УДК 004.9

О.М. ЯШИНА
Хмельницький національний університет

ОБҐРУНТУВАННЯ АЛГОРИТМУ КЕРУВАННЯ ДОСТУПОМ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ТОРГІВЕЛЬНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ СМАРТ-ТЕХНОЛОГІЙ

В даній статті надано у формалізованому вигляді аспекти реалізації алгоритму керування доступом до інформаційних ресурсів торгівельних мереж.

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

OKSANA YASHYNA
Khmelnytsky National University

JUSTIFICATION OF THE ALGORITHM TO CONTROL ACCESS TO THE INFORMATION SYSTEM OF THE TRADING NETWORK WITH THE USE OF SMART TECHNOLOGIES

This article presents the formalized aspects of the implementation of the algorithm to control access to information resources of trading networks. Approaches to access control have significant drawbacks. To access the information system a supermarket requires certain elements and procedures. The main point in the access algorithm to the management of information system of supermarket retail chain is the rejection of different types of managed resources. The aim of the article was the formalized representation of aspects of the algorithmic implementation of access control to the information system of trading networks with the use of smart technologies.

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

Постановка задачі

Торговельне підприємство – основна ланка сфери обігу, що володіє господарською і юридичною самостійністю, здійснює просування товарів від виробників до споживачів за допомогою купівлі-продажу і реалізує власні інтереси на основі задоволення потреб людей, представлених на ринку. Функціонування підприємства забезпечує його персонал – сукупність осіб, що працюють та вкладають свою працю, фізичні та розумові здібності, знання та навички у проведенні господарської, фінансової діяльності, реалізують його статутні завдання (закупівлю та реалізацію товару, виробництво продукції, надання послуг та інше). Частина персоналу (в залежності від підприємства це можуть бути бухгалтера, менеджери, керівники, охорона та інші) на підприємстві має доступ до фінансових операцій, документації, конфіденційної інформації, яка може бути вкрадена. На сьогоднішній день відомості про діяльність практично усіх торгових підприємств зосереджені у інформаційних системах.

Зростання складності інформаційних систем, підвищення ступеня інтеграції бізнес-процесів підприємств, подальша глобалізація світової економіки, зростання темпів бізнесового середовища вимагає створення інформаційних систем, які здатні аналізувати поточну ситуацію та швидко адаптуватися до змін [1, 2]. На ймовірність злому інформаційної системи впливає ряд контрольованих та неконтрольованих факторів.

Неконтрольовані фактори: температура навколишнього середовища; нерівномірність напруги в електромережі; зношування обладнання внаслідок експлуатації і т.д.

До контрольованих факторів віднесемо плинність кадрів; використання картки із корисницьких мотивів; довжина магнітного запису (особливості безпеки смарт-карт).

Саме тому при проектуванні 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. [4].

Процес впровадження нових інформаційних систем, при усій їх незаперечній корисності, несе у собі нові витрати та ризики для компанії. Зловмисником може бути як стороння людина, так і працівник підприємства. Саме тому на підприємствах доцільним є використання захисних систем – систем контролю доступу, які включають в себе необхідні елементи для захисту інформації підприємства. У [1, 2] розглядається можливість та доцільність використання смарт-карти для доступу до інформаційних ресурсів торгівельних мереж супермаркету, які забезпечують необхідний рівень захисту. В зв'язку із цим є актуальним алгоритмічне забезпечення контролю доступу до інформаційних систем торгівельних мереж із застосуванням смарт-технологій.

Метою статті є формалізоване подання аспектів алгоритмічної реалізації керування доступом до інформаційної системи торгівельних мереж із застосуванням смарт-технологій.

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

На нашу думку, підходи до керування доступом мають багато досить істотних недоліків, до яких можемо віднести відсутність документованого обґрунтування рішення з присвоєння або позбавлення прав доступу; відсутність шаблонів прав доступу; різнотипність керованих ресурсів і т.д.

В результаті права доступу є часто неадекватними до завдань, які виконує працівник – прав доступу забагато або замало. Недостатність прав доступу призводить до неможливості або істотних затримок у виконанні завдання, що негативно впливає на бізнес-процес загалом.

Надлишок прав доступу, хоч і створює додаткові можливості для працівника щодо вибору різних способів вирішення завдання, загалом зменшує захищеність інформаційної системи і не відповідає принципу найменших прав доступу.

