НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра математичного моделювання та аналізу даних

«До захисту допущено»
В.о. завідувача кафедри
_____ Іван ТЕРЕЩЕНКО
«__» _____ 2023 р.

Дипломна робота

на здобуття ступеня бакалавра

зі спеціальності: 113 Прикладна математика
на тему: **«Моделі і методи атак відмови в обслуговуванні в кібер-фізичних системах критичної інфраструктури»**

Виконала: студентка 4 курсу, групи ФІ-91
Сириця Валентина Олександрівна

Керівник: д.т.н., проф. Новіков Олексій Миколайович _____

Консультант: _ _____

Рецензент: д.т.н., проф. Данилов Валерій Якович _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент _____

Київ — 2023

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра математичного моделювання та аналізу даних

Рівень вищої освіти — перший (бакалаврський)
Спеціальність (освітня програма) — 113 Прикладна математика,
ОПП «Математичні методи моделювання, розпізнавання образів та комп'ютерного зору»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ Іван ТЕРЕЩЕНКО
«__» _____ 2023 р.

ЗАВДАННЯ
на дипломну роботу

Студентка: Сириця Валентина Олександрівна

1. Тема роботи: «*Моделі і методи атак відмови в обслуговуванні в кібер-фізичних системах критичної інфраструктури*»,

керівник: д.т.н., проф. Новіков Олексій Миколайович,

затверджені наказом по університету №__ від «__» _____ 2023 р.

2. Термін подання студентом роботи: «__» _____ 2023 р.

3. Вихідні дані до роботи: *опубліковані джерела за тематикою дослідження.*

4. Зміст роботи: *розробка та дослідження моделі DDoS-атаки на критичну інфраструктуру, яка відрізняється від тих, що існує, врахуванням фізичного впливу, і порівняння її з DDoS-атакою в кіберпросторі за звичайних умов.*

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо): *презентація доповіді.*

6. Дата видачі завдання: 29 вересня 2022 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання	Примітка
1	Узгодження теми роботи із науковим керівником	Вересень-жовтень 2022 р.	Виконано
2	Огляд опублікованих джерел за тематикою дослідження	Жовтень-листопад 2022 р.	Виконано
3	Імплементація SIR-подібної моделі	Грудень 2022 р.	Виконано
4	Розширення цієї моделі до урахування фізичного впливу	Січень 2023 р.	Виконано
5	Дослідження створеної моделі	Лютий 2023 р.	Виконано
6	Імплементація моделі атаки за допомогою IoT-ботнету	Березень 2023 р.	Виконано
7	Порівняння моделей	Квітень 2023 р.	Виконано
8	Обробка результатів	Травень 2023 р.	Виконано
9	Оформлення дипломної роботи	1-15 червня 2023 р.	Виконано

Студент _____ Сириця В.О.

Керівник _____ Новіков О.М.

РЕФЕРАТ

Кваліфікаційна робота містить: 41 сторінку, 17 рисунків, 16 джерел.

Метою дослідження є розробка та дослідження моделі DDoS-атаки на критичну інфраструктуру, яка відрізняється від тих, що існує, врахуванням фізичного впливу, і порівняння її з DDoS-атакою в кіберпросторі за звичайних умов. Об'єктом дослідження є розподілені атаки відмови в обслуговуванні. Предметом дослідження є модель розподіленої атаки відмови в обслуговуванні на критичну інфраструктуру.

У роботі виконано дослідження та порівняння моделей атак відмови в обслуговуванні на кіберфізичні системи. Порівняння відбувалося між моделлю атаки відмови в обслуговуванні на критичну інфраструктуру, яка враховує фізичний вплив, і моделлю атаки на критичну інфраструктуру за звичайних умов.

Отримані результати свідчать про те, що фізична така заважає проведенню кібератаки, і чим більший кінетичний вплив, тим менша потужність атаки відмови в обслуговуванні.

РОЗПОДІЛЕНІ АТАКИ ВІДМОВИ В ОБСЛУГОВУВАННІ, ЕПІДЕМІЧНІ МОДЕЛІ, КРИТИЧНА ІНФРАСТРУТКТУРА, ФІЗИЧНИЙ ВПЛИВ

ABSTRACT

Qualification work contains: 41 pages, 17 figures, 16 sources.

The purpose of the study is to develop and study a model of a DDoS attack on critical infrastructure that differs from those that exist by taking into account physical impact and comparing it with a DDoS attack in cyberspace under normal conditions. The object of research is distributed denial of service attacks. The subject of the study is a model of a distributed denial of service attack on critical infrastructure.

The paper studies and compares models of denial-of-service attacks on cyber-physical systems. The comparison was made between the model of a denial-of-service attack on critical infrastructure that takes into account physical impact and the model of an attack on critical infrastructure under normal conditions.

The results show that physical impact hinders the cyberattack, and the greater the kinetic impact, the lower the power of the denial of service attack.

DISTRIBUTED DENIAL OF SERVICE ATTACKS, EPIDEMIC MODELS, CRITICAL INFRASTRUCTURE, PHYSICAL IMPACT

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

DoS — Denial-of-Service Attack

DDoS — Distributed Denial-of-Service Attack

DRDoS — Distributed Reflective Denial of Service

IoT — Internet of Things

SIR — Susceptible-Infected-Recovered

SIS — Susceptible-Infected-Susceptible

ПЗ — програмне забезпечення

ВСТУП

Актуальність дослідження. Системи критичної інфраструктури включають різні сектори, об'єкти та послуги, які є життєво важливими для функціонування суспільства та його економіки. Ці системи є необхідними для забезпечення безпеки, здоров'я, добробуту та безперебійного функціонування суспільства в умовах надзвичайних ситуацій або криз. Будь-яка їхня недоступність чи несправність може мати серйозні наслідки.

Збільшення рівня інформатизації робить системи критичної інфраструктури вразливими до кібератак, зокрема до атак відмови в обслуговуванні. До того ж у сучасних умовах кіберзагрози не тільки стають все складнішими та розповсюдженішими, а і можуть підкріплюватися фізичними атаками. Тому необхідно не тільки створювати нові моделі атак відмов в обслуговуванні, які будуть враховувати кінетичний вплив, але і вивчати як саме фізична атака буде впливати на кібератаку. Це дозволить не тільки краще зрозуміти цей тип загроз, його характеристики та особливості, але і підвищити ефективність методів захисту.

Метою дослідження є розробка та дослідження моделі DDoS-атаки на критичну інфраструктуру, яка відрізняється від тих, що існує, врахуванням фізичного впливу, і порівняння її з DDoS-атакою в кіберпросторі за звичайних умов.

Завдання дослідження:

1) дослідження математичної моделі розповсюдження ботнету на основі епідемічного моделювання;

2) розширення моделі з урахуванням фізичного впливу;

3) дослідження математичної моделі атаки на кіберфізичну систему за допомогою ботнету, сформованого з IoT пристроїв;

4) аналіз і порівняння моделей.

Об'єктом дослідження є розподілені атаки відмови в обслуговуванні.

Предметом дослідження є модель розподіленої атаки відмови в обслуговуванні на критичну інфраструктуру.

При розв'язанні поставлених завдань використовувались такі *методи дослідження*: методи диференційних рівнянь, епідемічного та комп'ютерного моделювання.

Наукова новизна. Розроблено та досліджено нову епідемічну модель розподільної атаки відмови в обслуговуванні, яка б враховувала фізичний вплив, порівняно її з моделлю DDoS-атаки в кіберпросторі за звичайних умов.

Практичне значення результатів. Робота допомагає оцінити вплив кінетичних атак на ефективність розподільних атак відмов в обслуговуванні на критичну інфраструктуру, що надалі можна застосовувати для покращення стратегій захисту або використовувати для точнішого планування кібератак.

Апробація результатів та публікації. Результати дослідження представлені на всеукраїнській науково-практичні конференції "Theoretical and Applied Cybersecurity"(TACS-2023).

1 ТЕОРЕТИЧНІ ВІДОМОСТІ

У цьому розділі наведено опис теоретичного підґрунтя, необхідного для розуміння тематики дослідження.

1.1 Атаки на відмову в обслуговуванні та їхні види

Атаки на відмову в обслуговуванні розрізняються між собою, але в будь-якому разі метою таких атак є перекриття доступу легітимних користувачів до ресурсу або системи, заважаючи їм виконувати необхідні дії або отримувати необхідні послуги. Це може мати серйозні наслідки для бізнесу або організацій, залежно від того, наскільки вони залежать від доступності своїх мереж або ресурсів.

1.1.1 Типові атаки на відмову

Атака на відмову в обслуговуванні (Denial of Service) є типом кібератаки, спрямованої на забезпечення недоступності ресурсу, мережі або комп'ютерної системи для легітимних користувачів шляхом перевантаження цільового сервісу або використання вразливостей у програмному забезпеченні.

У DoS-атаках зловмисники намагаються перевантажити цільовий ресурс або систему, забираючи у них доступні ресурси, такі як пропускна здатність мережі, процесорний час, пам'ять або мережеві з'єднання. Це може бути досягнуто різними способами, включаючи надсилання великої кількості запитів на обробку(атака переповнення), використання вразливостей у програмному забезпеченні(експлуатація вразливості) або використання ботнетів (мережі комп'ютерів, що керуються зловмисниками).

