ПРОГРАМНА СИСТЕМА ВИЯВЛЕННЯ КОМП'ЮТЕРНИХ ВТОРГНЕНЬ НА ОСНОВІ КОМПЛЕКСНОГО ВИКОРИСТАННЯ ФУНКЦІЇ ЧУТЛИВОСТІ ТА BDS-ТЕСТУ

д-р. техн. наук, с.н.с. С.Г. Семенов, магістр. О.В. Мовчан, Національний технічний університет "Харківський політехнічний інститут", м. Харків

Сучасні методи аналізу виявлення комп'ютерних вторгнень базуються на виявленні окремих файлів, що мають підозрілу поведінку. Але з часом кількість файлів на жорсткому диску, а також кількість можливих варіантів вторгнення збільшується. Тому потрібно розробити комплексну систему, що аналізує поведінку систему в цілому.

Один із способів дослідження поведінки системи для виявлення вторгнень – використання функції чутливості. Для успішного її використання необхідно урахувати властивості нелінійності зовнішніх впливів і незалежності внутрішніх збурень; виконати апроксимацію функції чутливості на багаторівневі системи; уточнити функцію чутливості з урахуванням можливої залежності деструктивних змін внутрішніх характеристик.

Іншим ефективних підходом при виявленні залежностей в інформаційнім трафіку є BDS-статистика, що будується на базі BDS-тестів. BDS-тести являють собою ефективні методи виявлення залежностей у часових рядах. Їх мета полягає в перевірці нульової гіпотези о незалежності и тотожному розподілі значень часового ряду.

Програмна реалізація системи виявлення зовнішніх вторгнень на основі комплексного використання функції чутливості та BDS-тесту дозволить підвищити рівень комп'ютерної безпеки.