КОМП'ЮТЕРНІ НАУКИ

УДК 004.8/681.5 DOI: https://doi.org/10.32515/2414-3820.2025.55.298-308

Р.М. Минайленко, доц., канд. техн. наук, **П.С. Усік**, доктор філософії, **Л.І. Поліщук**
Центральноукраїнський національний технічний університет, Кропивницький, Україна
e-mail: aron70@ukr.net

Аналіз методів протидії ботнет в системах IoT

У статті здійснено аналіз методів боротьби з ботнетами в системах Інтернету речей (IoT). Сьогодні термін "Інтернет речей" дедалі частіше використовується для опису ситуацій, у яких підключення до мережі та обчислювальні можливості поширюються на широкий спектр об'єктів, пристроїв, датчиків тощо. Головна ідея IoT полягає у підключенні різноманітних об'єктів, які людина використовує у повсякденному житті. Ці пристрої повинні бути обладнані вбудованими сенсорами або датчиками, здатними збирати інформацію з навколишнього середовища, обмінюватися даними і виконувати певні дії на основі отриманої інформації.

Відсутність уніфікованих стандартів захисту таких автономних мереж наразі уповільнює інтеграцію технологій Інтернету речей у щоденне життя. Це створює численні вразливості у швидкозростаючій галузі IoT, яка широко застосовується у всьому світі. Забезпечення інформаційної безпеки та конфіденційності є одними з ключових аспектів під час вибору відповідної системи. Без гарантій захисту даних користувача та їхньої приватності IoT-системи ризикують втратити конкурентоспроможність.

користувач, система IoT, ботнет, захист інформації

Постановка проблеми. Термін "Інтернет речей" (IoT) було вперше запропоновано Кевіном Ештоном для опису системи, де фізичні об'єкти можуть взаємодіяти з датчиками та мережею Інтернет. Метою Ештона було показати потенціал радіочастотної ідентифікації (RFID), яка застосовується в логістичних системах для автоматичного підрахунку та відстеження товарів без участі людини. Сьогодні цей термін широко використовується для означення ситуацій, коли Інтернет-з'єднання та обчислювальні можливості інтегруються в безліч пристроїв, об'єктів і датчиків. Основна концепція IoT полягає в можливості підключення різноманітних предметів, які ми використовуємо в повсякденному житті, таких як холодильники, кондиціонери, автомобілі, велосипеди тощо [1, 2, 3].

Усі ці об'єкти повинні бути оснащені вбудованими датчиками, спроможними зчитувати дані про навколишнє середовище, обмінюватися інформацією між собою та виконувати певні автоматизовані дії, враховуючи отримані дані. Наприклад, одними з реальних впроваджень цієї концепції є системи "розумний будинок" або "розумна теплиця". Такі рішення дозволяють аналізувати навколишні умови і автоматично налаштовувати певні параметри, наприклад, регулювати температуру у приміщенні без втручання людини [4, 5, 6-15].

Водночас, відсутність наразі загальновизнаних стандартів захисту для мереж автономних систем частково гальмує поширення IoT у повсякденному житті. Швидке зростання цієї галузі у світі супроводжується численними ризиками безпеки. Захист даних і забезпечення конфіденційності є ключовими аспектами при виборі таких систем споживачами. Без належного рівня впевненості в безпеці та приватності користувацьких даних системи IoT будуть неконкурентоспроможними [3, 5, 16, 17].

Аналіз останніх досліджень і публікацій. Сьогодні інтернету речей приділяється значна увага на найвищому рівні. Починаючи з 2009 року, у Брюселі за підтримки Єврокомісії регулярно проводяться конференції Annual Internet of Things, де виступають єврокомісари, науковці та керівники провідних IT-компаній. За прогнозами аналітиків, інтернет речей переживає стрімкий розвиток, і в найближчі роки очікується справжній бум. Згідно з прогнозами Gartner, до 2027 року кількість пристроїв, підключених до інтернету, досягне 29 мільярдів, а ринок обладнання, програмного забезпечення та супутніх послуг приноситиме дохід у розмірі 2,9 трильйонів доларів. Інші аналітичні агентства висловлюють ще більш оптимістичні оцінки [17-21].

Щоб об'єднати повсякденні речі в єдину мережу, необхідно використовувати різні технології:

– Для ідентифікації кожного об'єкта потрібна компактна технологія, здатна збирати й накопичувати інформацію про ці предмети. Це завдання можуть виконувати RFID-мікросхеми (Radio-Frequency IDentification), які передають дані без необхідності у власних джерелах енергії. Альтернативний підхід — використання QR-кодів. Для визначення місцезнаходження об'єктів актуально застосування технології GPS, яка вже широко використовується у смартфонах і навігаторах.

– Для моніторингу змін стану пристроїв або навколишнього середовища необхідно оснастити їх сенсорами.

– Для обробки та збереження отриманих даних потрібні малогабаритні вбудовані обчислювальні пристрої на зразок Raspberry Pi або Intel Edison.

– Для передачі даних між пристроями можуть використовуватися бездротові мережі, такі як Wi-Fi, Bluetooth, ZigBee або 6LoWPAN [3, 5, 6].

