Methods of information systems protection

УДК 004.932, 528.854 **doi: 10.20998/2522-9052.2018.1.11**

О. В. Барабаш [1], Н. В. Лукова-Чуйко [2], А. П. Мусієнко [2], В. В. Собчук [3]

[1] *Державний університет телекомунікацій, Київ, Україна*
[2] *Київський національний університет імені Тараса Шевченка, Київ, Україна*
[4] *Східноєвропейський національний університет імені Лесі Українки, Луцьк, Україна*

ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ СТІЙКОСТІ ІНФОРМАЦІЙНИХ МЕРЕЖ НА ОСНОВІ РОЗРОБКИ МЕТОДУ ПРОТИДІЇ DDoS-АТАКАМ

Предметом вивчення в статті є процес забезпечення властивості функціональної стійкості інформаційних мереж. **Метою** є розробка методу протидії DDoS-атакам, що дозволяє ефективно захищати інформаційну мережу, як від атак на всьому часовому інтервалі, так і від повільних атак. **Завдання:** розробити алгоритми виявлення та блокування DDoS-атак, що описують послідовність дій при застосуванні методу протидії; провести оцінку ефективності запропонованого методу протидії DDoS-атакам. Використовуваними **методами** є: графовий підхід, математичні моделі оптимізації, методи розв'язання нелінійних задач. Отримані такі **результати.** Побудовані алгоритми виявлення та блокування DDoS-атак, що описують послідовність дій при застосуванні методу протидії. Алгоритм виявлення атак реалізується на аналізаторі вхідного трафіку, який перевіряється на предмет наявності DDoS-атак. У разі виявлення такої атаки визначається її тип. Після цього реалізується алгоритм блокування, який зчитує з бази даних джерела шкідливого трафіку та перенаправляє його на програмний шлюз, який забирає на себе подальший деструктивний вплив. **Висновки.** Наукова новизна отриманих результатів полягає в наступному: ми запропонували метод протидії DDoS-атакам, що дозволяє ефективно захищати інформаційну мережу як від атак на всьому часовому інтервалі, так і від повільних атак. Даний метод дозволяє забезпечити функціональну стійкість інформаційної мережі та базується на використанні алгоритмів виявлення та блокування DDoS-атак, а також збору інформації про вхідний трафік із записом до бази даних «Джерела шкідливого трафіку». При виявленні атаки визначається її тип та запускається механізм її блокування, що реалізується в два етапи. На першому етапі виконується пошук джерел шкідливого трафіку, використовуючи зібрану в базі даних інформацію про вхідні пакети. На другому етапі виконується безпосереднє блокування виявлених джерел шляхом відправлення пакетів-відповідей по резервному каналу зв'язку через програмний шлюз, на якому вихідна адреса серверу у пакетах підміняється адресою шлюзу, що дає змогу замаскувати сервер від зовнішнього деструктивного впливу (у разі атаки ззовні). При атаці з внутрішньої мережі відключаються порти комутатора, до яких підключені джерела шкідливого трафіку. Після цього оповіщається системний адміністратор, який негайно приступає до пошуку та знешкодження шкідливого програмного забезпечення.

Ключові слова: інформаційна мережа; функціональна стійкість; DDoS-атака; системи виявлення вторгнення; база даних; аналізатор трафіку; маршрутизатори; комутатори.

Вступ

Сучасні інформаційні технології розвиваються швидкими темпами. Надання інформаційних послуг відбувається повсякчас – це є невід'ємною частиною життя суспільства. З одного боку, отримання документів та їх відпрацювання у електронному вигляді, проведення платежів та отримання інформаційних послуг – це дуже зручно та швидко, але це вимагає проведення ряду заходів з врегулювання механізмів надання та обробки інформації у електронному вигляді [1].

Для обробки та передачі документів у електронному вигляді використовуються відкриті канали зв'язку, що у свою чергу робить можливим блокування, втрату або заволодіння інформацією для подальшого її використання у злочинних цілях.

Стрімке зростання якості та низька собівартість інформаційного обладнання дає можливість розгортання інформаційних ресурсів будь-якої складності, але саме ці причини призводять до стрімкого зростання кібернетичних загроз. За даними світових аналітичних агенцій, зростання кількості кіберзагроз відбувається у експоненційній залежності [2]. Ключову роль, на сьогодні, відіграють розподілені інформаційні системи.

Функціональна стійкість (ФС) інформаційної системи (ІС), в першу чергу, обумовлена її здатністю надавати регламентовані послуги на протязі визначеного часу [3]. Для своєчасного виявлення фактів неавторизованого доступу та (або) несанкціонованого управління інформаційною системою через мережу інтернет застосовують системи виявлення вторгнень (СВВ). У частині поняття функціональної стійкості інформаційної системи, СВВ повинна мати спроможність отримувати та обробляти сигнатурну інформацію на початковому етапі мережевої атаки. Це надасть змогу своєчасно класифікувати загрозу та виробити необхідні адміністративні впливи на систему інформаційної безпеки ІС. При цьому, збір сигнатурної інформації повинен бути прихованим [4].

Аналіз основних публікацій. Показники функціональної стійкості характеризують результат її забезпечення шляхом перерозподілу існуючої надмірності або ресурсів у позаштатних ситуаціях [5-7].

Дослідження показали, що функціональна стійкість інформаційної системи поєднує властивості надійності (безвідмовності), відмовостійкості і жи-

© Барабаш О. В., Лукова-Чуйко Н. В., Мусієнко А. П., Собчук В. В., 2018

вучості. Функціональна стійкість розглядається, як властивість системи успішно завершити завдання при регламентованому числі змін в стані самої системи, тобто зберегти її працездатність після прояву припустимого числа відмов і зовнішніх збурювань [8]. Реалізація функціональної стійкості досягається за рахунок використання у складній технічній системі, до якої можна віднести інформаційні системи, різних уже існуючих видів надмірності (інформаційної, функціональної, структурної, часової, навантажувальної та ін.) шляхом перерозподілу ресурсів з метою парирування наслідків позаштатних ситуацій. Принциповим є те, що на етапі проектування не повинна вводитися додаткова надмірність, а парирування наслідків позаштатних ситуацій здійснюється перерозподілом уже існуючих ресурсів. Проблема полягає у виявленні вже наявної надмірності та формуванні сигналів у потрібний момент на її перерозподіл [9]. У цьому є основна відмінність задачі забезпечення функціональної стійкості від задачі побудови структурно надмірних систем.