У випадку атаки, спрямованої на переповнення ресурсів, спостерігається надмірне навантаження ресурсів цільової системи за допомогою значних обсягів трафіку. Боротьба з цією формою атак ускладняється, оскільки пакети можуть бути будь-якого типу, а значний обсяг трафіку заважає детальному аналізу частот. [1]

1.1.2 Розподілені атаки на відмову

Розподілена атака на відмову в обслуговуванні(Distributed Denial-of-Service Attack) є підтипом DoS-атаки, де зловмисники використовують багато комп'ютерів або пристроїв з метою перевантаження цільового ресурсу або системи.

У DDoS-атаках зловмисники здатні мобілізувати ботнет, що складається з багатьох заражених комп'ютерів або пристроїв (часто за допомогою вірусів, троянських програм або іншого шкідливого програмного забезпечення), і використовують їх для одночасного відправлення великої кількості запитів або трафіку на цільовий ресурс. Це надмірне навантаження перевантажує ресурс або систему, що робить їх недоступними для легітимних користувачів.

DDoS-атаки можуть бути реалізовані за допомогою різних типів трафіку. Ці атаки можуть мати різні форми, включаючи атаки на мережевий рівень, аплікаційні атаки, а також ампліфікаційні атаки, де зловмисники використовують вразливості у мережевих протоколах для збільшення обсягу трафіку, який вони відправляють до цілі.

Типова DDoS-атака складається з наступних етапів:

1. Ідентифікацію потенційних цілей атаки та встановлення необхідного програмного забезпечення на комп'ютери, які можуть бути використані для здійснення атаки.

2. Зловмисник надсилає команду через захищений канал зараженим комп'ютерам для здійснення атаки на вибрану жертву. Пакети трафіку атаки можуть містити фальшиву IP-адресу джерела, що

ускладнює ідентифікацію комп'ютерів, що атакують, жертвою. Кількість керованих агентів, які беруть участь у DDoS-атаці, може варіюватися від кількох десятків до десятків тисяч скомпрометованих машин.

Розподілені атаки на відмову мають кілька особливостей, які притаманні тільки їм:

1. Обсяг трафіку розподіленої атаки настільки великий, що може перевантажити можливості більшості корпоративних Інтернет-з'єднань.

2. При розподіленій атаці пакети трафіку надходять з різних джерел, що знаходяться в різних географічних регіонах. Це значно ускладнює процес відстеження IP-адрес, з яких відбувається атака.

3. Шкідливий трафік може мало відрізнятися від звичайного, що ускладнює фільтрацію фальшивих пакетів без шкоди для звичайних користувачів. Таким чином, трафік розподіленої атаки може виглядати цілком «легітимним», що додатково ускладнює завдання виявлення та відсіювання шкідливого трафіку.

Варто зазначити, що атаки такого типу подібні до явища, відомого як «скупчення» (flash crowd), яке виникає тоді, коли велика кількість звичайних користувачів одночасно звертається до сервера. Однак, для успішної розподіленої атаки необхідна значна кількість джерел трафіку, зазвичай на рівні декількох тисяч. [1]

Надалі в роботі буде розглядатися саме цей вид атак.

1.1.3 Віддзеркалені розподілені атаки на відмову

Розподілена віддзеркалена атака відмови в обслуговуванні(Distributed Reflective Denial of Service) — це розширена форма DDoS-атаки, в якій зловмисники використовують вразливість у протоколах мережі або серверів, щоб надсилати запити на велику кількість вузлів-ампліфікаторів і перенаправляти їх до жертви. DRDoS-атаки є особливо ефективними, оскільки зловмисники можуть значно збільшити обсяг трафіку, і тим самим підсилити ефект атаки.

У DRDoS-атаках використовуються так звані «ампліфікатори» — це сервери або пристрої, які можуть надсилати відповідь на запит більшого розміру, ніж початковий. Зловмисники виконують спуфінг пакетів, використовуючи IP-адресу жертви, як адресу відправки. Це призводить до того, що велика кількість відповідей, багато разів більша, ніж початковий запит, спрямовується на цільову жертву, перевантажуючи її мережу та сервери та викликаючи перебої в обробці легітимного трафіку, що призводить до відмови в обслуговуванні.

До того ж сервери не зберігають інформацію, яка стосується користувачів, що звертаються до них із запитом. Зупинка даного сервісу також виявляється неможливою, через його широке використання значною кількістю звичайних користувачів. Залежно від наявних ресурсів і обсягу запитів цих серверів, можливо попередити віддзеркалену атаку шляхом обмеження кількості відповідей на конкретну адресу. Але варто відзначити, що такий підхід передбачає необхідність зберігання певної інформації в пам'яті, а це потенційно може призвести до значних навантажень на ресурс.[1]

Типова віддзеркалена атака описана в [5].

1.2 Визначення боту та ботнету

Бот — це підконтрольний зловмиснику комп'ютер чи IoT пристрій.

Ботнет – це мережа комп'ютерів або пристроїв, що контролюється зловмисником і використовується для керування ботами.

Зазвичай ці комп'ютери або пристрої заражені шкідливим програмним забезпеченням, таким як віруси, троянські програми або черв'яки.

Здебільшого ботнети мають можливість підтримувати комунікаційний зв'язок зі зловмисником та виконувати різноманітні завдання, включаючи атаки на відмову. Для ефективного керування такими атаками використовується складна система параметрів, які

визначають частоту пересилки та розмір пакетів, використовуваних у процесі атаки.

Однією зі значущих характеристик ботнетів є їх здатність до оновлення програмного забезпечення через віддалений сервер. Цей механізм надає зловмиснику можливість додавати нові функціональні можливості та виправляти помилки у власному програмному коді. Наприклад, зловмисник може завантажувати нові механізми атаки на боти, що дозволяє гнучко реагувати на зміни у захисному забезпеченні жертви та забезпечувати керування атакою протягом її здійснення. [1]

Основними напрямками використання ботнет-мереж є: розсилання спаму, DDoS-атаки, крадіжка даних, розповсюдження шкідливого програмного забезпечення, викрадення обчислювальних ресурсів, фінансові шахрайства.

1.3 Інтернет речей як джерело розповсюдження ботнету

Інтернет речей (Internet of Things) — це концепція, що визначає підключення до Інтернету фізичних об'єктів, які зазвичай не мають здатності до мережевого зв'язку. Ці об'єкти можуть бути різного типу, наприклад, побутові пристрої, електроніка, сенсори, транспортні засоби, медичні пристрої, промислове обладнання та багато інших.

Головна ідея за концепцією IoT полягає в тому, щоб забезпечити цим об'єктам можливість обміну даними та взаємодії через мережу Інтернет. Це дозволяє збирати, обробляти і аналізувати великі обсяги даних з різних джерел, що дозволяє здійснювати розумний аналіз та приймати відповідні рішення на основі цих даних.

Однак, впровадження IoT також вносить виклики та проблеми щодо приватності та безпеки.

Недостатньо захищені пристрої Інтернету речей відіграють роль потенційних точок входу для кібератак, що дозволяє зловмисникам вплинути на пристрій шляхом перепрограмування або спричинення його

неправильної роботи. Недосконало спроєктовані пристрої можуть насамперед загрожувати безпеці користувачів, піддаючи їхні особисті дані ризику крадіжки, оскільки потоки цих даних не належним чином захищені. Крім того, пристрої, що несправні або некоректно функціонують, можуть створювати вразливості, які можуть бути використані для порушення безпеки системи. [2]

Дані проблеми мають однакову актуальність як для невеликих, доступних та широко поширених смартпристроїв в Інтернеті речей, так і для комп'ютерів, що традиційно виступають як кінцеві точки підключення до Інтернету. Вартість і технічні обмеження пристроїв IoT, зумовлені конкурентним середовищем, змушують виробників розробляти адекватні механізми безпеки для цих пристроїв. Однак це створює потенційні вразливості щодо безпеки та тривалості підтримки, які можуть бути більш значущими порівняно з їхніми традиційними комп'ютерними аналогами.

Поряд з можливими недоліками в проєктуванні систем безпеки, саме зростання кількості та різноманітності пристроїв Інтернету речей може збільшити потенційні можливості для атак. У поєднанні зі складною взаємозалежністю між пристроями Інтернету речей, кожен недостатньо захищений пристрій, підключений до мережі, може потенційно впливати на безпеку та стійкість Інтернету на глобальному рівні, а не лише в локальному середовищі. Наприклад, холодильник або телевізор у США, заражені шкідливим програмним забезпеченням, можуть використовувати домашнє Wi-Fi з'єднання власника для надсилання тисяч шкідливих електронних листів зі спамом отримувачам по всьому світу. [16]

1.4 Епідемічні моделі як інструмент дослідження DDoS-атак

Епідемічні моделі є відомим інструментом для дослідження DDoS-атак. Вони дозволяють змоделювати процес інфікування пристроїв та їх подальшу участь у ботнеті, який потім може бути використаний для запуску розподілених атак відмови в обслуговуванні. Зазначені моделі спрямовані на вивчення динаміки поширення атаки в мережі та її впливу на кілька мережевих пристроїв, таких як хости, маршрутизатори або сервери, які надалі стануть джерелами атаки. [3]

Вони мають ряд переваг, наприклад:

1. **Аналогія зі швидким поширенням хвороби**. Епідемічні моделі в основі мають принципи поширення захворювання в популяції. Це дає можливість досліджувати DDoS-атаки як «інфекційні» процеси, де «зараження» відбувається шляхом передачі трафіку між комп'ютерами чи мережевими вузлами. Такий підхід дозволяє розуміти швидкість та масштаб поширення атаки.

