УДК 004.056.53+519.876.5 DOI: 10.31673/2412-4338.2024.012644

Савченко Віталій Анатолійович
Державний університет інформаційно-комунікаційних технологій, Київ
ORCID 0000-0002-3014-131X

Степанченко Богдан Сергійович
Державний університет інформаційно-комунікаційних технологій, Київ
ORCID 0009-0003-9776-4727

РОЗРОБКА КОНЦЕПЦІЇ ПРОГНОЗУВАННЯ ЧАСУ ПОЧАТКУ DDOS АТАКИ НА ОСНОВІ ДОСЛІДЖЕННЯ ДИНАМІКИ ПОВЕДІНКИ ЕВОЛЮЦІЙНИХ РІВНЯНЬ

Анотація: *Сучасний інформаційний простір сформовано мережами складних технічних системи взаємопов'язаних девайсів та пристроїв, які обмінюються інформацією та ресурсами. Вони є фундаментальним базисом для багатьох сучасних технологій, включаючи* Internet*, мережі передачі даних, соціальні мережі і т.і. Беззаперечною передумовою забезпечення стійкості сучасних інформаційних систем від несанкціонованого доступу в цілому та DDoS атак зокрема є реалізація концепції проактивного захисту. Це означає, що заходи кібербезпеки повинні бути впроваджені до того, як відбудеться прецедент несанкціонованою доступу до даних чи атака. В роботі проаналізовано нинішній стан та підходи до виявлення кіберзагроз для інформаційних систем корпоративних мереж, наведено класифікацію кіберзагроз та дано характеристику анатомії DDoS атак. В роботі досліджуються анатомія DDoS-атак та методи протидії DDoS-атакам, що дозволяють ефективно захищати інформаційну мережу від атак зловмисників. Розроблено математичний апарат для ідентифікації кіберзагроз та визначення стратегій мінімізації ризиків несанкціонованого доступу зловмисників до інформаційних ресурсів мережі, що ґрунтується на методах якісної теорії систем диференціальних рівнянь з імпульсною дією. Використовуючи методи фазової площини, вивчаються особливості поведінки складних систем, математичні моделі яких представлено системами диференціальних рівнянь з імпульсною дією. Отримано конструктивні умови стійкості та асимптотичної стійкості SIR-моделі, яка є математичною моделлю вразливості мережі в наслідок агресивних дій зловмисників. Встановлено умови мінімізації уразливостей елементів мережі через реалізацію різних стратегій зменшення кількості інфікованих пристроїв: стратегії «постійної вакцинації», стратегії «імпульсної вакцинації» та періодичного випадку реалізації концепції оновлення та актуалізації програмного забезпечення для протидії DDoS-атакам. Встановлено, що загрозостійкість мережі обернено пропорційно визначається відношенням швидкості вразливості пристроїв у мережі до вибувших і відновлених пристроїв та отримано оцінку періоду оновлення програмного забезпечення для захисту від кіберзагроз.*

Ключові слова: *кібератака, DDoS-атака, ботнет, SIR-модель, стійкість, стратегія протидії кібератакам.*

Savchenko Vitalii
State University of Information and Communication Technologies, Kyiv
ORCID 0000-0002-3014-131X

Stepanchenko Bohdan
State University of Information and Communication Technologies, Kyiv
ORCID 0009-0003-9776-4727

© Савченко В.А., Степанченко Б.С. 2024

DEVELOPMENT OF THE CONCEPT OF PREDICTING THE START TIME OF A DDOS ATTACK BASED ON THE STUDY OF THE DYNAMICS OF THE BEHAVIOR OF EVOLUTIONARY EQUATIONS

Abstract: *The modern information space is formed by networks of complex technical systems of interconnected devices and devices that exchange information and resources. They are the fundamental basis for many modern technologies, including the Internet, data networks, social networks, etc. An undeniable prerequisite for ensuring the stability of modern information systems against unauthorized access in general and DDoS attacks in particular is the implementation of the concept of proactive protection. This means that cybersecurity measures must be implemented before a data breach or attack occurs. The paper analyzes the current state and approaches to detecting cyber threats for information systems of corporate networks, provides a classification of cyber threats and describes the anatomy of DDoS attacks. The work examines the anatomy of DDoS-attacks and methods of countering DDoS-attacks, which allow effective protection of the information network, as well as against attacks by intruders. A mathematical apparatus for identifying cyberthreats and determining strategies for minimizing the risks of unauthorized access by attackers to network information resources has been developed, which is based on the methods of the qualitative theory of systems of differential equations with impulse action. Using the methods of the phase plane, the peculiarities of the behavior of complex systems are studied, the mathematical models of which are represented by systems of differential equations with impulse. Constructive conditions of stability and asymptotic stability of the SIR-model, which is a mathematical model of network vulnerability due to aggressive actions of attackers, have been obtained. The conditions for minimizing the vulnerabilities of network elements through the implementation of various strategies for reducing the number of infected devices have been established: the strategy of "permanent vaccination", the strategy of "pulse vaccination" and the periodic case of implementing the concept of updating and updating software to counter DDoS attacks. It was established that the threat resistance of the network is inversely proportionally determined by the ratio of the vulnerability rate of devices in the network to the lost and restored devices, and an estimate of the software update period for protection against cyber threats was obtained.*

Keywords: *cyber-attack, DDoS attack, botnet, SIR model, stability, cyber-attack strategy.*

1. Вступ.

Якість функціонування сучасних інформаційних мереж в значній мірі визначається методами забезпечення стійкості мереж до несанкціонованого впливу зловмисників, захищеності інформації як від витоку, так і від втрат в наслідок кібератак чи інших неправомірних дій зловмисників [1].

Сучасні інформаційні мережі – це складні системи взаємопов’язаних девайсів та пристроїв, які обмінюються інформацією та ресурсами. Вони складають фундаментальну основу для багатьох сучасних технологій, включаючи Internet, мережі передачі даних, електронну пошту, відеоконференції, соціальні мережі тощо [2].

Стрімкий розвиток технологій, водночас призвів до відповідного росту загроз для мереж передачі даних і серверів зберігання даних. Чим складнішою стають мережі тим більш вишуканими та небезпечними стають як методи несанкціонованого доступу так і методи знищення даних.

Вищесказане обумовлює *актуальність* і необхідність проведення досліджень в напрямку розробки методів виявлення кіберзагроз та ефективних стратегій протидії останнім.

2. Аналіз літературних даних і постановка проблеми.

Природньо, що стрімкий розвиток інформаційно-комунікаційних технологій супроводжується відповідним ризиком впливу зовнішніх та внутрішніх дестабілізуючих факторів різної природи. Відтак проблематика розробки методів, які забезпечують функціональну стійкість складних технічних систем в цілому та інформаційних систем зокрема повсякчас у фокусі уваги багатьох дослідників. Широке коло питань за цим напрямком розкрито у [3].

У роботі [4] розроблено методологію забезпечення функціональної стійкості інформаційної системи об’єктів критичної інфраструктури шляхом представивлення

функціонування системи у вигляді формалізованого процесу, в якому накопичення перевірок, аналіз перевірочних посилань, діагностика несправності модулів та відновлення функціонування системи є основними видами процедур.

Ключовими етапами забезпечення функціональної стійкості мереж є постійна діагностика з метою виявлення вузлів, які відмовили при контролі та діагностика вражених вузлів для забезпечення необхідних параметрів автономності роботи мереж. У [5] представлено методику самодіагностування мереж, коли при заданій інтенсивності процедур контролю на основі функціональної залежності ймовірності пропуску відмов від різних значеннях ймовірності помилки контролю другого роду. Відповідні результати для сенсорних мереж детально досліджено у [6,7].

У статті [8] розроблена модель структури інтегральної інформаційної мережі на основі нестаціонарної ієрархічної та стаціонарної гіпермережі, з врахуванням руйнівних впливів різного характеру. У роботі розроблено методичний апарат для забезпечення повноцінного функціонування мереж в умовах ризиків виходу з ладу вузлів мережі аж до руйнування каналів.

Методи підвищення завадостійкості системи виявлення, розпізнавання і локалізації цифрових сигналів в інформаційних системах досліджено у [9]. Робота [10] розкриває підхід до оцінки економічних витрат на систему захисту інформації в мережах. Це вкрай важлива проблематика, з огляду на величезну значущість захищеності інформаційного простору протягом останнього часу.

У роботі [11] розглядаються елементи інформаційного простору, їх параметри і зв'язки, які утворюють єдиний інформаційний простір виробничого підприємства з критичною інфраструктурою. Одним з ключових аспектів побудови єдиного інформаційного простору є інтеграція автоматизованих систем усіх підрозділів в єдиний інформаційний простір. Реалізація такої концепціє є запорукою підвищення ефективності технологічних процесів, скорочення термінів освоєння нових продуктів, підвищенню загальних обсягів обміну даними. Більше того, це відбувається з одночасною глибокою інтеграцією проектних груп різних підрозділів в єдину високопрофесійну команду, яка націлена на досягнення єдиної цілі.

Розвиток моделей кібератак у площині інформаційної безпеки підприємства досліджено у статті [11]. Робота [12] розкриває підхід до забезпечення функціональної стійкості інформаційних мереж на основі розробки методу протидії DDoS-атакам.