Інтеграція з інтернетом передбачає використання IP-адрес для унікальної ідентифікації пристроїв. Проте через обмежене адресне поле IPv4 (4,3 мільярда унікальних адрес) пристрої інтернету речей переходять на IPv6. Цей протокол дозволяє надати до 300 мільйонів унікальних адрес на кожного мешканця планети. У систему будуть інтегровані не лише сенсорні пристрої, але й виконавчі елементи, такі як лампочки чи замки, якими можна буде керувати через інтернет.

Майбутній розвиток інтернету речей значною мірою залежатиме від широкого впровадження IPv6 – це стане ключовим фактором успіху. Розвиток бездротової передачі даних значною мірою залежить від таких характеристик: ефективність, відмовостійкість, адаптивність і здатність до самоорганізації. У цьому контексті важливими є рішення на основі стандарту IEEE 802.15.4, який забезпечує енергоефективність персональних мереж і слугує основою для протоколів ZigBee, Wi-Fi, Bluetooth та 6LoWPAN.

Окремо варто виділити технології PLC, які забезпечують передачу даних через лінії електропередач. Вони є особливо актуальними для додатків із доступом до електромереж, таких як торговельні автомати, банкомати, розумні лічильники й системи керування освітленням.

Постановка завдання. Кількість «розумних» пристроїв у світі стрімко зростає і, за прогнозами, у найближчому майбутньому вона перевищить чисельність населення планети в кілька разів. Водночас питання безпеки цих пристроїв залишаються недостатньо опрацьованими. Виробники не завжди забезпечують належні механізми захисту: немає автоматичних нагадувань про зміну стандартних паролів під час первинного налаштування, відсутні повідомлення про випуск нових версій прошивок, а сам процес оновлення часто є складним і незручним для пересічних користувачів. Це робить IoT-пристрої привабливою мішенню для кіберзлочинців, адже їх легше інфікувати, ніж персональний комп'ютер. До того ж такі пристрої можуть посідати

важливе місце у домашній мережі: одні контролюють інтернет-трафік, інші записують відео, а деякі керують іншими механізмами, наприклад, кліматичними системами [9, 10, 21].

Кількість і якість шкідливого програмного забезпечення для IoT-пристроїв постійно зростають. У зловмисників з'являються нові експлойти, які активно використовуються для самопоширення шкідників. Інфіковані пристрої застосовують для крадіжки персональних даних, майнінгу криптовалют тощо.

Для зниження ризику зараження IoT-пристроїв можна використовувати кілька простих рекомендацій:

– Заблокувати доступ зовнішніх мереж до пристрою.

– Регулярно перезавантажувати пристрій, що може допомогти позбутися шкідливих програм (хоча це не гарантує захисту від повторного зараження).

– Систематично перевіряти наявність оновлень для прошивки та встановлювати їх.

– Використовувати складні паролі довжиною не менше 8 символів, які включають комбіновані літери різного регістру, цифри та спеціальні символи.

– Одразу змінювати заводські паролі при першому запуску пристрою, навіть якщо система цього не запитує.

– Закривати або блокувати невикористовувані порти – наприклад, якщо немає потреби доступу через Telnet, слід вимкнути відповідний порт (TCP) для зменшення можливих точок атаки.

Однак такі заходи лише частково вирішують проблему. Першопочаткові принципи розробки пристроїв інтернету речей залишаються незмінними, що створює підґрунтя для виникнення нових вразливостей. Тому необхідно знайти системний підхід до підвищення безпеки IoT-пристроїв, щоб ускладнити їх компрометацію та здорожчати проведення атак, зокрема продаж ботнетів як сервісу[3, 7, 20].

Аналіз сучасних проблем безпеки IoT показує, що:

– Основними джерелами загроз в інтернеті речей є особи або групи людей, мотивовані фінансово, політично чи ідейно.

– Чимало вразливостей походять із недоліків ще на етапі проектування та розробки пристроїв IoT.

– У більшості атак на IoT пристрої зловмисники інфікують їх для створення ботнетів.

– Близько 20% атак із 2016 року використовували ботнет Mirai або його модифікації.

На сучасному етапі розвитку IoT відсутній міжнародний стандарт розробки пристроїв та систем інтернету речей, тому їх захищеність залишається відкритим питанням у сфері кібербезпеки [3, 5, 20, 21].

Виклад основного матеріалу. Традиційні методи боротьби з ботнетами зазвичай зводяться до пошуку слабких точок в їхній інфраструктурі, щоб виконати маніпуляції чи блокування. Найпоширеніший спосіб – це співпраця з Інтернет-провайдером для забезпечення доступу та відключення центрального компонента ботнету. Цей підхід призводить до втрати контролю з боку власника ботнету, який більше не зможе віддавати команди. Подібні дії зазвичай здійснюються в рамках реагування на вже активний інцидент, наприклад, під час атаки DDoS. Цей підхід довів свою ефективність у багатьох випадках. Наприклад, відключення сервера C&C (Command and Control) на базі IRC припиняє передачу команд ботам. Зрештою, пристрої, які беруть участь у нападі, перевантажуються або стають недієздатними. Однак такий спосіб потребує доступу до ПК користувачів та тісної співпраці з

відповідними організаціями й установами [4-9, 21].

