованої форм / В. Г. Фурик, Л. М. Ткачук, А. О. Гринь // Економіка і суспільство. – 2018. – №16. Режим доступу :http://economyandsociety.in.ua/index.php/journal-16.

20. Коваль Н.О.Саморегуляція соціальної політики в умовах безперервного розвитку економічної системи / Н. О. Коваль, Л. М. Ткачук // Економіка і суспільство. – 2018. – №19. Режим доступу :http://economyandsociety.in.ua/index.php/journal-19.

Мурза Сергій Павлович*- студент групи КІН-18мі, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця.*

Нікіфорова Лілія Олександрівна *- к.е.н., доцент каф. ЕПВМ, Вінницький національний технічний університет, м. Вінниця, e-mail:nikiforovalilia@gmail.com, nikiforova@vntu.edu.ua*

Шиян Анатолій Антонович *- канд. фіз.-мат. наук, професор кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет*

Хошаба Олександр Мирославович *- к.т.н., доцент кафедри програмного забезпечення, Вінницький національний технічний університет, м. Вінниця, e-mail: oleksandr.khoshaba@gmail.com*

Murza Serhii P. *- student, faculty of management Vinnitsa National Technical University, Vinnitsa.*

Nikiforova Liliya Oleksandrivna *– Ph.D. (Econ.), Associate Professor, Associate Professor of Business Economics and Production Management, Vinnytsia National Technical University, Vinnytsa.*

Shiyan Anatoliy A. *– PhD, Professor of Department of Management and Information Systems Security, Vinnytsia National Technical University, Vinnytsia, email : Anatoliy.a.shiyan@gmail.com*

Khoshaba Olexandr *– PhD (Tech), asistant professor of Department of software, Vinnytsia National Technical University, Vinnytsa.*