функціонування систем захисту інформації (ЗІ); проведення аналізу надійності систем ЗІ; класифікація показників безпеки інформації; обґрунтування та вибір критерію для оптимізації технічної системи ЗІ; проведення аналізу ризиків інформаційної безпеки і виділити їхні наслідки; огляд методів впливу дестабілізуючих факторів на завадостійкість передачі інформації; визначити критерії невидимості для схованих каналів; проведення досліджень і аналізу захищеності бездротових корпоративних мереж; практична реалізація криптографічних методів ЗІ; методи вилученого адміністрування для несанкціонованого доступу до інформаційних ресурсів.

В особливий клас можна виділити завдання ведення інформаційних війн, системи керування вмістом і безпека веб-сайтів, застосування штучних нейронних мереж систем ЗІ, економічної безпеки держави.

Що стосується математичного моделювання інформаційної безпеки (ІБ) багатьма науковцями ведеться робота щодо розробки моделей аналізу загроз ІБ у комп'ютерній мережі.

Для розв'язання задачі захисту конфіденційної інформації, яка передається на великі відстані, існує фактично два методи: прокладати власні лінії зв'язку; використовувати існуючі лінії зв'язку МЗК (телефонні мережі, Інтернет і т.д.).

Перший метод має кілька очевидних недоліків: витрати фінансів та часу, не гарантує надійного захисту комунікацій, обмежений у застосуванні.

Другий метод – застосування відкритих комунікаційних каналів має лише один, але дуже істотний недолік: повна відсутність захищеності даних, що передаються. Усунути цей недолік покликані системи захисту інформації, які створюють захищений закритий канал усередині відкритого каналу МЗК, запобігаючи, таким чином, несанкціонованому зніманню інформації при передачі від абонента до абонента за принципом точка-точка.

IV. Висновок

Отже, проведений аналіз задач захисту інформаційних потоків в мережах загального користування дозволив виділити основні переваги та недоліки основних методів збереження конфіденційності інформації, яка передається на великі відстані.

Список використаних джерел

1. Ленков СВ. Методы и средства защиты информации: в 2 т. / С.В.Ленков, Д.А.Перегудов, В.А.Хорошко. — К.: Арий— Т.2: Информационная безопасность. — 2008. — 344 с.
2. Хома В.В. Методи та засоби забезпечення конфіденційності телефоних повідомлень. / Хома В.В. // Сучасна спеціальная техніка, №3(18), 2009. – С. 50-59.
3. 3 Петров А.А. Особенности проектирования математических моделей защиты информации // Вісник СНУ ім. В.Даля. – 2009. - №131.– С. 122-127.
4. Живко З.Б. Ризики інформаційної безпеки та їх наслідки. / С.В. Малкуш, М.О. Живко // Сучасна спеціальна техніка. – 2010. – №1(20). – С. 21-29.

УДК 683.1

МЕТОД МОДЕЛЮВАННЯ ЗАХИСТУ СИСТЕМИ ВІД ЗАГРОЗ ЛІНІЙНОГО ВИДУ

Яциковська У.О.[1)], Якименко І.З.[2)], Маланчук М.В. [3)]

[1)]Тернопільський національний технічний університет ім.І. Пулюя, к.т.н.;
Тернопільський національний економічний університет
[2)] к.т.н.; [3)] магістрант

І. Постановка проблеми

Останнім часом несанкціонований доступ до інформації сприяє значному росту злочинності у КМ. Для власників важливих інформаційних даних, комп’ютерна злочинність, а саме атаки на інформаційні потоки призводять до небажаних великих фінансових збитків. Найпоширенішими видами лінійних атак в КМ є DoS/DDoS/DRDoS-атаки (Denial of Service / Distributed Denial of Service / Distributed Reflection Denial of Service). Тому актуальною задачею є удосконалення системи безпеки інформаційних даних в КМ.