Результати цих робіт грають суттєву роль для забезпечення стійкого функціонування інформаційних мереж в умовах наявності ризиків різної природи. Однак дані роботи спираються переважно на методи теорії ймовірностей для математичного опису функціонування мереж. При цьому зовсім не вивченою є проблема встановлення залежностей росту кіберризиків від часу та еволюції функціонування мережі за таких обставин. Математичний формалізм на основі еволюційної SIR-моделі [18] для опису DDoS-атак був запропонований в роботі [19]. Серед багатьох узагальнень цієї епідеміологічної моделі в контексті протидії DDoS-атакам особливий інтерес становлять ті, що враховують вакцінацію [20-24]. Адекватним математичним апаратом в цьому випадку, як показано в роботі [25], може слугувати теорія диференціальних рівнянь з імпульсною дією.

3. Мета і задачі дослідження.

Метою дослідження є вдосконалення і розробка способу прогнозування моментів початку DDoS атак на основі дослідження динаміки поведінки еволюційних рівнянь.

Для досягнення поставленої мети вирішено такі завдання:

– проаналізовані нинішній стан та підходи до виявлення кіберзагроз для інформаційних систем корпоративних мереж;

– наведено класифікацію кіберзагроз та дано характеристику анатомії DDoS атак;

– розроблено математичний апарат для ідентифікації кіберзагроз та визначення стратегій мінімізації ризиків несанкціонованого доступу зловмисників до інформаційних

ресурсів мережі, що ґрунтується на методах якісної теорії систем диференціальних рівнянь з імпульсною дією.

4. Характеристика сучасних кіберзагроз.

Стрімкий розвиток інформаційних технологій та всеохоплююча автоматизація процесів в самих різноманітних індустріях водночас призводить до зростання загроз для інформаційних ресурсів від несанкціонованого впливу зловмисниками. Загрози постійно еволюціонують, і постійне збільшення підключених до Internet пристроїв робить інформаційні системи більш вразливими. Забезпечення адекватного захисту мережі, систем та особистих даних є надзвичайно важливим для запобігання як хакерським атакам так іншим типам несанкціонованого доступу до інформаційних ресурсів.

4.1 Загрози інформаційній безпеці в корпоративному секторі.

Протягом багатьох років спостерігається щорічне зростання хакерських атак на 25-35%. При цьому варто зазначити, що в корпоративному секторі у 2023 році спостерігається суттєве зростання внутрішніх інцидентів.

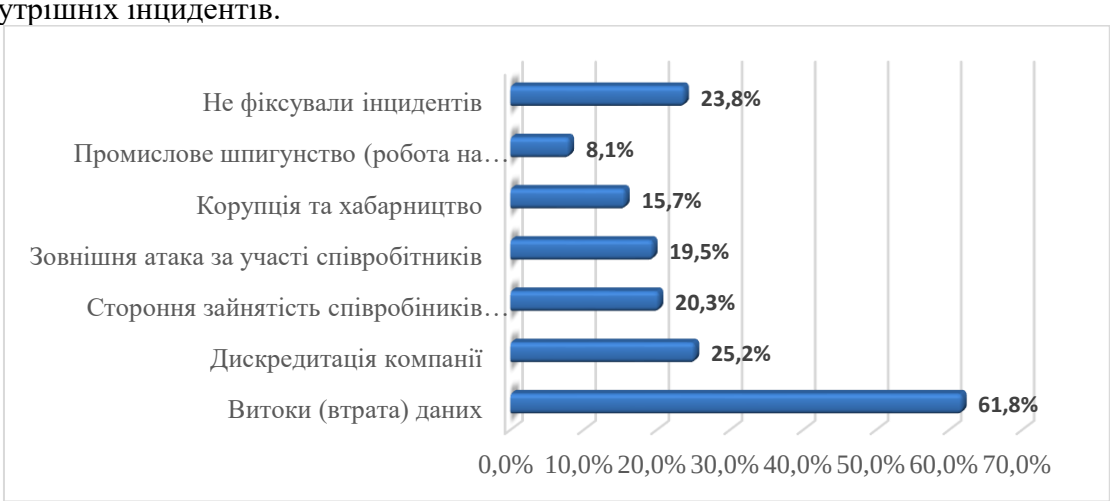

Рис. 1. Структура внутрішніх інцидентів в корпоративному секторі у 2023 році

Зокрема, понад 59% компаній у корпоративному секторі 2023 році зіткнулися зі спробами витоку інформації. Найчастіше «інсайдери» цікавились інформацію про споживачів та угоди (45%), технічну документацію та персональні дані (36%), фінансову інформацію (30%). Зауважимо що тут і наступних розкриттях даних нормальний розподіл не завжди можливий, оскільки респонденти можуть одночасно входити в кілька груп.

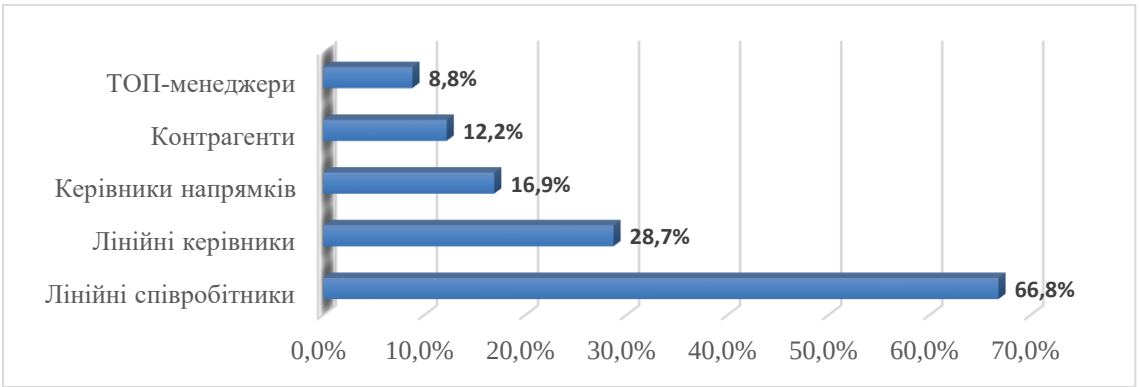

Рис. 2. Ролі винуватців внутрішніх інцидентів в структурах компаній корпоративного сектору у 2023 році

Крім того, інші інциденти безпеки також насамперед включають дискредитацію компанії (зокрема, поширення негативної чи то завідома неправдивої інформації в соціальних мережах тощо) співробітниками (25,2%), участі в роботі сторонніх компаній (20,3%), зовнішні атаки із задіянням співробітників (19,5%), корупція та хабарництво (15,7%). Варто зазначити, що з промисловим шпигунством стикались 8% компаній. Власне цікавою є структура інцидентів, в яких безпосередньо задіяні співробітники компаній (рис 1.).

Зауважимо також, що де-факто на сьогодні майже кожна четверта компанія взагалі не моніторить даних ризиків. І в наш час це радше поле для зловживань співробітників і, водночас, полігон для тренувань зловмисників. Тим більш небезпечною є ситуацію з огляду на ролі винуватців у структурах компаній (рис.2.)

Водночас актуальною є проблема зростання дефіциту кадрів у сфері інформаційної безпеки. Зокрема в корпоративному секторі констатують, що не вистачає кваліфікованих фахівців з інформаційної безпеки (ІБ), про це заявили 68% компаній. 10% респондентів наголосили, що дефіцит ІБ-кадрів посилився. Лише 3% опитаних зауважили, що кадровий голод ослаб, а 4% відповіли, що фахівців на ринку достатньо (рис. 3.).

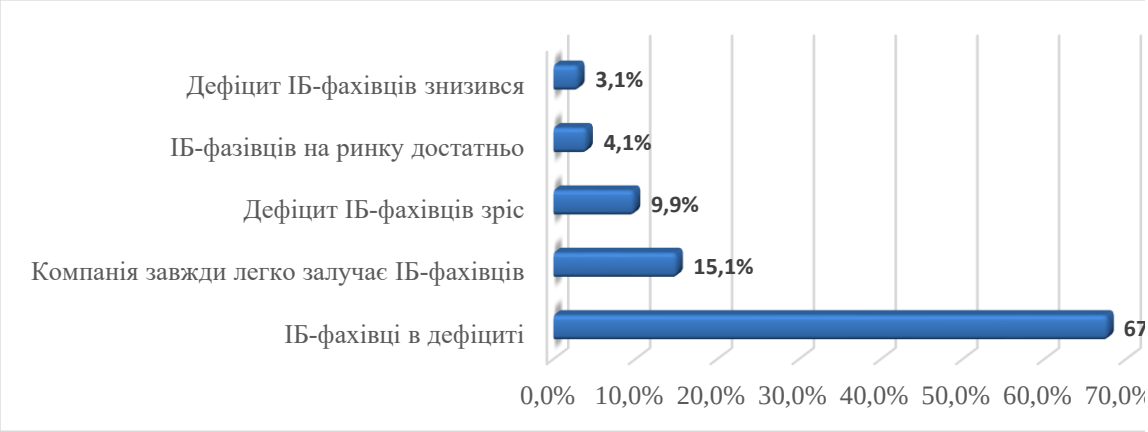

Рис. 3. Динаміка зміни підбору ІБ-фахівців компаніями корпоративного сектору у 2023 році у порівнянні з попередніми періодами

Найслабші місця у зовнішньому периметрі компаній корпоративного сектору є підтримка протоколу TLS версії 1.0/1.1, використання нестійких алгоритмів шифрування в SSL. Ці вразливості призводять до того, що канали підключення до віддаленого ресурсу, будуть незахищений, або сучасні браузери сповіщатимуть користувачів, що ресурс небезпечний, що може призвести до відтоку клієнтів. Також ІБ-фахівці незадоволені сертифікати SSL, відсутність застосування заголовку HSTS (RFC 6797), використання в SSL/TLS модуля Діффі-Хеллмана ≤ 1024 біт (Logjam), підпис SSL-сертифіката нестійким алгоритмом хешування тощо.