Класичні методи протидії ботнетам спрямовані на три основні мети:

1. Сервер управління (C&C).

2. Трафік ботнету.

3. Інфіковані комп'ютери.

Найперспективнішим підходом у протидії ботнетам є видалення їх центрального елемента – сервера C&C (Command and Control). Деактивація такого сервера дозволяє нейтралізувати ботнет повністю й відразу.

Однак це можливо лише за дотримання кількох ключових умов:

1. Ботнет використовує централізовану структуру.

2. Місцезнаходження сервера C&C відоме.

3. Провайдер хостингу співпрацює з правоохоронними органами або технічними спеціалістами.

Якщо будь-яка із зазначених умов не виконується, видалення сервера стає неможливим. Варто зауважити, що сучасні ботнети дедалі рідше спираються на централізовану модель. Вони застосовують однорангові мережі (P2P) або багатошарові проксі-механізми, що суттєво ускладнює ідентифікацію їх розташування. У випадках, коли ботнет використовує кілька стаціонарних серверів, необхідно знешкоджувати всі ці вузли одночасно.

Ще одним фактором є готовність провайдерів співпрацювати. Часто C&C-сервери знаходяться у хостинг-компаній із так званою "кулестійкою" політикою, які ігнорують запити або передають сервери своїм дочірнім компаніям до завершення зовнішнього тиску. Організації, що займаються моніторингом кіберзлочинів, зазвичай отримують масу інформації про потенційні сервери C&C, але через обмежені ресурси часто неспроможні реагувати на кожен сигнал окремо. Деактивація C&C-серверів не гарантує повного знищення ботнету, оскільки заражені машини можуть мати автономні функції для подальшого поширення або активації альтернативної логіки у разі втрати зв’язку з сервером. Це призводить до додаткового трафіку та може спричинити нові хвилі заражень кінцевих пристроїв [9, 10, 11-14].

Якщо видалення сервера C&C неможливе, альтернативним рішенням може бути перенаправлення шкідливого трафіку на так звані "свердловини" — спеціальні системи для запису та аналізу трафіку. Вони допомагають запобігти досягненню цілі ботнету через маніпуляцію маршрутом передачі даних. Наприклад, технологія "нуль-маршрутизації DDoS" дозволяє скидати підозрілий трафік і збирати його для подальшого аналізу. Хоча цей підхід є перспективним у боротьбі із DDoS-атаками, він все ж має свої обмеження.

Зокрема, існують труднощі з точною ідентифікацією атакувального трафіку та обробкою великих потоків даних на ранніх етапах виявлення. Зазвичай такі методи можуть бути реалізовані лише на рівні інтернет-провайдера, що додає ще більше технічних викликів [15, 19].

Очищення заражених систем є одним із найефективніших способів боротьби з ботнетами, хоча й залишається одним із найскладніших для реалізації. Цей процес передбачає видалення всіх встановлених ботів із уражених комп'ютерів, що суттєво послаблює потужність ботнету.

Однак відповідальність за чистоту систем досі покладається на їхніх власників або адміністраторів, які мають вживати заходів на основі рекомендацій і технічних консультацій. Проблема полягає в тому, що багато користувачів не усвідомлюють факт зараження свого комп’ютера, а тим більше не готові виконувати складні дії для його очищення.

Як показує приклад із вірусом Conficker, навіть масові інформаційні кампанії не гарантують активності користувачів, що робить глобальне очищення практично недосяжним. Для захисту систем від ботнетів зазвичай рекомендують використовувати брандмауери та сучасне антивірусне програмне забезпечення (AV). Брандмауери є превентивною мірою безпеки, яка у багатьох випадках блокує атаки зовні.

Однак нові вектори зараження, включаючи drive-by-атаки через вразливості браузерів або поширення шкідливого ПЗ через ноутбуки та USB-накопичувачі, часто можуть обходити ці засоби захисту.

Антивірусне програмне забезпечення виконує реактивну функцію захисту. Воно здатне виявляти загрози лише тоді, коли підписи для них уже створені та доступні. Якщо підпис для певного шкідливого ПЗ відсутній, система залишається вразливою. Тести ефективності різних баз даних антивірусів показали, що у деяких випадках рівень виявлення інфекцій не перевищував 80%. У ситуаціях, коли система вже заражена, бот може продовжувати поширювати себе чи виконувати шкідливі функції доти, доки потрібні AV-підписи не стануть доступними.

Крім того, існує проблема застарілих баз даних антивірусного ПЗ, які регулярно не оновлюються. Ще більшу складність додає той факт, що деякі боти здатні відключати антивірусне програмне забезпечення або маскувати свою діяльність так, що їх неможливо виявити за допомогою звичайних сканерів. У деяких випадках упоратися з такими загрозами можливо лише на рівні інтернет-провайдерів, наприклад, шляхом сегментування трафіку високої пропускної здатності або перехоплення злоякісних даних на ранніх стадіях атаки [19-21].

