ІНФОКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ ТА ЕЛЕКТРОННА ІНЖЕНЕРІЯ
INFORMATION AND COMMUNICATION TECHNOLOGIES, ELECTRONIC ENGINEERING

№ 2 (2), 2021 https://doi.org/10.23939/ictee2021.02.019

ЗАСОБИ ВИЯВЛЕННЯ КІБЕРНЕТИЧНИХ АТАК НА ІНФОРМАЦІЙНІ СИСТЕМИ

С. Толюпа, Н. Лукова-Чуйко, Я. Шестак

Київський національний університет імені Тараса Шевченка, вул. Володимирська, 60, Київ, 01033, Україна

Відповідальний за рукопис: С. Толюпа (e-mail: tolupa@i.ua).

(Подано 26 грудня 2021)

Системи виявлення мережевих вторгнень і виявлення ознак кібератак на інформаційні системи вже давно застосовують як один із необхідних рубежів оборони інформаційних систем. Сьогодні системи виявлення вторгнень і атак – це зазвичай програмні або апаратно-програмні рішення, які автоматизують процес контролю подій, що відбуваються в інформаційній системі або мережі, а також самостійно аналізують ці події в пошуках ознак проблем безпеки. Оскільки кількість різних типів і способів організації несанкціонованих проникнень у чужі мережі за останні роки значно збільшилася, системи виявлення атак (СВА) стали необхідним компонентом інфраструктури безпеки більшості організацій. Незважаючи на існування численних методів виявлення аномалій, їхня слабка стійкість, відсутність верифікації, велика кількість хибних спрацьовувань, вузька спеціалізація та дослідницький характер не дають змоги широко їх використовувати. Одним із найпоширеніших типів атак є DDoS-атака – атака типу "відмова в обслуговуванні", яка за допомогою переривання або призупинення обслуговування хост-сервера робить онлайн-сервіс недоступним для користувачів. У статті запропоновано аналіз такої атаки, можливості її виявлення та реалізації.

Ключові слова: *атака; інформаційна система; сервер; система виявлення вторгнень; мережа.*
УДК 004.056.4:18.08

1. Вступ

Основним засобом захисту інформаційних систем та мереж (ІС) від інформаційно-руйнівних впливів (втручань) у вигляді кібернетичних вторгнень (КВ) є системи виявлення та/або запобігання вторгненням (СВВ/СЗВ), основне завдання яких зводиться до оперативної їх ідентифікації (встановлення відповідності між об'єктом і його ідентифікатором (унікальним атрибутом) та в ідеальному випадку ініціювання ефективного захисного сценарію щодо припинення факту порушення конфіденційності, доступності та цілісності інформаційних ресурсів, сервісів. Практика застосування СВВ сформувала два напрями протидії КВ: виявлення зловживань (Misuse detection) та виявлення аномалій (Anomaly detection).

Всі розробники систем виявлення атак і організації, які використовують СВА, повинні розуміти й вивчати їх класифікацію, щоб вибрати найкращі рішення для систем захисту інформації. За умови дослідження різних аспектів таксономії та застосування різних варіантів можна досягти вищого рівня безпеки інформаційних систем [1, 2].

Виявлення вторгнень є сферою активних досліджень вже кілька десятиліть. Існує велика кількість різних методів і підходів для виявлення віддалених мережевих атак. Для захисту інформаційної системи використовують такі найпоширеніші засоби і методи: політика безпеки корпора-

тивної мережі; міжмережеві екрани; захист на рівні маршрутизаторів; мережевий аудит; системи виявлення вторгнень; регламент реагування на виявлені атаки.

Сьогодні вирішення питань забезпечення безпеки в інформаційних системах та управління станом їх захищеності висвітлено в роботах вітчизняних та закордонних дослідників, а саме: В. Л. Бурячка, С. С. Бучика, С. О. Гнатюка, В. Б. Дудикевича, С. П. Євсеєва, С. В. Казмирчук, О. Г. Корченко, О. О. Кузнецова, І. Ю. Субача, В. О. Хорошко, T. Ptaceka, G. Elmasry, P. Albers, O. Camp та інших.

Сьогодні для захисту інформації потрібно не просто розробити приватні механізми захисту, а реалізувати системний підхід, що охоплює комплекс взаємопов'язаних заходів. Головною метою будь-якої системи забезпечення інформаційної безпеки є створення умов функціонування підприємства, запобігання кіберзагрозам його безпеки, захист законних інтересів підприємства від протиправних посягань, недопущення розкрадання фінансових засобів, розголошення, втрати, витоку, спотворення і знищення службової інформації, забезпечення цього в межах діяльності установи. Всі ці питання доволі детально розкрито в [3, 4].

Системи виявлення мережевих вторгнень і ознак кібератак на інформаційні системи вже давно застосовують як один із необхідних рубежів оборони інформаційних систем. Розробники систем захисту інформації та консультанти в цій галузі активно використовують такі поняття, як захист по периметру, стаціонарний і динамічний захист, пропонують власні терміни, наприклад, проактивні засоби захисту [5].

Сьогодні системи виявлення вторгнень і атак – це зазвичай програмні або апаратно-програмні рішення, які автоматизують процес контролю подій, що відбуваються в інформаційній системі або мережі, а також самостійно аналізують ці події в пошуках ознак проблем безпеки. Оскільки кількість різних типів і способів організації несанкціонованих проникнень у чужі мережі за останні роки значно збільшилася, системи виявлення атак (СВА) стали необхідним компонентом інфраструктури безпеки більшості організацій [6].

Взагалі кажучи, сучасні системи виявлення вторгнень і атак ще далекі від ергономічних і ефективних із погляду безпеки рішень. А підвищення ефективності необхідне не тільки задля виявлення зловмисних дій на інфраструктуру захищених об'єктів інформатизації, але і з погляду повсякденної експлуатації цих засобів, а також економії обчислювальних та інформаційних ресурсів власника системи захисту.

Сценарій атаки – це граф переходів, аналогічний графу кінцевого детермінованого автомата. А фази атак можна описати, наприклад, так: випробування портів; ідентифікація програмних і апаратних засобів; збирання банерів; застосування експлойтів; дезорганізація функціонала мережі за допомогою атак на відмову в обслуговуванні; управління через бекдори; пошук встановлених троянів; пошук проксі-серверів; видалення слідів присутності тощо.