4.2. Класифікація кіберзагроз.

Нині чи не ключову загрозу інформаційній безпеці становлять загрози хакерських атак. Останнім часом склалась певна класифікація кіберзагроз за характером їх дії (рис. 4.).

Malware (зловмисне програмне забезпечення): включає в себе різноманітні види вірусів, троянів, шпигунського програмного забезпечення та програм-вимагачів. Це програми, які використовуються для незаконного доступу до комп'ютерів або систем, крадуть конфіденційні дані або блокують доступ до файлів, вимагаючи викуп тощо.

Phishing and social engineering. Хакери використовують фішингові атаки, намагаючись обманом отримати конфіденційну інформацію (паролі, номери кредитних карток тощо). Вони також можуть використовувати соціальну інженерію для маніпулювання людьми з метою отримання доступу до інформаційних систем або інформації.

DDoS attacks (атаки на відмову в обслуговуванні) — атаки, які мають на меті

переповнити сервери або мережу великою кількістю запитів, що призводить до перебоїв у роботі системи та відмови в обслуговуванні для користувачів.

Attacks on IoT devices. Зі зростанням популярності розумних пристроїв з'явилася загроза хакерських атак на ці підключені до Internet пристрої. Хакери використовують низьку захищеність цих пристроїв для отримання доступу до мережі або для здійснення інших видів атак.

Cyberespionage and cyberwar. Державні суб'єкти або хакерські групи можуть здійснювати кібершпигунство, викрадаючи конфіденційні дані або здійснюючи кібернапади на інфраструктурні об’єкти та об’єкти критичної інфраструктури для досягнення своїх геополітичних цілей.

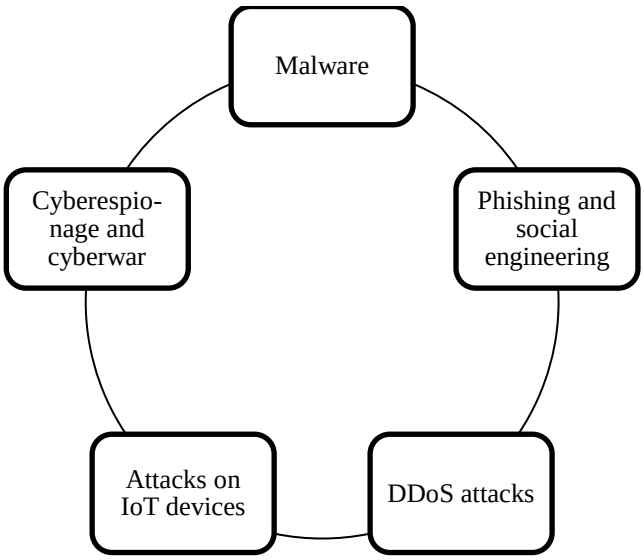

Рис. 4. Основні типи загроз кібезпеці

Зупинимось детальніше на проблематиці атак на відмову у масовому обслуговуванні. Власне DDoS-атаки (анг. *Distributed Denial-of-Service*) — це тип атак на відмову в обслуговуванні, при яких атакуючий використовує велику кількість комп’ютерів, щоб завантажити цільову систему, що робить її недоступною для законних користувачів. DDoS-атаки можуть бути використані для виведення з ладу веб-сайтів, серверів, мереж або навіть цілих Інтернет-провайдерів.

Перші DDoS атаки були відносно простими. Вони здійснювалися за допомогою одного або декількох комп'ютерів, які відправляли велику кількість запитів до цільової системи. Ці атаки були ефективними проти невеликих систем, але їх було легко блокувати більшими системами.

У 2000-х роках DDoS атаки стали більш складними. З’явилися ботнети (анг. *botnet* – скорочення двох слів *ro**bot*** і ***net**work* – робот і мережа) — це комп’ютерна мережа, що складається з певної кількості хостів, із запущеними ботами — автономним програмним забезпеченням (ПЗ). Зазвичай бот у складі ботнета є програмою, що приховано встановлена на комп’ютері жертви і дозволяє зловмисникам виконувати певні дії, використовуючи ресурси інфікованого комп'ютера. Тобто ботнети є власне мережами зламаних комп’ютерів, які можна використовувати для здійснення DDoS атак. Відтак ботнети дозволили зловмисникам використовувати велику кількість комп’ютерів для здійснення атак, що зробило їх більш ефективними.

У 2010-х роках DDoS атаки продовжили еволюціонувати. З’явилися нові технології, які дозволили атакуючим здійснювати більш потужні атаки. Наприклад, атаки з використанням ампліфікації дозволили атакуючим використовувати законні системи для відправлення запитів до цільової системи, що призвело до більшої кількості запитів і, відтак, до більшої перевантаження. Ампліфікація (лат. *amplificatio* біологічний термін) — це процес утворення

додаткових копій ділянок хромосомної ДНК, зазвичай, містять певні гени чи сегменти структурного гетерохроматину. Саме за схожість специфіки поведінки з біологічною системою термін увійшов у глосарій кібербезпекових понять.

У 2020-ті роки DDoS атаки, очевидно, продовжують еволюціонувати. З'являються нові технології, які дозволять атакуючим здійснювати ще більш потужні атаки. Наприклад, атаки з використанням штучного інтелекту можуть дозволяти атакуючим адаптувати свої атаки до цільової системи, що ускладнює їхнє блокування.

4.3. Анатомія DDoS-атаки.

За означенням під час DDoS-атаки певна сукупність пристроїв атакують один сервер або цільову систему. Така атака має на меті перевантажити цільовий сервер або цільову мережу численними імітованими запитами, щоб дестабілізувати трафік цільового сервера чи мережі. Як наслідок, це перевантажує мережеві ресурси, і природній технологічний трафік функціонує з перебоями в обслуговуванні. DDoS-атаки здійснюються за допомогою мереж підключених до Internet девайсів, включаючи персональні ком'ютери та інші пристрої (наприклад, пристрої Інтернету речей (IP)), які є носіями шкідливого програмного забезпеченням і, відтак, мають вразливість до віддаленого управління. Такі пристрої класифікують як боти.

Використання ботнетів чи то груп скомпрометованих комп'ютерів як основного джерела атак, робить DDoS-атаки надзвичайно ефективними. Встановивши ботнет, зловмисник отримує можливість керувати атакою, надсилаючи віддалені команди кожному боту. Кожен із ботів у бот-мережі надсилає запити на IP-адреси цільового сервера-жертви, що може призвести до перевантаження мережі та суттєво утруднити природній технологічний трафік. Оскільки кожен бот є реальним мережевим пристроєм в Internet, то відрізнити атаки від природнього трафіку часто дуже складно. Таким способом, тут і надалі вважатиме, що архітектуру DDoS-атаки формують зловмисник, ботнет та цільова мережа або сервери [14].

Різні архітектури формуються в залежності від того, як здійснюється управління бот-мережами. В загальному випадку розрізняють централізовану або децентралізовану архітектуру DDoS-атак (рис. 5). Зокрема, на рис. 5 а) представлено централізовану архітектуру DDoS-атаки. Таку архітектуру формують зловмисник, цільовий сервер, ботнет і система управління та керування (C&C). В такій архітектурі девайси-боти в бот-мережі не взаємодіють один з одним. Натомість кожен бот підтримує зв'язок із системою C&C. Відтак контроль за ботнетом здійснюється за допомогою повідомлень, надісланих безпосередньо кожному девайсу.

Рис. 5. Архітектура DDoS-атак: а) централізова; б) децентралізована

У децентралізованій архітектурі (рис. 5 б)) ботнет є одноранговою (P2P) мережею. Зловмисником для початку DDoS-атаки надсилається запит на атаку певному боту. Після цього цей бот пересилає команди через P2P іншим роботам у мережі. Порівняльні характеристики двох архітектур DDoS-атак наведено у таблиці 1.

Таблиця 1

Порівняльні характеристики архітектур DDoS-атак

Архітектура	Переваги	Обмеження
Централізована архітектура	• безпечна; • гнучка;	• висока вартість управління ботнетом; • ненадійна.
Децентралізована архітектура	• надійна; • гнучка;	• слабка безпека; • високі витрати на керування ботнетом.

Оскільки в централізованій архітектурі ботнет не можна виявити, ідентифікуючи лише комунікації між ботами, безпека такої архітектури є дуже високою. Натомість, на відміну від децентралізованої архітектури, шаблони зв'язків P2P між ботами можуть бути розпізнаними, що суттєво полегшує ідентифікацію ботнету. Після виявлення ботнету можна визначити і джерело атаки і, більше того, силу таких атак, яка стає несуттєвою. Крім того, в централізованій архітектурі зловмисник може просто змінити стратегію атаки за допомогою контролю ботнету в режимі реального часу.