2. **Моделювання поведінки атаки**. Епідемічні моделі дозволяють відтворювати та аналізувати поведінку DDoS-атаки в часі. Це дозволяє з'ясувати, як швидко атака розповсюджується, які вузли стають її джерелами та як атака впливає на роботу мережі. Такі візуалізації та аналізи допомагають зрозуміти особливості атаки та розробити ефективні заходи протидії.

3. **Тестування заходів протидії**. За допомогою епідемічних моделей можна провести численні симуляції та експерименти для оцінки ефективності різних заходів протидії DDoS-атакам. Наприклад, можна випробувати різні алгоритми виявлення атаки чи методи блокування шкідливого трафіку. Такі дослідження допомагають розробити та оптимізувати алгоритми захисту.

4. **Валідація заходів захисту**. Епідемічні моделі можуть бути

використані для валідації та перевірки ефективності розроблених заходів захисту в реальному часі. Це дозволяє перевірити, як добре застосовані заходи протидії працюють під час симуляцій атаки та виявляти можливі слабкі місця в системі захисту.

Згідно з науковими дослідженнями, епідемічні моделі пропонують гіпотезу, що збільшена кількість заражених хостів сприяє вищій ймовірності успішної DDoS-атаки, оскільки такі атаки можуть генерувати більший обсяг трафіку. Таким чином, епідемічні моделі забезпечують кількісну оцінку впливу DDoS-атак, враховуючи швидкість поширення інфекції. [15]

Проте, варто відзначити, що епідемічні моделі мають свої обмеження. Наприклад, вони не є придатними для аналізу стійкості системи до атак. Попри це, можна стверджувати, що зниження швидкості поширення і покращення швидкості відновлення сприяють зменшенню ймовірності успіху атаки. [3]

Крім того, важливо відзначити, що епідемічні моделі, як системи диференційних рівнянь, можуть дати добрі результати в великому масштабі, що стосується загальної поведінки системи. Однак, вони можуть бути менш застосовними для аналізу невеликих локальних мереж або окремих хостів. [4]

Наведені у наступних пунктах моделі не є єдиними представниками цього класу, але саме вони лежать в основі даної роботи.

1.5 SIR-модель

Вперше описана Кермаком і МакКендріком у [7], дана модель розглядає поділ населення на три категорії: *сприйнятливі (S), інфіковані (I) та відновлені (R).* За припущенням, усі особи мають однакову схильність до захворювання, а імунітет досягається лише після повного одужання від інфекції. Тривалість захворювання дорівнює тривалості перебігу інфекції зі сталими темпами передачі та одужання. [6]

1.5.1 SIR-модель без життєвої динаміки

Для закритої популяції розміром N робиться припущення, що змішування індивідів є однорідним і виконується закон масової дії. Крім того, для великих класів інфекційних захворювань більш реалістично розглядати силу інфекції, яка залежить від частки інфікованого населення стосовно до загальної постійної популяції N, а не від абсолютної кількості інфікованих суб'єктів. Виходячи з цього припущення, стандартний рівень захворюваності визначається як $\frac{\beta SI}{N}$, а загальний рівень одужання - як γI.

З урахуванням цього, можна записати систему диференційних рівнянь (1.1), яку ілюструє Рис. 1.1:

$$\begin{aligned} \frac{dS}{dt} &= -\frac{\beta S}{N} \\ \frac{dI}{dt} &= \frac{\beta S}{N} - \gamma I \\ \frac{dR}{dt} &= \gamma I \end{aligned} \tag{1.1}$$

Де β — інтенсивність контакту, γ — інтенсивність відновлення, $S + I + R = N$.

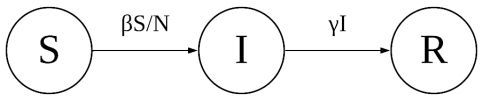

Рисунок 1.1 – SIR-модель без життєвої динаміки

Наявність епідемії визначається значенням $R_0 = \frac{\beta}{\gamma}$ — базового коефіцієнту розмноження. Епідемія наявна при $R_0 > 1$, коли при $R_0 < 1$ вона не спостерігається. [6]

1.5.2 SIR-модель з життєвою динамікою

Якщо систему (1.1) переписати з урахуванням постійних показників народжуваності та смерті, то отримаємо систему (1.2), яку ілюструє Рис. 1.2:

$$\begin{aligned} \frac{dS}{dt} &= bN - \frac{\beta S}{N} - \mu S \\ \frac{dI}{dt} &= \frac{\beta S}{N} - (\gamma + \mu) I \\ \frac{dR}{dt} &= \gamma I - \mu R \end{aligned} \tag{1.2}$$

Тут μ — коефіцієнт смертності, а b — коефіцієнт народжуваності. Так як середній час інфікування займає $\frac{1}{\gamma+\mu}$ та інфіковані особи заражають інших з коефіцієнтом β, то базовий коефіцієнт розмноження визначається $\frac{\beta}{\gamma+\mu}$. [6]

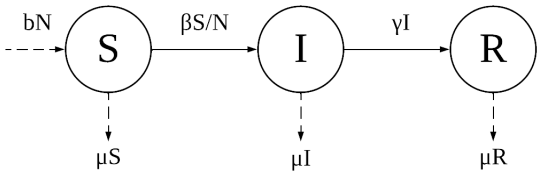

Рисунок 1.2 – SIR-модель з життєвою динамікою

1.6 SIS-модель

Випадки, коли після одужання представник популяції знову повертається до сприйнятливого класу, описуються моделлю *SIS(сприйнятливий-інфікований-сприйнятливий)*.

У цьому підрозділі визначення коефіцієнтів і базового коефіцієнту розмноження аналогічно до попереднього.

1.6.1 SIS-модель з життєвою динамікою

При $b \neq \mu$ і $S + I = N$ система (1.3) враховує показники народжуваності та смерті, вона ілюструється Рис. 1.3 [6]

$$\begin{aligned} \frac{dS}{dt} &= bN + \gamma I - \frac{\beta S}{N} - \mu S \\ \frac{dI}{dt} &= \frac{\beta S}{N} - (\gamma + \mu) I \end{aligned} \tag{1.3}$$

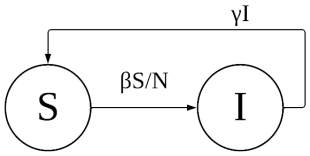

Рисунок 1.3 – SIS-модель з життєвою динамікою

1.6.2 SIS-модель без життєвої динаміки

Якщо ми розглядаємо випадок, коли популяція незмінна, то модель описується системою диференційних рівнянь (1.3) з $b = \mu$. Вона ілюструється Рис. 1.4 [6]

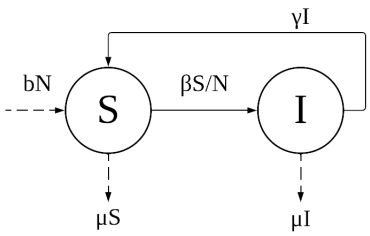

Рисунок 1.4 – SIS-модель з життєвою динамікою

Висновки до розділу 1

У цьому розділі наведено опис теоретичного підґрунтя, що необхідне для розуміння тематики дослідження. Наприклад: класифікація атак відмов в обслуговуванні, перелік основних епідемічних моделей.

2 ПОБУДОВА МОДЕЛЕЙ

У цьому розділі описані математична модель розповсюдження ботнету на основі епідемічного моделювання, її розширення з урахуванням фізичного впливу, математична модель атаки на кіберфізичну систему за допомогою ботнету, сформованого з IoT пристроїв.

2.1 SIR-подібна епідемічна модель розповсюдження ботнету

Для моделювання розповсюдження ботнету обрано SIR-подібну модель, оскільки, поведінка шкідливого ПЗ з функцією саморозповсюдження (wormable malware) подібна до поведінки вірусів в популяції людей.

За основу було взяту модель, запропоновану в [8]. Її особливість полягає в тому, що модель розглядає два рівні захисту(низький і високий), а при відновленні вузли підвищують свій рівень захисту та більше не повертаються до попереднього. Це є більш реалістичним сценарієм поведінки у порівнянні з попередніми відомими роботами, де відновлені вузли лишалися на тому ж рівні захисту.

Розглядаємо замкнуту мережу, де кількість учасників (хостів) мережі незмінна. Відповідно, $S(t)+I(t)+R(t) = N$ для будь-якого моменту часу t, де N — загальна кількість хостів в мережі.

Мережа складається з двох підмножин: *та, що атакує (attack)*, і *цільова (target)*.

Сприйнятливі хости — вразливі комп'ютери, сервери, IoT пристрої в мережі, що можуть бути інфіковані.

Інфіковані хости — елементи мережі, що заражені шкідливим ПЗ і є членами ботнету. Через них відбувається поширення шкідливого ПЗ.

Відновлені хости — елементи мережі, що були членами ботнету, але є з нього вилученими (на карантині, видалені, запатчені).