Переваги такого підходу очевидні – у разі роздільного оброблення різних етапів атаки з'являється можливість розпізнавати загрозу ще в процесі її підготовки і формування, а не на стадії її реалізації, як це відбувається в наявних системах. Елементною базою для розпізнавання може бути як сигнатурний пошук, так і виявлення аномалій, використання експертних методів та інтелектуальних систем, довірчих стосунків та інших інформаційних, вже відомих і реалізованих, мережевих і локальних примітивів оцінювання того, що відбувається в інформаційному середовищі потоку подій. Узагальнювальний підхід до аналізу дає змогу визначати відповідно й розподілені загрози, як у логічному, так і у фізичному просторі. Загальна схема оброблення вхідних подій також уможливлює пошук розподілених атак за допомогою подальшої агрегації даних із різних джерел і конструювання метаданих про відомі інциденти. Системи виявлення атак, як і більшість сучасних програмних продуктів, повинні задовольняти певні вимоги. Це й сучасні технології розроблення, і орієнтування на особливості сучасних інформаційних мереж, і сумісність з іншими програмами. Щоб зрозуміти, як правильно використовувати СВА, потрібно чітко уявляти, як вони працюють і які їх вразливі місця [7].

Результати порівняльного аналізу методів виявлення кібератак показують, що для більшості поведінкових методів характерним недоліком є слабка верифікованість та стійкість. З іншого боку, основною їх перевагою є адаптивність та здатність виявляти раніше не відомі атаки. Основним недоліком методів на основі знань є слабка їх адаптивність до виявлення ще не класифікованих кібератак, а більшість методів ІАД слабковерифіковані. Проте серед них можна виділити методи, які показали найповнішу відповідність заданим критеріям аналізу, є одночасно верифікованими, адаптивними та стійкими: експертні системи та методи на основі нечіткої логіки.

Результати досліджень наведено в табл. 1, де *H* – спостереження на рівні вузла; *N* – спостереження на рівні мережевої взаємодії; *HG* – спостереження на різних рівнях.

Таблиця 1

Результати аналізу методів виявлення кібератак

	Аномалії/ зловживання	Верифікованість	Адаптивність	Стійкість	Обчислювальна складність
Сигнатурний аналіз	-/+	+	-	+	ln(n)
Аналіз систем станів	-/+	+	-	+	> O(n)
Графи сценаріїв атак	-/+	+	+	+	NP
Методи на специфікаціях	-/+	+	-	-	ln(n)
Методи на сплайнах	-/+	-	+	-	> O(n)
Експертні системи	+/+	+	+	+	NP
Мережі Петрі	-/+	+	-	+	NP
Генетичні алгоритми	+/+	-	+	+	ln(n)
Нейронні мережі	+/+	-	+	-	> O(n)
Імунні мережі	+/+	-	+	-	> O(n)
Нечітка логіка	+/+	+	+	+	> O(n)
Метод опорних векторів	+/+	-	+	-	ln(n)
Дерева рішень	+/+	+	-	-	NP
Мережі Баєса	+/+	-	+	+	> O(n)
Роєві алгоритми	+/+	+	+	-	P
Регресійний аналіз	+/+	-	+	-	P
Статичний аналіз	+/-	-	+	-	> O(n)
Вейвлет-аналіз	+/-	-	+	-	NP
Кластерний аналіз	+/+	-	+	-	> O(n)
Спектральний аналіз	+/-	-	+	-	NP
Фрактальний аналіз	+/-	-	+	-	> O(n)
Аналіз ентропії	+/-	+	+	-	> O(n)
Біометрія поведінки	+/-	-	+	-	> O(n)

Аналіз відомих методів і СВВ дає підстави зробити висновок про відсутність СВВ, адаптивної до невідомих кібератак. Ці програмні рішення використовують на базовому рівні ту чи іншу реалізацію сигнатурного методу виявлення (запобігання) вторгнень. Реалізації відрізняються рівнем розгляду системи, алфавітом сигнатур, структурою, архітектурою і способом побудови сигнатур – від простого пошуку до повноцінної реалізації регулярних виразів за заданим алфавітом.

Хоч методів виявлення аномалій чимало, через низьку стійкість, відсутність верифікації, велику кількість хибних спрацьовувань, вузьку спеціалізацію та дослідницький характер їх неможливо широко використовувати.

Одним із найпоширеніших типів атак є DDoS-атака – це атака типу “відмова в обслуговуванні”, яка за допомогою переривання або призупинення обслуговування хост-сервера робить онлайн-сервіс недоступним для користувачів. Суть у тому, що DDoS використовує підключені до інтернету пристрої, щоб привести шкідливий трафік. Між DDoS та DoS. DDoS існує відмінність. DoS. DDoS – розподілена атака з багатьох джерел, а DoS – з одного джерела (рис. 1).

Рис. 1. Схема DoS атаки

Найвідомішими різновидами DoS-атак є такі: Flood, ICMP flood, Identification flood, TCP SYN flood, Ping of Death, Tribe Flood Network, Trinco, Stacheldracht, Trinity та багато інших. Серед них лише атаку TCP SYN flood, що полягає у надсиланні великої кількості запитів на ініціалізацію TCP-з'єднань з вузлом-мішенню, якому в результаті доводиться витрачати всі свої ресурси на те, щоб відстежувати ці частково відкриті з'єднання, фахівці вважають найефективнішою. Це найвідоміший спосіб переповнення інформаційного каналу SYN-пакетами, внаслідок якого сервер не відповідає на запити користувачів. Під час Flood ("затоплення") та ICMP flood (flood ping – "потік пінгів") атак на систему надсилається відповідно велика кількість ICMP (найчастіше) або UDP-пакетів, які не несуть корисної інформації, та так званих ехо-запитів ICMP (пінг системи). Наслідок цього – зменшення перепускної смуги каналу, незначне завантаження комп'ютерної системи аналізом "сміття", що надійшло, та генерацією відповідей на нього (довідково: ICMP-пакети система не аналізує за замовчуванням, а відповіді на них не займають багато CPU-time).

