Науково-дослідна частина
Національного університету
кораблебудування
імені адмірала Макарова

54025, м. Миколаїв,
пр. Героїв України, 9
Тел.: (0512) 70-91-04
http://conference.nuos.edu.ua
e-mail: conference@nuos.edu.ua

Навчально-науковий інститут
автоматики та електротехніки
Національного університету
кораблебудування
імені адмірала Макарова

54021, м. Миколаїв,
пр. Центральний, 3
Тел.: (0512) 47-70-95
http://iae.nuos.edu.ua
e-mail: university@nuos.edu.ua

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

НАУКОВО-ТЕХНІЧНІ КОНФЕРЕНЦІЇ
Національний університет кораблебудування
імені адмірала Макарова

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

МАТЕРІАЛИ

XI ВСЕУКРАЇНСЬКОЇ НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ З МІЖНАРОДНОЮ УЧАСТЮ

23-24 листопада 2023 р.

Миколаїв ■ НУК ■ 2023

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

СПІБТ–2023

МАТЕРІАЛИ

XI Всеукраїнської науково-технічної конференції з міжнародною участю

23–24 листопада 2023 року

Національний університет кораблебудування
імені адмірала Макарова
Навчально-науковий інститут автоматики та електротехніки
просп. Центральний, 3, м. Миколаїв

МИКОЛАЇВ • НУК • 2023

УДК 004
У 45

ОРГАНІЗАТОРИ:

1. Міністерство освіти і науки України
2. Національний університет кораблебудування імені адмірала Макарова
3. ТОВ «БЕЗПЕКАІНФОСЕРВІС»
4. Науково-технічний центр «Квант»

Матеріали публікуються за оригіналами, наданими авторами.
Претензії до організаторів не приймаються.

Відповідальна за випуск В. В. Трибулькевич

У–45 **Сучасні** проблеми інформаційної безпеки на транспорті: матеріали XI Всеукраїнської науково-технічної конференції з міжнародною участю. – Миколаїв : НУК, 2023. – 223 с.

У збірнику подано матеріали XI Всеукраїнської НТК "Сучасні проблеми інформаційної безпеки на транспорті".

Розглянуті питання теорії та практики систем інформаційної безпеки транспортних засобів і систем, захисту інформації в каналах зв'язку та глобальних мережах передачі даних, захисту інформації на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах, системи Інтернет речей (IoT), моделювання об'єктів і процесів технічного захисту інформації, а також питання підготовки кадрів у галузі знань «Інформаційна безпека».

Збірник може бути корисним для наукових співробітників, викладачів, інженерів та студентів.

УДК 004

УДК 621.318; 004.056

ЗАГРОЗИ ГЛОБАЛЬНІЙ МАРШРУТИЗАЦІЇ В СУЧАСНОМУ КІБЕРПРОСТОРІ

Автор: *Турти М.В., к.т.н., доцент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

На даний час наявна тенденція до поширення практики зберігання даних окремими особами і організаціями в банках даних і хмарах, зростання кількості онлайн-сервісів та загального обсягу адресного передавання даних через Інтернет, який є незахищеним середовищем і регулюється тільки системою глобальної маршрутизації, на яку зловмисниками здійснюються тисячі атак щорічно [1].

Метою даної є розробка класифікації загроз глобальної маршрутизації.

Для досягнення поставленої мети необхідно шляхом аналізу відкритих літературних джерел визначити загрози та ризики глобальної маршрутизації, їх особливості та взаємозв'язки.

Прикладами інцидентів в системі глобальної маршрутизації є [2, 3]:

– 2018 рік: атака «викрадання префіксу» хмарного сервісу Amazon AWS і до якого були прив'язані його DNS сервери. Тривалість атаки – кілька годин. Метою викрадання інфраструктурного IP-префіксу Amazon AWS була фішингова атака на криптовалютний сервіс MyEtherWallet. В процесі атаки DNS-запити користувачів, що використовували DNS-сервери Amazon AWS, перенаправлялися на DNS-сервер зловмисників, де імена хостів з суфіксом, що відповідав криптовалютному сервісу, підмінялися IP-адресами фішингових сайтів, які працювали за протоколом HTTP і, на відміну від HTTPS, не дозволяли провести автентифікацію сервера. В результаті було викрадено значну кількість криптовалют і скомпроментовано дані користувачів;