Глобальна очистка, необхідна для ефективного позбавлення ботнетів доступу до влади, наразі здається нездійсненною. Раніше фахівці відзначали, що зупинка серверів управління та контролю (C&C) майже не має сенсу, адже їх швидко заміняють нові, ще більш захищені системи. Ця безперервна гонитва озброєнь у кіберпросторі зрештою може призвести до створення ще складнішої технології ботнетів. Виключно оборонний підхід залишає потенційні цілі сам на сам із існуючими загрозами, а обмеженість методів пом'якшення наслідків для запобігання або блокування поточних атак фактично є визнанням безпорадності. Тому необхідно комбінувати класичні захисні методи з проактивними стратегіями [5-10].

Проактивні заходи та стратегії відіграють ключову роль. Хоча класичні контрзаходи допомагають зменшити вплив ботнетів, вони поступово втрачають свою ефективність. Сучасні ботнети застосовують складніші стратегії, що ускладнює використання традиційних методів через перелічені вище причини. Проте нові архітектури ботнетів створюють можливості для більш інтенсивних контратак [14, 17].

Дослідження структури ботнету зазвичай є першим кроком до визначення вразливих місць для потенційних контрзаходів. Унікальною характеристикою цих мереж є те, що вони повинні дозволяти приєднання нових машин, навіть із ненадійних платформ. Це відкриває додаткові можливості для протидії: не лише спостерігати іззовні, а й проникати в мережу, досліджуючи її внутрішні механізми як частину самої інфраструктури. Такий підхід може включати навіть дестабілізацію чи руйнування ботнету зсередини.

Крім того, боти продовжують поширення інфекцій, що збільшує масштаб мережі. Отримання зразків шкідливого програмного забезпечення (навіть якщо це вимагає значних зусиль) дає змогу їх аналізувати, наприклад, через реверс-інжиніринг, для розкриття внутрішніх компонентів. Розуміння функціональних аспектів роботи бота дозволяє створити фальшивий бот, який може стати частиною ботнету для спостереження або порушення внутрішніх комунікацій. Такий підхід можливий

завдяки тому, що вся інформація про початкове завантаження міститься в бінарних файлах шкідливого програмного забезпечення і може бути скопійована [4,7,14].

Наступальні стратегії протидії ботнетам можна поділити на три основні категорії:

– пом'якшення наслідків;

– маніпуляції;

– експлуатація.

Ефективність обраної стратегії здебільшого визначається топологією ботнету. Зокрема, децентралізовані або мобільні структури значно ускладнюють або навіть зводять нанівець застосування подібних контрзаходів.

Стратегії пом'якшення наслідків передбачають використання технічних засобів, спрямованих на уповільнення роботи ботнетів через виснаження їхніх ресурсів. Це може включати, наприклад, тимчасові атаки типу DoS на сервери C&C, створення численних підключень до заражених пристроїв або блокування зловмисних доменів.

Маніпулятивні стратегії працюють із командним рівнем ботнету. Знання про командні протоколи, включаючи криптографію, є вирішальними для успішного втручання та корегування команд. Навіть використання захищених методів криптографії, таких як RSA або AES, не є абсолютною перешкодою. Дослідження прикладу Waledac демонструє можливість маніпулювати ботнетами навіть за умов складного криптографічного захисту. Серед ймовірних маніпуляцій можна виділити зміну або видалення команд для проведення DDoS-атак чи розповсюдження спаму, а також управління завантаженням і виконанням програм для цілей очищення інфікованих пристроїв. Менш агресивні підходи можуть полягати у вилученні конфіденційних даних, таких як фінансова інформація (номер кредитної картки або банківські реквізити), із подальшою підміною цих даних фальшивими, або ж у ініціації команд, що припиняють збір таких даних.

Стратегія експлуатації спрямована на використання помилок у роботі ботів. Подібно до вразливостей у звичайному програмному забезпеченні, ці помилки можна використовувати для проведення певних операцій на заражених пристроях. Експлуатація вважається найбільш потужною, але водночас і ризикованою стратегією, оскільки введення в експлуатацію вразливостей може призвести до пошкодження систем або виходу пристроїв з ладу. Однак далеко не кожен підхід застосовується до будь-якого ботнету, оскільки ефективність стратегій значною мірою залежить від специфіки топології мережі ботнету [2, 8, 20].

Атака на адресний рівень. При розгляді стратегій, спрямованих на маршрутизацію та адресний рівень інфраструктури ботнетів, варто зазначити, що механізм маршрутизації, який застосовується ботнетом, є критично важливим для визначення адрес хостів або серверів управління та контролю (C&C). У той час як командний рівень забезпечує функціонування мережі комунікації, накладеної на пов’язані пристрої, він працює з верхніми шарами адресної схеми. Найбільш поширений спосіб, за якого бот підключається до центрального сервера C&C, базується на використанні імен DNS, які перенаправляють його до відповідної IP-адреси. Цей процес включає два етапи адресації. Кожна з цих фаз є потенційною точкою для зовнішнього втручання [3, 5, 20].