Розподілена DDoS-атака (Distributed Denial of Service) – це підтип DoS-атаки, що здійснюється одночасно з великої кількості IP-адрес (комп'ютерів) на систему об'єкта атаки та має за мету зробити мережу недоступною для звичайного використання. Для цього створюють так звані ботнети (інакше – бот-мережі або зомбі-мережі) із групи заражених шкідливими програмами комп'ютерів, які одночасно надсилають запити до ресурсу, який атакують. У результаті сервер не справляється із навантаженням, і доступ до атакованого ресурсу ускладнюється або взагалі стає неможливим.

Сучасні засоби захисту від DDoS-атак дають можливість з високим ступенем ефективності виявити атаку й зменшити збитки, завдані ресурсам операторів і їхніх клієнтів, або запобігти цьому. Нині, наприклад, компанія "NVisionGroup" пропонує комплексне рішення для захисту від DDoS-атак на основі технології Cisco Clean Pipes, що забезпечує оперативну реакцію на DDoS-атаки, легко масштабується, має високу надійність і швидкодію. Технологія Cisco Clean Pipes припускає використання модулів Cisco Anomaly Detector і Cisco Guard, а також різні системи статистичного аналізу мережевого трафіку, основані на даних, одержуваних із маршрутизаторів за протоколом Cisco Netflow. При цьому Anomaly Detector і системи статистичного аналізу трафіку виступають як системи виявлення DDoS-атак, а Cisco Guard – як засіб протидії вже виявленій атаці.

Є підстави стверджувати, що позбутися деструктивного впливу кібератак нині практично неможливо. Однак запропоновано певні загальні способи для послаблення їхніх негативних наслідків. Вони ґрунтуються передусім на вивченні слабких місць прикладних програм за даними корпорацій *Bugtrad* (*http://www.securityfocus.com*) і CERT (*http://www.cert.com*); застосуванні, крім системного адміністрування систем розпізнавання атак (IDS технологій), додаткового програмного забезпечення (ПЗ), що дасть можливість відстежувати всі пакети, які проходять через визначений мережевий інтерфейс; аналізуванні спеціальних аналітичних додатків із використанням логфайлів операційних систем та мережевих логфайлів; застосуванні евристичних механізмів захисту, антивірусних програм та персонального *Firewall* тощо.

Реалізуючи DoS-атаки, що використовують недостатню кількість ресурсів системи, зловмисник намагається захопити такі системні ресурси, як оперативна і фізична пам'ять, процесорний час тощо. Як правило, такі атаки здійснюються, якщо зловмисник вже володіє певною кількістю ресурсів.

Метою атаки є захоплення додаткових ресурсів. Зловмисник намагається максимально навантажити центральний процесор сервера, заповнити усю вільну оперативну або фізичну пам'ять, внаслідок чого виникає відмова в обслуговуванні. Нижче висвітлено способи реалізації цього виду атак.

Сьогодні найефективнішими є повільні DoS-атаки, які важко виявити. Можливість реалізації такої атаки зумовлена особливостями роботи протоколу TCP, а саме механізму тайм-ауту та повторного передавання пакета. Цей механізм працює так: після відправлення пакета очікується пакет-відповідь протягом інтервалу часу RTO (Retransmission TimeOut). Якщо пакет-відповідь не приходить упродовж цього інтервалу часу, пакет передається повторно, а RTO збільшується у два рази. Якщо знову пакет-відповідь не приходить упродовж інтервалу часу RTO, ще раз виконується повторне передавання, а RTO збільшується ще удвічі, і так далі. Цю особливість використовує зловмисник для реалізації атаки. Він відправляє імпульс трафіку в необхідний момент часу, а саме в кінці інтервалу RTO. Внаслідок цього канал зв'язку переповнюється в момент, коли очікуються пакети-відповіді, їх не отримують, а інтервал часу RTO збільшується в два рази. Далі зловмисник повторює свої дії. Пакети-відповіді знову не одержують. Наслідок цього – стійка непрацездатність системи і відмова в обслуговуванні легітимних користувачів.

Поки що не існує ефективних засобів виявлення та захисту від повільних DDoS-атак. Тому розроблення методу протидії DDoS-атакам, що реалізуються переповненням каналу зв'язку, особливо повільним, є актуальним науково-прикладним завданням [9].

Для боротьби із DDoS-атаками, що націлені на переповнення каналу зв'язку на всьому часовому інтервалі, існує метод, що полягає у збиранні під впливом атаки статистичних даних про вхідний трафік, що дає підстави для висновку про її наявність з достатньою ймовірністю тільки після 37-ї секунди від початку (рис. 2). Для блокування атаки використовується розподілена мережа центрів фільтрації (рис. 3), що звільняють канал зв'язку сервера від шкідливого трафіку.

Для виявлення атаки очікують послідовність піків трафіку, які надалі порівнюють із шаблонами, що займає 45 с. Після виявлення розпочинається процес блокування атаки із відкиданням найінтенсивнішого потоку трафіку в разі завантаженості каналу зв'язку менше ніж на 65 %. В іншому випадку виконується зміна протокольних характеристик.

Отже, існує декілька методів протидії DDoS-атакам і один метод протидії повільним атакам. Останній дає змогу виявити повільну атаку через 45 с від її початку, що є достатньо тривалим інтервалом часу. Тому необхідно покращити цей метод. Інші методи протидії DDoS-атакам основані на організаційних заходах, на нарощуванні ресурсів або розділенні компонентів системи на зовнішні та внутрішні, що не дає гарантованого захисту, особливо за атаки високої інтенсивності.

Характерною особливісттю повільних DOS-атак є експоненціальне зменшення інтенсивності атаки залежно від інтервалу часу. Сумарна швидкість атаки в десятки разів менша, ніж розподілених DOS-атак, що ускладнює їх виявлення наявними апаратними та програмними засобами.

З вищевказаного випливає, що мінімальна швидкість таких DOS-атак визначається розрахунковими параметрами значення шкали часу повторного передавання. Швидкість може бути збільшена, однак у такому разі підвищується вірогідність виявлення таких атак влаштованими механізмами маршрутизаторів.