Вирішенню проблеми забезпечення функціональної стійкості складних технічних систем присвячено низку наукових праць О.А. Машкова, О.В. Барабаша, Ю.В. Кравченка, С.М. Неділька, Д.М. Обідіна та інших вчених. Однак широке їх використання в практичних задачах оцінки функціональної стійкості різних варіантів побудови інформаційних систем ускладнене за багатьох причин.

Метою роботи є розробка методу протидії DDoS-атакам, що дозволяє ефективно захищати інформаційну мережу як від атак на всьому часовому інтервалі, так і від повільних атак.

Основна частина

На сьогодні, існує досить велика кількість методів протидії та кібернетичним атакам. 70% таких методів гуртуються на сигнатурному пошуку загроз [10]. Це дуже зручно – не треба прописувати спеціальних алгоритмів або модулів при виявленні нових загроз, достатньо мати єдину спільну базу сигнатур пошуку, програми, що базуються на таких методах захисту є простими у реалізації, мають високу швидкодію. Але з-поміж всі переваг, мають один суттєвий недолік – вони не в змозі розпізнати загрози, сигнатури яких не містяться у базі пошуку. Щоб виправити даний недолік, створюються методи, що аналізують фактори поведінки користувачів. Існує велика кількість варіацій даних методів, але з-поміж недоліків слід виділити неможливість апріорного реагування на ситуацію.

Як правило, дані методи реагують на атаку та протидіють їй на етапі завершення. Саме цей факт викликає необхідність розробки та впровадження методу, що буде:

– не залежати від факту розкриття механізмів проведення атаки, тобто сигнатур атак;

– дозволить блокувати атаку не на кінцевому етапі її проведення, а ще до того часу, як шкідливий трафік потрапить на кінцевий мережевий пристрій. Необхідно забезпечити взаємодію та управління прикордонними маршрутизаторами;

– дозволить проводити аналітику та збереження інформації про стан системи в цілому;

– забезпечить приховане управління мережею прикордонних пристроїв;

– дозволить використати всі переваги раніше запропонованих методів пошуку аномалій.

Тобто, новий метод повинен бути уніфікованим відносно включення в себе будь-яких критеріїв пошуку кібернетичних загроз та мати широку розгалужену мережу індикаторів, що повинні базуватися на комунікаційних пристроях для фізичного розведення навантаження і трафіку.

Структуру методу протидії DDoS-атакам можна представити у вигляді рис. 1.

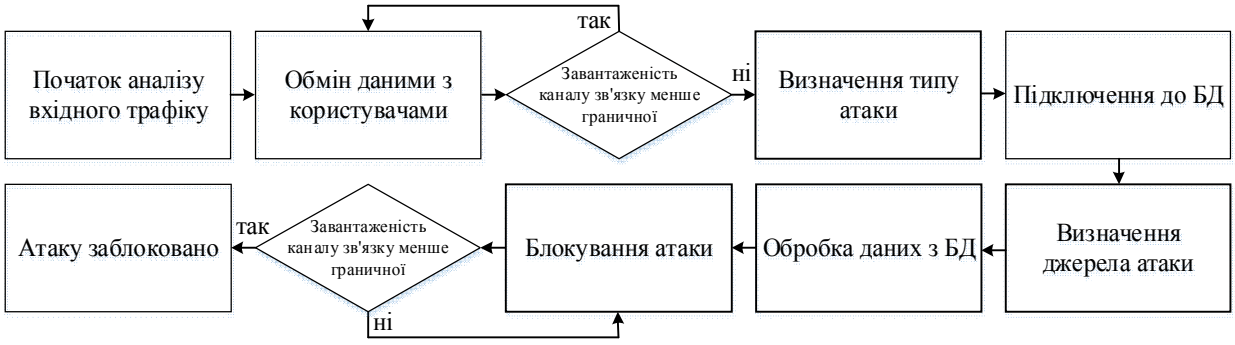

Рис. 1. Структура методу протидії DDoS-атакам

Даний метод базується на аналізі вхідного трафіку на предмет наявності DDoS-атаки, що реалізується шляхом постійної перевірки завантаженості каналу зв'язку під час обміну даними з користувачами системи. Якщо виявлене перевищення граничного рівня завантаженості каналу, виконується визначення типу атаки шляхом аналізу характеру перевищення. Після цього виконується підключення до бази даних, в яку записується весь вхідний трафік. Далі в залежності від джерела атаки проводиться обробка даних, отриманих з бази даних (БД). Після цього виконується блокування першого в черзі джерела шкідливого трафіку. Якщо перевищення продовжує мати місце, блокується наступне джерело. І так далі, поки завантаженість не стане менше граничної, що означає успішне блокування атаки.

Для виявлення та подальшого блокування DDoS-атак пропонується застосовувати аналізатор вхідного трафіку, що розміщується в інформаційній мережі так, як показано на рис. 2.

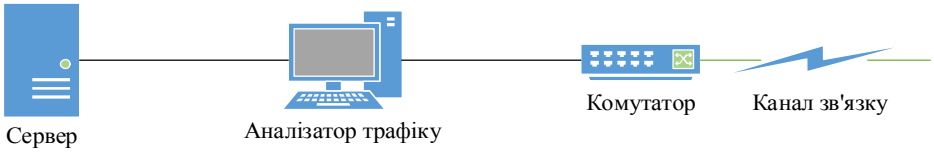

Рис. 2. Розміщення аналізатору трафіку в інформаційній мережі

Аналізатор трафіку представляє собою електронно-обчислювальну машину зі спеціальним програмним забезпеченням. Він аналізує трафік, що поступає на сервер, на предмет наявності DDoS-атак. Якщо такий трафік виявлений, то виконується пошук джерел шкідливого трафіку з метою їх подальшого блокування. Аналізатор трафіку функціонує наступним чином. Увесь вхідний трафік записується до бази даних «Джерела шкідливого трафіку». Під записом до бази даних розуміється занесення у відповідну таблицю бази даних вихідних програмних портів (source ports) вхідних сегментів, їх порядкових номерів, що відображають хронологію їх отримання, часу прибуття, а також вихідних IP-адрес пакетів, в які інкапсульовані дані сегменти. У разі наявності DDoS-атаки запускається механізм виявлення джерел шкідливого трафіку. При цьому запис вхідних сегментів не припиняється.