Як приклад можна навести роботу запитів DNS. Вони часто обробляються локальним DNS-резолвером, який передає запит до авторитетного DNS-сервера. Локальним DNS-резолвером зазвичай керує адміністратор сайту, який може налаштувати його таким чином, щоб генерувати маніпуляційні відповіді на конкретні запити.

Аналогічний підхід застосовується до маршрутизації IP-трафіку: локальні маршрутизатори можуть містити змінені таблиці маршрутизації для блокування певних адрес або перенаправлення їх на інші вузли. Таке перенаправлення, відоме як sinkholing, дозволяє переадресувати шкідливий трафік на спеціальний сервер, який використовується для виявлення заражених пристроїв. Результатом таких дій є неможливість ботів у локальній мережі зв'язатися з вихідним сервером C&C. Натомість вони можуть бути спрямовані на псевдосервер, який керується адміністраторами або дослідниками. Ці втручання зазвичай вимагають застосування стратегій типу «людина посередині» (man-in-the-middle). Хоча в окремих випадках навіть не потрібно змінювати конфігурацію пристроїв – більш просунуті методи дозволяють маніпулювати відповідним мережевим трафіком динамічно.

Сучасні ботнети застосовують складніші моделі адресації, які функціонують як накладні мережі поверх традиційного інтернет-протоколу (IP). Однією з таких моделей є однорангові мережі (peer-to-peer), які використовують власні схеми адресації для підвищення масштабованості та децентралізації. Щоб здійснити проникнення в адресний рівень подібних ботнетів, потрібне стратегічно вигідне розташування в мережі. Загальна тактика включає впровадження контрольованого вузла, який ідеально імітує оригінал [1. 3,19,21].

У разі, якщо сервери C&C фізично недоступні, вони залишаються вразливими в інтернет-просторі, адже боти повинні періодично підключатися до них для отримання команд. Це відкриває шлях до нападів типу DoS (Denial of Service), які можуть тимчасово паралізувати сервер. Організований союзником DDoS-напад може забезпечити його повне відключення. Крім того, ботнети часто покладаються на технології, що мають слабкі місця, які можна використовувати для здійснення цілеспрямованих атак.

Наприклад, протокол транспортного рівня TCP. Черга резервного копіювання TCP-сервера C&C може бути перевантажена спробами з’єднання, що призведе до відмови в обслуговуванні, effectively перетворюючи ботнет у зброю проти самої себе. Такий підхід особливо ефективний для більшості бот-серверів на основі HTTP, де для кожного командного запиту створюється нове з’єднання. Було виконано тестування різних комбінацій служб та операційних систем, в ході якого ідентифікували TCP DoS-атаку, яку можливо реалізувати без значних витрат ресурсів. У результаті досліджень вдалося знизити ймовірність встановлення з’єднань із TCP-серверами до менш ніж 5% лише за допомогою одного клієнтського пристрою.

Один хост здатен утримувати чергу резервної копії служби жертви, блокуючи подальші спроби з’єднання, тим самим не даючи ботам отримувати або надсилати командні запити. Ця тактика може бути реалізована так, щоб спроби з’єднання виглядали ідентично активності самих ботів. Як наслідок, будь-які контрзаходи, що спрямовані на блокування таких запитів, також обмежуватимуть роботу "легітимних" ботів, а не тільки атакувальних. Результати показали, що один пристрій може підтримувати з’єднання зі службою TCP практично необмежено довго. Така атака значно обмежує кількість ботів, які мають змогу контактувати з сервером C&C і брати участь у подальших зловмисних діях [5, 15-21].

Існує ще одна подібна атака – це флуд серверної мережі C&C або її каналів зв’язку за допомогою масового надсилання пакетів, які споживають усю доступну пропускну здатність. Водночас така операція вимагає значно більше ресурсів, оскільки потрібно генерувати великий обсяг трафіку. Для підвищення інтенсивності атаки можна використовувати віддзеркалюючий метод, але це передбачає залучення сторонніх ресурсів і згоду власників залучених сайтів [7, 8, 9].

Атаки на командному рівні також можуть стати ефективним інструментом протидії ботнетам. Для таких дій потрібно знати специфіку протоколу, який використовується мережею ботнету.

Наприклад, у ботнетах на основі IRC існують команди видалення, які наказують ботам самознищуватися на заражених машинах. Багато класичних ботів підтримують таку команду. Для запуску подібної операції необхідно або отримати контроль над сервером C&C, або перенаправити ботів на інший сервер шляхом атаки на адресному рівні, після чого поширити через нього команду видалення. Деякі боти не мають функції видалення, але підтримують оновлення – це можна використати для заміни шкідливої програми на корисний додаток, здатний виявляти та видаляти інших ботів. Поєднання атак на адресному і командному рівнях відкриває додаткові можливості.