Зважаючи на зазначене вище, важливу роль як у здійсненні повільної DOS-атаки, так і в її виявленні відіграє час затримки повторного передавання. Надалі розрахункові проміжки часу затримок повторного передавання називатимемо еталонними проміжками часу виявлення, оскільки вирішується завдання саме виявлення.

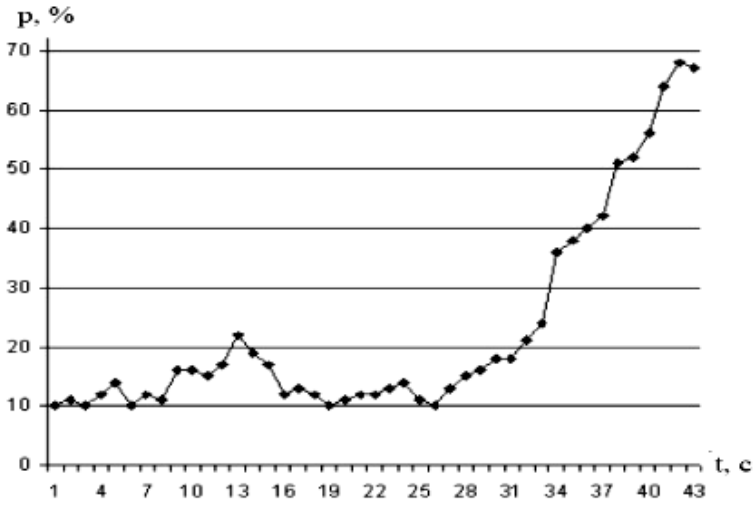

Рис. 2. Залежність ймовірності виявлення DDoS-атаки від часу її впливу

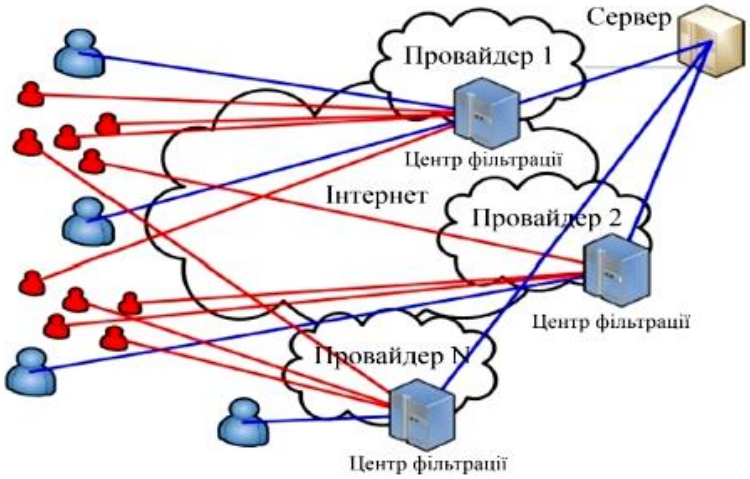

Рис. 3 Програмно-апаратний комплекс блокування DDoS-атаки

Для протидії повільним DDoS-атакам існує метод, відображений на рис. 4.

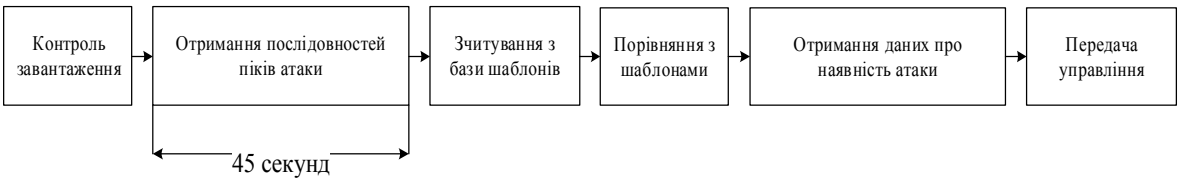

Рис. 4. Програмно-апаратний комплекс блокування DDoS-атаки

Із урахуванням специфіки повільної DOS-атаки та специфіки стандарту RFC 739, не беручи до уваги затримок у каналі зв'язку та маскувальних впливів на проведення атаки, розрахуємо еталонні проміжки часу затримок повторного передавання.

Розрахуємо інтервали часу між досягненням кожного з піків атаки:

$$D = T_{i+1} - T_i, \tag{1}$$

де D – інтервал часу; T – граничне значення закінчення інтервалу повторного передавання. Результати подано у табл. 2.

Значення, наведені в табл. 2, вказують на те, що у випадку виникнення першого піка навантаження для усіх потоків даних пакети не отримають підтвердження про доставку, виникне тайм-аут і вони будуть очікувати повторного передавання упродовж тривалості інтервалу D, до настання порогового значення закінчення інтервалу. Після досягнення повторного піка навантаження необхідно перейти до наступного інтервалу, якщо ж його не досягнуто, протокол TCP повертається до роботи за часовою шкалою RTT.

В результаті візьмемо отримані значення за еталонні, щоб розрахувати, як виявити факт впливу засобами повільної DOS-атаки на інформаційний сервер.

За відсутності маскувальних впливів з боку джерела атаки, в ідеальному випадку за відсутності будь-яких затримок у каналі зв'язку, повільна DOS-атака виглядатиме так: у вказані еталонні інтервали часу (рядок 2 табл. 2) сервер отримає піки навантаження, що приводить до синхронізації потоків та значних втрат пропускної здатності. Тобто зловмисник, створюючи перебої в каналі зв'язку з низькою інтенсивністю, яка зменшується за експоненціальною залежністю, досягає того, що сервер дає тайм-аут усім потокам.

В такому разі достатнім способом для виявлення таких впливів є співвідношення між досягнутими піками атаки та еталонними значеннями. Але з боку джерела атаки унеможливлюється проста відповідність еталонним значенням часів виникнення піків завантаження. Затримки в каналі зв'язку призведуть до незначних відхилень від еталонних значень. Маскувальні впливи з боку джерела атаки можуть призвести до істотних відхилень від еталонних значень, що необхідно враховувати під час виявлення повільних DOS-атак.