Для роботи механізму блокування джерел шкідливого трафіку необхідні вихідні дані, що збираються аналізатором трафіку в процесі його роботи, та записуються в базу даних «Джерела шкідливого трафіку», що знаходиться безпосередньо на аналізаторі. Розглянемо детальніше її структуру. Трафік, що надходить на сервер, записується у таблицю «Вихідні IP-адреси та порти відправників» з метою подальшого використання в процесі виявлення джерел шкідливого трафіку. Дана таблиця має колонки: порядковий номер вхідного пакету, що показує хронологію прибуття пакетів на сервер; вихідна IP-адреса відправника, яка зчитується з відповідного поля вхідного пакету; вихідний програмний порт відправника, який зчитується з відповідного поля вхідного сегмента; момент часу прибуття пакету на сервер.

Описані вище дії з базою даних «Джерела шкідливого трафіку» необхідні для виявлення джерел шкідливого трафіку, без чого неможливе їх блокування. Так як DDoS-атака реалізується шляхом відправлення трафіку багатьма комп'ютерами одночасно, то однозначно виявити всі джерела неможливо. Але ті джерела, з яких надійшла найбільша кількість пакетів, можливо вважати такими, з яких надходить шкідливий трафік. Тому блокується джерело, з якого отримано найбільшу кількість пакетів. Як наслідок, сумарний вхідний трафік зменшиться. Якщо при цьому рівень завантаженості каналу зв'язку зменшився та став меншим, ніж граничний, то інформаційна мережа може надавати послуги своїм легітимним користувачам з заданою якістю, а атака вважається припиненою. Якщо ж завантаженість каналу зв'язку не зменшилася до припустимого рівня, то береться наступне за кількістю вхідних пакетів джерело і блокується. І так повторюється до тих пір, поки завантаженість не стане меншою, ніж гранична.

Тепер перейдемо до безпосереднього блокування джерел шкідливого трафіку. Для подальшого блокування виявлених атак необхідно розширити представлену агент-орієнтовану систему, додавши до неї програмний шлюз. Для цього пропонується застосовувати таку структуру інформаційно-телекомунікаційної мережі, яка показана на рис. 3.

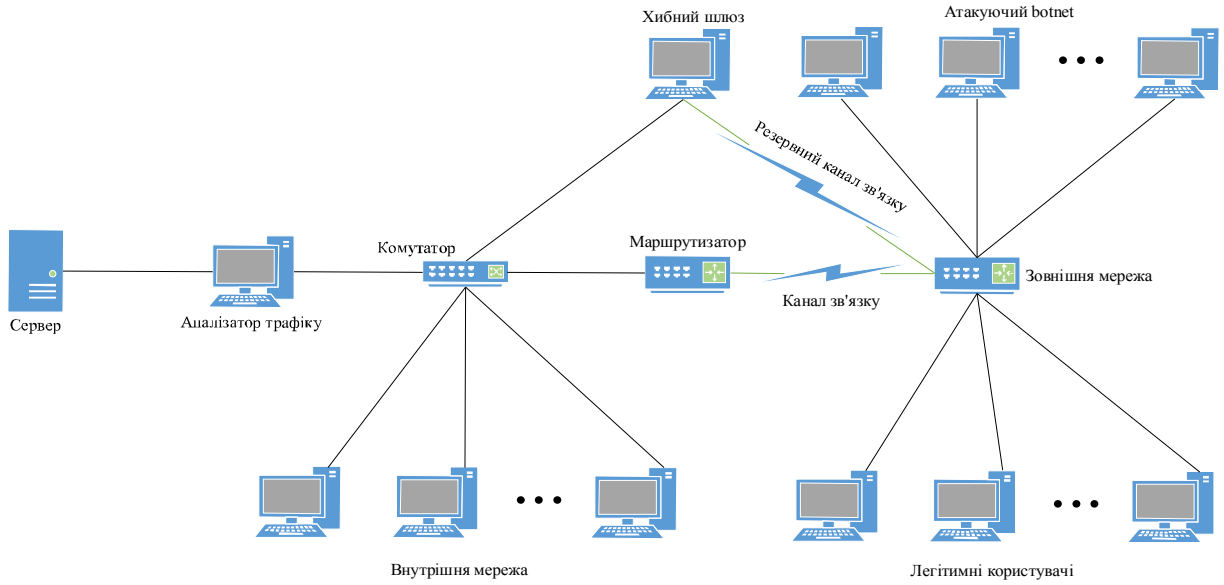

Рис. 3. Структура інформаційної мережі, що забезпечує блокування повільної DDoS-атаки

Представлена структура інформаційної мережі являє собою програмно-апаратний комплекс виявлення та блокування DDoS-атак, що складається з ключових елементів, представлених нижче.

Аналізатор трафіку реалізує механізм виявлення DDoS-атак, їх блокування у частині виявлення джерел шкідливого трафіку та запису і зберіганні необхідної інформації в базі даних «Джерела шкідливого трафіку». Комутатор з'єднує робочі станції, що входять до складу інформаційної мережі та сервер між собою, а також з маршрутизатором та програмним шлюзом, що з'єднують мережу з зовнішньою. Маршрутизатор є крайньою точкою інформаційної мережі та з'єднує останню з її зовнішніми користувачами. Програмний шлюз застосовується при формуванні альтернативного шляху передачі інформації та маскування під сервер для переадресації на нього шкідливого трафіку з метою ізоляції від цього трафіку серверу та основного каналу зв'язку. Він безпосередньо реалізує блокування джерел шкідливого трафіку наступним чином.