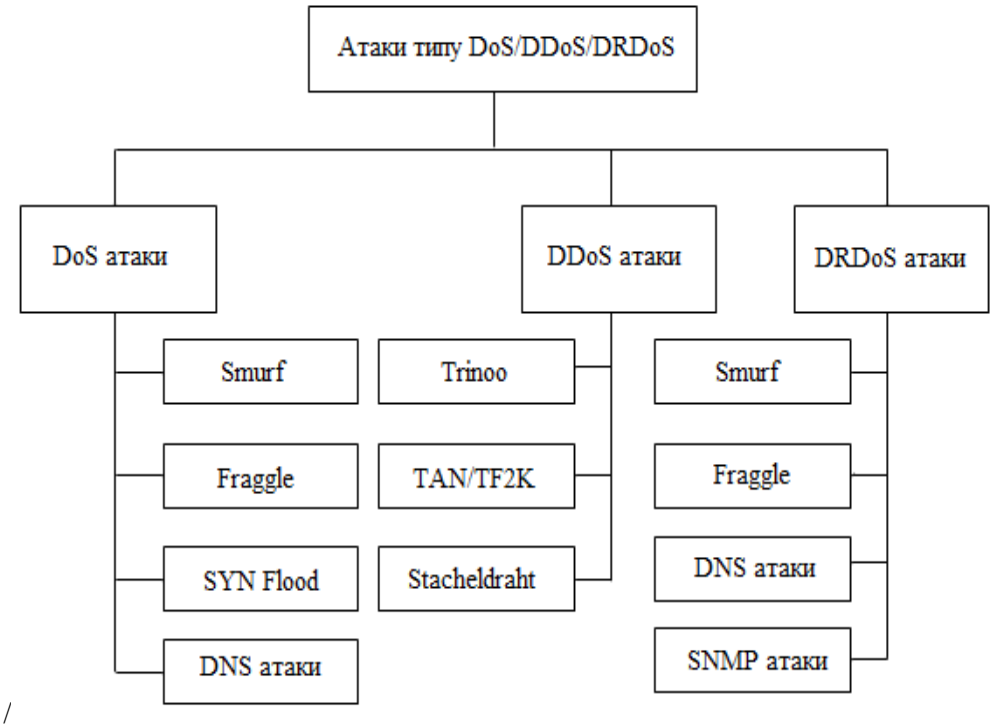
II. Мета роботи.

Удосконалення захисту системи клієнт-сервер за рахунок розроблення методу та засобів моделювання безпечної комунікації підвищеної ефективності щодо виявлення та локалізації атак лінійного виду DoS/DDoS/DRDoS у системі клієнт-сервер.

III. Формалізована математична модель на основі класифікації атак лінійного виду DoS/DDoS/DRDoS

Проаналізовані атаки DoS/DDoS/DRDoS, які зображено на рисунку 1, дозволяють структурувати та класифікувати їх за типами.

DoS/DDoS/DRDoS-атаки переважно спрямовані на конкретний сервер із великим обсягом інформації, фальшивим трафіком із координованим і розподіленим нападами, що є серйозною загрозою для стабільної роботи в мережі Інтернет. Такі атаки важко відслідкувати [1].



/

Рисунок 1 - Класифікація видів DoS/DDoS/DRDoS атак

Наступним етапом досліджень атак DoS/DDoS/DRDoS є виявлення вразливих точок вузлів КМ та вдосконалення методів протидії несанкціонованому доступу. Важливим є виявлення змін використання ресурсів та скорочення часу виявлення. Такі аномальні зміни можуть бути виявлені статично [2, 3].

В результаті аналізу класифікації DoS/DDoS/DRDoS-атак запропоновано формалізовану математичну модель (1), яка дозволяє визначити рівень впливу показників атак на КМ [1]:

$$\begin{aligned} P_{DoS} &= \beta_1 P_{Smurf} + \beta_2 P_{Fraggle} + \beta_3 P_{SYNFlood} + \beta_4 P_{DNS}, \\ P_{DDoS} &= \delta_1 P_{Trinoo} + \delta_2 P_{TFN/TFN2K} + \delta_3 P_{Stacheldraht}, \\ P_{DRDoS} &= \mu_1 P_{Smurf} + \mu_2 P_{Fraggle} + \mu_3 P_{DNS} + \mu_4 P_{SNMP}, \end{aligned} \quad (1)$$

де β_i, δ_i, μ_i – вагові коефіцієнти впливу показників DoS-, DDoS-, DRDoS-атак, причому $\sum_{i=1}^{4}\beta_i = 1$, $\sum_{i=1}^{3}\delta_i = 1$, $\sum_{i=1}^{4}\mu_i = 1$.

Вагові коефіцієнти визначають внесок основних видів атак DoS/DDoS/DRDoS у КМ та дають змогу врахувати зазначені атаки при розробці та експлуатації систем захисту інформації. За допомогою даних показників та коефіцієнтів можна визначити основні види загроз та їх вплив на рівень безпеки КМ, що дозволить ефективно проектувати системи захисту інформації з урахуванням інформаційних загроз.

IV. Висновок

Отже, запропоновані нові математичні моделі інформаційних структур імовірності загроз DoS/DDoS/DRDoS на основі використання показників цілісності, конфіденційності, доступності, які, на відміну від відомих, дозволяють визначити рівень впливу показників і критеріїв загроз на КМ.

Список використаних джерел

1. Яциковська, У. О. Дослідження реалізації розподілених атак в комп'ютерній мережі [Текст] / У. О. Яциковська, І. В. Васильцов, М. П. Карпінський // Сучасна спеціальна техніка. – 2011. – № 2 (25). – С. 124–127.
2. Чанг Шу (Китай). Метод адаптивного формування потоків трафіка обчислювальних мереж : автореф. дис. на здобуття наук. ступеня канд. техн. Наук : спец. 05.13.05 "Комп'ютерні системи та компоненти" / Шу Чанг, Нац. авіаційний ун-т України. – К., 2009. – 20 с.
3. Тихонов В. А. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты [Учебное пособие] / В. А. Тихонов, В. В. Райх. – М. : Гелиос АРВ, 2006. – 528с.