Відповідно розглядаємо три змінні в залежності від часу (кількості ітерацій — якщо розглядати дискретні проміжки часу):

1. Частка сприйнятливих елементів мережі $S(t)$;
2. Частка заражених $I(t)$;
3. Частка відновлених (вилікуваних) $R(t)$.

Частку сприйнятливих хостів популяції, що атакує, позначимо $S_a(t)$, інфікованих хостів — $I_a(t)$. Причому $S_a(t) + I_a(t) = 1$.

Цільова популяція хостів мережі поділяється на дві підгрупи:

1. *Слабко захищені* (засоби безпеки не застосовуються або некоректно налаштовані). Позначимо їх відповідно $S_{low}(t)$, $I_{low}(t)$, $R_{low}(t)$.

2. *Добре захищені* (засоби безпеки впроваджені, але присутні вразливості). Позначимо їх відповідно $S_{high}(t)$, $I_{high}(t)$, $R_{high}(t)$.

Причому $S_{low}(t) + I_{low}(t) + R_{low}(t) + S_{high}(t) + I_{high}(t) + R_{high}(t) = 1$.

$$
\begin{aligned}
\frac{dS_a}{dt} &= \mu - \beta S_a I_a - \mu S_a + \xi I_a \\
\frac{dI_a}{dt} &= \beta S_a I_a - (\xi + \mu) I_a \\
\frac{dS_{low}}{dt} &= -\lambda S_{low} \\
\frac{dI_{low}}{dt} &= \lambda S_{low} - \gamma_{low} I_{low} \\
\frac{dR_{low}}{dt} &= \lambda_{low} I_{low} - \xi_{low} R_{low} \\
\frac{dS_{high}}{dt} &= -\lambda(1-\varepsilon) S_{high} + \xi_{high} R_{high} + \xi_{low} R_{low} \\
\frac{dI_{high}}{dt} &= \lambda(1-\varepsilon) S_{high} - \gamma_{high} I_{high} \\
\frac{dR_{high}}{dt} &= \gamma_{high} I_{high} - \xi_{high} R_{high}
\end{aligned}
\tag{2.1}
$$

Схема моделі наведена на рис. 2.1. Значення параметрів наступні:

1) μ — коефіцієнт набору в ботнет;

2) η — параметр модифікації, який враховує передачу атаки заражених цільових вузлів для припущеного скорочення (у відсіках I_{low}, I_{high});

3) β — швидкість поширення шкідливого ПЗ;

4) γ — коефіцієнт відновлення (вилучення) атакованих хостів;

5) ξ — відновлення хостів цільової мережі, які переходять у сприйнятливий стан;

6) ε — рівень кібербезпеки цільової мережі;

7) σ — кінетичний вплив на цільову мережу.

Сприйнятливі вузли цільової системи можуть бути атаковані при рівні $\lambda = \beta(I_a + \eta(I_{high} + I_{low}))$.

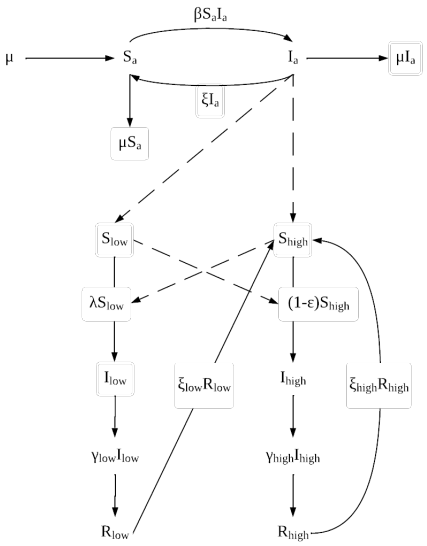

Рисунок 2.1 – SIR-подібна епідемічна модель розповсюдження ботнету

Базовий коефіцієнт розмноження для всієї моделі R_0 визначається як максимальний базовий коефіцієнт розмноження слабко захищеної цьової популяції $R_{0low} = \frac{\beta}{\gamma_{low}}$, сильно захищеної цільової популяції $R_{0high} = \frac{\beta(1-\varepsilon)}{\gamma_{high}}$ і популяції, що атакує, $R_{0a} = \frac{\beta}{\xi+\mu}$.

Рівняння системи показують:

1. **Зміну кількості вразливих хостів в мережі із часом** — залежить від кількості контактів між вразливими та інфікованими хостами мережі (ботами), а також від швидкості розповсюдження шкідливого ПЗ.

2. **Зміну кількості інфікованих хостів (ботів)** — є різницею між новими інфікованими хостами та тими, що відновлені.

3. **Приріст відновлених (видалених з ботнета) хостів** пропорційний кількості інфікованих (коефіцієнт відновлення є константою).

2.2 Розширення моделі до урахування фізичного впливу

За схемою з [9] перепишемо систему рівнянь з урахуванням життєвої динаміки. Уведемо у систему новий параметр σ, який показує зовнішній фізичний вплив на елементи системи. Тоді система (2.1) буде мати вигляд:

$$\begin{aligned}
\frac{dS_a}{dt} &= \mu - \beta S_a I_a - \mu S_a + \xi I_a \\
\frac{dI_a}{dt} &= \beta S_a I_a - (\xi + \mu) I_a \\
\frac{dS_{low}}{dt} &= -(\lambda + \sigma_{low}) S_{low} \\
\frac{dI_{low}}{dt} &= \lambda S_{low} - (\gamma_{low} + \sigma_{low}) I_{low} \\
\frac{dR_{low}}{dt} &= \lambda_{low} I_{low} - \xi_{low} R_{low} \\
\frac{dS_{high}}{dt} &= -\lambda(1-\varepsilon) S_{high} + \xi_{high} R_{high} + \xi_{low} R_{low} - \sigma_{high} S_{high} \\
\frac{dI_{high}}{dt} &= \lambda(1-\varepsilon) S_{high} - (\gamma_{high} + \sigma_{high}) I_{high} \\
\frac{dR_{high}}{dt} &= \gamma_{high} I_{high} - \xi_{high} R_{high}
\end{aligned} \tag{2.2}$$

2.3 Модель атаки на кіберфізичну систему за допомогою IoT-ботнету

У дослідженні [10] була розроблена подвійна епідемічна модель, яка враховує вплив внутрішніх і зовнішніх чинників. Перша складова моделі передбачає атаку на пристрої Інтернету речей (IoT) на основі моделі SIS і залучення зовнішніх вузлів. У цій частині дослідження вивчаються механізми, за допомогою яких зловмисники здійснюють компрометацію великої кількості пристроїв IoT з метою створення ботнету. Друга складова передбачає моделювання розподіленої атаки DDoS на цільові ресурси з використанням SIR-моделювання.

Мережа складається з двох підмножин: *та, що атакує (attack)*, і *цільова (target)*.

Сприйнятливі хости — вразливі комп'ютери, сервери, IoT пристрої в мережі, що можуть бути інфіковані.

Інфіковані хости — елементи мережі, що заражені шкідливим ПЗ і є членами ботнету та через яких відбувається подальше поширення шкідливого ПЗ.

Відновлені хости — елементи мережі, що були членами ботнету, але є з нього вилученими (на карантині, видалені, запатчені).

Зовнішні хости — це вузли або об'єкти, які знаходяться за межами цільової мережі і відповідають за запуск атак на мережу.

Відповідно розглядаємо чотири змінні в залежності від часу (кількості ітерацій — якщо розглядати дискретні проміжки часу):

1. Частка сприйнятливих елементів мережі $S(t)$
2. Частка заражених $I(t)$
3. Частка відновлених (вилікуваних) $R(t)$
4. Частка зовнішніх E(t)

Частку сприйнятливих хостів популяції, що атакує, позначимо $S_a(t)$, інфікованих — $I_a(t)$, зовнішніх — $E_a(t)$. Причому $S_a(t) + I_a(t) + E_a(t) = 1$.

Частку сприйнятливих хостів цільової популяції позначимо $S_t(t)$, інфікованих — $I_t(t)$, одужалих — $R_t(t)$. Причому $S_t(t) + I_t(t) + R_t(t) = 1$.