У алгоритмі, запропонованому нами, основним моментом є відмова від різнотипних керованих ресурсів, що зберігають окремі варіанти облікових записів однієї й тієї ж самої людини, оскільки це призводить до того, що користувачу необхідно запам’ятовувати велику кількість паролів

Для доступу до інформаційної системи супермаркету необхідні певні елементи та процедури. На рис. 1 подано схему алгоритму доступу до інформаційної системи супермаркету на основі смарт-технологій.

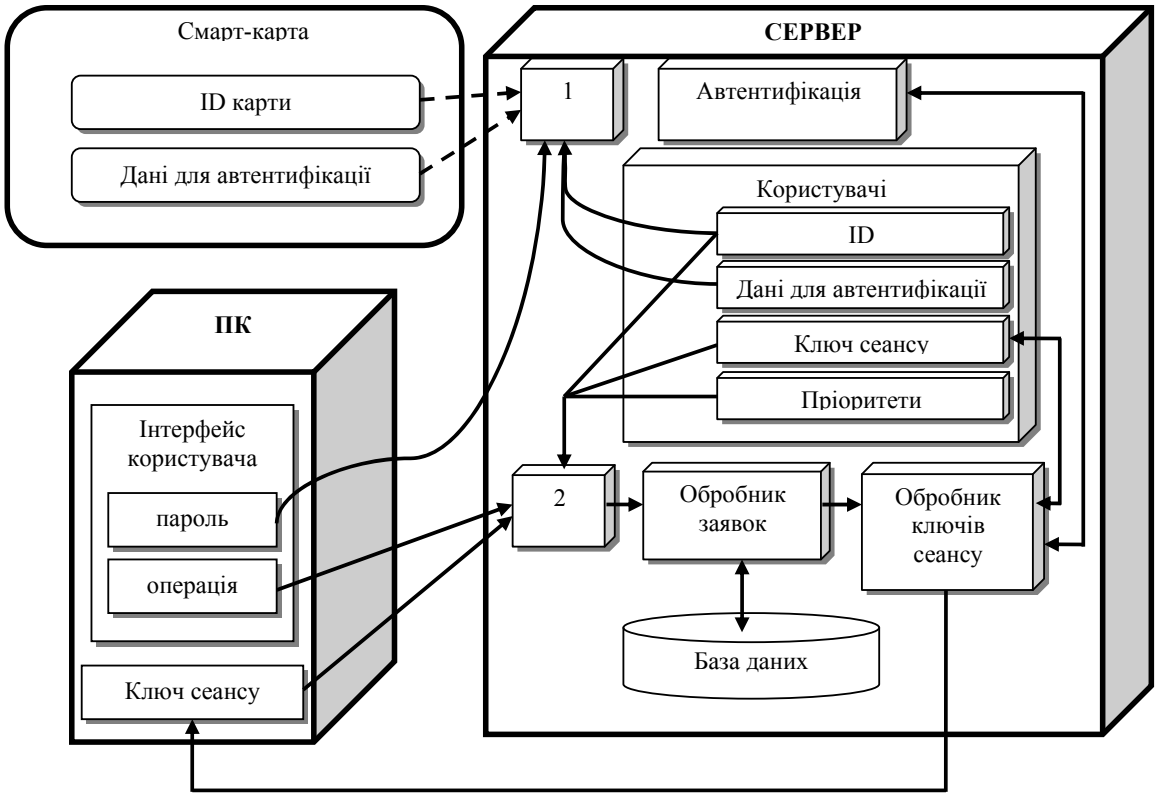

Рис. 1. Схема алгоритму доступу до інформаційної системи торгівельної мережі супермаркету на основі смарт-технологій

Елементами надання доступу до інформаційної системи торгівельної мережі супермаркету є смарт-карта, персональний комп’ютер (ПК), сервер. На смарт-карті зберігається її ідентифікатор (ID), за яким проводиться ідентифікація користувача (працівника супермаркету) в базі користувачів на сервері, а також «дані для автентифікації» – дані, що надані смарт-картою.

Персональний комп’ютер представляє собою блок, який виконує дві функції: служить каналом зв’язку між смарт-картою та сервером, і є засобом спілкування користувача (працівника супермаркету) із сервером. Інтерфейс (Користувач) – блок, який забезпечує взаємодію з користувачем. Під паролем мається на увазі спосіб, яким користувач підтверджує свою особу, тут під паролем розуміється все, що необхідно пред’явити користувачу для підтвердження своєї особи. Операція – дії, які необхідно виконати з базою даних, задається користувачем після авторизації.

Ключ сеансу – деякий код, який надається в користування «ПК» на певний термін. Він видається при виконанні користувачем автетифікації. На сервері зберігаються всі дані для автентифікації і пріоритетного проведення операцій (заявок).

