окупованих територій, які обороняють значні сили противника. По-друге ми побачили, що ефективно використовувати подібні засоби може навіть армія середніх можливостей. Відповідно досвід даної військової кампанії має уважно вивчатися, а відповідна техніка, середні БПЛА та баражируючі боєприпаси, має бути використана Збройними силам України для деокупації територій.

к.т.н., доц. Муляр І.В. (ХмНУ)
к.т.н., с.н.с. Мірошніченко О.В. (ВІКНУ)
к.т.н., доц. Якименко І.З. (ТНЕУ)
Соколюк Я.В. (ХмНУ)

Інструментарій для раннього виявлення розподілених атак

DDoS-атака - абревіатура від англійського Distributed Denial of Service, розподілена атака, спрямована на відмову в обслуговуванні. Атаки такого типу можуть швидко виснажити мережеві ресурси або потужності сервера, що призведе до неможливості отримати доступ до ресурсу і викличе серію негативних наслідків: втрачений прибуток, неможливість скористатися послугами і зробити різні транзакції і т.д. У DDoS-атаці в ролі атакуючого виступає так звана бот-мережа, або зомбі-мережа. Зомбі-мережа може налічувати від декількох десятків до тисяч хостів. Зазвичай це нейтральні комп'ютери, які в силу якихось причин (відсутність файрволу, застарілі бази антивіруса і т.д.) були заражені, шкідливими програмами. Програми, працюючи у фоновому режимі, безперервно посилають запити на сервер що атакується, виводячи його таким чином з ладу. На даний момент не існує якогось універсального засобу для протидії DDoS-атакам. Навіть такі великі компанії, як Microsoft, eBay, Amazon, Yahoo, страждають від DDoS-атак і не завжди можуть з ними впоратися.

Засоби протидії, спеціалізовані саме на забезпечення безпеки невеликих і середніх ресурсів, отримали менший розвиток через переважання в минулому саме великих атак. І в даний час відстають від еволюції самих DDoS-атак.

Метою дослідження є створення актуальною методу та інструментарію для раннього виявлення розподілених атак, спрямованих на відмову в обслуговуванні, і подальшого виявлення шкідливого трафіку на стороні ресурсу, що атакується і його блокування власними силами.

Для досягнення зазначеної мети в дипломній роботі поставлено і вирішено такі завдання:

1. Проведено моніторинг сучасних DDoS-атак. Виявлено тенденцію до розвитку атак середньої і малої потужності, спрямованих на регіональні ресурси.

2. Розглянуто засоби протидії атакам невеликої потужності.

3. Досліджено особливості DDoS-атак регіонального рівня. Вироблені вимоги до методики та засобу з виявлення атак і подальшої їм протидії.

4. Вирішено завдання по створенню методу і програмного комплексу по виявленню DDoS-атак і шкідливих запитів.

Список використаних джерел:

1. Теоретические основы компьютерной безопасности / П. Н. Девянин, О. О. Михальский, Д. И. Правиков, А. Ю. Щербаков. – М.: Радио и связь, 2015. – 192 с.

к.військ.н., ст.досл. Нікіфоров М.М. (ВІКНУ)
к.т.н., доц. Пампуха І.В. (ВІКНУ)
д.фіз.-мат.н., проф. Ільченко В.В. (КНУ імені Тараса Шевченка)
Корчак Ю.О. (ВІКНУ)

Аналіз сейсмоакустичних методів ведення дистанційної розвідки

На даний час основна тенденція виявлення сейсмічної події в автоматичному режимі полягає у використанні відносно простих процедур обробки вимірювальних даних, які дозволяють оперативне здійснювати аналіз даних, але при цьому збільшується щільність мережі сейсмічних спостережень. Територіальна обмеженість мережі сейсмічних спостережень зумовлює необхідність розробки методологічних засад вирішення завдань сейсмічного моніторингу окремим пунктом спостереження. Тому виникає необхідність провести аналіз існуючих методів виявлення сейсмічних сигналів з метою визначення пріоритетних напрямків досліджень та надання рекомендацій щодо удосконалення існуючих та розробки нових методів виявлення сейсмічних сигналів, ідентифікації їх складових, визначення місцеположення осередку сейсмічної події та оцінки її параметрів.

Вирішення завдань сейсмічного моніторингу складається з наступних етапів: виявлення сейсмічного сигналу, ідентифікація складових сейсмічного запису (встановлення типів сейсмічних хвиль), локація осередку сейсмічної події, оцінка параметрів сейсмічного джерела. При однопозиційних спостереженнях останні два етапи вирішуються за умови впевненого вирішення задачі виявлення та визначення основних складових сейсмічного запису. Тому, при аналізі існуючих методів виявлення та обробки сейсмічних даних основна увага приділятиметься саме можливості вирішення цих задач.

Розглянемо основні методи виявлення сейсмічних сигналів, які використовуються у Міжнародному та Національних центрах обробки сейсмічних даних.

Алгоритм STA/LTA. На даний час основна тенденція виявлення сейсмічної події у автоматичному режимі полягає у використанні відносно простих процедур обробки вимірювальних даних, таких як, наприклад, алгоритм STA/LTA. Даний алгоритм дозволяє здійснювати аналіз даних за рахунок порівняння енергії сейсмічного сигналу в ковзних вікнах.

Алгоритм кумулятивних сум. Алгоритм являє собою послідовний критерій відношення ймовірностей для двох простих гіпотез H_1 та H_2. Ідея алгоритму полягає в аналізі поведінки кумулятивної суми.

Узгоджений фільтр будується на основі критерію максимуму пікового відношення сигнал/шум та призначений для встановлення факту наявності сейсмічного сигналу у прийнятій реалізації. При цьому вважається, що