Таблиця 2

Значення між інтервалами виникнення піків завантаження

	Значення часу згідно з номером інтервалу					
Номер інтервалу	0	1	2	3	4	5
Граничні значення закінчення інтервалу	1	3	9	27	81	243
Тривалість інтервалу	2	6	18	54	162	

Маскувальні впливи можуть проявлятись у вигляді застосування різних законів змінення часу впливу на сервер для створення короткочасних перебоїв. Що частіші перебої на сервері, то ефективнішою стає атака, але тим самим перетворюється на розподілену DOS-атаку, а відповідно простіше її виявити та запобігти їй. Навантаження на сервер є випадковою величиною, а значення навантаження у заданий момент часу – значенням випадкової величини.

Необхідно отримати графік залежності завантаження від часу (рис. 5), що показує значення випадкової величини, яких набуває завантаження сервера. Дані одержано в результаті моделювання, виконаного методом запису інформації про завантаження сервера на реальному об'єкті прикладної програми Wireshark. Це програмне забезпечення дає змогу здійснювати мережевий аналіз трафіку для перехоплення та подальшого аналізу або тільки аналізу мережевого трафіку, призначеного для інших вузлів.

В такому випадку джерело атаки повинно зробити свої дії найнепередбачуванішими, не виходячи за межі еталонного значення порогового рівня закінчення інтервалу. Це можливо за умови використання рівномірного закону розподілу, тобто, маскуючи власні дії із формування та надсилання чергового піка навантаження щодо часу, необхідно застосовувати рівномірний закон розподілу.

У такому випадку передбачити час надходження чергового піка навантаження стає важче, а завдання виявлення повільної DOS-атаки набуває характеру виявлення попередньо відповідності еталонним значенням проміжків часу досягнення піків трафіку з урахуванням рівномірного закону

розподілу. Графік залежності значення завантаження від часу у ході повільної DOS-атаки в ідеалізованому вигляді зображено на рис. 5.

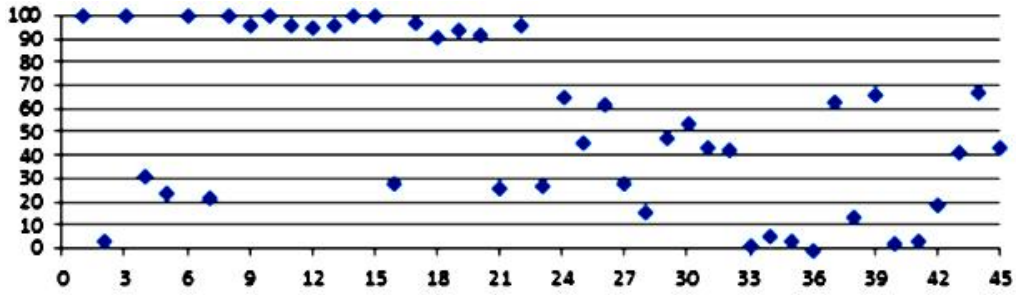

Рис. 5. Значення завантаження сервера з дискретністю в одну секунду

Як видно на рис. 5, отримання пікових навантажень у розраховані інтервали часу призводить до істотного зниження пропускної здатності. Такий випадок можливий тільки за умови ведення повільної DOS-атаки в середині локальної мережі. Наведений графік отримано в результаті здійснення експерименту на локальній мережі з використанням сервера та 24 локальних ЕОМ, одна з яких була генератором шкідливого трафіку, а інші генераторами випадкових запитів до сервера. Загальне навантаження на сервер у початковий момент часу атаки становило близько 40 %.

Графік проведення повільної DOS-атаки, коли шкідливий DOS-трафік передано засобами інтернету, подано на рис. 6.

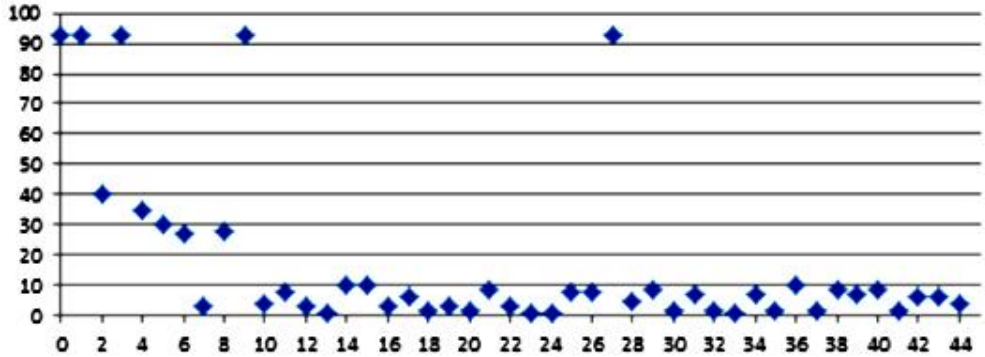

Рис. 6. Ідеалізований вигляд повільної DOS-атаки

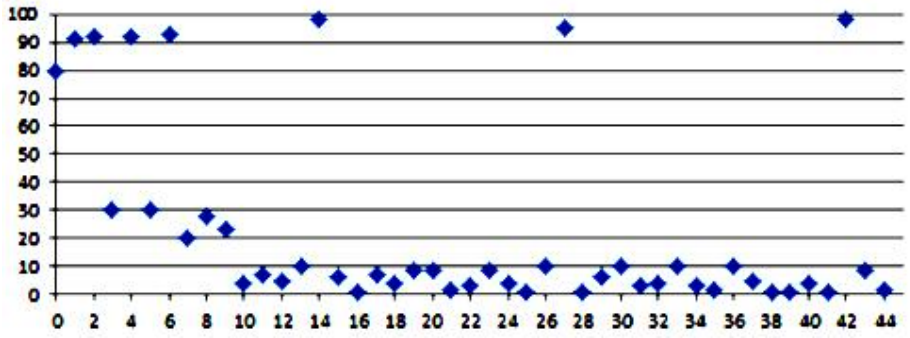

Рис. 7. Залежність значення навантаження від інтервалу часу за нелокального впливу

Порівнюючи отримані графіки значень випадкової величини, бачимо, що відбувається зниження пропускної здатності каналу зв'язку. В разі нелокального впливу піки навантаження виникають значно частіше. Із цього ж випливає, що для виявлення шкідливого впливу недостатньо

