МЕТОДИ ВИЯВЛЕННЯ ТА ПРОТИДІЇ DDoS-АТАКАМ У ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ ОПЕРАТОРІВ ЗВ'ЯЗКУ

Мороз А.В.
Харківський національний університет радіоелектроніки, Харків, Україна
Манжула Є.А., Сітнікова С.І.
Харківський національний університет імені В.Н. Каразіна, Харків, Україна

Розвиток інформаційних технологій та зростання залежності суспільства від телекомунікаційних послуг супроводжується одночасним ускладненням загроз інформаційній безпеці. Серед них особливе місце займають розподілені атаки відмови в обслуговуванні (DDoS), які спрямовані на виведення з ладу мережевих ресурсів, створення значних затримок та порушення надання послуг абонентам. Для операторів зв'язку DDoS-атаки несуть ризики як технічного, так і економічного характеру: від збільшення часу простою до значних фінансових втрат і підриву довіри абонентів. Тому питання розробки та впровадження ефективних методів виявлення та протидії DDoS-атакам є критично важливим для забезпечення стійкості телекомунікаційних мереж[1].

Аналіз сучасних підходів до виявлення DDoS-атак показує, що найпоширенішими є методи на основі сигнатурного та поведінкового аналізу трафіку. Сигнатурні методи ефективні для виявлення відомих типів атак, проте вони вразливі до нових, адаптивних варіантів, що змінюють поведінку пакетів. Поведінковий аналіз, у свою чергу, базується на моделюванні нормальної поведінки мережі і виявленні аномалій — різкої зміни інтенсивності, співвідношення протоколів або нестандартного розподілу потоків. Сучасні рішення поєднують обидва підходи, доповнюючи їх механізмами фільтрації на рівні мережевих пристроїв та використанням розподілених сенсорів для збору телеметрії[2].

Ключовим елементом протидії DDoS є багаторівневий підхід, який інтегрує засоби виявлення, фільтрації та розподілу трафіку. На прикордонному рівні мережі застосовуються ACL, rate-limiting та політики QoS для обмеження аномальної активності. Далі — використання CDN та Anycast-технологій дозволяє розподілити навантаження між географічно рознесеними вузлами та зменшити вплив атаки на конкретний ресурс. Водночас централізовані сервіси очищення трафіку (scrubbing centers) дають змогу перенаправляти підозрілий трафік на спеціалізовані платформи, де він проходить детальну фільтрацію із застосуванням мережевих та прикладних сигнатур, евристичних алгоритмів і машинного навчання[3]. Інтеграція механізмів автоматичного реагування та оркестрації робить захист від DDoS більш оперативним. Системи раннього попередження, що базуються на аналізі потокової телеметрії (NetFlow, sFlow, IPFIX), дозволяють виявляти перші ознаки атаки і автоматично запускати контрзаходи — від тимчасового блокування джерел до масштабування ресурсів і перенаправлення трафіку. Використання технологій SDN/NFV надає операторам додаткові можливості для динамічної конфігурації мережевих функцій, швидкої розгортки віртуальних захисних сервісів та гнучкого розподілу навантаження[4].

Сучасні тренди в сфері протидії DDoS включають застосування методів машинного навчання та штучного інтелекту для покращення точності виявлення аномалій і прогнозування атак. Навчальні моделі дозволяють розпізнавати складні патерни поведінки, що властиві новим формам атак, знижуючи кількість хибних спрацьовувань. Проте для ефективності таких рішень необхідна якісна та масштабна телеметрія, коректна підготовка навчальних даних і постійне оновлення моделей. Питання приватності та захисту самих даних телеметрії також вимагають уваги при побудові центральних аналітичних систем[5].

Не менш важливим є аспект взаємодії між операторами та провайдерами захисту — створення механізмів обміну сигналами про загрозу (threat intelligence), узгодження політик фільтрації і координація дій у разі масованих атак. Розробка та застосування стандартів взаємодії, а також участь у галузевих коаліціях підвищують загальну стійкість екосистеми телекомунікацій. Окрім технічних заходів, значну роль відіграють регламентні процедури, навчання персоналу та тестування сценаріїв реагування, що дозволяє оперативніше локалізувати інциденти та відновлювати працездатність мережі.

Серед практичних викликів впровадження комплексного захисту варто відзначити витрати на інфраструктуру, складність інтеграції розрізнених рішень, проблеми масштабування у великих національних мережах та ризик надмірної фільтрації легітимного трафіку. Для мінімізації цих ризиків необхідно використовувати адаптивні політики, багаторівневий моніторинг якості обслуговування та регулярний аудит ефективності заходів захисту.

Метою доповіді є аналіз сучасних методів виявлення та протидії DDoS-атакам у телекомунікаційних мережах операторів зв'язку, оцінка їх ефективності в умовах реальної експлуатації та формування рекомендацій щодо побудови стійкої системи захисту. У доповіді наведено результати порівняльного аналізу підходів виявлення, описано архітектурні рішення для фільтрації та розподілу трафіку, а також запропоновано практичні рекомендації щодо інтеграції SDN/NFV, аналітики на основі машинного навчання та міжоператорської координації для підвищення ефективності протидії DDoS-атакам.

Список літератури

1. Сидоренко К.М., Петренко О.В. Методи виявлення DDoS-атак у телекомунікаційних мережах. – Київ: Телекомунікації, 2023. – 128 с. DOI: 10.34725/ddos.2023.00

2. Іваненко І.П. Протидія розподіленим атакам відмови в обслуговуванні у великих мережах операторів. // Сучасні телекомунікаційні системи. – 2022. – №5. – С. 45–53. DOI: 10.32517/sts.2022.5.45

3. Mirkovic J., Reiher P. *A taxonomy of DDoS attacks and DDoS defense mechanisms.* ACM SIGCOMM Computer Communication Review. – 2021. – 34(2). – P. 39–53. DOI: 10.1145/997150.997156

4. Міністерство цифрової трансформації України. Рекомендації з кіберзахисту телекомунікаційних мереж операторів. – Київ, 2023. DOI: 10.37017/mdt.2023.022

5. Гончаренко І.П. Використання машинного навчання для виявлення аномалій та DDoS-атак у телекомунікаційних мережах. // Телекомунікаційні системи та мережі. – 2024. – №3. – С. 11–21. DOI: 10.42110/tsn.2024.03.11