Якщо джерела шкідливого трафіку розмішені у внутрішній мережі інформаційної мережі, то використовується таблиця «Відсортовані вхідні пакети», я якої зчитується IP-адреса під номером один. Аналізатор трафіку відправляє на комутатор команду про відключення порта, до якого підключена ЕОМ з цією адресою. Якщо завантаженість каналу зв'язку стала меншою, ніж гранична, то атака вважається припинено. Якщо ні, то процес повторюється для наступної IP-адреси в таблиці. І так повторюється до припинення атаки. Після цього формується повідомлення системному адміністратору про наявність атаки, в якому вказується її тип та джерела. Останній повинен негайно прийняти міри по пошуку та знешкодженню шкідливого програмного забезпечення на відключених від мережі ЕОМ, а після його виявлення та знешкодження перевірити на предмет наявності такого програмного забезпечення решту ЕОМ мережі.

Якщо джерела шкідливого трафіку розмішені у зовнішній мережі інформаційної мережі, то використовується таблиця «Відсортовані вхідні сегменти», я якої зчитується порт під номером один. Аналізатор трафіку сегменти, що адресуються даному порту, відправляє по резервному через програмний шлюз, який підміняє вихідну IP-адресу серверу на свою, внаслідок чого наступні пакети, що містять сегменти визначеним вихідним портом, будуть адресуватися не серверу, а програмному шлюзу. Крім того, програмний шлюз дублює функціональність серверу для джерел шкідливого трафіку, що дозволяє маскуватися під сервер, захищаючи останній від деструктивних впливів ззовні. Якщо після цього завантаженість каналу зв'язку стала меншою, ніж гранична, то атака вважається припиненою. Якщо ні, то процес повторюється для наступного порта. І так повторюється до припинення атаки.

Алгоритм виявлення DDoS-атак. Розглянемо алгоритм виявлення DDoS-атак, схема якого представлена на рис 4. Він працює наступним чином. Інформаційна мережа постійно обмінюється пакетами зі своїми користувачами, що відображається блоком 2. При цьому виконується аналіз вхідного трафіку на предмет перевищення граничного рівня завантаженості каналу зв'язку, що вказано в блоці 3. Якщо перевищення зафіксовано в інтервалі часу до однієї секунди, то виконується перехід до блоку 4. В противному випадку – перехід до блоку 2. У блоці 4 відображена перевірка наявності перевищення граничного рівня завантаженості каналу зв'язку в інтервалі часу від першої секунди до другої. Якщо перевищення зафіксовано, то виконується перехід до блоку 5. В противному випадку – до блоку 12.

В блоці 5 виконується перевірка протоколу прикладного рівня, дані якого інкапсульовані в отримані від джерел шкідливого трафіку сегменти. Якщо дані сегменти на прикладному рівні містять протокол HTTP, то виводиться повідомлення про наявність HTTP-флуда, що відображається в блоці 6. Якщо даний протокол не знайдений отриманих сегментах, то виконується перехід до блоку 7. В цьому блоці перевіряється протокол транспортного рівня отриманих сегментів. Якщо це протокол ICMP, то робиться висновок про наявність ICMP-флуда, що відображається в блоці 8. В противному випадку