простого порівнювання з еталонними величинами. Еталонні величини необхідно змінювати залежно від виникнення піків трафіка. Застосувавши математичне сподівання рівномірного закону розподілу, отримуємо таке співвідношення для еталонного часу виникнення піків навантаження:

$$T_{\text{ві}} = {T_{i+1} + T_i}/{2}.$$

Також обов'язково необхідно враховувати час виникнення чергового піка навантаження та його порядковий номер. Якщо задовольняється умова: $\Delta \geq 0$, де $\Delta = T_{i+1} - T_{ni}$, T_{ni} – час отримання піка трафіку; T_{i+1} – розрахункове еталонне значення на наступному етапі, то необхідно знайти відхилення від T_{ei}, $\Delta_{oi} = T_{ei} - T_{ni}$, і це відхилення може набувати від'ємного значення. В разі, якщо $\Delta \neq 0$, необхідно від отриманого пікового значення відкласти тривалість інтервалу залежно від номера відліку (табл. 2, рядок 2) та продовжити ітерації для розрахунку T_i і T_{ei}. Тобто після отримання чергового піка навантаження еталонні значення необхідно перераховувати.

Після виникнення чотирьох піків трафіку необхідно підсумувати Δ_{oi} Це дасть можливість прийняти рішення про наявність чи відсутність повільної DOS-атаки.

Дослідно, в результаті експериментів, отримано відхилення для $\sum \Delta_{oi}$, яке не повинно перевищувати 5 с; якщо одержано негативний час – це означає, що атака відбувається інтенсивніше від очікуваного рівня і її можна зарахувати до класу розподілених. У разі отримання від'ємного значення Δ необхідно приймати виявлений пік навантаження за початок відліку і продовжувати перевірку.

Запропонований метод дає змогу виявляти факт шкідливого інформаційного впливу на механізм рестарту протоколу TCP з ймовірністю 93 %, що підтверджують проведені експерименти. Загалом здійснено 200 реалізацій повільної DOS-атаки на сервер: 100 реалізацій за рахунок локальної обчислювальної мережі та 100 реалізацій із зовнішніми впливами на сервер з підключеними локальними і нелокальними абонентами. У разі локальної реалізації запропонований механізм виявлення спрацьовував правильно в 95 випадках, однак відзначено три хибні спрацювання за відсутності такої атаки і два невиявлення за її наявності. У разі здійснення зовнішніх впливів в 93 випадках запропонований метод правильно виявляв повільну DOS-атаку, було чотири помилкові спрацьовування за наявності хаотичних посилок пікових навантажень і три неспрацьовування за наявності правильної послідовності пікових навантажень.

Запропонований метод дає змогу виявити DOS-атаку та відповідно увімкнути механізми протидії такому інформаційному впливу і запустити механізми пошуку джерела атаки [9].

Розглянемо ще додатково атаку SYN-flood, яка звичайно реалізовується проти серверів, та можливість її реалізації. Зловмисник відправляє велику кількість SYN-пакетів на цільовий хост по порту сервісу, який він хоче призупинити, від імені випадкових IP-адрес. Оскільки SYN-пакети використовуються у потрійному з'єднанні під час встановлення TCP-з'єднання, цільовий хост відповідає на них пакетами SYN-ACK, резервує місце в буфері під кожне з'єднання та чекає пакета ACK у відповідь, який повинний закінчити з'єднання, за деякий проміжок часу.

Пакет-підтвердження SYN-ACK передається на помилкову адресу джерела SYN-пакета, в довільну точку мережі чи взагалі не знайде адресата, чи буде просто проігнорований. У результаті, за постійного потоку SYN-запитів, цільовий хост постійно триматиме свій буфер заповненим непотрібним очікуванням завершення напіввідкритих помилкових з'єднань і не зможе обробити SYN-запити від справжніх легальних користувачів.

Змоделюємо таку атаку за допомогою мережі Петрі– Маркова (рис. 8) . Визначення елементів цієї мережі наведено нижче: S_j – позиції; t_j – переходи: s_1 – готовий; s_2 – готовий прийняти пакети SYN з адресою, яка не існує, у чергу невідкритих з'єднань; t_1 – запуск та налаштування

додатка для SYN-flood; s_3 – програма запущена та налаштована; t_2 – відправка пакетів SYN та поміщення їх у чергу А; s_4 – запити поставлено в чергу очікуваних з'єднань А; t_3 – переповнення черги А; s_5 – А не має здатності опрацювати інші запити; t_4 – перехоплення та аналіз трафіку А.

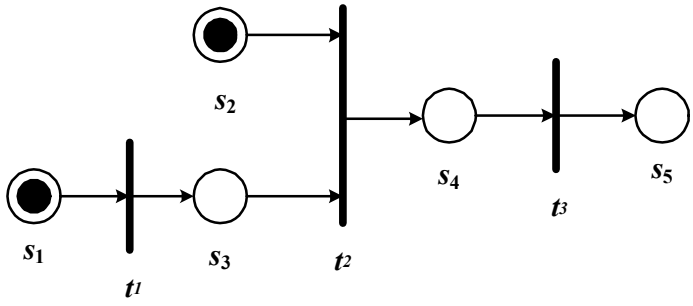

Рис. 8. Мережа Петрі–Маркова етапів реалізації атаки SYN-flood

Елементи матриці, які визначають логічні функції спрацювання мережі, можна записати (без урахування спрямованості дуг графа) так, як наведено у табл. 3.

Таблиця 3

Визначення логічних функцій

		t_1	t_2	t_3
$vs_1t_3 =$	S_1	1	0	0
	S_2	0	1	0
	S_3	1	1	0
	S_4	0	$s_1 t_2 \cap s_3 t_2$	1
	S_5	0	0	1

Для цієї мережі Петрі – Маркова запишемо систему інтегральних диференціальних рівнянь:

$$\Phi_{S_i t_1}(t) = \pi_{11} \int_0^t f_{S_1 t_1}(\tau) d\tau$$

$$\Phi_{S_2 t_2}(t) = \pi_{22} \int_0^t f_{S_2 t_2}(\tau) d\tau$$

$$\Phi_1(t) = \int_0^t f_{S_2 t_2}(\tau)\Phi_{S_2 t_2}(\tau) + f_{S_2 t_2}(\tau)\Phi_{S_2 t_2}(\tau) d\tau$$

$$\Phi_{S_4 t_3}(t) = \pi_{43} \int_0^t f_{S_4 t_3}(\tau)\Phi_1\left(t-\tau\right) d\tau$$

Вважаємо, що густина розподілу вірогідності є експоненціальною залежністю і має такий вигляд, якщо $i = 1,...,6;\ j = 1,...,4$:

$$f_{S_i i_j}(t) = \lambda_{ij} e^{-\lambda_{ij} t}.$$

Для оцінки середнього часу реалізації цієї атаки необхідно врахувати такі показники: s – розмір черги для напіввідкритих TCP-з'єднань; T – час перебування з'єднання в черзі; R – інтенсивність надсилання SYN-пакетів зловмисником.