Відомо, що зловмисники можуть використовувати так звану «ощадну» архітектуру, яка складається з DDoS-атаки, цільового сервера та ботнету. У цій архітектурі стратегія атаки реалізується засобами написанням шкідливого бота з модулем атаки. Це практично усуває проблеми з керуванням ботнетами, які властиві для інших архітектур. Таким способом, витрати на управління такою архітектурою рівні нулю. Оскільки немає управлінсько-контрольної підсистеми, дана архітектура є надійною та застосовною для пристроїв з обмеженими ресурсами.

Необхідно зазначити, що незалежно від архітектури, DDoS-атаки мають цілком чітку мету. Як проілюстровано на рис. 5 а)-5 б), боти, керовані обробниками, надсилають пакети атаки. Ці пакети концентрується на цільовому сервері, щоб перевантажити його ресурси. Перевантаження ресурсів сервера може бути досягненим за рахунок пропускної здатності сервера, розміру пам'яті або циклів центрального процесора. Ймовірність перенасичення пропускної здатності цільового сервера можна оцінити [15] за допомогою такого співвідношення:

$$P_O = \frac{\left(\frac{a^k}{k!}\right)}{\sum_{i=0}^{k} \frac{a^i}{i!}} \quad (1)$$

де

$$a = \frac{1}{O_T}\left[\frac{\delta_{OA}}{\tau_{OA}} + \frac{\delta_{ON}}{\tau_{ON}}\right] \quad (2)$$

У (1) P_O – ймовірність перевантаження пропускної спроможності смуги каналу зв'язку, k – кількість незадіяних смуг каналу зв'язку, O_T – загальний задіяна пропускна смуга. Обсяг пакетів зловмисника (атакуючого, eng. attacking) та природнього (нормального, eng. normal) клієнтів представлені δ_{OA} та δ_{ON} відповідно; τ_{OA} – швидкість надходження атакуючого пакета, τ_{ON} –швидкість надходження легітимного пакету. У випадку, коли атакуючий та природній пакети мають однаковий розмір, отримуємо $\delta_{OA} = \delta_{ON} = \delta_O$. Тоді a можна виразити таким способом:

$$a = \frac{\delta_O}{O_T}\left[\frac{1}{\tau_{OA}} + \frac{1}{\tau_{ON}}\right], \quad (3)$$

$$a = j \times \frac{1}{\tau_{OA}}. \quad (4)$$

Співвідношення (3), (4) показують, що швидкість прибуття атакуючого трафіку має

суттєвий вплив на ймовірність перенасичення пропускної здатності каналу. У даній моделі розподіл природнього трафіку є гаусовим, тоді як швидкість надходження пакетів від атакуючого клієнта моделюється за допомогою розподілу Пуассона. Загальна ймовірність виснаження ресурсів жертви P_{TA} можна записати так:

$$P_{TA} = 1 - (1 - P_O)(1 - P_M), \quad (5)$$

де P_M – ймовірність насичення ресурсів споживання пам'яті.

Необхідно зазначити, що стрімке зростання кількості пристроїв у Internet призвели до того, що ботнети нині не обмежуються лише персональними комп'ютерами. Зловмисники при плануванні DDoS-атак можуть додатково збільшити трафік, який вони створюють, використовуючи різноманітні пристрої та пристрої Інтернету речей [15]. Атаки еволюціонують і стають більш складними, оскільки зловмисники намагаються масово використовувати пристрої IoT (маршрутизатори Wi-Fi, камери безпеки та смарт-телевізори тощо), щоб використовувати властиві їм слабкі сторони в ході атак. Власне такі вразливі пристрої зловмисники намагаються використати для перевантаження цільових мереж трафіком і, як наслідок, для виведення з ладу їх серверів. Пристрої IoT вразливі до віддаленого управління зловмисниками через відкритість Internet та обмежених можливостей мікропрограмного забезпечення, яким керуються IoT пристрої. Після враження пристрої IoT інтегруються в ботнети та починають атакувати цільовий сервер або службу [15]. Швидкий ріст кількості незахищених пристроїв IoT призвів до розширення пулу ресурсів DDoS-атак.

Очевидно, що за таких обставин вкрай важливо є задача оперативної ідентифікації загроз кібератак та запровадження стратегій ефективної їх протидії

5. Методи виявлення DDoS-атак

Однією з основних задач є послаблення атаки за допомогою запровадження ефективної методології виявлення атак. Даній проблемі присвячено численні дослідження, в яких запропоновано різні підходи до виявлення атак із різним ступенем успіху [13]. Загалом дослідники методології виявлення атак DDoS умовно розрізняють три їх основні категорії: традиційні методи виявлення атак, ідентифікація на основі сигнатур та ідентифікація на основі аномалій (рис. 6).

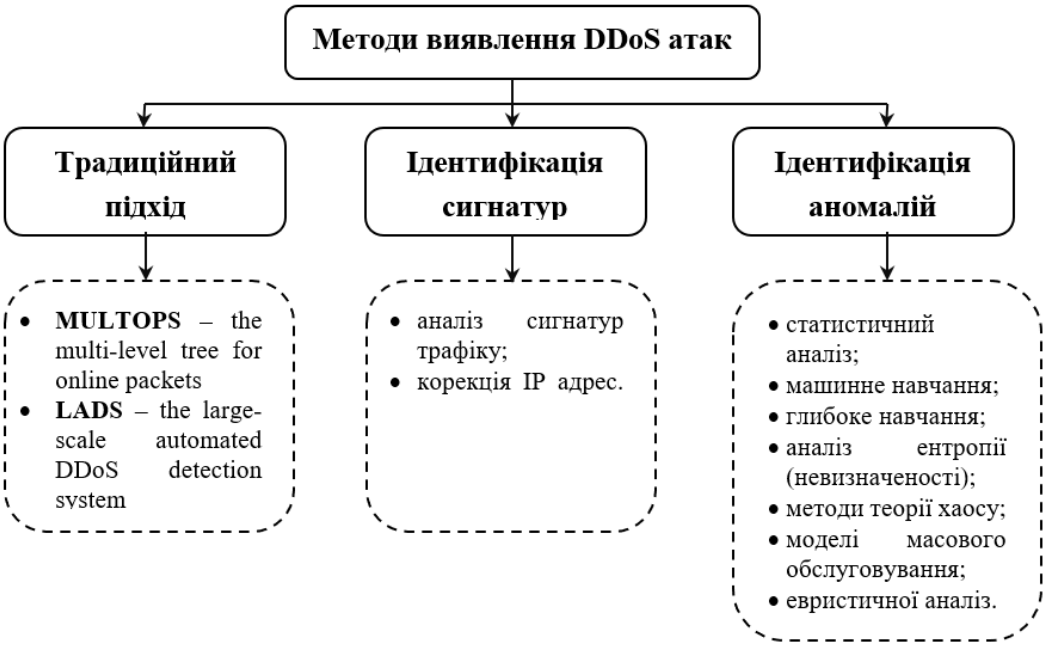

Рис. 6. Методи ідентифікації DDoS-атак

Традиційний підхід базується на методах, що зосереджені на вимірюванні обсягу трафіку

– коли обсяг трафіку перевищує заздалегідь визначений рівень, ідентифікується DDoS-атака. Варто зазначити, що не зважаючи на те, що традиційний підхід є швидким, його застосовність до сучасних загроз кібербезпеці обмежена точністю виявлення та частотою хибних тривог.

