УДК 004.9

О.М. ЯШИНА
Хмельницький національний університет

КЕРУВАННЯ ДОСТУПОМ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ТОРГІВЕЛЬНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ СМАРТ-ТЕХНОЛОГІЙ В КОНТЕКСТІ ПОЛІТИКИ БЕЗПЕКИ

В даній статті розглядаються теоретичні аспекти реалізації та дотримання політики безпеки в торгівельних мережах в єдиному просторі з системою керування доступом до інформаційної системи.

Ключові слова: смарт-технології, інформаційні технології, інформаційні системи, доступ до інформаційної системи, політика безпеки.

OXANA YASHYNA
Khmelnytsky National University

THE ACCESS CONTROL OF INFORMATION SYSTEM OF THE COMMERCIAL NETWORK WITH THE USE OF SMART TECHNOLOGIES IN THE CONTEXT OF SECURITY POLICY

This article discusses the theoretical aspects of the implementation and observance of security policy in trade networks in the same space with access control system to the information system. The access control of information system of the commercial network can be represented as a set of graphs. This set of graphs of access is considered as a phase space, and the functioning of the information system of trading network is the trajectory of this phase space. Therefore, the protection of information is to avoid undesirable trajectories that is to prevent unwanted access to information system of distribution network.

Keywords: smart technology, information technology, information systems, access to information system, security policy.

Постановка задачі

На сьогоднішній день інформаційні технології впроваджуються у всі сфери життєдіяльності людини: освіту, науку, економіку і т.д. В сучасному суспільстві інформація є основою для всіх державних, наукових, економічних та інших процесів, тому дуже важливим є оперативний доступ до потрібної інформації, причому інформаційні потоки настільки потужні, що це дійсно є проблемою номер один [1, 2].

Саме тому в ході проектування та експлуатації інформаційних систем різного призначення проблеми забезпечення інформаційної безпеки грають ключову роль. Керування доступом повинно враховувати, з одного боку, як наявність штатних засобів реалізації механізмів забезпечення безпеки (механізми, вбудовані в операційні середовища), так і наявність різних рівнів керування – персональний, корпоративний, регіональний і т.д. [3].

Безперечно, що захисту інформації при створенні інформаційних систем приділяється велика увага. Однак, рівень готовності до теоретичних та практичних рішень проблеми безпеки далекий від бажаного. В методології проектування систем безпеки основною проблемою є відсутність єдиного обґрунтованого підходу до розкриття та експлуатації захищених інформаційних систем.

Системи безпеки в інформаційних системах, як правило, вбудовуються в уже готові програмно-технічні рішення. Саме тому виникає певна синтетична задача – реалізація політики безпеки та гарантоване її виконання в конкретній системі.

Для підтримки гарантій політики безпеки необхідно розглядати певну модель керування доступом до інформаційної системи. При цьому процеси керування повинні бути конструктивними, виконуваними та оптимальними з тої чи іншої точки зору (наприклад, з точки зору трудомісткості роботи адміністратора чи об'єму об'єктів збереження, що описують захист).

Метою статті є визначення теоретичних аспектів реалізації та дотримання політики безпеки в торгівельних мережах в єдиному просторі з системою керування доступом до інформаційної системи.

Аналіз досліджень та публікацій

Як уже зазначалось у [1], методологічною основою нашого дослідження стали праці Фороузана Б. А., Шнайера Б. та інших. Деякими аспектами застосування смарт-технологій займались такі російські вчені, як Шорін Д. В., Шкурко М.І., Борисенко О. В., Стасенко Л., Куліков А.Л. Загалом же в теперішній час виконується велика кількість різноманітних досліджень, присвячених застосуванню інформаційних технологій в розв'язанні економічних, соціальних та інших задач. Однак, потрібно відмітити, що проблема керування доступом займає незначне місце у вітчизняних та зарубіжних роботах. Керування зазвичай декларується чи зводиться до планування [4]. Опис систем керування доступом для конкретних операційних середовищ чи прикладних систем залишає відкритим питання про те, наскільки різноманітні помилки в керуванні доступом порушують захищеність та не дозволяють говорити про певний ґрунтовний системний підхід в організації керування. Не зважаючи на те, що дослідження в галузі застосування смарт-технологій постійно проводяться, наукових робіт, присвячених застосуванню смарт-технологій для забезпечення безпеки доступу користувачів до інформаційних систем супермаркету в системі політики безпеки, недостатньо, що і обумовило виявлення до цього питання підвищеного наукового та практичного інтересу.