Наприклад, оригінальні команди можуть бути перехоплені та змінені для досягнення необхідного ефекту. Деякі спеціалізовані протоколи створені для захисту від таких маніпуляцій, але поки такі механізми не були виявлені в більшості сучасних ботнетів. Загалом, успішна атака для нейтралізації ботнету потребує комплексного підходу: одночасного впливу на рівні адресації та команд. Переадресація ботів на контрольований сервер із метою поширення інструкцій на самознищення або нейтралізацію є одним із найефективніших стратегічних заходів боротьби на рівні інфраструктури [15, 21].

Експлуатація ботнетів, побудованих на системах Інтернету речей, базується на використанні їхніх вразливостей. Такі ботнети часто страждають від помилок у програмуванні та конфігурації, що відкриває доступ до критичних компонентів, таких як C&C-сервер, або до окремих заражених пристроїв. Вразливості можуть включати елементарні помилки налаштування і серйозні порушення, наприклад, віддалене переповнення буфера.

Стратегії мінімізації ризиків або маніпуляцій із ботнетами зазвичай не спрямовані на активне пошкодження заражених пристроїв. Однак команди, які запускають виконавчі програми або експлуатують вразливості, є агресивнішими. Написання експлуатаційного коду вимагає значних зусиль і врахування специфіки операційної системи чи конфігурації цільового об’єкта. Використання інструментів типу Metasploit полегшує створення такого коду, однак підвищує ризик незворотного виходу з ладу віддалених систем. Це особливо важливо враховувати у випадках, де йдеться про критичні інфраструктури [3, 7, 10].

Перед використанням вразливостей необхідно провести ідентифікацію заражених пристроїв. У децентралізованих мережах це можна зробити через аналіз спроб підключення до ботів-учасників. У централізованих топологіях корисну інформацію можливо отримати з логів осідання. Інші методи включають розгортання honeypots, застосування підписів системи виявлення вторгнень (IDS) або використання сканерів для моніторингу мережевих діапазонів з метою пошуку заражених вузлів.

Актуальність вразливостей у ботах не є новою проблемою. Багато різновидів Rbot і Sdbot мають спільну кодову базу з подібними вадами. Потенційний спосіб ліквідації ботнетів містить виявлення заражених машин, використання їхніх слабких місць і впровадження коду, який вимкне шкідливе програмне забезпечення. Впродовж років приклади виправлення таких вразливостей траплялись і в новітньому шкідливому ПЗ.

Наприклад, у Conficker.B використовувалася криптографічна хеш-функція MD6, яка містила вразливість переповнення буфера. Ця помилка була виправлена у версії Conficker.C завдяки оновленню, хоча конкретно цю прогалину безпеки не було використано. Це підкреслює, що навіть складне шкідливе програмне забезпечення не

захищене від критичних вразливостей.

Проактивні стратегії протидії ботнетам демонструють широкий потенціал для зменшення загроз ще до того, як вони завдадуть шкоди. Хоча такі підходи є технічно здійсненними, їх впровадження ускладнюється етичними та правовими аспектами, які необхідно ретельно враховувати.

Однією з основних проблем наступальних методів є їхня потреба в максимально прихованих діях. Розробники ботнетів здатні адаптуватися до специфічних спроб усунути їхні атаки, вносячи невеликі зміни в протоколи або запроваджуючи цифрові підписи. Крім того, вразливості, які експлуатуються, можуть бути усунені за короткі терміни. Якщо метою є повне вимкнення ботнету, це має відбуватися швидко і на глобальному рівні, щоб залишити мінімум можливостей для контрзаходів з боку атакувальної команди [4, 15].

Експерти зазначають, що переслідування творців ботнетів навряд чи значною мірою зменшить глобальну загрозу. Ефективна боротьба потребує технічного підходу, що включає сукупні зусилля міжнародних безпекових груп у співпраці з державними організаціями. Проактивні дії повинні стати результатом координації на глобальному рівні, щоб забезпечити максимальну ефективність у протидії шкідливим мережам.

Висновки. Інтернет речей здатен докорінно змінити повсякденне життя, пропонуючи користувачам нові рівні комфорту. Однак, якщо його компоненти не будуть належним чином захищені від несанкціонованого доступу за допомогою сучасних криптографічних алгоритмів, існує великий ризик замість користі отримати серйозну шкоду. Зловмисники можуть скористатися вразливостями, відкриваючи шлях до зламу, що може поставити під загрозу інформаційну безпеку.

Пристрої з вбудованими комп'ютерами зазвичай акумулюють значні обсяги чутливих даних про своїх власників, включаючи інформацію про місцезнаходження. Доступ до таких даних у руках зловмисників може стати інструментом для реалізації злочинів. Відсутність на сьогодні чітких стандартів захисту цих автономних мереж значно гальмує їх інтеграцію в наше повсякдення. Це залишає швидко зростаючу сферу IoT-технологій із численними вразливостями, що викликає занепокоєння споживачів. Забезпечення конфіденційності та безпеки інформації є ключовим критерієм під час вибору таких систем. Якщо користувачі не відчуватимуть впевненості у захищеності своїх даних, IoT-рішення ризикують втратити свою конкурентоспроможність.

Наразі успіх контрзаходів проти ботнетів значною мірою залежить від організаційних та політичних факторів. Оскільки досягнення домовленостей і координація міжнародної співпраці потребують тривалого часу, такі підходи не можуть бути оперативно застосованими для реагування на поточні атаки [7-10].