У результаті, маємо систему диференціальних рівнянь (2.3):

$$\begin{aligned}
\frac{dS_t}{dt} &= -\beta S_t I_a + \xi_t \\
\frac{dI_t}{dt} &= \beta S_t I_a - \gamma I_t \\
\frac{dR_t}{dt} &= \gamma I_t - \xi_t R_t \\
\frac{dS_a}{dt} &= -\beta S_a I_a - \mu S_a + \xi_a I_a + \rho E_a - \alpha S_a \\
\frac{dI_a}{dt} &= \beta S_a I_a - \mu I_a - \xi_a I_a - \alpha S_a \\
\frac{dE_a}{dt} &= \alpha S_a + \alpha I_a - \rho E_a + \mu - \mu E_a
\end{aligned} \tag{2.3}$$

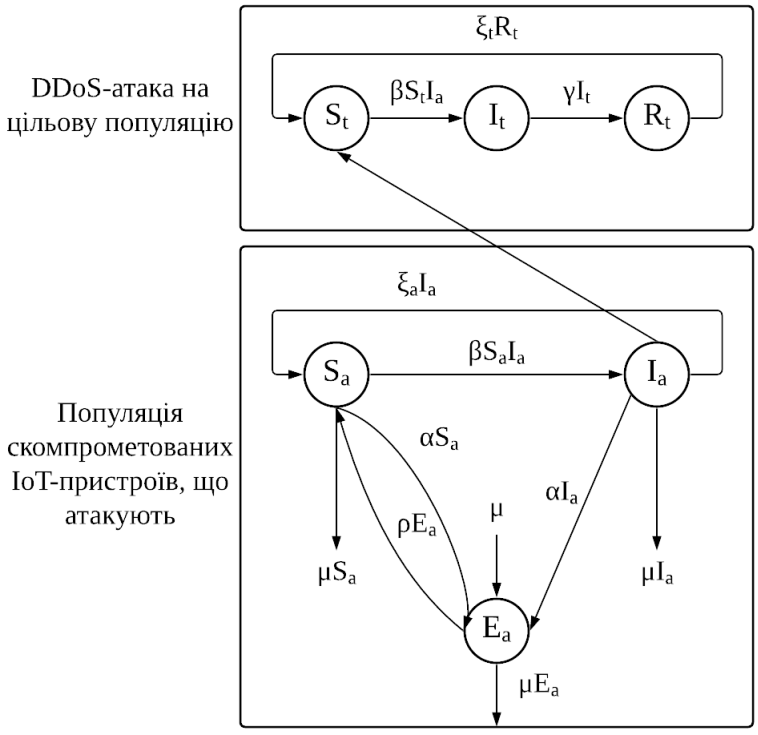

Рисунок 2.2 – Модель атаки за допомогою ботнету, сформованого з IoT пристроїв

Значення параметрів наступні:

1) β — швидкість поширення шкідливого ПЗ;

2) γ — швидкість відновлення інфікованих цільових вузлів;

3) ξ — швидкість, з якою відновлені вузли стають вразливими;

4) α — швидкість відключення від інтернету вузлів, що атакують (після чого вони приєднуються до зовнішніх вузлів, що атакують);

5) ρ — швидкість підключення до інтернету зовнішніх вузлів (після чого вони приєднуються до вразливих вузлів, що атакують);

6) μ — природна смертність і народжуваність вузлів, що атакують.

Базовий коефіцієнт розмноження для цієї моделі $R_0 = \sqrt{\frac{\beta^2}{(\mu+\xi_a+\alpha)\gamma}}$.

Висновки до розділу 2

У цьому розділі описані з усіма необхідними поясненнями та викладками:

1. Математична модель розповсюдження ботнету на основі епідеміологічного моделювання.

2. Розширення цієї моделі з урахуванням фізичного впливу.

3. Математична модель атаки на кіберфізичну систему за допомогою ботнету, сформованого з IoT пристроїв.

Наведені всі значення параметрів, а також схематичні ілюстрації моделей.

3 ЧИСЕЛЬНІ ЕКСПЕРИМЕНТИ

У цьому розділі будуть проведені чисельні експерименти з моделями (2.2) і (2.3), дослідження впливу вагомих коефіцієнтів системи (2.2) на поведінку розв'язку, а також порівняння моделей.

3.1 SIR-подібна модель з урахуванням фізичного впливу

Наступний приклад ілюструє графічний розв'язок системи (2.2). Графіки моделі наведені на Рис. 3.1

Початкові умови:

$(S_a(0), I_a(0), S_{low}(0), I_{low}(0), R_{low}(0), S_{high}(0), I_{high}(0), R_{high}(0)) =$

$= (0.875, 0.125, 0.375, 0.125, 0, 0.375, 0.125, 0)$

Значення коефіцієнтів задані наступним чином:

$(\beta, \varepsilon, \eta, \gamma_{low}, \gamma_{high}, \xi_{low}, \xi, \xi_{high}, \mu, \sigma_{low}, \sigma_{high}) =$

$= (0.495, 0.61, 0.5, 0.0401, 0.0401, 0.055, 0.134, 0.4, 0.07005, 0.03, 0.0001)$

Базовий коефіцієнт розмноження для моделі $R_0 \approx 12.34$, що свідчить про високий рівень епідемії.

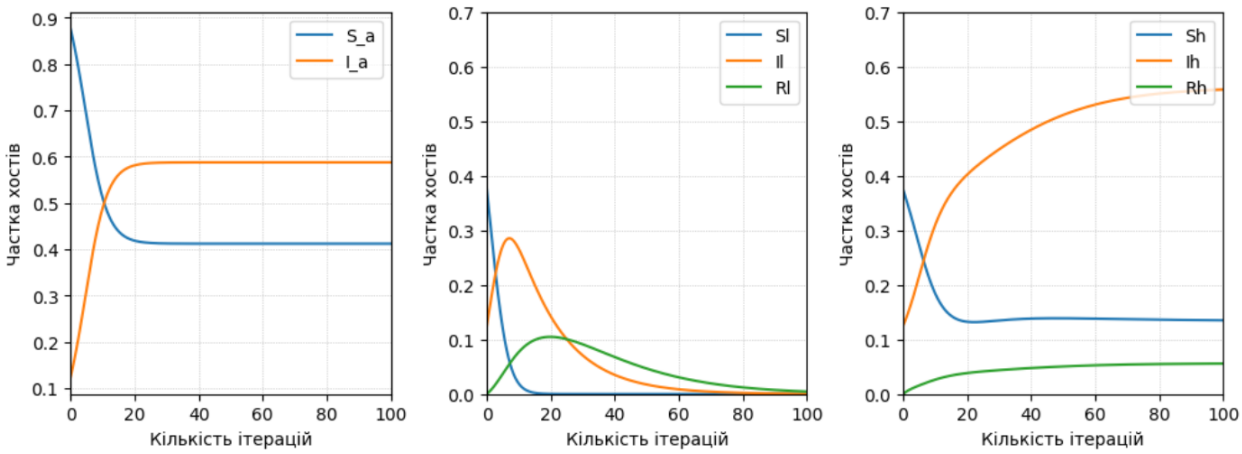

Рисунок 3.1 – Модель атаки за допомогою ботнету, сформованого з IoT пристроїв

Система демонструє очікувану поведінку: хости переходять у стан кращого захисту, тобто поступово впроваджуються захисні механізми та закриваються вразливості, що призводили до атаки.

3.2 Вплив основних коефіцієнтів на модель

Найбільш важливими для дослідження моделі (2.2) є коефіцієнти:

1) β — швидкість поширення шкідливого ПЗ;

2) ε — рівень кібербезпеки цільової мережі;

3) σ — кінетичний вплив на цільову мережу.

Наступні підпункти описують вплив цих параметрів на поведінку системи.

3.2.1 Вплив швидкості поширення шкідливого ПЗ

Швидкість поширення програмного забезпечення прямим чином впливає на наявність і перебіг епідемії у системі.

Наприклад, при максимальному значенні $\beta = 1$ можна спостерігати різкий спалах зараження в цільовій популяцій. Популяція, що атакує, при цьому, складається майже лише з заражених вузлів (Рис. 3.2).

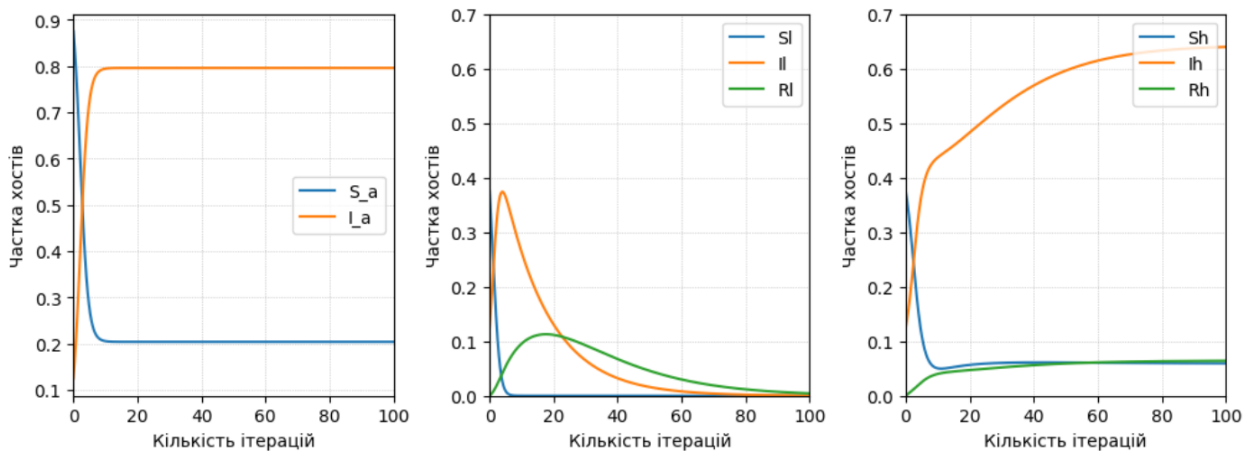

Рисунок 3.2 – Рішення системи (2.2) для $\beta = 1$

При значенню, трохи менше за середнє, $\beta = 0.405$, спостерігається плавний перебіг епідемії, без різкого підвищення рівня захворюваності та великої кількості інфікованих хостів. При цьому, не спостерігається тенденції до того, що епідемія припиниться сама собою (Рис. 3.4).

