УДК 621.326
Коваленко В.– ст. гр. СІм-51
Тернопільський національний технічний університет імені Івана Пулюя

МЕТОДИ ЗАХИСТУ МЕРЕЖЕВИХ СЕРВЕРІВ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Науковий керівник: доцент Осухівська Г.М.

Kovalenko V.
Ternopil Ivan Pul`uj National Technical University

METHODS OF PROTECTING NETWORK SERVERS FROM UNAUTHORIZED ACCESS

Supervisor :assot. prof. OsukhivskaH.M.

Ключові слова: безпека, фізичний захист, логічний захист, комплексний захист.
Keywords: security, physicalsecurity, logicalsecurity, comprehensiveprotection .

На сьогодні широке застосування комп'ютерних технологій в автоматизованих системах обробки інформації та управління призвело до загострення проблеми захисту інформаціївід несанкціонованого доступу, що є в комп'ютерних системах.Проблема захисту інформації від несанкціонованого доступу особливо загострилася з широким розповсюдженням локальних і, особливо, глобальних комп’ютерних мереж.У зв’язку з цим, крім контролю доступу, необхідним елементом захисту інформації в комп’ютерних мережах є розмежування повноважень користувачів.Саме тому за мету дослідженнябуло поставлено пошук та аналізоптимальнихметодівзахистумережевихсерверіввіднесанкціонованого доступу для забезпеченнянадійності, швидкодіїкомп'ютерноих систем та мереж.

Базовими принципами інформаційної безпеки, які повинна забезпечувати комп’ютерна мережа, є:

– цілісність даних – захист від збоїв, що ведуть до втрати інформації, а також неавторизованого знищення або створення даних;

– конфіденційність інформації;

–доступність інформації для всіх авторизованих користувачів.

Рівень захисту комп’ютерної мережі залежить від її розміру та інформації, яку потрібно безпечно передавати. При чому використовують фізичний та/або логічний захист інформації.

Для забезпечення фізичного захисту сервери встановлюють в окреме приміщення з обмеженим доступом. При логічному захисті здійснюється виконання персоналом компанії певних правил роботи та використання спеціалізованого програмного забезпечення. До логічного захисту можна віднести використання логіну (імені користувача), паролю, аудит, шифрування даних, захист від вірусів, резервне копіювання, використання джерел безперебійного живлення та створення відмовостійких систем. Тому варто досліджувати можливі більш ефективні підходи для забезпечення захисту комп’ютерних систем та мереж.