РЕФЕРАТ

Магістерська дисертація: 88 с., 26 рис., 13 табл., 7 додатків, 22 джерел.

Актуальність. На сьогоднішній день питання безпеки інформаційної системи є надзвичайно важливим. Нерідко з’являються повідомлення у засобах масової інформації про те, що новий комп’ютерний вірус став загрозою для нормального функціонування значної частини комп’ютерів. Яскравим прикладом може бути виявлений нещодавно вірус «Wanna Cry», що вражає операційну систему Microsoft Windows шляхом шифрування файлів.

Тому доцільним є створення апаратно-методологічного комплексу, що аналізує і фільтрує трафік в режимі реального часу, формує активності пристроїв, опираючись на пакетні дані.

Зв'язок роботи з науковими програмами, планами, темами. Робота виконувалась на кафедрі автоматизованих систем обробки інформації та управління Національного технічного університету України «Київський політехнічний інститут ім. Ігоря Сікорського» в рамках ініціативної теми «Методи візуального програмування Петрі-об’єктних моделей» д/р №0117U000918.

Мета дослідження – покращення процесу виявлення загроз з мережі Інтернет, шляхом розробки та впровадження апаратно-методологічного комплексу, що аналізуватиме і фільтруватиме трафік в реальному часі для пошуку шкідливих сигнатур.

Для досягнення мети необхідно виконати наступні **задачі**:

- виконати огляд відомих результатів з розв’язання задачі для пошуку виявлення загроз з мережі Інтернет;
- розробити програмне забезпечення, що буде виявляти шкідливий трафік на основі сигнатур мереж Петрі;
- виконати експериментальне дослідження роботи комплексу
- провести аналіз отриманих результатів.

Об’єкт дослідження – процес виявлення шкідливого трафіку пристроїв однієї підмережі.

Предмет дослідження – методи виявлення шкідливого трафіку пристроїв однієї підмережі та його фільтрацію.

Наукова новизна отриманих результатів

Запропоновано альтернативний архітектурний підхід для впровадження файєрволу в підмережу, шляхом проведення атаки man-in-the-middle. Тобто фізичної взаємодії програмно-апаратного комплексу і пристроїв підмережі немає. Проведено аналіз існуючих підходів до пошуку шкідливого трафіку пристроїв однієї підмережі. Серед проаналізованих методів обраний сигнатурний та поведінковий аналіз. Проведено експерементальне дослідження отриманого комплексу та проаналізовано отримані результати.

Публікації. Матеріали роботи опубліковані у тезах Всеукраїнської науково-практичної конференції молодих вчених та студентів «Інформаційні системи та технології управління»

МЕРЕЖІ ПЕТРІ, ВРАЗЛИВІСТЬ СИСТЕМИ, АНАЛІЗ ТРАФІКУ, КІБЕР АТАКА