

УДК 004.67

О.В. Левенець

(Тернопільський національний технічний університет ім. І. Пулюя)

РОЗРОБКА МЕТОДИКИ ПІДВИЩЕННЯ РІВНЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ

UDC 004.67

O.V. Levenets

DEVELOPMENT OF METHODS FOR INCREASING THE SECURITY LEVEL OF THE INFORMATION AND COMMUNICATION SYSTEM

Актуальність проблеми підвищення захищеності інформаційно-комунікаційних систем зростає зі швидкістю, пропорційною збільшенню обсягів та важливості даних, що зберігаються в інформаційних системах. А на сьогодні в Україні це дані про здоров'я, освіту, господарську та фінансову діяльність, державні документи тощо. Кожні 8 років обсяг цифрових даних у світі збільшується вдесятеро. За оцінками Forbes, світовий обсяг даних до 2025 р. становитиме 175 зеттабайтів.

Огляд публікацій із захисту інформації виявив, що поняття «захищеність інформаційної системи» належить до базових. Можливо тому більшість вчених не вважають за потрібне його досліджувати та сприймають як інтуїтивно зрозуміле. Зазначають [1], що захищеність – це одна із характеристик якості, що найскладніше формалізується, призначення і функції якої тісно пов'язані з особливостями функціональної придатності інформаційної системи. Захищеністю інформаційно-комунікаційної системи ми вважаємо її здатність забезпечувати цілісність, конфіденційність та доступність інформації, виявляти зловмисні втручання та не допускати їх впливу на інформацію.

У магістерській роботі ми розглядаємо інформаційно-комунікаційну систему, захист якої можливий з використанням різноманітного програмного забезпечення та апаратного обладнання, профіль захищеності обирається адміністратором мережі з урахуванням обмеженого кошторису щодо їх придбання та експлуатації.

Корпоративна мережа має вразливості, що можуть призвести до порушення цілісності, конфіденційності та доступності інформації, внаслідок чого організації завдається матеріальна шкода зловмисником. Вважатимемо, що загрози корпоративній мережі відомі (із статистичних даних та бібліотек атак CAPEC, ISACA, OWASP Top Ten та ін.).

Визначено та засобами математичного апарату теорії ігор вирішено завдання вибору профілю захищеності інформаційно-комунікаційної системи: при заданому векторі загроз обрати оптимальну комбінацію засобів захисту корпоративної мережі від локальних та мережних загроз за критерієм мінімізації потенційних збитків від атак при обмеженому бюджеті організації.

Література.

1. Калиберда Е. А., Рыбкин А. А. Анализ уязвимостей по степени их влияния на защищённость и качество структурно-сложных информационных систем / Вестник Омского университета, 2014, № 2, С. 130–135.