Необхідно обчислити кількість повторень відправлення зловмисником пакетів, яке призведе до переповнювання черги атакованого хоста. У разі, коли $TR >> s$, це $n \le s$.

Застосовуючи пуассонівське наближення, одержуємо середній час переміщення по мережі Петрі-Маркова з початкової позиції до кінцевого переходу і вірогідність цього переміщення:

$$\tau_{32} = nT$$

$$\tau_1 = \tau_{11} + \tau_{32}$$

$$\tau_2 = \frac{\tau_1^2 + \tau_1\tau_{22} + \tau_{22}^2}{\tau_1 + \tau_{22}}$$

$$\tau = \frac{\left(nT + \tau_{11}\right)^2 + \left(nT + \tau_{11}\right)\tau_{22} + \tau_{22}^2}{\left(nT + \tau_{11}\right) + \tau_{22}} + \tau_{43},$$

де початкові параметри атаки набувають таких значень: τ_{11} – середній час налаштування програми; s = 10 – розмір черги з'єднань для Windows 10; T_c = 75 с – середній час очікування встановлення з'єднання; R = 100 – кількість SYN-пакетів, які надходять у чергу за секунду.

Отже, зловмиснику необхідно повторити передавання SYN-пакета в середньому n = 10 разів. Середній час підготовки, відправлення і поміщення пакета в чергу з урахуванням інтервалу між пакетами – T_n = 0,015 с.

Без застосування заходів захисту від цієї атаки час переходу хоста, що атакують, у недоступний стан наближається до нуля: $\tau_{32} \to 0$ (рис. 9). Тоді середній час переходу по всій мережі дорівнює:

$$\tau = nT + \tau_{11} = 10 * 0{,}015 + 11 = 11{,}15\, c.$$

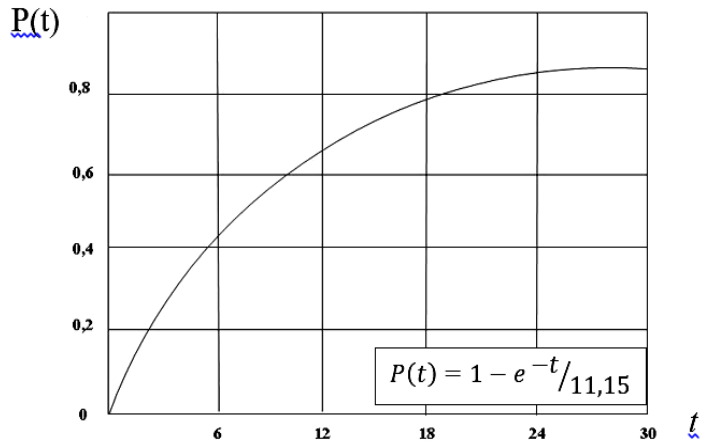

Рис. 9. Залежність вірогідності реалізації атаки SYN-flood від часу

Особливу увагу потрібно звернути на те, що ця залежність враховує етап запуску і налаштування програми, який займає значно більший середній час, ніж всі решта етапів. Розглянемо характеристики вірогідності реалізації атаки із застосуванням заходів протидії.

Використовування міжмережевого екрана (для міжсегментної атаки). Сьогодні робота із протидії таким кібератакам покладена на міжмережеві екрани. Коли ззовні приходить SYN-пакет, міжмережевий екран не пропускає його у внутрішню мережу, а сам відповідає на нього від імені сервера призначення. Якщо з'єднання із зовнішнім клієнтом все ж таки встановлюється, то він створює з'єднання з сервером від імені клієнта та надалі виступає як невидимий посередник, про якого ні внутрішній сервер, ні зовнішній клієнт не здогадуються.

Якщо ж відповідь від клієнта на SYN-ACK-пакет у визначений проміжок часу не отримано, оригінальний SYN-пакет не буде переданий всередину мережі. Для такої моделі застосування

міжмережевого екрана впливає на зменшення вірогідності π_{22} переходу d_{22}, значення якої залежить від типу й особливостей функціонування мережі та міжмережевого екрана.

Для протидії атакам такого типу запропоновано використовувати механізм SYN-cookies. У разі використання SYN-cookies як міри протидії цій кібератаці за такої інтенсивності запитів хост залишається доступним для легітимних з'єднань навіть у випадку переповнювання черги очікування хосту, що захищається, він стає практично невразливим до кібератаки SYN-flood. У такій моделі це виражається як наближення вірогідності π_{32} переходу d_{11} до нуля.

Зменшення часу очікування відповіді. У разі зменшення часу очікування відповіді до 10 с n = 10,1, що істотно не змінює вірогідності реалізації кібератаки за заданих розміру черги та інтенсивності.

Збільшення черги запитів. У разі збільшення черги запитів для успішної реалізації кібератаки інтенсивність запитів повинна мати таке значення, за якого черга заповниться до закінчення часу очікування з'єднання, оскільки потім пакети видалятимуться з черги з такою ж інтенсивністю, тобто $R > slTc$, у цьому випадку R > 866, якщо T_c = 75, що більше відповідає розподіленій кібератаці з участю декількох машин зловмисника (DDoS). Для розміру черги s = 65000 й інтенсивності кібератак R = 1000 середній час реалізації кібератаки $\tau = 88$ с, а вид залежності показано на рис. 10.