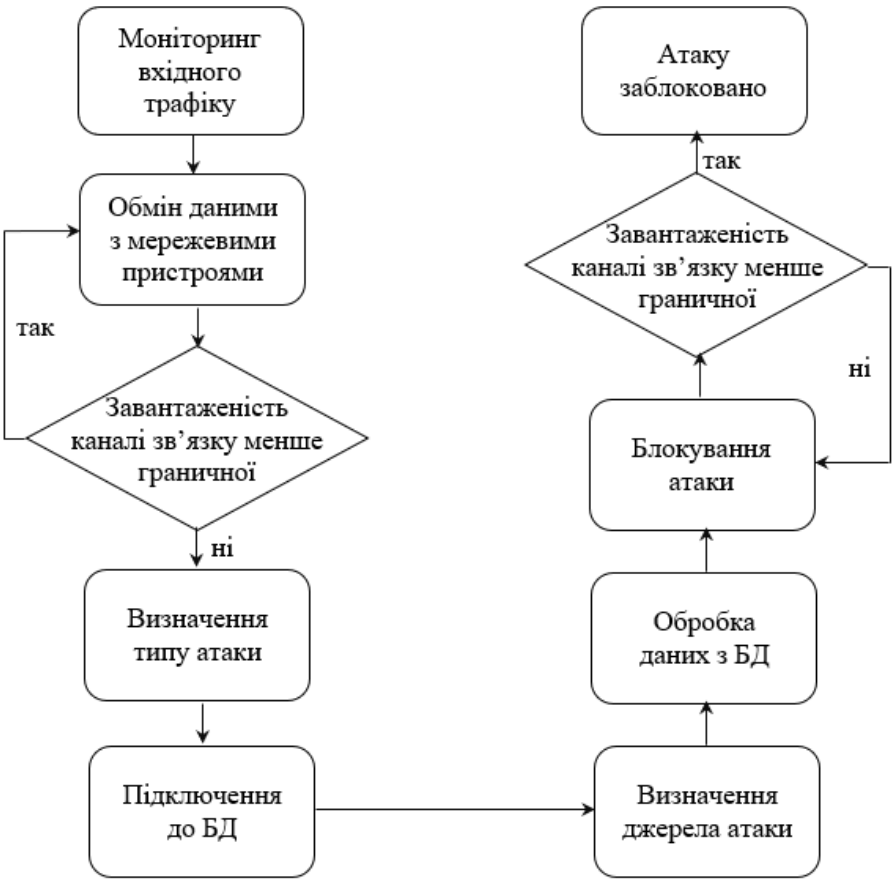

Рис. 7. Структура методу протидії DDoS-атакам

Ідентифікація на основі сигнатур – це метод при якому використовуються сигнатури атак, які зберігаються в спеціалізованій базі даних. Метод передбачає відстеження моделей трафіку та порівняння їх із уже відомими сигнатурами (рис. 7). Будь-які відмінності від раніше заданих шаблонів вказують на наявність стороннього (зловмисного) трафіку. Відтак, це означає, що можуть бути виявлені лише атаки, сигнатури яких були попередньо збережені в спеціалізованій базі даних. Даний метод має високу точність виявлення відомих атак за умови своєчасної актуалізації спеціалізованої бази даних. При цьому варто зазначити, що будь-які відмінності від відомих сигнатур атаки або поява нового шаблону атаки унеможливлює ідентифікацію загрози атаки. Метод ідентифікації DDoS-атак на основі сигнатур не може виявити невідому атаку чи навіть різновиди відомої атаки, оскільки не виявляє жодних змін у вже існуючих шаблонах сигнатур атаки. Відтак, у цьому випадку спрацьовує багато хибних тривог. А отже, маємо ситуацію, що вимагає регулярного оновлення спеціалізованої бази даних сигнатур атаки, що в загалі кажучи може бути дорогим і іноді складним завданням.

Ідентифікація на основі аномалій. Метод передбачає збір даних щодо типової поведінки трафіку протягом заздалегідь визначеного періоду та створення базового профілю. Будь-який вхідний шаблон, який виходить за межі базового, розглядається як аномалія, яка свідчить про те, що відбулися атаки. Метод добре працює при виявленні невідомих зловмисників і зловмисників нульового дня. Основна перевага ідентифікації на основі аномалій перед ідентифікацією на основі сигнатур полягає в тому, що даний метод дозволяє локалізувати нові атаки, сигнатури яких виходять за межі звичайних моделей трафіку. Однак швидкість їх виявлення відносно низька, оскільки вимагає ретельного моніторингу та значне задіяння використовуваних ресурсів. Крім того, маємо справу із більшими обчислювальними витрати,

оскільки вимагається глибоке вивчення характеристик поведінки мережевого трафіку.

Переважна більшість підходів, які застосовуються нині для ефективного виявлення DDoS-атак крім безпосередньої ідентифікації атак вимагає організації кібербезпеки в такий спосіб, щоб потенційно вразливі об'єкти критичної інфраструктури чи сервери даних мали чіткі стратегії протидії несанкціонованим агресивним діям зловмисників.

6. Концепція стратегії моделювання DDoS-атак.

Першим кроком у створенні стратегії моделювання DDoS-атак є аналіз ризиків. Це включає в себе оцінку потенційних цілей атак, типів атак, які можуть бути використані, та можливих наслідків атак. На основі аналізу ризиків власне необхідно розробляти стратегію виявлення та протидії атакам.

Одним з ключових ризиків є загрози концентрації зловмисниками необхідного пулу ботнетів, які будуть слугувати простором, що потенційно може бути трансформований у безпосередній фронт DDoS-атаки. Відтак моделювання атак є важливим для розуміння як загрози глибини так оцінки пов'язаних факторів успіху [16], що, власне, може сприяти оцінці ефективності механізмів захисту [17]. Таким способом, моделювання атак є невід'ємною складової еволюції існуючих рішень в системах кіберзахисту. Крім того, моделювання атак може бути корисним у симуляції і емуляції мереж та перевірки надійності мережі на етапі проектування.

В даній роботі ми детально зупинимось на застосуванні апарату якісної теорії нелінійних диференціальних рівнянь для моделювання процесів еволюційних процесів організації та динаміки DDoS-атак. З цією метою, в якості найбільш природнього математичного формалізму, що описує еволюційні процеси, які розвиваються з урахуванням безпосередніх впливів факторів антропогенної природи, використовуватимемо SIR-моделі [18,19].

Дослідимо математичні аспекти класичної SIR-моделі з урахуванням «процедури вакцинації» для моделювання еволюції ботнету. Вважатимемо, що всі показники в моделі нормовані, тобто йдеться про частки сегментованої сукупності мережі.

Нехай сукупність мережевих девайсів та пристроїв ділиться на три групи:

$S(t)$ – сприятливі до ураження вузли мережі;

$I(t)$ – уражені вузли мережі, що можуть поширювати ураження;

$R(t)$ – вузли, що відновились і вже не заразяться.

Враховуючи, що мережа функціонує як еволюційна система, в ній присутні процеси вибуття частини пристроїв та поповнення мережі новими, що є аналогом природної народжуваності та смертності певної популяції. Тоді математичну модель функціонування такої мережі можна записати за допомогою системи нелінійних диференціальних рівнянь:

$$\begin{cases} \dfrac{dS(t)}{dt} = -\lambda S(t)I(t) + \mu - \mu S(t), \\ \dfrac{dI(t)}{dt} = \lambda S(t)I(t) - \gamma I(t) - \mu I(t). \end{cases} \tag{6}$$

При цьому, необхідно зауважити, що виконується умова

$$R(t) = 1 - S(t) - I(t).$$

В системі (1) $\lambda > 0$ параметр, що характеризує інтенсивність контактів, тобто характеризує швидкість переходу вузлів з класу сприятливих до ураження вузлів мережі до уражених («інфікованих»); $\mu > 0$ – параметр, що характеризує смертність уражених DDoS-атакою пристроїв у зовнішній мережі (цей же параметр характеризує й появу нових пристроїв у зовнішній мережі, власне він характеризує народжуваність/смертність потенційних суб'єктів ботнету), $\gamma > 0$ – параметр, що характеризує інтенсивність відновлення пристроїв внутрішньої мережі, тобто , так би мовити, швидкість їх «одужання».

Власне, природній інтерес викликає відношення між описаними вище параметрами. Зокрема загрозостійкість мережі залежить від відношення швидкості вразливості пристроїв у мережі до вибувших та відновлених пристроїв. Відтак, для розуміння еволюційних процесів у

мережі введемо таких біфуркаційний параметр

$$\delta = \frac{\lambda}{\gamma + \mu}.$$

Дослідимо якісну поведінку систему (6) в області

$$\mathcal{D} = \{(S, I) \mid S \geq 0,\ I \geq 0,\ S + I \leq 1\}.$$

Варто зазначити, що використовуючи методи якісної теорії диференціальних рівнянь можна отримати важливу інформацію про поведінку системи, яка не може бути отримана за допомогою аналітичних методів розв'язання диференціальних рівнянь. Така інформація може бути використана для прогнозування поведінки системи, її аналізу та проектування.

Зокрема, методи якісної теорії дозволяють визначити, які типи траєкторій існують в фазовому просторі системи, як вони розташовані в просторі і як взаємодіють між собою. Наприклад, можна визначити, чи існують в системі періодичні траєкторії, стаціонарні точки, атрактори і репелери. Також можна визначити чи є система стійкою, тобто чи будуть її траєкторії близькі до початкової траєкторії при малих відхиленнях від початкових умов. Й зрештою встановити як змінюється поведінка системи при зміні її параметрів.

Відтак, якісна теорія еволюційних рівнянь може слугувати ефективним інструментарієм як для прогнозування вразливостей мережі до кібератак, так і для розробки стратегій прогнозування та протидії останнім.

Система (6) має два положення рівноваги. У фазовій площині SOI розрізнятимемо їх так:

- «infection free» $S_0^* = 1$, $I_0^* = 0$ – без уражень (тобто відсутні будь-які ознаки вразливості діями зловмисників);
- «epidemic» $S_1^* = \frac{1}{\sigma}$, $I_1^* = \frac{\mu(\delta - 1)}{\lambda}$ – ситуація вразливості порогової кількості пристроїв мережі (аналог досягнення порогу епідемії інфекційної хвороби в антропогенному середовищі).

За таких обставин якісний аналіз поведінки системи (6) характеризується значенням параметра δ. Справедлива теорема.

Теорема 1. [21] *Для* $\forall \delta > 0$ *область* $\mathcal{D}$ *є інваріантною, тобто* $\forall (S_0, I_o) \in \mathcal{D}$ *розв'язок системи* (6) $S(t), I(t)$ *з початковими умовами* $S(0) = S_0, I, I(0) = I_0$ *залишається в* $\mathcal{D}$, $\forall t \geq 0$, *тобто* $\big(S(t), I(t)\big) \in \mathcal{D}$, $\forall t \geq 0$.

Для $\forall \delta > 0$ *в області* $\mathcal{D}$ *немає замкнених траєкторій системи* (6).

При $\delta \leq 1$ точка (S_0^*, I_o^*) є *глобально асимптотично стійким положенням рівноваги* в області $\mathcal{D}$ (зауваження: в цьому випадку $(S_1^*, I_1^*) \notin \mathcal{D}$) (рис 8. а).

При $\delta > 1$ точка (S_0^*, I_o^*) є *нестійким положенням рівноваги* в області $\mathcal{D}$ (єдина траєкторія, що притягується до (S_0^*, I_0^*) – це $I(t) \equiv 0$, $S(t) = (S_0 - 1)e^{-\mu^t} + 1$). Точка (S_1^*, I_1^*) є *асимптотично стійким положенням рівноваги* з областю протягування $\mathcal{D} \setminus \{(S, 0) \mid 0 \leq S \leq 1\}$ (рис 8. б).