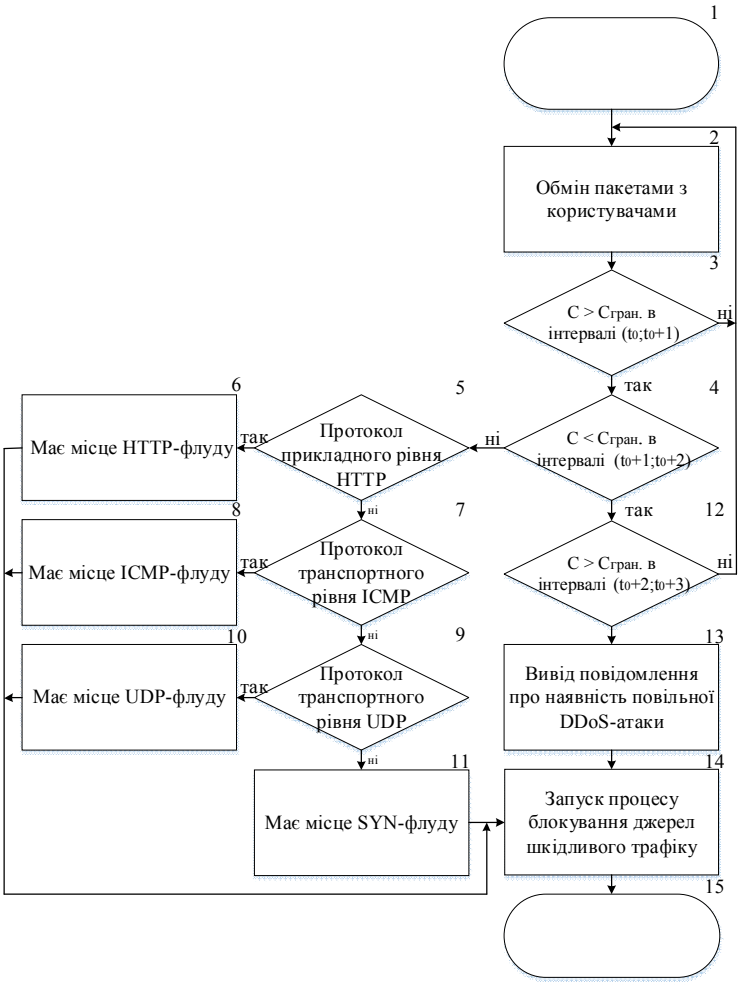

Рис. 4. Схема алгоритму виявлення DDoS-атак

виконується перехід до блоку 9. В даному блоці перевіряється чи протоколом транспортного рівня є UDP. Якщо так, то виконується вивід повідомлення про наявність UDP-флуда, що відображається в блоці 10. В противному випадку виконується перехід до блоку 11, де робиться висновок про наявність SYN-флуду з виводом відповідного повідомлення. Після чого робиться перехід до блоку 14. В блоці 12 перевіряється наявність перевищення граничного рівня завантаженості каналу зв'язку в інтервалі часу від другої секунди до третьої. Якщо перевищення не було зафіксовано, то виконується перехід до блоку 2, що свідчить про відсутність будь-яких атак типу «відмова в обслуговуванні» та продовження нормального обміну інформацією між сервером інформаційної мережі та її легітимними користувачами. Якщо перевищення зафіксовано, то виконується перехід до блоку 13, де виводиться повідомлення про наявність повільної DDoS-атаки. Після чого виконується перехід до блоку 14, в якому запускається процес блокування джерел шкідливого трафіку. Після цього виконується перехід до блоку 15 та завершення процесу виявлення атак.

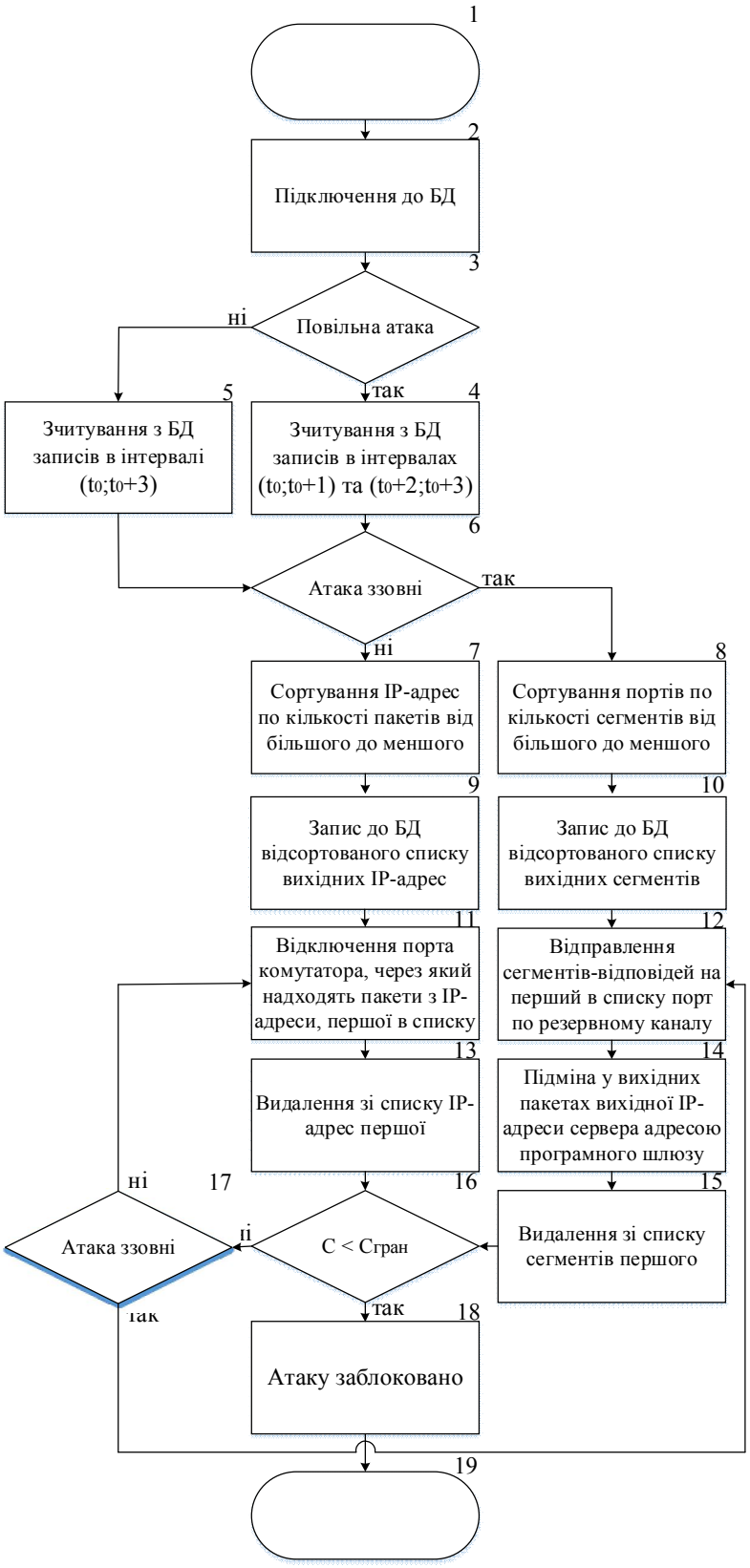

Рис. 5. Схема алгоритму блокування DDoS-атак

Алгоритм блокування DDoS-атак. Вище був розглянутий алгоритм виявлення DDoS-атак, який програмно реалізується на аналізаторі трафіку. Тепер перейдемо до розгляду алгоритму блокування даного типу атак, що реалізується як на аналізаторі трафіку, так і на програмному шлюзі. Блок-схема даного алгоритму представлена на рис. 5.