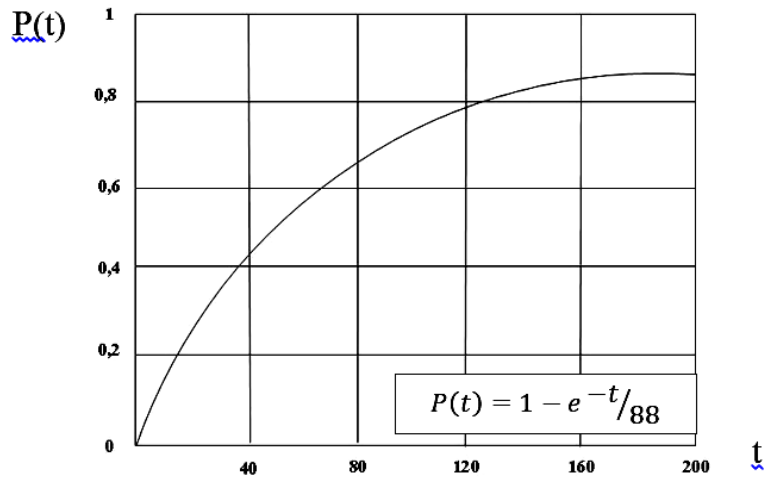

Рис. 10. Залежність часу реалізації кібератаки SYN-flood, у разі збільшеної черги очікування з'єднань й інтенсивності запитів 1000 за секунду

У випадку динамічного збільшення черги запитів час і можливості реалізації кібератаки визначаються ресурсами системи. Відомо, що для підтримки одного напіввідкритого з'єднання в черзі ОС іноді потрібна пам'ять до 30 кбайт, тому за наявності на хості серверної ОС є можливість підтримки очікування достатньо великої кількості з'єднань.

Висновки

Аналізуючи викладені відомості про здійснення кібернетичних атак, можна дійти висновку, що розглянуті вище можливості захисту даних не будуть повною мірою ефективними, якщо їх не використовувати у єдиному комплексі.

Кібернетичні атаки на інформаційну систему реалізуються переважно за рахунок таких атак: аналіз мережевого трафіку; сканування мережі; загроза виявлення пароля; підміна довіреного об'єкта мережі й передавання по каналах зв'язку повідомлень від його імені з присвоєнням його прав доступу; нав'язування помилкового маршруту мережі; несанкціоноване введення об'єкта мережі; відмова в обслуговуванні; видалений запуск додатків,

Засоби виявлення кібернетичних атак забезпечують одержання даних із мережі про зловмисну активність із перетворенням на зрозумілу інформацію, яку можна використати для усунення підтверджених порушень безпеки і забезпечення відповідності нормативним документам. Набір зручних у використанні апаратних засобів віддзеркалення загроз дає змогу адміністраторам централізовано знаходити, визначати пріоритетність і відображати загрози за допомогою вже упроваджених в інфраструктуру мережевих пристроїв і пристроїв захисту.

Отже, з урахуванням майбутнього розвитку інформатизації, проникнення інформаційних технологій у найважливіші сфери життя суспільства необхідно передбачити перехід від принципу гарантування безпеки інформації до принципу інформаційної безпеки.

Список використаних джерел

[1] *Павлов І. М., Толюпа С. В., Ніщенко В. І. Аналіз таксономії систем виявлення атак у контексті сучасного рівня розвитку інформаційних систем. Сучасний захист інформації. 2014. № 4. С. 44–52.*

[2] *Толюпа С. В., Штаненко С. С., Берестовенко Г. Класифікаційні ознаки систем виявлення атак та напрямки їх побудови. Збірник наукових праць Військового інституту телекомунікацій та інформатизації імені Героїв Крут. 2018. Вип. № 3. С. 56–66.*

[3] *Белоус А. И., Солодуха В. А. Кибероружие и кибербезопасность. О сложных вещах простыми словами. Москва: Вологда: Инфра-Инженерия, 2020. 692 с.*

[4] *Белоус А. И., Солодуха В. А. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения. Москва: Техносфера, 2021. 482 с.*

[5] *Даник Ю. Г., Воробієнко П. П., Чернега В. М. Основи кібербезпеки та кібероборони: підручник. Одеса: ОНАЗ ім. О. С. Попова, 2019. 320 с.*

[6] *Гулак Г. М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. Київ: Видавництво НА СБ України, 2021. 256 с.*

[7] *Моделирование систем безопасности: монография / [В. И. Новосельцев, А. В. Душкин, В. И. Сумин, С. С. Кочедыков, Д. Е. Орлова]. ФКОУ ВО Воронежский институт ФСИН России. Воронеж, 2019. 197 с.*

[8] *Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам. Под ред. проф. РАН, д-ра техн. наук Д. П. Зегжды. Москва: Горячая линия-Телеком, 2020. 560 с.*

[9] *Системи виявлення вторгнень та функціональна стійкість розподілених інформаційних систем до кібернетичних загроз: монографія / Н. В. Лукова-Чуйко, С. В. Толюпа, В. С. Наконечний, М. М. Браіловський. Київ: Формат, 2021. 407 с.*

MEANS OF DETECTING CYBERNETIC ATTACKS ON INFORMATION SYSTEMS

S. Tolyupa, N. Lukova-Chuiko, J. Shestak

Taras Shevchenko National University of Kyiv, 60, Volodymyrska Str., Kyiv, 01033, Ukraine

Systems for detecting network intrusions and detecting signs of cyber attacks on information systems have long been used as one of the necessary lines of defense of information systems. Today, intrusion and attack detection systems are usually software or hardware-software solutions that automate the process of monitoring events occurring in the information system or network, as well as independently analyze these events in search of signs of security problems. As the number of different types and methods of organizing unauthorized intrusions into foreign networks has increased significantly in recent years, attack detection systems (IAS) have become a necessary component of the security infrastructure of most organizations. Despite the fact that there are a large number of methods for detecting anomalies, their weak stability, lack of verification, a large number of false positives, narrow specialization and research nature, do not allow their widespread use. One of the most common types of acacia is a DDoS-attack, a denial-of-service attack that interrupts or suspends host server service to make the online service inaccessible to users. The article offers an analysis of this attack and the possibility of its implementation.

Key words: *attack; information system; server; intrusion detection system; network.*