УДК 004.056

МЕТОД АВТЕНТИФІКАЦІЇ ВІДДАЛЕНИХ КОРИСТУВАЧІВ З ПРИВ'ЯЗКОЮ ДО ПАРАМЕТРІВ РОБОЧИХ СТАНЦІЙ

Баришев Ю.В.,
к.т.н., доцент кафедри захисту інформації,
Вінницький національний технічний університет,
yuriy.baryshev@gmail.com

Войтович О.П.,
к.т.н., доцент,
доцент кафедри захисту інформації,
Вінницький національний технічний університет

Анотація. *У роботі наведено аналіз відомих методів автентифікації користувачів. запропоновано метод автентифікації, який передбачає використання як секретних даних користувача, так і робочої станції. Наведено схему авторизації користувачів, що базується на цьому методі. Визначено перспективи використання цієї схеми авторизації.*

Одним з найбільш стійких методів автентифкації вважається автентифікація, що базується на основі криптографічних алгоритмів. Проте на практиці трапляється, що користь від використання таких потужних методів захисту інформації нівелюється впливом людського фактору [1, 2]. Зокрема у випадку халатності працівник підприємства, який має право віддаленого доступу до конфіденційної інформації, може спричинити її витік внаслідок візуального зняття з екрану. Саме тому актуальною є розробка методу комплексного захисту конфіденційності інформації для користувачів мережевих сервісів, який би дозволяв обмежувати доступ авторизованих користувачів до даних, якщо він відбувається з незахищених робочих місць.

Метою даного дослідження є покращення захисту конфіденційності інформації, доступ до якої надається через мережу.

Для досягнення мети необхідно проаналізувати відомі методи автентифікації користувачів та розробити метод автентифікації на основі гешування та прив'язки до параметрів робочої станції;

Процедура автентифікації в загальному випадку передбачає такі етапи [3-4]:

- введення користувачем особистий ідентифікатора та секретних даних, за наявністю яких його автентифікують (включаючи біометричні показники);
- захист цих даних за допомогою криптографічних протоколів або перетворень;
- надсилання даних на сервер, де відбувається порівняння їх з еталонними.

З аналізу цих етапів випливає, що автентифікація робочих станцій відбувається незалежно від автентифікації їх користувачів. У часи, коли не було портативних комп'ютерних систем такий підхід був виправданим. Однак, сьогодні, коли користувач має більше одного засобу для отримання даних він використовуватиме для авторизації той з них, який найбільш зручний для нього в конкретний момент часу, не враховуючи, що даний засіб не підтримує необхідний рівень захисту даних, що за його допомогою обробляються. Таким чином використовувати такі методи автентифікації – покладатися на те, що успішно авторизований, користувач не буде виконувати обробку інформації із застосуванням незахищеної робочої станції. З урахуванням, що причиною інцидентів у галузі інформаційної безпеки в переважній більшості випадків є людський фактор [1-3] такі міркування –оптимістичні, а тому не можуть мати місце при розробці розподілених інформаційних систем, в яких обробляється інформація цінна не лише для користувачів

цієї системи. Тому пропонується метод, який під час автентифікації передбачає автентифікація на основі геш-значення секретних даних користувача та параметрів робочої станції. На рис. 1 зображено схему авторизації користувача і робочої станції, що пропонується у даному методі.

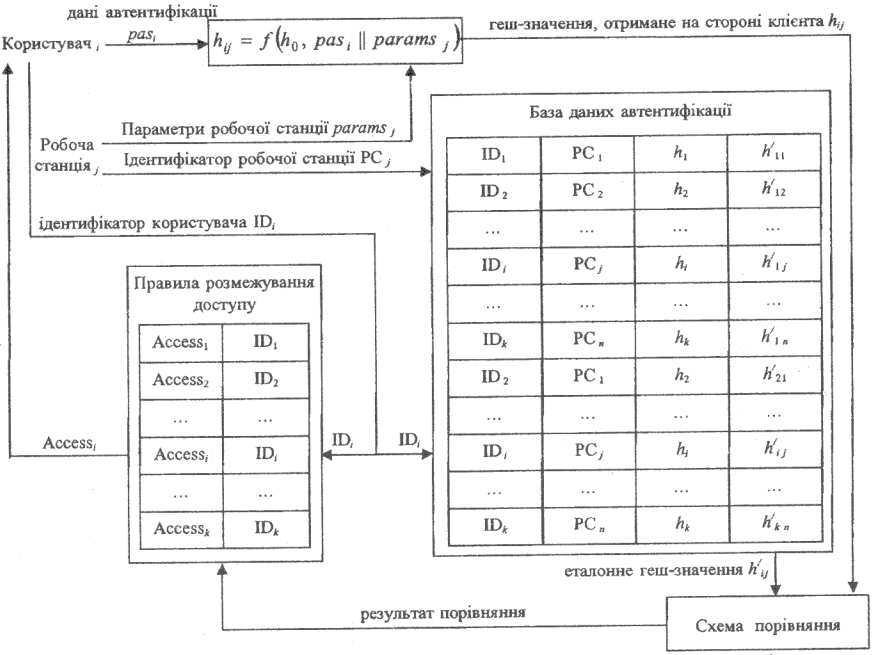

Рис. 1. Модифікована схема авторизації користувача з використанням паролів

Запропонований варіант автентифікації не передбачає пересилання додаткових даних, а тому може бути впровадженим до існуючих засобів автентфикації віддалених користувачів. Однак його впровадження передбачає необхідність його інтеграції до політики інформаційної безпеки, що потребує високої компетентності адміністратора комп'ютерної системи.

Література:

1. Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире / Брюс Шнайер. – СПб. : Питер, 2003. – 368 с.

2. Просис К. Расследование компьютерных преступлений / Крис Просис, Кевин Мандиа. – М.: Лори, 2012 – 416 с.

3. Баришев Ю. В. Метод автентифікації віддалених користувачів для мережевих сервісів / Ю. В. Баришев, В. А. Каплун // Інформаційні технологій та комп'ютерна інженерія. – 2014. – №2. – С. 13-17.

4. Грайворонський М. В. Безпека інформаційно-комунікаційних систем. / М. В. Грайворонський, О. М. Новіков. – К.: Видавнича група BHV, 2009. – 608 с.

5. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов. / А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов и др.; Под ред. А. А. Шелупанова, С. Л. Груздева, Ю. С. Нахаева. – М.: Горячая линия-Телеком, 2009. – 552 с.