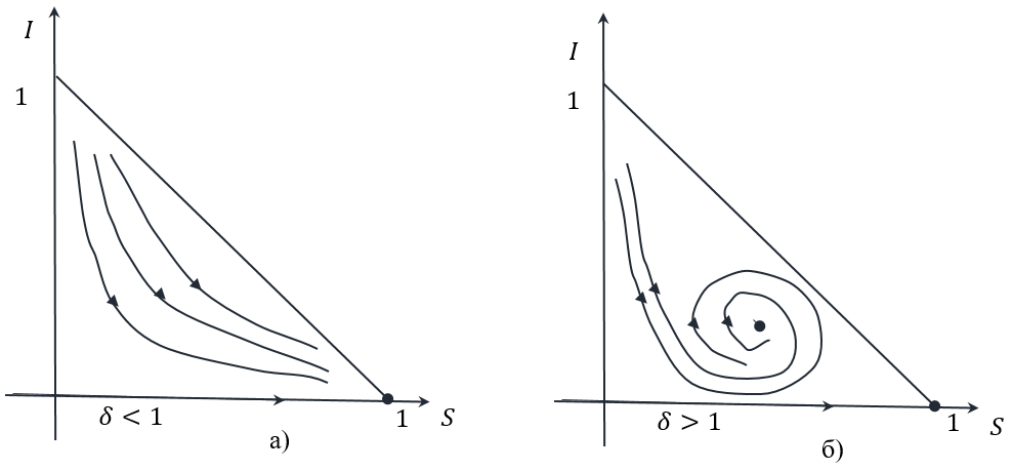

Рис. 8. Фазовий портрет системи (1)

Таким чином, можемо стверджувати, що коли параметр $\delta \leq 1$, то, незалежно від початкової ситуації, кількість заражених пристроїв з часом стає як завгодно малою. Натомість, при $\delta > 1$ спостерігаємо ситуацію критичного ураження з часом порогової кількості пристроїв мережі (S_1^*, I_1^*), що є асимптотично стійким положенням рівноваги з областю протягування $\mathcal{D} \setminus \{(S,0) \mid 0 \leq S \leq 1\}$.

Відповідно до умов теореми 1 інваріантість області $\mathcal{D}$ дозволяє нам говорити про те, що така поведінка буде характерною для багатьох мереж, оскільки жодних умов щодо параметрів та характеристик пристроїв які формують мережу ми не вимагали.

На практиці для прикладного вироблення стратегії протидії DDoS-атакам важливо дослідити основну задачу: *як при* $\delta > 1$ *зменшити рівень інфікованих суб'єктів*?

I. ***Стратегія постійної*** («constant») ***вакцинації*** передбачає налагодження системної роботи оснащення всіх нових пристроїв мережі найсучаснішим програмним забезпеченням, що може ідентифікувати та знешкодити кіберзагрози (тобто є аналогом вакцинації новонароджених в антропогенних системах). Якщо покладемо, що p – це частка оснащених відповідним програмним забезпеченням пристроїв мережі, то при $\delta > 1$ маємо систему:

$$\begin{cases} \dfrac{dS(t)}{dt} = (1-p)\mu - (\lambda I(t) + \mu)S(t), \\ \dfrac{dI(t)}{dt} = \lambda S(t)I(t) - (\gamma + \mu)I(t). \end{cases} \tag{7}$$

Положеннями рівноваги системи (2) є точки:

$$\hat{S}_0^* = 1 - p, \quad \hat{I}_0^* = 0;$$
$$\hat{S}_1^* = \frac{1}{\sigma}, \quad \hat{I}_1^* = I_1^* - \frac{\mu}{\mu+\gamma}p.$$

Якісна картина в системі (7) характеризується певним пороговим значенням параметра $p_* = 1 - \frac{1}{\delta}$.

Теорема 2. [22] *Для* $\forall p \in (0,1)$ *область* $\mathcal{D}$ *є інваріантною в* (7). *В області* $\mathcal{D}$ *немає замкнених траєкторій системи* (7).

При $p > p_*$ точка $\left(\hat{S}_0^*, \hat{I}_o^*\right)$ є *асимптотично стійким положення рівноваги* в області $\mathcal{D}$; $\left(\hat{S}_1^*, \hat{I}_1^*\right)$ *– нестійке положення рівноваги*.

При $p < p_*$ точка $\left(\hat{S}_0^*, \hat{I}_o^*\right)$ є *нестійким положення рівноваги* в області $\mathcal{D}$; $\left(\hat{S}_1^*, \hat{I}_1^*\right)$ – *асимптотично стійке положення рівноваги*.

Тобто стійкість, а, відтак, невразливість мережі при $p > p_*$ забезпечується в точці $\left(\hat{S}_0^*, \hat{I}_o^*\right)$, а $p < p_*$ в точці $\left(\hat{S}_1^*, \hat{I}_1^*\right)$. А от у ситуації, коли $p > p_*$ в околі точки $\left(\hat{S}_1^*, \hat{I}_1^*\right)$ і коли $p < p_*$ в околі точки $\left(\hat{S}_0^*, \hat{I}_o^*\right)$ стійкість до кіберзагроз буде втрачено, а сама мережі, відповідно, характеризуватиметься суттєвою вразливістю. В такій ситуації *адміністраторам мережі необхідно вживати заходів щодо мінімізації загроз кібератак*.

II. ***Стратегія імпульсної*** («pulse») ***вакцинації*** – в антропогенних системах передбачає в певні моменти часу вакцинацію частини популяції, що може заразитись. Аналогом в мережах є оновлення та актуалізації програмного забезпечення для виявлення знешкодження підозрілого та вірусного програмного забезпечення для потенційно вразливих сегментів мережі, тобто $S(t)$. В якості модельної абстракції, вважатиме, що час оновлення програмного забезпечення неспівмірно малий з часом його ефективної експлуатації, тобто вважатимемо, що оновлення програмного забезпечення здійснюється як регламентна процедура за час, яким можна нехтувати (миттєво, імпульсно).

Нехай послідовність $\{t_n\}_{n=0}^{\infty}$ моментів оновлення програмного забезпечення. Тоді задача при $\delta > 1$ має вигляд:

$$\begin{cases} \dfrac{dS(t)}{dt} = -\lambda S(t)I(t) + \mu - \mu S(t), & t \neq t_n, \\ \dfrac{dI(t)}{dt} = \lambda S(t)I(t) - \gamma I(t) - \mu I(t), & t \neq t_n, \end{cases} \quad (8)$$

$$\Delta S|_{t=t_n} := S(t_n + 0) - S(t_n - 0) = -\varphi\big(S(t_n - 0)\big). \quad (9)$$

При цьому вважаємо, що $\varphi(S) \leq 0$ при $S \geq 0$, і вважаємо функцію $S(t)$ неперервною справа в точках $\{t_n\}$. Тоді для системи (8), (9) якісний аналіз залежить від імпульсних параметрів $\{t_n\}$ і $\varphi(S)$.

Умова (9) є математичним формалізмом, що описує процес оновлення програмного забезпечення та передбачає, щ після кожної такої процедури мережа функціонувати за законом (8) до наступного моменту здійснення регламентних заходів з програмного зменшення кіберризиків. Підкреслимо, що в даному випадку стратегія кібербезпеки безпосередньо має корелювати з регулярністю та повнотою регламентних процедур оновлення програмного та апаратного захисту мережі.

III. ***Періодичний випадок***. Нехай $t_n = nT$, $n = 0,1,\ldots$. Тобто в даному випадку передбачається, що регламентні процедури оновлення програмного забезпечення мають періодичну природу з визначеним періодом. Покладемо

$$\varphi(S) = -p \cdot S, \qquad p \in (0,1).$$

Тоді, важливим є граничне число сприятливих до ураження вузлів мережі

$$S_* = \frac{(1-p)(e^{\mu T} - 1)}{p - 1 + e^{\mu T}}.$$

Справедлива теорема.

Теорема 3. [23] *Система* (8), (9) *має імпульсний періодичний розв'язок («infection -free» periodic solution)*

$$\bar{S}(t) = \begin{cases} 1 + \dfrac{p \cdot e^{\mu T}}{1 - p - e^{\mu T}} \cdot e^{-\mu(t - t_n)}, & t \in [t_n, t_{n+1}), \\ S_*, & t = t_{n+1}, \end{cases}$$

$$\bar{I}(t) \equiv 0.$$

Цей розв'язок є асимптотично стійким за умови

$$\frac{1}{T}\int_0^T \bar{S}(t)\, dt < \frac{1}{\delta}. \quad (10)$$

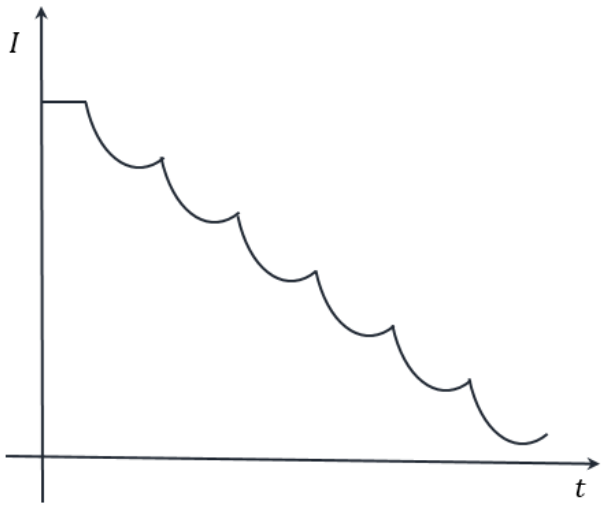

Рис. 9. Ілюстрація поведінки $I(t)$, $I(0) = I_0 \in (0,1)$ при $t \to \infty$

Оцінка (10) вказує, що загрозостійкість мережі обернено пропорційно визначається відношенням швидкості вразливості пристроїв у мережі до вибувших та відновлених

пристроїв. Власне насичення мережі новими захищеними пристроями при періодичному оновленні програмного забезпечення забезпечуватиме в часі стійку роботу мережі навіть в умовах вразливості певних сегментів мережі.