Робота даного алгоритму починається з підключення до бази даних «Джерела шкідливого трафіку», що виконується в блоці 2. Після цього в блоці 3 визначається тип атаки. Якщо має місце повільна DDoS-атака, то з бази даних зчитуються записи за першу та третю секунди від її початку (блок 4). При наявності атаки на всьому часовому інтервалі зчитуються записи за три секунди від початку атаки (блок 5). Далі визначається джерело атаки. Якщо атака з внутрішньої мережі, то в блоці 7 виконується сортування IP-адрес по кількості пакетів від більшого до меншого. Після цього в блоці 9 відсортований список вихідних адрес записується у таблицю «Відсортовані вхідні пакети» бази даних. Потім в блоці 11 виконується відключення порта комутатора, через який надходять пакети з IP-адреси, першої в списку. Далі в блоці 13 перша адреса в списку видаляється. Якщо атака ззовні, то в блоці 8 виконується сортування портів по кількості сегментів від більшого до меншого. Потім в блоці 10 відсортований список вихідних сегментів записується в таблицю «Відсортовані вхідні сегменти» бази даних. Після чого в блоці 12 викону-

ється відправлення сегментів-відповідей на перший в списку порт по резервному каналу зв'язку. Далі в блоці 14 виконується підміна у вихідних пакетах адреси серверу адресою програмного шлюзу з подальшим видаленням зі списку сегментів першого в блоці 15. Після виконання блокування першого джерела шкідливого трафіку виконується перевірка завантаженості каналу зв'язку в блоці 16. Якщо завантаженість більше граничної, то, перевіривши в блоці 17 джерело атаки, виконується блокування наступного в списку джерела, що змістилося з другого номеру на перший. Якщо завантаженість стала меншою, ніж гранична, в блоці 18 робиться висновок, що атаку заблоковано, і процес блокування завершується.

Оцінка ефективності запропонованого методу протидії DDoS-атакам. Перейдемо до оцінки ефективності запропонованого методу протидії DDoS-атакам, що реалізується шляхом аналізу вхідного трафіку на предмет наявності останньої і подальшого виявлення джерел шкідливого трафіку та їх блокування. Для цього застосуємо критерії ефективності, що базується на забезпеченні оперативності управління в інформаційній мережі. У якості показника ефективності застосовується час недоступності інформаційної мережі.

Було знайдено середнє значення часу кругового обігу пакетів в мережі Інтернет RTT = $5*10^{-2}$ секунд, що дозволило оцінити час недоступності інформаційної мережі в залежності від кількості комп'ютерів в мережі, що здійснює атаку.

Залежність часу недоступності від кількості комп'ютерів в мережі, що здійснює атаку, представлена на рис. 6.

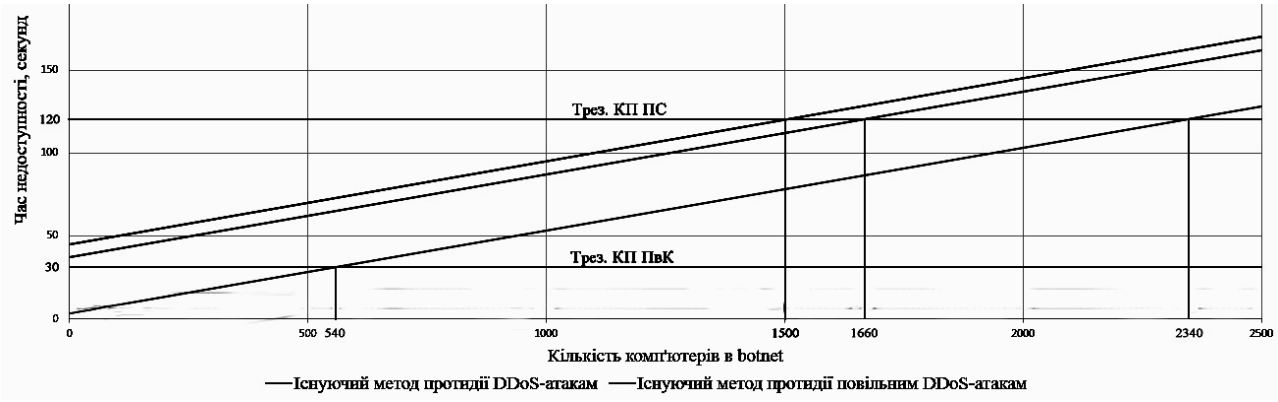

Рис. 6. Залежність часу недоступності від кількості комп'ютерів в мережі

На даному рисунку відображені значення резервного. Також на ньому порівняно існуючи методи протидії DDoS-атакам, як повільним, так і на всьому часовому інтервалі. Видно, що запропонований метод дозволяє забезпечити однакову з існуючими оперативність управління при можливості блокування атаки значно більшою за розміром мережі.

Було проведено експериментальне дослідження ефективності роботи запропонованого методу протидії повільним DDoS-атакам, результати якого приведені у табл. 1.

Таблиця 1 – **Експериментальне дослідження ефективності запропонованого методу при наявності DDoS-атаки**

Кількість випробувань	Кількість вірних рішень	Кількість невірних рішень	
		Неспрацювання	Хибне спрацювання
10000	9696	203	101

Випробування проводилися на імітаційній моделі інформаційної мережі під впливом повільної DDoS-атаки та атаки на всьому часовому інтервалі. Кількість випробувань була обмежена 10000, в зв'язку з тим, що результати дослідження по досягненні даного числа випробувань проявляли стійку тенденцію.

Можна розрахувати, що ймовірності прийняття вірного рішення про наявність або відсутність повільної DDoS-атаки та її успішного блокування, а також ймовірності помилок. Ймовірність прийняття вірного рішення становить 97%, помилки першого роду – 2 % та помилки другого роду – 1 %.

Таким чином, запропонований метод протидії DDoS-атакам дозволяє значно скоротити час недоступності інформаційної мережі (28 секунд) у порівнянні з існуючими (45 секунд), показує значний відсоток успішних спрацьовувань (97 %), що гарантує забезпечення заданих вимог до оперативності управління в інформаційній мережі під впливом DDoS-атаки.

Висновки

Запропоновано метод протидії DDoS-атакам, що дозволяє ефективно захищати інформаційну мережу як від атак на всьому часовому інтервалі, так і від повільних атак. Даний метод дозволяє забезпечити функціональну стійкість інформаційної мережі та базується на використанні алгоритмів виявлення та блокування DDoS-атак, а також збору інформації про вхідний трафік з записом до бази даних «Джерела шкідливого трафіку». При виявленні атаки визначається її тип та запускається механізм її блокування, що реалізується в два етапи.

На першому етапі виконується пошук джерел шкідливого трафіку, використовуючи зібрану в базі даних інформацію про вхідні пакети.