– 2018 рік: збій в BGP-маршрутизації, що спричинив DoS-ефект щонайменше протягом 74 хвилин для таких сервісів Google як G Suite, Google Пошук і Google Аналітика, для внутрішніх систем Google і для сторонніх сервісів, в тому числі Spotify. Причиною збою стало анонсування 212 префіксів, що належали дата-центрам Google, невеликим нігерійським провайдером MainOne Cable Company сусіднім провай-

дерам. Хибна інформація поширилася серед інших провайдерів, один з яких – державний китайський провайдер China Telecom передав транзитом анонси до інших мереж, але сам зафільтрував трафік, що надходив до Google цими маршрутами. Тоді аналітики компанії Oracle і фахівці ряд дослідників США та Ізраілю звинуватили China Telecom в навмисному улаштуванні BGP-збоїв і навмисно некоректній передачі трафіку західних країн;

– 2022 рік: крадіжка префіксів BGP, які які належали південнокорейській криптовалютній платформі, і крадіжка префіксу, який використовував Twitter. Префікс криптовалютної платформи було використано зловмисниками для крадіжки криптовалюти на суму 1,9 мільйона доларів шляхом видачі сертифікату на домен через ZeroSSL для обслуговування шкідливого файлу JavaScript;

– 2023 рік: були виявлені три нові уразливості в програмній реалізації протоколу BGP, які зловмисник може використати для організації DoS-атак на вразливі вузли BGP. Аналіз семи реалізацій BGP показав, що у версії 8.4 FRRouting, що є поширеним набором протоколів маршрутизації з відкритим кодом для платформ Linux і Unix і використовується декількома провайдерами, що створює умови для ланцюгової реакції збоїв, містяться вразливості читання поза межами під час обробки неправильно сформованого повідомлення BGP OPEN із опцією Extended Optional Parameters Length (CVE-2022-40302 (оцінка CVSS: 6,5) і CVE-2022-40318 (оцінка CVSS: 6,5)) та неправильно сформованого повідомлення BGP OPEN, яке раптово закінчується октетом довжини опції (CVE-2022-43681 (оцінка CVSS: 6,5)). Ці вразливості зловмисники можуть використати для досягнення умови DoS для вразливих однорангових вузлів BGP, припиняючи таким чином всі сеанси BGP, викривлюючи таблиці маршрутизації та переставляючи одноранговий пристрій на реакцію. При цьому стан DoS може бути продовжений на невизначений термін шляхом повторного надсилання неправильно сформованих пакетів. Крім того, зловмисник може підробити дійсну IP-адресу довіреного однорангового вузла BGP або використати інші недоліки та неправильні конфігурації, щоб скомпрометувати законний одноранговий вузол, а потім видати спеціально створене небажане повідомлення

BGP OPEN. Це досягається завдяки тому, що FRRouting починає обробляти повідомлення OPEN (наприклад, декапсуляцію додаткових параметрів) до того, як він отримає можливість перевірити ідентифікатор BGP і поля ASN вихідного маршрутизатора;

– 2023 рік: словацька компанія ESET (розробник NOD32 Antivirus) виявила, що старі маршрутизатори, які раніше використовувалися в бізнес-мережевих середовищах, зберігають конфіденційні дані, включаючи корпоративні облікові дані, деталі VPN, криптографічні ключі та іншу важливу інформацію про клієнтів. Дані, зібрані із старих маршрутизаторів, включаючи дані клієнтів, ключі автентифікації між маршрутизаторами, списки програм та ін. є достатніми для кібератаки.