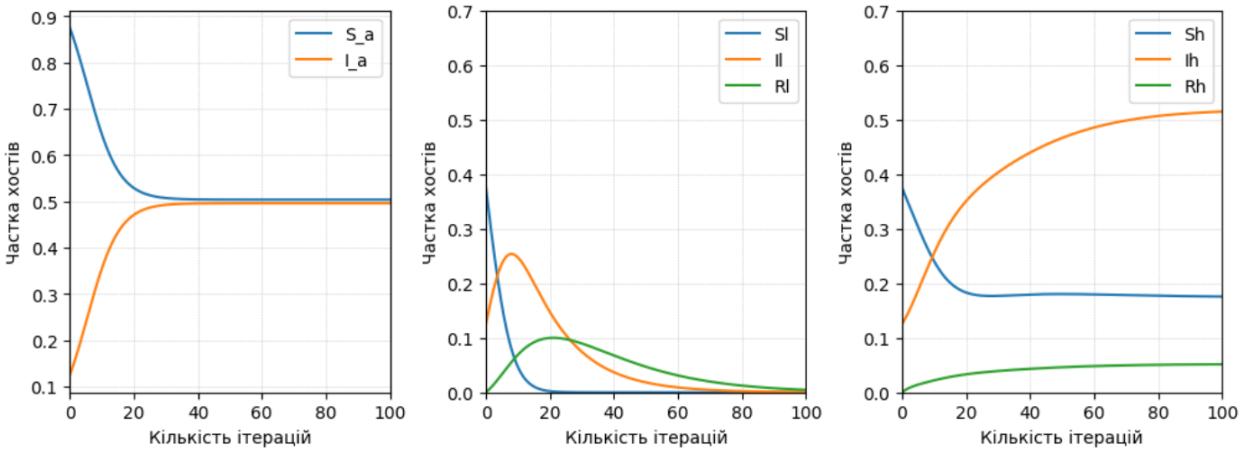

Рисунок 3.3

Рисунок 3.4 – Рішення системи (2.2) для $\beta = 0.405$

При значенні коефіцієнту, що близьке до 0 ($\beta = 0.1$) можемо бачити відсутність захворюваності взагалі, попри $R_0 \approx 2.5 > 1$ (Рис. 3.5).

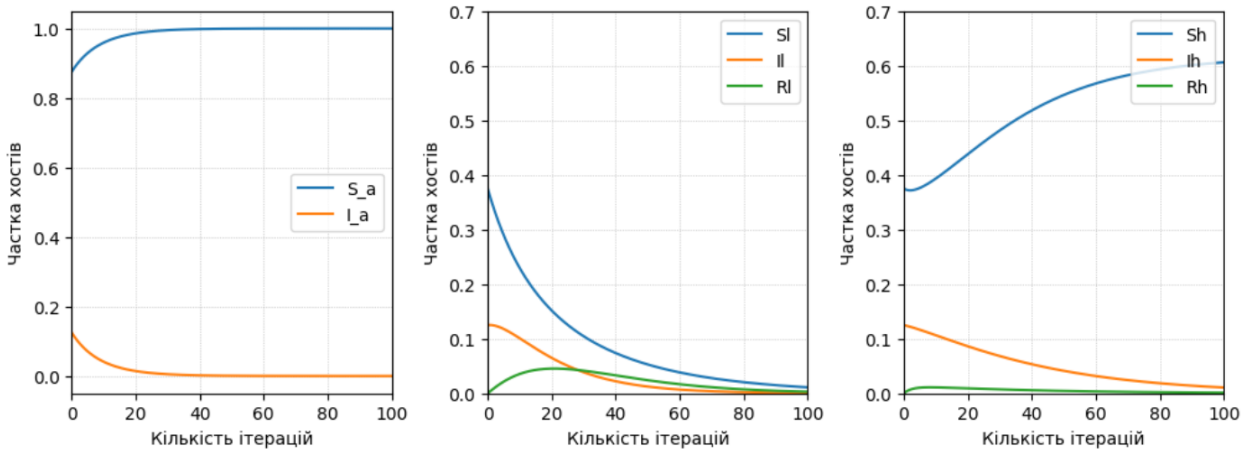

Рисунок 3.5 – Рішення системи (2.2) для $\beta = 0.1$

3.2.2 Вплив рівня кібербезпеки цільової мережі

Рівень кібербезпеки цільової мережі ε впливає на ефективність атаки на систему. Наприклад, на максимальному рівні захисту $\varepsilon = 1$, попри наявність значної кількості інфікованих вузлів у популяції, що атакує, а також значенню $R_0 \approx 12.34 > 1$ можна спостерігати відсутність епідемії. (Рис. 3.6)

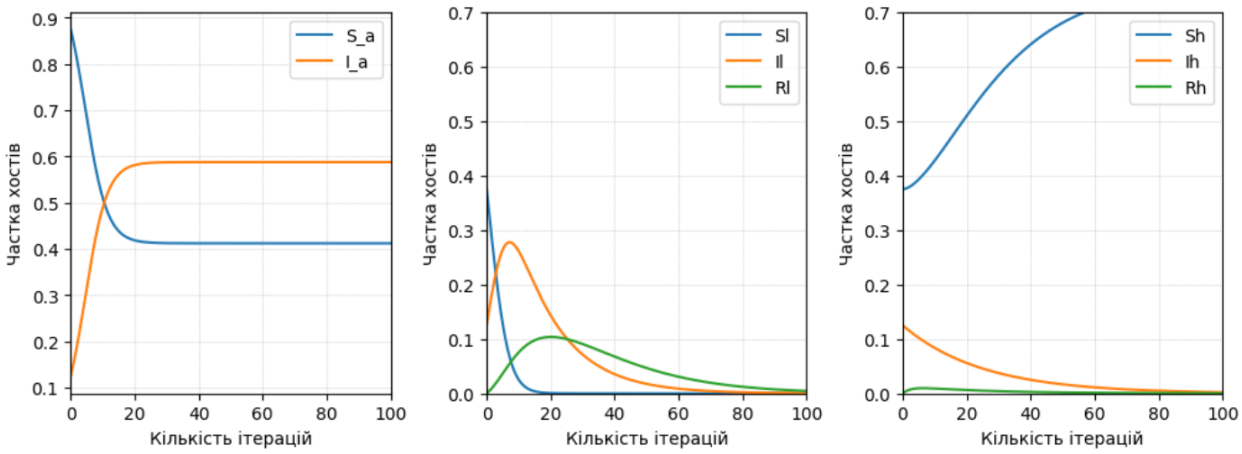

Рисунок 3.6 – Рішення системи (2.2) для $\varepsilon = 1$

При значенні, що близьке до 0 ($\varepsilon = 0.1$) можна прослідкувати різкий спалах захворюваності (Рис. 3.7).

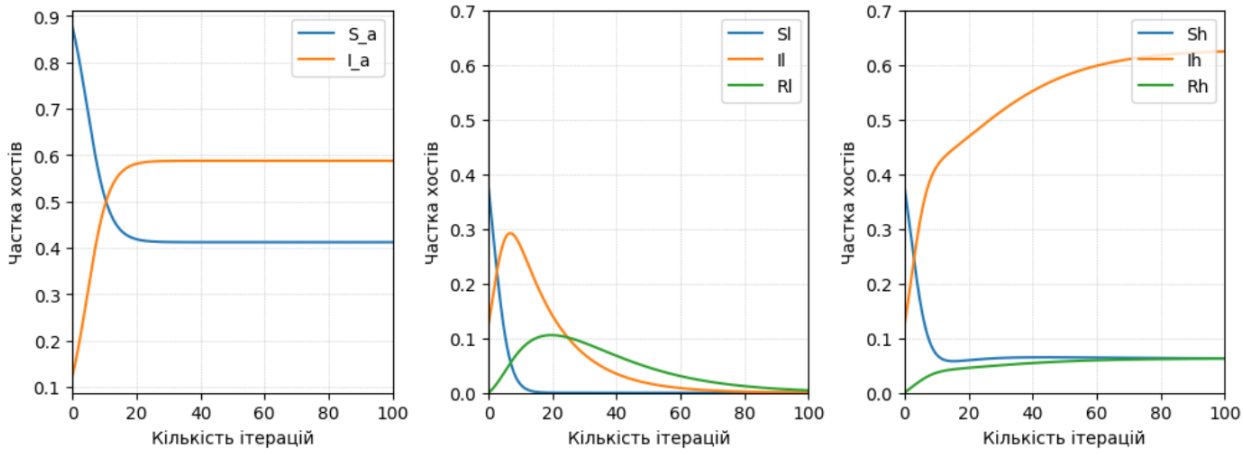

Рисунок 3.7 – Рішення системи (2.2) для $\varepsilon = 0.1$

3.2.3 Кінетичний вплив на цільову мережу

Загальна тенденція полягає в тому, що чим більший вплив фізичної атаки, тим гірше проходить кібератака.

Рис. 3.8 – Рис. 3.9 ілюструють це твердження для σ_{high}.

