

УДК 004.056.52:004.7

Ореховський Д.В., здобувач вищої освіти
Сисоєнко С.В., канд. техн. наук, доцент

Черкаський державний технологічний університет, s.sysoienko@chdtu.edu.ua

ДОСЛІДЖЕННЯ ШЛЯХІВ УДОСКОНАЛЕННЯ СИСТЕМ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ У КОРПОРАТИВНОМУ СЕРЕДОВИЩІ

Одним з ключових завдань сучасної інформаційної безпеки є забезпечення надійного контролю доступу до корпоративних інформаційно-телекомунікаційних систем (КІТС). Із зростанням масштабів корпоративних мереж та ускладненням архітектур, зростає і кількість потенційних загроз, зокрема з боку внутрішніх і зовнішніх порушників. У таких умовах ефективна ідентифікація та авторизація користувачів стає критичною для забезпечення конфіденційності, цілісності та доступності інформації [1].

У роботі було акцентовано увагу на важливості застосування комплексного підходу до захисту інформації, що включає як організаційні, так і технічні заходи [2]. Особливу увагу приділено огляду сучасних методів аутентифікації. Протокол RADIUS (Remote Authentication Dial-In User Service) – забезпечує централізовану аутентифікацію, авторизацію та облік через UDP. Застосовується у великих мережах, дозволяє керувати доступом до мережевих ресурсів [3]. TACACS+ – більш гнучкий протокол, який відокремлює процеси аутентифікації, авторизації та обліку. Працює через TCP, використовується у середовищах з підвищеними вимогами до безпеки [3]. Kerberos – протокол з відкритим ключем, який базується на симетричному шифруванні та довірених сторонах (центральному сервері аутентифікації). Широко використовується у корпоративних мережах та системах з доменною структурою [4]. Під час дослідження виявлено, що застосування TACACS+ разом із біометричними системами забезпечує високий рівень захищеності у великих організаціях з багатьма користувачами.

За результатами дослідження пропонуються наступні рекомендації щодо впровадження систем ідентифікації та авторизації:

Впровадження багатофакторної аутентифікації (MFA).

Централізоване управління політиками доступу з використанням RADIUS або TACACS+.

Регулярний аудит журналів доступу і аналіз дій користувачів.

Використання Kerberos у мережах з високим рівнем довіри.

Інтеграція біометричних методів у середовищах з підвищеними вимогами до контролю доступу.

Навчання персоналу та підвищення обізнаності.

Створення політики паролів.

Отримані результати можуть бути використані для підвищення рівня безпеки в корпоративних мережах, а також як основа для подальших досліджень у сфері кібербезпеки.

Список посилань

1. ISO/IEC 27001. Information Security Management Systems Protocol [Електронний ресурс]. – Режим доступу: <https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en>

2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». [Електронний ресурс]. – Режим доступу:

<https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>

3. RADIUS vs. i TACACS+: What's the Difference? [Електронний ресурс]. – Режим доступу: <https://rublon.com/blog/radius-vs-tacacs/>

4. MIT. Kerberos: The Network Authentication Protocol [Електронний ресурс]. – Режим доступу: <https://web.mit.edu/kerberos/>