Причини поширення атак на глобальну маршрутизацію у сучасному кіберпросторі:

– ефект ланцюгової реакції – проблеми одного провайдера швидко поширюються на інших;

– теоретично необмежений вплив на мережу – помилки в адресації, допущені оператором чи провайдером або спричинені діями зловмисників за ланцюговою реакцією розповсюджуються на інших;

– висока ймовірність наявності недоліків налаштування роутерів, зокрема підтримки в діючому стані фільтрів маршрутів, хоча б одним провайдером;

– здатність атак на глобальну маршрутизацію завдати шкоди у великих масштабах – мільйонам мережевих пристроїв та користувачів. В останні роки інциденти, пов'язані із глобальною маршрутизацією за масштабом перевищують розповсюджені DDoS-атаки на кілька порядків;

– відносна «дешевизна» атак на глобальну маршрутизацію порівняно із розподіленими атаками на відмову в обслуговуванні (DDoS) і використанням програм-вимагачів (Ransomware);

– наявність уразливостей у базових протоколах глобальної маршрутизації;

– складність усунення проблем глобальної маршрутизації, що вимагає узгодження дій в ідеалі всіх провайдерів і операторів.

Серед інцидентів інцидентів глобальної маршрутизації можна виділити типові атаки, наведені в табл..1 і комплексні атаки на базі по-

рушення безпеки глобальної маршрутизації, яке може створювати умови успішної реалізації зловмисником DDoS атак або відслідковування трафіку.

Таблиця 1 – Типові загрози глобальній маршрутизації

№	Назва	Зміст	Наслідки
1	"Викрадення" префіксів / маршрутів (route hijacking)	Оператор або зловмисник видає себе за іншу мережу, імітуючи, що сервер або мережа – це їх клієнт	Пакети направляються за хибною адресою, що може спричинити DDoS-ефект або перехоплення трафіку
2	Витік маршрутів (route leaks)	Оператор через кілька апстрімів (часто через випадкову неправильну конфігурацію) анонсує одному апстрім-провайдеру, що в нього є маршрут до пункту призначення через іншого апстрім-провайдера	Може використовуватися для відслідковування та перехоплення трафіку
3	Підробка IP адрес (IP address spoofing)	Зловмисник створює пакети з підробною IP адресою джерела, щоб унеможливити ідентифікацію відправника або видати себе за іншу автономну систему (AS)	Передумова створення DDoS атак

При аналізі ризиків, пов’язаних із загрозами системі глобальної маршрутизації приймаються до уваги умови (сценарії) і ймовірності виникнення загроз та можливі наслідки реалізації загроз (табл..2), тяжкість яких залежить від параметрів автономної системи-жертви.

Таблиця 2 – Умови, ймовірності і наслідки атак

Атака	Ймовірність	Умови	Наслідки
Відмова в обслуговуванні	Дуже висока	Зловмисник має можливість: 1) перехопити маршрути; 2) створити чорну діру; 3) спрямувати увесь трафік, який адресований жертві, або його частину у чорну діру. Не потребує отримання та аналізу трафіку	Порушення доступності.
Підміна мережевих об'єктів	Висока	Зловмисник має можливість реалізувати наступний алгоритм: 1) IP-адреси мережі жертви присвоюються іншим мережевим пристроям, якими керує зловмисник; 2) зловмисник анонсує IP-адреси жертви так, щоб новий хибний маршрут мав вищий пріоритет порівняно з істинним маршрутом	Зловмисник набуває можливості скоювати певні дії в мережі з власних мережевих пристроїв, маскуючи їх під пристрої жертви (у граничному випадку – ініціювати та приймати повноцінні сеанси клієнт-сервер). Реалізація цієї атаки створює умови для виникнення інших загроз.

Атака	Ймовірність	Умови	Наслідки
Розголошування інформації	Висока	Зловмисник має можливість: 1) перехопити трафік; 2) провести аналіз трафіку і визначити особливості побудови мережевих протоколів рівня застосувань; 3) повернути трафік в мережу з метою маскування	Порушення конфіденційності
Модифікація даних	Середня	Зловмисник має можливість: 1) створити хибний анонс; 2) перехопити трафік; 3) модифікувати трафік; 4) повернути модифікований трафік в Інтернет з метою доставки істинному адресату. Така атака може відбуватись з підміною мережевих об'єктів або без неї.	Порушення цілісності даних. Якщо зловмисник має можливість модифікувати дані, то він також може прослуховувати трафік, аналізувати його, впроваджувати шкідливий код
Відмова від авторства		Зловмисник має можливість реалізувати підміну мережевих об'єктів	Відмова від авторства, маскування

Порушення безпеки глобальної маршрутизації можливе завдяки наявності вразливостей протоколів маршрутизації. Відповідно, загрози глобальної маршрутизації можуть бути класифіковані за протоко-

лами, типами протоколів, вразливості яких спричинили появу загрози, і за самими протоколами, BGP, BGPsec тощо.