Ситуацію ускладнює те, що сучасні ботнет-інфраструктури зазвичай не належать одному суб'єкту. Розподілені однорангові мережі діють глобально, і відключення локальних сегментів, які часто представлені окремими пристроями, не дає бажаного результату. У цілому, контрзаходи, які вимагають тісної міжнародної співпраці, наразі є малоефективними як у технічному, так і в політичному сенсі.

Список літератури

1. Most Wanted Malware: Attacks Targeting IoT and Networking doubled since May 2018. *Check Point Software Tech. LTD* URL: https://www.checkpoint.com/press-releases/julys-wanted-malware-attacks-targeting-iot-networking-vulnerabilities-rise/ (date of application: 15.03.2025)
2. Menachem Domb. An Adaptive Lightweight Security Framework Suited for IoT**.** *Internet of Things - Technology, Applications and Standardization.* URL: https://www.intechopen.com/chapters/59350 (date of application: 15.03.2025)
3. Leder F., Werner T., and Martini P. Proactive Botnet Countermeas An Offensive Approaches. URL:

https://ccdcoe.org/uploads/2018/10/15_LEDER_Proactive_Coutnermeasures.pdf (date of application: 15.03.2025)
4. Ivo van der Elzen Jeroen van Heugten – «Techniques for detecting compro- mised IoT devices». URL: https://www.os3.nl/_media/2016-2017/courses/rp1/p59_report.pdf (date of application: 15.03.2025)
5. Understanding the mirai botnet. / Antonakakis M. itc. *SEC'17: Proceedings of the 26th USENIX Conference on Security Symposium.* P. 1093–1110. URL: https://dl.acm.org/doi/10.5555/3241189.3241275
6. Doshi R., Apthorpe N., Feamster N. Machine Learning DDoS Detection for Consumer Internet of Things Devices. *2018 IEEE Security and Privacy Workshops.* P. 29–35 URL: https://ieeexplore.ieee.org/document/8424629
7. Sebastian-Dan Naste. A multidisciplinary study on DDoS attacks in the EU IoT ecosystem
8. OWASP–«IoT Vulnerabilities Project». URL: https://www.owasp.rg/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Vu lnerabilities (date of application: 15.03.2025)
9. OWASP – «IoT Attack Surface Project». URL: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Att ack_Surface_Areas (date of application: 15.03.2025)
10. Daniel Elizalde – «IoT Hardware – Introduction and Explanation». URL: https://www.iotforall.com/iot-hardware-introduction-explanation/ (date of application: 15.03.2025)
11. Earlence Fernandes та співавтори «FlowFence: Practical Data Protection for Emerging IoT ApplicationFrameworks». URL: https://www.usenix.org/ system/files/conference/usenixsecurity16/sec16 _paper_ferna ndes.pdf(date of application: 15.03.2025)
12. HESSELDAHL A. «The Hacker's Eye View of the Internet of Things.». URL: http://recode.net/2015/04/07/a- hackers- eye- view- of- the- internet- of- things/. (date of application: 15.03.2025)
13. FERNANDES, E., JUNG, J., AND PRAKASH, A.. – «Security analysis of emerging smart home applications». На IEEE Symposium on Security and Privacy (S&P)
14. Yi home camera. URL: https://www.yitechnology.com/yi- home- camera (date of application: 15.03.2025)
15. Hewlett Packard Enterprise – «Internet of things research study». URL: http://h20195.www2.hpe.com/V4/getpdf.aspx/4aa5- 4759enw (date of application: 15.03.2025)
16. «Internet of things (iot) security and privacy recommendations.».
17. S. Hilton – «Dyn analysis summary of friday october 21 attack.». URL: https://dyn.com/blog/ dyn-analysis-summary-of-friday-october- 21- attack/ (date of application: 15.03.2025)
18. V.Chandola, A.Banerjee, V.Kumar . «Anomaly detection: A survey», Vol. 41.3
19. E. Eskin, W. Lee, and W. Stolfo – «Modeling system call for intrusion detection using dynamic window sizes»
20. M. Qin and K. Hwang – «Frequent episode rules for internet anomaly detection»
21. M. Miettinen, S. Marchal, I. Hafeez, N. Asokan, A. Sadeghi, та S. Tarkoma «Iot sentinel: Automated device-type identification for security enforcement in IoT».