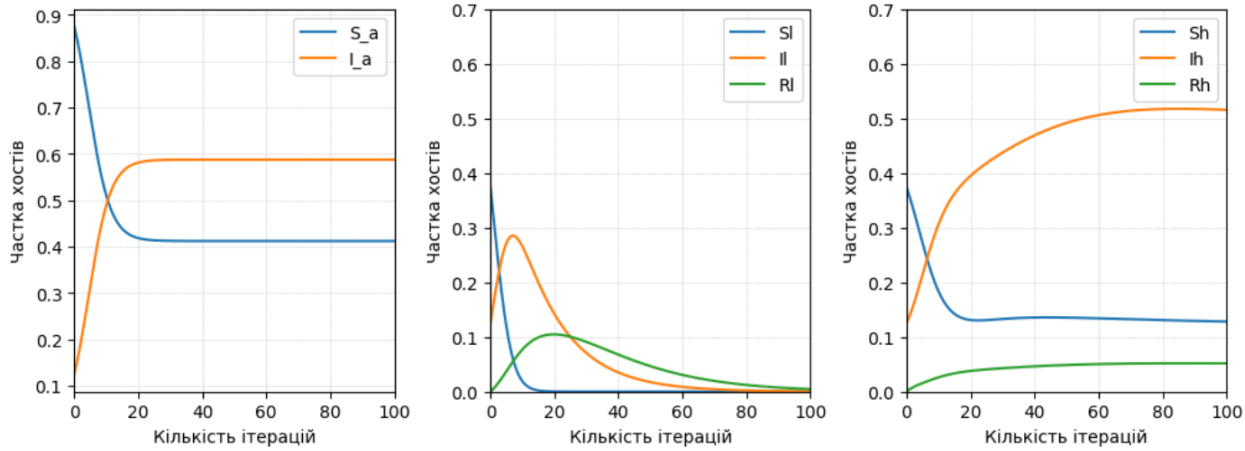

Рисунок 3.8 – Рішення системи (2.2) для $\sigma_{high} = 0.001$

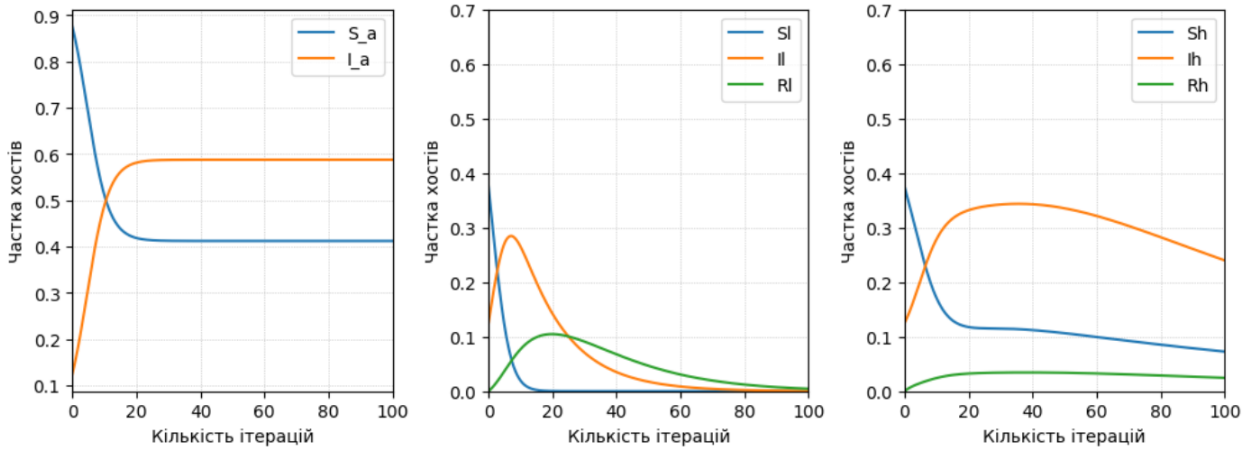

Рисунок 3.9 – Рішення системи (2.2) для $\sigma_{high} = 0.1$

Рис. 3.10 – Рис.3.11 ілюструють це твердження для σ_{low}.

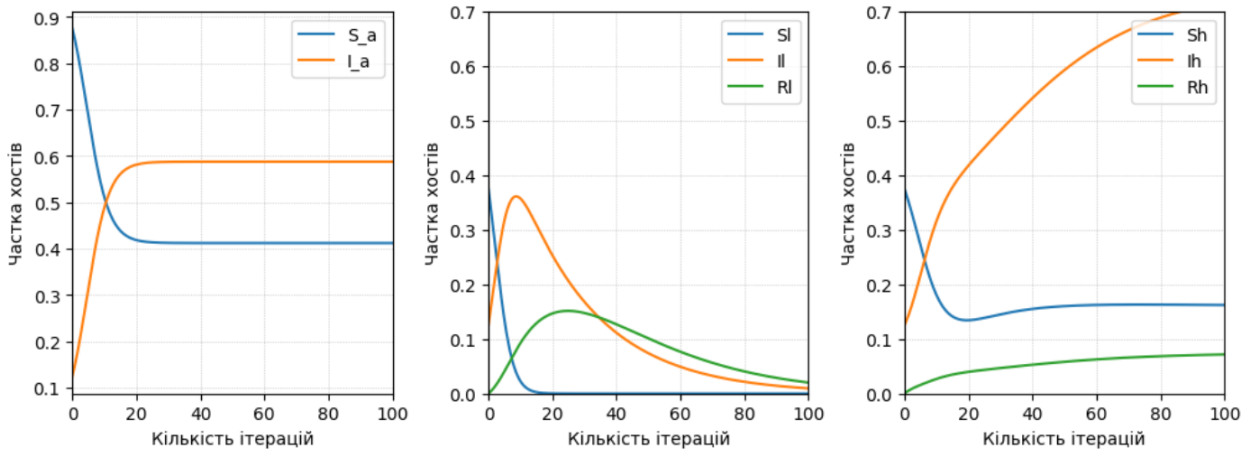

Рисунок 3.10 – Рішення системи (2.2) для $\sigma_{low} = 0.001$

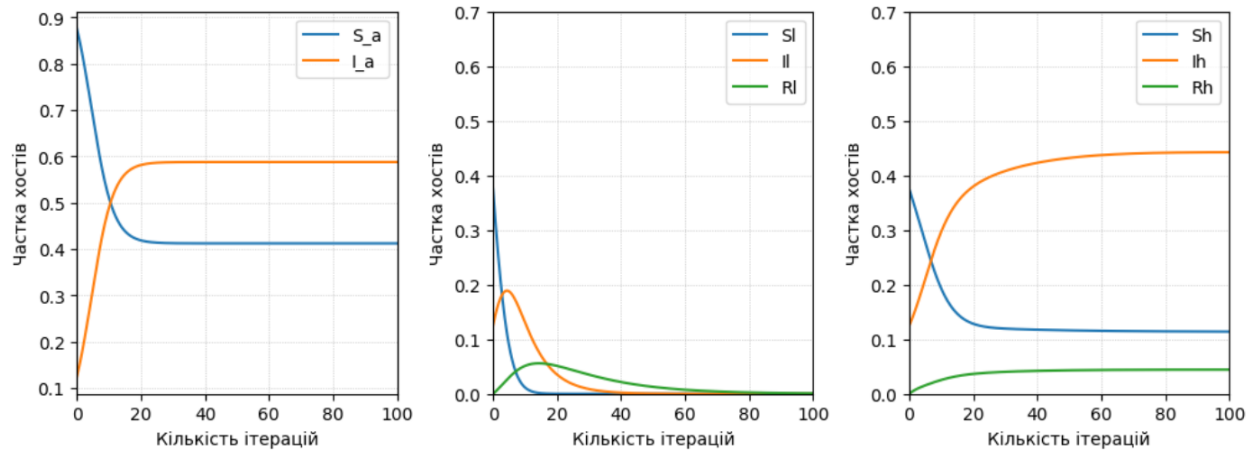

Рисунок 3.11 – Рішення системи (2.2) для $\sigma_{low} = 0.1$

3.3 Модель атаки на кіберфізичну систему за допомогою IoT-ботнету

Наступний приклад ілюструє графічний розв'язок системи (2.3).

Початкові умови:

$(S_t(0), I_t(0), R_t(0), S_a(0), I_a(0), E_a(0)) = (0.75, 0.25, 0, 0.125, 0, 0.65, 0.2, 0.15)$

Значення коефіцієнтів задані наступним чином:

$$(\beta, \xi_t, \gamma, \mu, \xi_a, \rho, \alpha) = (0.495, 0.134, 0.0401, 0.07005, 0.005, 0.2, 0.1)$$

Базовий коефіцієнт розмноження для моделі $R_0 \approx 8.48$, що свідчить про високий рівень епідемії.