Автентифікація – процес підтвердження особи користувача на основі одного з можливих способів

автентифікації, наприклад: введення паролю користувачем, біометричний пароль, тощо. Можлива багаторівнева автентифікація, коли потрібно підтвердити свою особу не лише одним паролем, наприклад, після ведення паролю потрібно ввести код, який приходить у вигляді смс-повідомлення на зв'язаний з даним користувачем номер або на електронну адресу;

Користувачі – база користувачів, тут для кожного користувача вказано ID його смарт-карти, дані для автентифікації, деякі з пріоритетів доступу а також ключ сеансу. ID – ідентифікатор картки що зв'язана з даним користувачем. Дані для автентифікації – надані сервером. Ключ сеансу – поле, в якому зберігається ключ сеансу за умови, що він виданий обробником ключів сеансу. Після закінчення терміну дії ключа сеансу, він видаляється і для того щоб отримати повторно доступ необхідно пройти процес авторизації. Пріоритети – список пріоритетів користувача.

Обробник заявок – блок в якому відбувається відбір або формування черги заявок за певним критерієм на основі пріоритетів отриманих з бази користувачів і пріоритетів заявки. Обробник ключів сеансу – контролює видачу та термін дії ключів сеансу. Ключ сеансу генерується випадковим чином після успішної автентифікації, далі цей ключ записується в базу користувачів в поле «ключ сеансу».

Доступ до інформаційної системи включає процедуру авторизації та процедуру виконання заявки. Для процедури авторизації необхідна наявність ідентифікатора смарт-карти, даних для автентифікації з боку смарт-карти та сервера, паролю з боку користувача і доступу до бази користувачів. В результаті при успішній автентифікації викликається обробник ключів сеансу і генерується ключ сеансу.

Для створення заявки необхідно представити ключ сеансу з боку користувача (ПК) і операцію яку він хоче виконати, з боку сервера потрібно мати доступ до бази користувачів, для того, щоб співставити ключ сеансу з ідентифікатором користувача і таким чином заповнити пріоритети доступу в заявці. Після створення заявки, вона передається в обробник заявок де поміщається в чергу на виконання, черга формується за певним критерієм на основі пріоритетів.

Оскільки заявка може провести час в черзі який перевищує час дії ключа сеансу тому перед виконанням заявки відбувається перевірка дійсності даного ключа. Якщо ключ виявляється недійсним то необхідно виконати авторизацію заново.

Висновки

Підходи до керування доступом мають суттєві недоліки, до яких можемо віднести відсутність документованого обґрунтування рішення з присвоєння або позбавлення прав доступу; відсутність шаблонів прав доступу; різнотипність керованих ресурсів і т.д.

У алгоритмі доступу до керування інформаційною системою торгівельної мережі супермаркету основним моментом є відмова від різнотипних керованих ресурсів, що зберігають окремі варіанти облікових записів однієї й тієї ж самої людини, оскільки це призводить до того, що користувачу необхідно запам'ятовувати велику кількість паролів.

Для доступу до інформаційної системи супермаркету необхідні певні елементи та процедури. До елементів відносяться смарт-карта, персональний комп'ютер (ПК), сервер. До процедур відносяться процедура авторизації та виконання заявки.

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. Обґрунтування 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. Яшина О.М. Керування доступом до інформаційної системи торгівельної мережі з використанням смарт-технологій в контексті політики безпеки / Яшина О.М. // Вісник Хмельницького національного університету. – Хмельницький : ХНУ, 2014. – № 6. – С. 133–135.

4. 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.

References

1. Shynkaruk O. M., Yashyna O. M. The Use of Smart Cards to Identify Users of Information Systems. Herald of Khmelnytsky National University. Khmelnitsky, 2013. Issue 1. P. 114–116.

2. Yashyna O. M. The Justification of Opportunities of the Use of smart cards to Control Access to information systems. Collection of scientific works on materials of VII international scientific-technical conference "Actual problems of computer technologies 2013". Khmelnytsky, 2013. P. 392–397.

3. Yashyna O. M. Access Control to the Information Systems of the Trade Network with the Use of Smart Technologies in the Context of Security Policy. Herald of Khmelnytsky National University. Khmelnitsky, 2014. Issue. 6. P. 133–135.

4. Shkurko M. I. Software for automation of information processing in the document management system based on distributed architecture with the use of smart technologies: dissertation of candidate of tech. sciences: 05.13.17. M., 2008. 158 p.

Рецензія/Peer review : 5.3.2015 р. Надрукована/Printed :15.4.2015 р.
Рецензент: стаття рецензована редакційною колегією