Виклад основного матеріалу

В захищених інформаційних системах завжди присутня активна компонента (суб'єкт), що виконує

контроль операцій суб'єктів над об'єктами та відповідає за реалізацію політики безпеки. Для виконання операцій над об'єктами в захищеній інформаційній системі необхідна додаткова інформація про дозволені та заборонені операції суб'єктів над об'єктами та об'єкт, що цю інформацію містить. Всі питання безпеки інформації описуються доступом суб'єктів до об'єктів.

Важливим є також той факт, що політика безпеки описує в загальному випадку нестаціонарний стан захищеності. Захищена система може змінюватись, доповнюватись новими компонентами (суб'єктами, об'єктами, операціями суб'єктів над об'єктами). Очевидним є те, що політика безпеки повинна підтримуватись у часі. А тому в процесі вивчення властивості захищеності системи повинні бути доповнені процедурами керування доступом.

З іншого боку, нестаціонарність захищеної інформаційної системи, а також питання реалізації політики безпеки в конкретних конструкціях захищеної системи передбачають необхідність розгляду задачі гарантування заданої політики безпеки.

Комп'ютерна безпека розв'язує чотири класи взаємопов'язаних задач:

- формулювання та вивчення політики безпеки;
- реалізація політики безпеки;
- гарантування заданої політики безпеки;
- керування доступом.

Розглядаючи питання безпеки інформації в інформаційній системі торгівельних мереж, можна говорити про наявність деяких «небажаних станів» цієї системи, що характеризують її «захищеність». Поняття «захищеність» принципово не відрізняється від будь-яких інших властивостей технічної системи, наприклад, «надійності роботи», та є для системи зовнішньою, тобто заданою.

Інтегральною характеристикою, що описує властивості захищеної системи є політика безпеки – якісний або кількісно-якісний опис захищеності, що виражається в термінах, які характеризують систему.

Найчастіше розглядаються політики безпеки, що пов'язані з поняттям «доступ» та контроль над цим доступом. Доступ – це категорія суб'єктно-об'єктної моделі (суб'єкти – активна компонента системи; активність розуміється як можливість виконання операцій над об'єктами – пасивною компонентою, що описує процес виконання операцій суб'єктів над об'єктами). Опис політики безпеки включає в себе множину можливих операцій над об'єктами, а також для кожної пари «суб'єкт – об'єкт» (S_i, O_j) множину дозволених операцій як підмножину множини можливих операцій [5].

Інформаційну систему торгівельної мережі представимо у вигляді сукупності взаємодіючих сутностей – суб'єктів (S) та об'єктів (O). Суб'єкт безпеки – активна системна складова, до якої застосовується політика безпеки, а об'єкт – пасивна.

У ролі суб'єктів у нас виступають користувачі інформаційної системи, тобто працівники торгівельного закладу (супермаркету). Об'єктом є данні, файли, системні таблиці і т.д.

На практиці реалізація політики безпеки полягає в присвоєнні суб'єктам та об'єктам ідентифікаторів та фіксації набору правил, що дозволяють визначити, чи має даний суб'єкт авторизацію, яка достатня для надання до даного об'єкту вказаного типу доступу.

Отже, якщо S – суб'єкт, O – об'єкт, то можливим є введення операції доступу, під якою розуміється використання *i*-м суб'єктом інформації з *j*-го об'єкту. Ця операція є інформаційним потоком від об'єкта O_j до суб'єкта S_i.

Оскільки суб'єкти в інформаційній системі можуть породжуватись тільки активною складовою (суб'єктами) з об'єктів, то в процесі породження нового суб'єкта приймає участь інший суб'єкт та деякий об'єкт, що є джерелом для породженого суб'єкту. В результаті з'являється новий суб'єкт: $S_i \to O_j \to S_n$.

В момент ідентифікації користувача інформаційної системи проходить створення ряду суб'єктів (системних процесів), за допомогою яких користувач може здійснювати доступ до об'єктів. Діяльність такого користувача може бути описана графом доступу (рис. 1).