Розв'язок моделі наведений на Рис. 3.12:

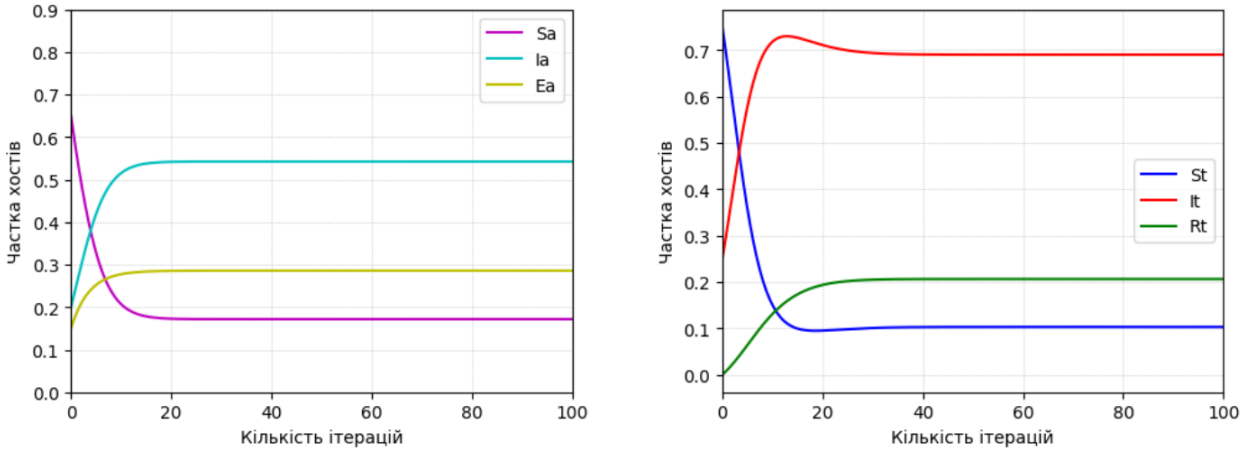

Рисунок 3.12 – Модель атаки на систему за допомогою IoT-ботнету

Модель демонструє цікаву поведінку. Попри швидкий рівень зараження хостів і, у цілому, успішну кібератаку, після досягнення пікової точки, епідемія перестає розвиватися в часі. З одного боку, це добре, бо ми точно знаємо, що кількість інфікованих хостів не буде збільшуватись. З іншого, це погано, бо неможливого казати про те, що епідемія припиниться сама по собі.

3.4 Порівняння моделей

З графіків видно, що після додавання кінетичного впливу зріст кількості атакованих хостів порівняно зменшився, що свідчить про те, що фізична атака заважає проведенню кібератаки.

Досліджені моделі демонструє, що фізичні кінетичні атаки обмежують створення ботнету. З одного боту фізичні атаки можуть

призвести до незворотної втрати доступу для цільової системи (атака успішна), але з іншого боту це негативно впливає на потужність атаки відмови в обслуговуванні. Загалом, розроблена та досліджена модель забезпечує основу для розуміння процесу розгортання ботнету і вплив захисних механізмів цільових систем на це.

Висновки до розділу 3

У цьому розділі були проведені чисельні експерименти з метою дослідити та порівняти дві моделі атак відмови в обслуговуванні на критичну інфраструктуру. У першій моделі враховується вплив фізичної атаки на систему, у другій маємо кібератаку за звичайних умов. Отримані результати в ході досліджень кажуть про те, що фізична атака заважає проведенню кібератаки.

ВИСНОВКИ

У роботі виконано розробку, дослідження та порівняння моделей атак відмови в обслуговуванні на кіберфізичні системи. Порівняння відбувалося між моделлю атаки відмови в обслуговуванні на критичну інфраструктуру, яка враховує фізичний вплив, і моделлю атаки на критичну інфраструктуру за звичайних умов.

Отримані результати свідчать про те, що фізична така заважає проведенню кібератаки, і чим більший кінетичний вплив, тим менша потужність атаки відмови в обслуговуванні.

Робота допомагає оцінити вплив фізичних атак на ефективність розподільних атак відмов в обслуговуванні на критичну інфраструктуру, що надалі можна застосовувати для покращення стратегій захисту або використовувати для точнішого планування кібератак.

У подальших дослідженнях можливі такі напрямки роботи:

1. Об'єднання моделей, що розглядалися в даній роботі з метою отримати опис поведінки розподіленої атаки відмови в обслуговуванні на системи критичної інфраструктури за допомогою ботнету, сформованого з IoT пристроїв, що мають два рівні захисту.

2. З метою отримання більш деталізованої карти динаміки атак і захисту, модель може бути розширена до врахування топології мережі та зв'язків між хостами.

3. Застосування моделі для розробки більш досконалих стратегій атаки на мережу, а також захисту від подібних атак відмови в обслуговуванні.

ПЕРЕЛІК ПОСИЛАНЬ

1. Ігнатенко О. Атаки на відмову: виникнення проблеми, огляд атак, класифікація./ Ігнатенко О. – Ін-т програмних систем, 2008.—32 с. – 9-13 с.

2. Rose K. The internet of things: An overview/K. Rose, S. D. Eldridge, L. Chapin// The internet society (ISOC) – 2015 – 20-21pp.

3. Balarezo J. F. A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks/ J. F. Balarezo, W. Song, K. Gomez Chavez, A. Al-Hourani, S. Kandeepan// Engineering Science and Technology, an International Journal – 2022, 31, 101065

4. Дякуненко М. С., Стьопочкіна І. В. Моделювання процесів розповсюдження шкідливого ПЗ в мережі інтернет // Теоретичні і прикладні проблеми фізики, математики та інформатики: матеріали XIX Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених (13-14 травня 2021 р., м. Київ, Україна). с. 212-215

5. Parxson V. An analysis of using reflectors for distributed denial-of-service attacks / V. Parxson. – ACM SIGCOMM Computer Communication Review, Vol. 31, N 3, 2001, pp 38 – 47.

6. Deterministic Models in Epidemiology: From Modeling to Implementation/[A. Dadlani, R. O. Afolabi, Jung H. et al]. – Gwangju, Gwangju Institute of Science and Technology, 2013 – 35 p. – pp. 3-10

7. A contribution to the mathematical theory of epidemics/ W. O. Kermack, A. G. McKendrick. – London: Royal Society London, Vol. 115, no. 772 – 1927. – pp. 700–721

8. Ahmad A. A Novel Model for Distributed Denial of Service Attack. Analysis and Interactivity/ A. Ahmad, Y. AbuHour, F. Alghanim // Symmetry. – 2021, 13, 2443.

9. Okabe Y. A Mathematical Model of Epidemics. A Tutorial for Students / Y. Okabe, A. Shudo // Mathematics – 2020, 8, 1174

10. Mishra B. K. Mathematical model on distributed denial of service attack through Internet of things in a network/ B. K. Mishra, A. K. Keshri, D. K. Mallick, and B. K. Mishra// Nonlinear Engineering – 2019; 8: 486–495

11. Brauer. F./ Mathematical Models in Population Biology and Epidemiology/F. Brauer, C. Castillo-Chávez. – Springer: New York, NY, USA, 2001.

12. Murray J.D. Mathematical Biology: I. An Introduction/ J.D. Murray – Springer: New York, NY, USA, 2002.

13. Brauer. F./ Mathematical Epidemiology/Brauer F., van den Driessche P., Jianhong W.– Springer: Berlin, 2008.

14. Vormayr G. Botnet communication patterns/ G. Vormayr, T. Zseby, J. Fabini// IEEE. Communications Surveys and Tutorials – 2017, 19 (4), 2768–2796

15. V. Matta, M. Di Mauro, M. Longo. Botnet identification in multi-clustered DDoS attacks/ European Signal Processing Conference (EUSIPCO), 2017, pp. 2171–2175.

16. Fridge Caught Sending Spam Emails in Botnet Attack: [Електронний ресурс]/ Starr M. // CNET, 19 Jan. 2014. Режим доступу: http://www.cnet.com/news/fridge-caught-sending-spam-emails-in-botnet-attack/

ДОДАТОК А ТЕКСТИ ПРОГРАМ

А.1 SIR-подібна модель

```
def ode_func(t, y):
    Sa, Ia, Sl, Il, Rl, Sh, Ih, Rh = y

# Обчислення lambda
lam = beta * (Ia + eta * (Ih + Il))

    # Обчислення диференціальних рівнянь
    dSdt = mu - beta * Sa * Ia - mu * Sa + xi * Ia
    dIdt = beta * Sa * Ia - (xi + mu) * Ia
    dSldt = -(lam + sigma_l) * Sl
    dIldt = lam * Sl - (gamma_l + sigma_l) * Il
    dRldt = gamma_l * Il - xi_l  * Rl
    dShdt = -lam * (1 - epsilon) * Sh + xi_h * Rh + xi_l * Rl - sigma_h * Sh
    dIhdt = lam * (1 - epsilon) * Sh - (gamma_h + sigma_h) * Ih
    dRhdt = gamma_h * Ih - xi_h * Rh
    return dSdt, dIdt, dSldt, dIldt, dRldt, dShdt, dIhdt, dRhdt
```

А.2 SIR-SIS модель зі зовнішніми хостами

```
def ode_func(t, y):
        St, It, Rt, Sa, Ia, Ea = y

        dStdt = -beta*St*Ia + xi_t*Rt
        dItdt = beta*St*Ia - gamma*It
        dRtdt = gamma*It - xi_t*Rt
        dSadt = -beta*Sa*Ia - mu*Sa + xi_a*Ia + rho*Ea - alpha*Sa
        dIadt = beta*Sa*Ia - mu*Ia - xi_a*Ia - alpha*Ia
        dEadt = alpha*Sa + alpha*Ia - rho*Ea + mu - mu*Ea

        return dStdt, dItdt, dRtdt, dSadt, dIadt, dEadt
```