На другому етапі виконується безпосереднє блокування виявлених джерел шляхом відправлення

пакетів-відповідей по резервному каналу зв'язку через програмний шлюз, на якому вихідна адреса серверу у пакетах підміняється адресою шлюзу, що дає змогу замаскувати сервер від зовнішнього деструктивного впливу (у разі атаки ззовні).

При атаці з внутрішньої мережі відключаються порти комутатора, до яких підключені джерела шкідливого трафіку. Після цього оповіщається системний адміністратор, який негайно приступає до пошуку та знешкодження шкідливого програмного забезпечення.

Отримані алгоритми виявлення та блокування DDoS-атак, що описують послідовність дій при застосуванні методу протидії. Алгоритм виявлення атак реалізується на аналізаторі вхідного трафіку, який перевіряється на предмет наявності DDoS-атак. У разі виявлення такої атаки визначається її тип. Після цього реалізується алгоритм блокування, який зчитує з бази даних джерела шкідливого трафіку та перенаправляє його на програмний шлюз, який забирає на себе подальший деструктивний вплив. Таким чином, алгоритм блокування атаки реалізується частково на аналізаторі трафіку та частково на програмному шлюзі.

Проведена оцінка ефективності запропонованого методу протидії DDoS-атакам. В якості показника ефективності обрано час недоступності інформаційної мережі для її користувачів. В порівнянні з існуючим методом протидії DDoS-атакам, запропонований метод здатний істотно скоротити час виявлення та блокування атаки. При цьому ймовірність прийняття вірного рішення при виявленні атаки становить 97 %, помилки першого роду – 2 % та помилки другого роду – 1 %.

СПИСОК ЛІТЕРАТУРИ

1. Математична модель структури розгалуженої інформаційної мережі 5 покоління (5G) на основі випадкових графів / І. П. Саланда, О. В. Барабаш, А.П. Мусієнко, Н.В. Лукова-Чуйко // Наукове періодичне видання «Системи управління, навігації та зв'язку». – Полтава: ПНТУ, 2017. – Вип. 6 (46). – С. 118–121.
2. Аналіз кібернетичних атак як істотних загроз інформаційній безпеці / І. В. Рубан, Є. С. Лошаков, Д. В. Прибильнов, О. П. Давікоза // Системи управління, навігації та зв'язку. – К., 2012. – № 4(24). – С. 102–105.
3. Саланда І. П. Система показників та критеріїв формалізації процесів забезпечення локальної функціональної стійкості розгалужених інформаційних мереж / І. П. Саланда, О. В. Барабаш, А. П. Мусієнко // Наукове періодичне видання «Системи управління, навігації та зв'язку». – Полтава: ПНТУ, 2017. – Вип. 1 (41). – С. 122 – 126.
4. Рубан І. В. Аналіз основних аспектів впливу DOS атак на працездатність мережі / І. В. Рубан, Є. С. Лошаков, Д. В. Прибильнов // Сучасні інформаційні технології у сфері безпеки та оборони. – К., 2013. – № 3 (18). – С. 90–92.
5. Mashkov V. A. Self-checking and Self-diagnosis of Module Systems on the Principle of Walking Diagnostic Kernel / V. A. Mashkov, O. V. Barabash // Engineering Simulation. – Amsterdam: OPA, 1998. – Vol. 15. – P. 43-51.
6. Барабаш О.В. Інформаційний підхід до забезпечення функціональної стійкості складних організаційних ерготехнічних систем / О. В. Барабаш, Д. П. Пашков, О. М. Горський // Системи обробки інформації. – Харків: ХУПС, 2016. – Вип. 9 (146). – С. 86–89.
7. Барабаш О. В. Методология построения функционально-устойчивых распределенных информационных систем специального назначения / О. В. Барабаш. – Киев: НАОУ, 2004. – 224 с.
8. Барабаш О. В. Методика накопичення діагностичної інформації в системах інтелектуального відеоконтролю / О. В. Барабаш, С. В. Бодров, А. П. Мусієнко // Наукове періодичне видання «Системи управління, навігації та зв'язку». – Полтава: ПНТУ, 2015. – Вип. 1 (33). – С. 118–121.
9. Барабаш О. В. Алгоритм самодіагностування технічного стану вузлів комутації інформаційних систем / О. В. Барабаш, Д. М. Обідін, А. П. Мусієнко // Сучасний захист інформації. – К., 2014. – № 2. – С. 114–121.
10. Рубан І. В. Обгрунтування вибору інтервалу спостереження при очікуванні повільної DoS-атаки / І. В. Рубан, Є. С. Лошаков, Д. В. Прибильнов // Системи обробки інформації. – Х., 2014. – Вип. 8 (124). – С. 135–137.

REFERENCES

1. Salanda, I.P., Barabash, O.V., Musienko, A.P. and Lukova-Chuiko, N.V. (2017), "Mathematical model of the structure of the 5th generation branched information network (5G) on the basis of random graphs", *Control systems, navigation and communication*, PNTU, Poltava, No. 6 (46), pp. 118-121.
2. Ruban, I.V., Loshakov, Ye.S., Pribilnov, D.V. and Davikoza O.P. (2012), "Analysis of cybernetic attacks as significant threats to information security", *Control, navigation and communication systems*, PNTU, Poltava, No. 4 (24), pp, 102-105.
3. Salanda, I.P., Barabash, O.V. and Musienko, A.P. (2017), "The system of indicators and criteria for formalizing the processes of ensuring the local functional stability of the branched information networks", *Control, navigation and communication systems*, PNTU, Poltava, No. 1 (41), pp, 122-126.
4. Ruban, I.V., Loshakov, Ye.S. and Pribilnov, D.V. (2013), "Analysis of the main aspects of the impact of DOS attacks on network performance", *Modern information technologies in the field of security and defense*, Kyiv, No. 3 (18), pp. 90-92.
5. Mashkov, V.A. and Barabash, O.V. (1998), "Self-checking and Self-diagnosis of Module Systems on the Principle of Walking Diagnostic Kernel", *Engineering Simulation*, OPA, Amsterdam, Vol. 15, pp. 43-51.
6. Barabash, O.V., Pashkov, D.P. and Gorsky, O.M. (2016), "Informational approach to ensuring the functional stability of complex organizational ergot systems", *Information Processing Systems*, KhUPS, Kharkiv, No. 9 (146), pp. 86-89.
7. Barabash, O.V. (2004), *Methodology for constructing functionally stable distributed information systems for special purposes*, NAOU, Kyiv, 224 p.
8. Barabash, O.V., Bodrov, S.V. and Musienko, A.P. (2015), "Method of accumulation of diagnostic information in systems of intellectual video control", *Control systems, navigation and communication*, PNTU, Poltava, No. 1 (33), pp. 118-121.

