УДК

С.П. Мурза
А.О. Азарова

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. 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 [2].

Необхідний комплекс заходів захисту підприємства від витоку інформації включає [3]:

- 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. Важливо зазначити що весь перелік зазначених заходів обов'язково необхідно планувати і використовувати з урахуванням особливостей функціонування інформаційної системи підприємства.

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. 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 [4].

Рольова модель безпеки сформувалася внаслідок розвитку дискреційної моделі. 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» [5]. 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. 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.

Розмежування доступу для кожної ролі потребує виокремлення набору повноважень, які являють собою набір прав доступу до об'єктів системи. Призначення повноваження ролям здійснюється у відповідності до принципу найменших привілеїв, тобто кожному користувачеві відводиться лише мінімально необхідні для виконання його роботи повноваження. Повноваження – це право здійснювати певні функціонально-логічні процедури над всією сукупністю об'єктів системи або ж над певною їх групою[6].

Використання рольової політики управління доступом здійснюється в дві стадії [5]:

- 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.

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

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.

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

***Азарова Анжеліка Олексіївна –** к.т.н, проф. каф. МБІС, заст. декана факультету менеджменту та інформаційної безпеки з наукової роботи та міжнародного співробітництва Вінницького національного технічного університету, м.Вінниця, e-mail: azarova.angelika@gmail.com.*

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

***Anzhelika Azarova** — Ph.D., Professor, Deputy dean of the Faculty of management and information security by scientific work and international cooperation Vinnytsia National Technical University, Vinnytsia, e-mail: azarova.angelika@gmail.com.*