Графік поведінки $I(t)$, уражених вузлів мережі, що можуть поширювати ураження: $I(0) = I_0 \in (0,1)$ при $t \to \infty$ представлено на рис. 9. Тобто періодичне виконання обов'язкових регламентів оновлення програмного забезпечення з часом мінімізує число вузлів, які можуть поширювати шкідливе програмне забезпечення звівши їх практично до нуля.

Зауважимо, що умову (10) можна записати у явному вигляді

$$\frac{(\mu T - p)(e^{\mu T} - 1) + \mu p T}{\mu T(p - 1 + e^{\mu T})} < \frac{1}{\delta}. \tag{11}$$

З теореми 3 та формул (10), (11) можемо зробити важливий висновок.

Висновок 1. *Якщо період оновлення програмного забезпечення для захисту від кіберзагроз*

$$T < T_* = \frac{1}{\mu}\ln\left(1 + \frac{p}{\delta - p}\right), \tag{12}$$

то виконуватиметься умова $I(t) \to 0$, $t \to \infty$.

Власне фактична ліквідація вузлів, які здатні поширювати шкідливе програмне забезпечення гарантується реалізацією періодичного оновлення захисного програмного забезпечення з періодом, що задовольняє умову (12).

Задачу про еволюціонування мережі (8) з імпульсним оновлення програмного забезпечення (9) можна узагальнити. Варто зосередити увагу на дослідженні таких задач.

Задача 1. *Періодичне оновлення програмного забезпечення з «нечіткою» інформацією* про кількість оновлених вузлів мережі: $t_n = nT$, $n = 0,1, \dots$.

$$\Delta S|_{t=t_n} \in \left[-\varphi_1\big(S(t_n - 0)\big), -\varphi_2\big(S(t_n - 0)\big)\right],$$

де φ_1, φ_2 – задані функції.

Задача 2. *«Майже-періодичне» оновлення програмного забезпечення*: нехай $\{t_n\}$ є квазіперіодичною («близькою» до періодичної), тобто $t_n = nT + \tau_n$, $\tau_n \in [0, T)$.

$$\Delta S|_{t=t_n} = -p \cdot S(t_n - 0).$$

Задача 3. *Оновлення програмного забезпечення з відомою статистичною інформацією про кількість оновлених вузлів мережі.* Нехай $\{t_n\}$ така, що

$$\overline{\lim_{\tau\to\infty}} \frac{N(t, t+\tau)}{\tau} < \infty,$$

де $N(t, t+\tau)$ – кількість моментів оновлення t_n на проміжку $(t, t+\tau)$, $\{p_n(\omega)\}$ – випадкові величини із заданими ймовірнісними характеристиками.

$$\Delta S|_{t=t_n} = -p(\omega) \cdot S(t_n - 0).$$

Дослідження якісної поведінки системи (8), (9) для задач 1-3 буде виконано у додаткових дослідженнях, щоб в цілому отримати комплексну методику вибору ефективних стратегій протидії кібрезагрозам.

7. Висновки.

Сучасний інформаційний простір сформовано мережами складних технічних системи взаємопов'язаних девайсів та пристроїв, які обмінюються інформацією та ресурсами. Вони є невід'ємним фундаментальним базисом для багатьох сучасних технологій, включаючи Internet, мережі передачі даних, соціальні мережі тощо.

Ключовою передумовою забезпечення стійкості сучасних інформаційних систем від несанкціонованого доступу в цілому та DDoS атак зокрема є реалізація концепції проактивного захист. Власне це означає, що заходи кібербезпеки мають передбачати впровадження комплексу відповідних заходів до того, як відбудеться прецедент несанкціонованою доступу до даних чи атака зловмисників.

В роботі проаналізовано нинішній стан та підходи до виявлення кіберзагроз для

інформаційних систем корпоративних мереж, наведено класифікацію кіберзагроз та дано характеристику анатомії DDoS атак. В роботі досліджуються анатомія DDoS-атак та методи протидії DDoS-атакам, що дозволяють ефективно захищати інформаційну мережу, як від атак зловмисників.

Розроблено математичний апарат для ідентифікації кіберзагроз та визначення стратегій мінімізації ризиків несанкціонованого доступу зловмисників до інформаційних ресурсів мережі, що ґрунтується на методах якісної теорії систем диферецiальних рівнянь з імпульсною дією.

Використовуючи методи фазової площини, вивчаються особливості поведінка складних них систем, математичні моделі яких представлено системами диференціальних рівнянь з імпульсною.

Отримано конструктивні умови стійкості та асимптотичної стійкості SIR-моделі, яка є математичною моделлю вразливості мережі в наслідок агресивних дій зловмисників. Встановлено умови мінімізації уразливостей елементів мережі через реалізацію різних стратегій зменшення кількості інфікованих пристроїв: стратегії «постійної вакцинації», стратегії «імпульсної вакцинації» та періодичного випадку реалізації концепції оновлення та актуалізації програмного забезпечення для протидії DDoS-атакам.

Встановлено, що загрозостійкість мережі обернено пропорційно визначається відношенням швидкості вразливості пристроїв у мережі до вибувших і відновлених пристроїв та отримано оцінку періоду оновлення програмного забезпечення для захисту від кіберзагроз.

Список використаної літератури

1. Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. DOI: 10.15587/978-617-7319-31-2

2. Yevseiev, S., Khokhlachova, Yu., Ostapov, S., Laptiev, O., Korol, O., Milevskyi, S. et. al.; Yevseiev, S., Khokhlachova, Yu., Ostapov, S., Laptiev, O. (Eds.) (2023). Models of socio-cyber-physical systems security. Kharkiv: PC TECHNOLOGY CENTER, 184.

3. Барабаш О.В., Мусієнко А.П., Собчук В.В. Основи забезпечення функціональної стійкості інформаційних систем підприємств в умовах впливу дестабілізуючих факторів: монографія. Київ: Міленіум, 2022. 272 с.

4. Barabash, O., Sobchuk, V., Musienko, A., Laptiev, O., Bohomia, V., Kopytko, S. (2023). System Analysis and Method of Ensuring Functional Sustainability of the Information System of a Critical Infrastructure Object. In: Zgurovsky, M., Pankratova, N. (eds) System Analysis and Artificial Intelligence. Studies in Computational Intelligence, vol 1107. Springer, Cham. https://doi.org/10.1007/978-3-031-37450-0_11

5. Собчук, В., Барабаш, О., & Мусієнко, А. (2021). Вплив методу адаптивного самодіагностування на процес попередження наслідків відмов модулів інформаційної системи підприємства. // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка, (70), 77–88. https://doi.org/10.17721/2519-481X/2021/70-08.

6. Sobchuk A.V., Sobchuk V.V., Barabash O.V., Lyashenko I.O. Functionally sustainable wireless sensor network technologies aspects analysis // Science and Education a New Dimension. Natural and Technical Sciences, 2019. – VII (23), Issue 193, Budapest, Hungary, pp. 46 – 48.

7. Собчук В.В., Довженко Н.М., Коваль М.О. Математична модель багатокритеріальної оптимізації якості обслуговування сенсорних мереж з використанням принципу справедливості // Науковий журнал «Телекомунікаційні та інформаційні технології». – К.: ДУТ. – № 3 (64). – С. 90 – 97.

8. Собчук В.В., Лаптєв О.А., Саланда І.П., Сачук Ю.В. Математична модель структури інформаційної мережі на основі нестаціонарної ієрархічної та стаціонарної гіпермережі //

Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2019. – Вип. 64. – С. 124 – 132.

9. Лаптєв О.А., Собчук В.В., Савченко В.А. Метод підвищення завадостійкості системи виявлення, розпізнавання і локалізації цифрових сигналів в інформаційних системах // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2019. – Вип. 66. – С. 90 – 104.

10. Laptiev, O., Sobchuk, V., Sobchuk, A., Laptiev, S. & Laptieva, T. (2021). Удосконалена модель оцінювання економічних витрат на систему захисту інформації в соціальних мережах. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка; 4(12), 19-28. https://doi.org/10.28925/2663-4023.2021.12.1928

11. Замрій І.В., Собчук В.В., Барабаш А.О. Ідентифікація вхідних елементів інформаційного простору та відновлення їх параметрів в єдиному інформаційному просторі виробничого підприємства з критичною інфраструктурою. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. № 75. 2022. С. 78 – 87. https://doi.org/10.17721/2519-481X/2022/75-08

12. Галахов Є.М., Собчук В.В. Розвиток моделей кібератак у площині інформаційної безпеки підприємства // Науковий журнал «Телекомунікаційні та інформаційні технології». – К.: ДУТ, 2019. – № 4 (65). – С. 12 – 24.