9. Barabash, O.V., Obidin, D.M. and Musienko, AP (2014), "The algorithm of self-diagnostics of the technical condition of the switching nodes of information systems", *Modern Information Protection*, Kyiv, No. 2, pp. 114-112.
10. Ruban, I.V., Loshakov, Ye.S. and Pribilnov, D.V. (2014), "Justification of the choice of the interval of observation in anticipation of a slow DoS-attack", *Information Processing Systems*, KhUPS, Kharkiv, No. 8 (124), pp. 135-137.

Надійшла (received) 21.02.2018
Прийнята до друку (accepted for publication) 11.04.2018

Обеспечение функциональной устойчивости информационных сетей на основе разработки метода противодействия DDOS -атакам

О. В. Барабаш, Н. В. Лукова-Чуйко, А. П. Мусієнко, В. В. Собчук

Предметом изучения в статье является процесс обеспечения свойства функциональной устойчивости информационных сетей. **Целью** является разработка метода противодействия DDoS-атакам, что позволяет эффективно защищать информационную сеть, как от атак на всем временном интервале, так и от медленных атак. **Задача:** разработать алгоритмы обнаружения и блокирования DDoS-атак, описывающих последовательность действий при применении метода противодействия; провести оценку эффективности предложенного метода противодействия DDoS-атакам. Используемыми **методами** являются: графов подход, математические модели оптимизации, методы решения нелинейных задач. Получены следующие **результаты**. Построены алгоритмы обнаружения и блокирования DDoS-атак, описывающих последовательность действий при применении метода противодействия. Алгоритм обнаружения атак реализуется на анализаторе входящего трафика, который проверяется на предмет наличия DDoS-атак. В случае выявления такой атаки определяется ее тип. После этого реализуется алгоритм блокировки, который считывает из базы данных источника вредного трафика и перенаправляет его на программный шлюз, который берет на себя дальнейшее деструктивное влияние. **Выводы.** Научная новизна полученных результатов заключается в следующем: мы предложили метод противодействия DDoS-атакам, что позволяет эффективно защищать информационную сеть как от атак на всем временном интервале, так и от медленных атак. Данный метод позволяет обеспечить функциональную устойчивость информационной сети и базируется на использовании алгоритмов обнаружения и блокирования DDoS-атак, а также сбора информации о входящем трафике с записью в базу данных «Источники вредоносного трафика». При обнаружении атаки определяется ее тип и запускается механизм ее блокировки, который реализуется в два этапа. На первом этапе выполняется поиск источников вредоносного трафика, используя собранную в базе данных информацию о входящих пакетах. На втором этапе выполняется непосредственная блокировка выявленных источников путем отправки пакетов-ответов по резервному каналу связи через программный шлюз, на котором исходный адрес сервера в пакетах подменяется на адрес шлюза, что позволяет замаскировать сервер от внешнего деструктивного воздействия (в случае атаки извне). При атаке с внутренней сети отключаются порты коммутатора, к которым подключены источники вредоносного трафика. После этого оповещается системный администратор, который немедленно приступает к поиску и обезвреживанию вредоносных программ.

Ключевые слова: информационная сеть; функциональная устойчивость; DDoS-атака; системы обнаружения торжения; база данных; анализатор трафика; маршрутизаторы; коммутаторы.

Providing functional stability of information networks Based on the development of method for countering ddos-attacks

O. Barabash, N. Lukova-Chuiko, A. Musienko, V. Sobchuk

The subject of study in the paper is the process of providing the property of the functional stability of information networks. **The goa**l is to develop the method of countering of DDoS- attacks, which allows to effectively protect the information network, both from attacks on the overall time interval, and from slow attacks. **The problem** is to develop algorithms for detecting and blocking of DDoS - attacks, which describe the sequence of actions when applying the method of countering of DDoS- attacks, to evaluate of the efficiency of the proposed method. The methods, which used are graph approach, mathematical models of optimization, methods of solving nonlinear problems tasks. The following **results** are obtained. Algorithms are constructed for detecting and blocking DDoS-attacks which describing the sequence of actions when applying the method of countering. The algorithm for detecting attacks is implemented on the analyzer of incoming traffic, which is checked for the presence of DDoS attacks. In case of detecting such an attack, its type is determined. After that, the blocking algorithm is implemented, which reads from the database of malicious traffic source and redirects it to the software gateway, which takes on itself the further destructive influence. **Conclusions.** Scientific novelty of the obtained results is as follows, we have proposed the method of countering of DDoS- attacks, which effectively protects the information network, both from attacks on the overall time interval, and from slow attacks. This method allows ensuring the functional stability of the information network and is based on the use of algorithms for detecting and blocking DDoS-attacks, and also collection of information about incoming traffic with the record in the database of "Sources of Malicious Traffic". When an attack is detected, it is determined her type it is started the mechanism for her blocking, which is realized in two stages. At the first stage, it is executed searching of sources of malicious traffic using the collected information about incoming packages in the database. At the second stage, it is performed direct blocking of detected sources by sending packets of replies on the backup channel through the software gateway on which, the outgoing address of server in packages replaced by the address of the gateway which it is allows to disguise the server from external destructive effects (in the case of the outside attack). When the attack from the internal network, switches ports to which connected sources of malicious traffic are disconnected. After that, the system administrator is notified, who immediately starts to search and eliminate of malicious software.

Keywords: information network; functional stability; DDoS-attack; systems of detecting an intrusion; database; analyzer of traffic; routers; switches.