References

1. Check Point Software Tech. LTD « Most Wanted Malware: Attacks Targeting IoT and Networking doubled since May 2018» URL: https://blog.checkpoint.com/2018/08/15/julys-most-wanted-malware-attacks-targeting-iot-and-networking-doubled-since-may-2018/
2. Menachem Domb – «An Adaptive Lightweight Security Framework Suited for IoT» URL: https://www.intechopen.com/books/internet-of-things-technology- applications-and-standardization/an-adaptive-lightweight-security-framework-suited- for-iot
3. Felix LEDER, Tillmann WERNER, and Peter MARTINI Institute of Computer Science IV, University of Bonn, Germany – «Proactive Botnet Countermeas- ures – An Offensive Approaches» URL: http://four.cs.uni-bonn.de/fileadmin/user_upload/leder/proactivebotnetcountermeasures.pdf
4. Ivo van der Elzen Jeroen van Heugten – «Techniques for detecting compro- mised IoT devices» URL: http://www.delaat.net/rp/2016-2017/p59/report.pdf
5. Manos Antonakakis – «Understanding the Mirai Botnet»
6. Rohan Doshi, Noah Apthorpe, Nick Feamster – «Machine Learning DDoS Detection for Consumer Internet of Things Devices»
7. Sebastian-Dan Naste – «A multidisciplinary study on DDoS attacks in the EU IoT ecosystem»
8. OWASP–«IoT Vulnerabilities Project» URL: https://www.owasp.rg/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Vu lnerabilities
9. OWASP – «IoT Attack Surface Project» URL: https://www.owasp.org/index.php/

OWASP_Internet_of_Things_Project#tab=IoT_Att ack_Surface_Areas
10. Daniel Elizalde – «IoT Hardware – Introduction and Explanation» URL: https://www.iotforall.com/iot-hardware-introduction-explanation/
11. Earlence Fernandes та співавтори «FlowFence: Practical Data Protection for Emerging IoT Application Frameworks» URL: https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_ferna ndes.pdf
12. HESSELDAHL A. «The Hacker's Eye View of the Internet of Things.» URL: http://recode.net/2015/04/07/a- hackers- eye- view- of- the- internet- of- things/.
13. FERNANDES, E., JUNG, J., AND PRAKASH, A.. – «Security analysis of emerging smart home applications». На IEEE Symposium on Security and Privacy (S&P)
14. Yi home camera. URL: https://www. yitechnology.com/yi- home- camera
15. Hewlett Packard Enterprise – «Internet of things research study». URL: http: //h20195.www2.hpe.com/V4/getpdf.aspx/4aa5- 4759enw
16. «Internet of things (iot) security and privacy recommendations.».
17. S. Hilton – «Dyn analysis summary of friday october 21 attack.» URL: https://dyn.com/blog/ dyn-analysis-summary-of-friday-october- 21- attack/
18. V.Chandola, A.Banerjee, V.Kumar – «Anomaly detection: A survey» vol. 41.3
19. E. Eskin, W. Lee, and W. Stolfo – «Modeling system call for intrusion detection using dynamic window sizes»
20. M. Qin and K. Hwang – «Frequent episode rules for internet anomaly detection»
21. M. Miettinen, S. Marchal, I. Hafeez, N. Asokan, A. Sadeghi, та S. Tarkoma «Iot sentinel: Automated device-type identification for security enforcement in IoT».

Roman Minailenko, Assoc. Prof., PhD tech. sci., **Pavlo Usik,** PhD, **Liudmyla Polishchuk**
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine

Analysis of bOtnet Countermeasures in IoT Systems

The article analyzes the methods of countering botnets in IoT systems. Today, the Internet of Things has become a popular term to describe scenarios in which Internet connectivity and computing power are spread across a multitude of objects, devices, sensors, etc.

The main concept of IoT is the ability to connect all kinds of objects (things) that a person can use in everyday life. These objects (things) must be equipped with built-in sensors or sensors that have the ability to process information coming from the environment, exchange it and perform certain actions depending on the received information.

The current lack of standards for the protection of such autonomous networks somewhat slows down the introduction of the Internet of Things into everyday life, so there are numerous vulnerabilities in the rapidly growing field of IoT technologies, which are used all over the world. Information protection and confidentiality is one of the priority components when choosing a certain system. Therefore, without adequate confidence in the security and privacy of user data, the IoT system will be uncompetitive.

The Internet of Things can cause huge changes in everyday life, bringing a whole new level of comfort to ordinary users. But if the elements of such a system are not properly protected from unauthorized intervention, with the help of a reliable cryptographic algorithm, they will bring harm instead of good, giving cybercriminals a loophole to undermine information security.

Since devices with built-in computers store a lot of information about their owner, including the ability to know their exact location, access to such information can help criminals commit a crime.

To date, the level of success of botnet countermeasures depends mainly on organizational and political general conditions. Given that the establishment of cooperation or diplomatic agreements takes time, it can be concluded that the establishment of appropriate relations that legitimize cooperation for joint action is not suitable as an ad hoc scheme to combat current attacks.

The situation is aggravated, given that modern botnet infrastructures are not under the responsibility of a single entity. In contrast, distributed peer-to-peer networks operate worldwide, so shutting down local parts (often no more than single computers) is not an effective solution. In general, countermeasures that require close cooperation are generally unfeasible today for both technical and political reasons

Experts believe that prosecuting botnet developers is unlikely to have a strong impact on the global threat. Instead, botnets need to be fought on a technical level. Proactive measures should be taken by joint efforts of international security groups together with pro-government structures.

user, IoT system, botnet, information protection

Одержано (Received) 29.04.2025 *Прорецензовано (Reviewed) 29.09.2025*
Прийнято до друку (Approved) 23.12.2025