13. Барабаш О.В., Лукова-Чуйко Н.П., Мусієнко А.П., Собчук В.В. Забезпечення функціональної стійкості інформаційних мереж на основі розробки методу протидії DDoS-атакам. // Сучасні інформаційні системи. – Харків: Національний технічний університет «Харківський політехнічний інститут», 2018. – Том 2. – № 1. – С. 56–63.

14. Adedeji, K.B.; Abu-Mahfouz, A.M.; Kurien, A.M. DDoS Attack and Detection Methods in Internet-Enabled Networks: Concept, Research Perspectives, and Challenges. *J. Sens. Actuator Netw.* 2023, *12*, 51. https://doi.org/10.3390/jsan12040051

15. Singh, K.J.; De, T. Mathematical modelling of DDoS attack and detection using correlation. J. Cyber Secur. Technol. 2017, 1, 175–186

16. B.F. Maier, D. Brockmann, Effective containment explains subexponential growth in recent confirmed COVID-19 cases in China, Science 368 (6492) (2020) 742–746, https://doi.org/10.1126/science.abb4557

17. Juan Fernando Balarezo ⇑, Song Wang, Karina Gomez Chavez, Akram Al-Hourani, Sithamparanathan Kandeepan A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks // Engineering Science and Technology, an International Journal 31 (2022) 101065 DOI: 10.1016/j.jestch.2021.09.011

18. Herbert W. Hethcote Three Basic Epidemiological Models // Applied Mathematical Ecology, Springer-Verlag, 1989

19. Helena Sofia Rodrigues Application of SIR epidemiological model: new trends // International journal of applied mathematics and informatics, 2016, vol.10

20. L. STONE, B. SHULGIN, Z. AGUR Theoretical Examination of the Pulse Vaccination Policy in the SIR Epidemic Model // Mathematical and Computer Modelling 31 (2000) 207-215

21. A. D'ONOFRIO Pulse Vaccination Strategy in the SIR Epidemic Model: Global Asymptotic Stable Eradication in Presence of Vaccine Failures // Mathematical and Computer Modelling 36 (2002) 473-489

22. Jianjun Jiao, Shaohong Cai, Limei Li Impulsive vaccination and dispersal on dynamics of an SIR epidemic model with restricting infected individuals boarding transports // Physica A, 2023

23. Ning Sun, Shaoyun Shi, Wenlei Li Singular renormalization group approach to sis problems // Discrete and continuous dynamical systems series B, Volume 25, Number 9, 2020

24. Jinyan Wang Dynamics and bifurcation analysis of a state-dependent impulsive SIS model // Advances in Difference Equations (2021) 2021:287

25. Petro Feketa , Vladimir Klinshov , Leonhard Lücken A survey on the modeling of hybrid behaviors: How to account for impulsive jumps properly // Commun Nonlinear Sci Numer Simulat, 103 (2021) 105955

References

1. Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. DOI: 10.15587/978-617-7319-31-2

2. Yevseiev, S., Khokhlachova, Yu., Ostapov, S., Laptiev, O., Korol, O., Milevskyi, S. et. al.; Yevseiev, S., Khokhlachova, Yu., Ostapov, S., Laptiev, O. (Eds.) (2023). Models of socio-cyber-physical systems security. Kharkiv: PC TECHNOLOGY CENTER, 184.

3. Barabash O.V., Musienko A.P., Sobchuk V.V. Basics of ensuring the functional stability of information systems of enterprises under the influence of destabilizing factors: monograph. Kyiv: Millennium, 2022. 272 p.

4. Barabash, O., Sobchuk, V., Musienko, A., Laptiev, O., Bohomia, V., Kopytko, S. (2023). System Analysis and Method of Ensuring Functional Sustainability of the Information System of a Critical Infrastructure Object. In: Zgurovsky, M., Pankratova, N. (eds) System Analysis and Artificial Intelligence. Studies in Computational Intelligence, vol 1107. Springer, Cham. https://doi.org/10.1007/978-3-031-37450-0_11

5. Sobchuk, V., Barabash, O., & Musienko, A. (2021). The influence of the method of adaptive self-diagnosis on the process of preventing the consequences of failures of modules of the information system of the enterprise. // Collection of scientific works of the Military Institute of Taras Shevchenko Kyiv National University, (70), 77–88. https://doi.org/10.17721/2519-481X/2021/70-08.

6. Sobchuk A.V., Sobchuk V.V., Barabash O.V., Lyashenko I.O. Functionally sustainable wireless sensor network technologies aspects analysis // Science and Education a New Dimension. Natural and Technical Sciences, 2019. – VII (23), Issue 193, Budapest, Hungary, pp. 46 – 48.

7. Sobchuk V.V., Dovzhenko N.M., Koval M.O. Mathematical model of multi-criteria optimization of service quality of sensor networks using the principle of fairness // Scientific journal "Telecommunications and Information Technologies". - K.: DUT. – No. 3 (64). - pp. 90 - 97.

8. Sobchuk V.V., Laptev O.A., Salanda I.P., Sachuk Yu.V. Mathematical model of the structure of the information network based on non-stationary hierarchical and stationary hyper-network // Collection of scientific papers of Taras Shevchenko Military Institute of Kyiv National University. - K.: VIKNU, 2019. - Issue 64. - pp. 124 – 132.

9. Laptev O.A., Sobchuk V.V., Savchenko V.A. A method of increasing the immunity of the system of detection, recognition and localization of digital signals in information systems // Collection of scientific papers of the Military Institute of Taras Shevchenko Kyiv National University. - K.: VIKNU, 2019. - Issue 66. – pp. 90 – 104.

10. Laptiev, O., Sobchuk, V., Sobchuk, A., Laptiev, S. & Laptieva, T. (2021). An improved model for estimating the economic costs of the information protection system in social networks. Electronic professional scientific publication "Cybersecurity: education, science, technology; 4(12), 19-28. https://doi.org/10.28925/2663-4023.2021.12.1928

11. Zamrii I.V., Sobchuk V.V., Barabash A.O. Identification of input elements of the information space and restoration of their parameters in the unified information space of the production enterprise with critical infrastructure. Collection of scientific works of the Military Institute of Taras Shevchenko Kyiv National University. No. 75. 2022. pp. 78– 87. https://doi.org/10.17721/2519-481X/2022/75-08

12. Galakhov E.M., Sobchuk V.V. The development of cyber attack models in the field of enterprise information security // Scientific Journal "Telecommunications and Information Technologies". - K.: DUT, 2019. - No. 4 (65). - pp. 12– 24.

13. Barabash O.V., Lukova-Chuiko N.P., Musienko A.P., Sobchuk V.V. Ensuring the functional stability of information networks based on the development of a method of countering DDoS attacks. // Modern information systems. - Kharkiv: National Technical University "Kharkiv Polytechnic Institute", 2018. - Volume 2. - No. 1. - pp. 56–63.

14. Adedeji, K.B.; Abu-Mahfouz, A.M.; Kurien, A.M. DDoS Attack and Detection Methods in Internet-Enabled Networks: Concept, Research Perspectives, and Challenges. *J. Sens. Actuator Netw.* 2023, *12*, 51. https://doi.org/10.3390/jsan12040051

15. Singh, K.J.; De, T. Mathematical modelling of DDoS attack and detection using correlation. J. Cyber Secur. Technol. 2017, 1, 175–186

16. B.F. Maier, D. Brockmann, Effective containment explains subexponential growth in recent confirmed COVID-19 cases in China, Science 368 (6492) (2020) 742–746, https://doi.org/10.1126/science.abb4557

17. Juan Fernando Balarezo ⇑, Song Wang, Karina Gomez Chavez, Akram Al-Hourani, Sithamparanathan Kandeepan A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks // Engineering Science and Technology, an International Journal 31 (2022) 101065 DOI: 10.1016/j.jestch.2021.09.011

Література+

18. Herbert W. Hethcote Three Basic Epidemiological Models // Applied Mathematical Ecology, Springer-Verlag, 1989

19. Helena Sofia Rodrigues Application of SIR epidemiological model: new trends // International journal of applied mathematics and informatics, 2016, vol.10

20. L. STONE, B. SHULGIN, Z. AGUR Theoretical Examination of the Pulse Vaccination Policy in the SIR Epidemic Model // Mathematical and Computer Modelling 31 (2000) 207-215

21. A. D'ONOFRIO Pulse Vaccination Strategy in the SIR Epidemic Model: Global Asymptotic Stable Eradication in Presence of Vaccine Failures // Mathematical and Computer Modelling 36 (2002) 473-489

22. Jianjun Jiao, Shaohong Cai, Limei Li Impulsive vaccination and dispersal on dynamics of an SIR epidemic model with restricting infected individuals boarding transports // Physica A, 2023

23. Ning Sun, Shaoyun Shi, Wenlei Li Singular renormalization group approach to sis problems // Discrete and continuous dynamical systems series B, Volume 25, Number 9, 2020

24. Jinyan Wang Dynamics and bifurcation analysis of a state-dependent impulsive SIS model // Advances in Difference Equations (2021) 2021:287

25. Petro Feketa , Vladimir Klinshov , Leonhard Lücken A survey on the modeling of hybrid behaviors: How to account for impulsive jumps properly // Commun Nonlinear Sci Numer Simulat, 103 (2021) 105955