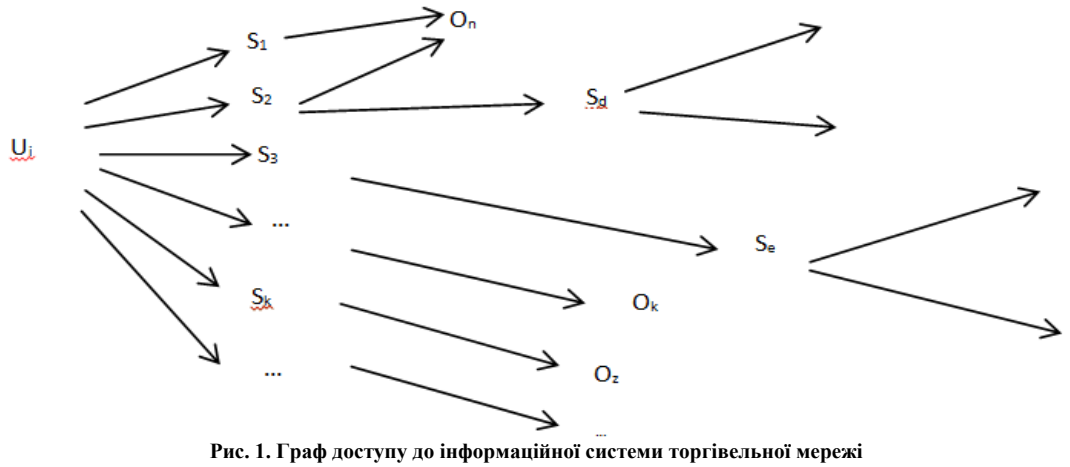

Рис. 1. Граф доступу до інформаційної системи торгівельної мережі

Множину графів доступу можна розглядати як фазовий простір, а функціонування конкретної системи – як траєкторію у фазовому просторі. Захист інформації в такому випадку полягає в уникненні небажаних траєкторій. Практично таке керування доступом стає можливим лише обмеженням доступу в кожний момент часу, тобто всі питання безпеки інформації визначаються описом доступів суб'єктів до об'єктів.

Висновки

Керування доступом до інформаційної системи торгівельної мережі можна подати у вигляді множини графів. Дана множина графів доступу розглядається як фазовий простір, а функціонування інформаційної системи торгівельної мережі полягає у траєкторії цього фазового простору.

Отже, уникнення небажаних траєкторій і є захистом інформації, тобто уникненням небажаного доступу до інформаційної системи торгівельної мережі.

Література

1. Шинкарук О.М. Використання смарт-карт для ідентифікації користувачів інформаційних систем / О.М. Шинкарук, О.М. Яшина // Вісник Хмельницького національного університету. – Хмельницький : ХНУ, 2013. – № 1. – С. 114–116.

2. Яшина О.М. Обгрунтування можливостей застосування смарт-технологій для управління доступом до інформаційних систем / О.М. Яшина // Збірник наукових праць за матеріалами сьомої міжнародної науково-технічної конференції «Актуальні проблеми комп'ютерних технологій 2013». – Хмельницький, 2013. – С. 392–397.

3. Шкурко М.И. Программные средства автоматизации обработки информации в системе документооборота на базе распределённой архитектуры с применением smart-технологий : дис. ... канд. техн. наук : 05.13.17 / Шкурко М. И. – М., 2008. – 158 с.

4. Биктимиров М.Р. Избранные главы компьютерной безопасности / М.Р. Биктимиров, А.Ю. Щербаков. – Казань : Изд-во Казанского математического общества, 2004. – 372 с.

5. Биктимиров М.Р. Модели управления доступом в распределенных компьютерных системах : дис. … канд. техн. наук : 05.13.18 / Биктимиров М.Р. – Казань, 2008. – 137 с.

References

1. Shynkaruk O. M., Yashina O. M. Using of smart cards for identification of users of information systems. Herald of Khmelnytsky National University. Khmelnytsky: KNU. Issue 1, 2013. P. 114–116.

2. Yashina O. M. Substantiation of opportunities of the smart technologies using for access control to information systems. Collection of scientific essays of materials of the 7 International scientific-technical conference "Actual problems of computer technologies 2013". Khmelnytsky, 2013. P. 392-397.

3. Shkurko M. I. Software of automation of information processing in the document management system based on a distributed architecture using smart technology: dissertation ... of candidate of technical sciences: 05.13.17. Moscow, 2008. 158 p.

4. Biktimirov M. R., A. Shcherbakov A.Y. Selected chapters of computer security. Kazan: Publishing house of Kazan mathematical society, 2004. 372 p.

5. Biktimirov M. R. Model of access control in distributed computer systems: dissertation ... of candidate of technical sciences: 05.13.18. Kazan, 2008. 137 p.

Рецензія/Peer review : 21.11.2014 р. Надрукована/Printed :29.11.2014 р.
Стаття рецензована редакційною колегією