Прикладом уразливостей безпеки BGP є фальшиві оновлення маршрутизації, що призводять до викрадення та перехоплення трафіку [4], яке може бути реалізоване різними методами, що також є критерієм класифікації атак:

– захоплення префіксу: вузол анонсує чужий префікс, тобто у якості джерела вказузе адресний простір, який йому не належить. Якщо фіктивний маршрут буде кротким, то BGP при виборі маршруту віддасть перевагу самк йому. Така атака може бути досить швидко виявлена за наявністю двох джерел з однаковим префіксом, що є помилкою у глобальній маршрутизації;

– захоплення маршруту: вузол легально отримує анонс чужого адресного простору і ретранслює його, пропонуючи транзит через себе. В цьому випадку хибний маршрут також конкурує з істинним, однак виявити захоплення маршруту важчк, ніж захоплення префіксу, бо джерело є істиним і не дублюється;

– захоплення підмереж: вузол ділить чужий адресний простір на дрібніші підмережі і анонсує їх специфічні префікси. Якщо конкуруючі префікси такого ж розміру відсутні, то анонсування більш специфічних префіксів має глобальний ефект, оскільки BGP при виборі маршруту віддає їм перевагу. Таким чином зловмисник, незважаючи на реальну топологічну віддаленість стає вузлом маршруту, який помилково вважається оптимальним;

– захоплення нерозподіленого або невикористаного адресного простору: зловмисник анонсує префікси нерозподіленого або невикористаного адресного простору, які не співпадають з іншими префіксами і тому не фільтруються, тобто мають змогу поширитися по всій мережі Інтернет. Захоплення нерозподіленого або невикористаного адресного простору може бути використане для короткострокової генерації довільного трафіку, в тому числі – для доставки шкідливого контенту, наприклад спаму. За більш складним сценарієм атаки перехоплений трафік спочатку використовується зловмисником для виконання певних дій (прослуховування, аналіз, модифікації даних), а потім повертається назад у мережу. При поверненні у мережу прослуханий, проаналізований чи содифікований трафік може просуватись далі легітимним маршрутом.

Перехоплення IP-адреси може статися випадково або може бути скоєне навмисно одним з перелічених вище способів, спільним для яких є отримуваний результат – пересилання процесів у невірну або тупикову частину мережі та порушення нормального процесу маршрутизації в мережі. Пакети, що потрапляють у неправильну частину мережі, потім або потрапляють у нескінченний цикл (і відкидаються), або опиняються у власності зловмисника. За фактом порушення доступності така атака може бути ідентифікована.

Зазвичай інтернет-провайдери фільтрують трафік BGP, дозволяючи оголошенням BGP зі своїх мереж містити тільки дійсний простір IP-адрес, однак на практиці можливі виключення.

Ризики глобальної маршрутизації мають ряд особливостей:

– загрози, з якими вони асоціюються, зазвичай виникають як результат навмисної діяльності або випадкових помилок суб'єктів глобальної маршрутизації (загрози типів A і D за ДСТУ ISO/IEC 27005:2023 [7]). Тобто, загрози природного походження (тип E) практично не аналізуються [2-6];

– вразливості, експлуатація яких дозволяє цим загрозам бути успішно реалізованими, є недоліками протоколів маршрутизації і/або недоліками налаштувань роутерів;

– наслідки реалізації цих загроз утворюють ієрархічну систему: на першому рівні – зміни в глобальній таблиці маршрутизації або її хибна інтерпретація, на другому рівні – несанкціонована зміна напрямку проходження мережевого трафіку, на третьому рівні – можливі дії зловмисника, який отримав доступ до трафіку (блокування трафіку чи його частини, модифікація даних тощо), на четвертому рівні результати певних дій зловмисника над трафіком (DDoS, спрямування на фальсифікований сайт, розсилання спаму тощо), на п'ятому рівні – наслідки для AS, на шостому рівні – наслідки для бізнес-процесів.

Висновки

В даній роботі проведено аналіз аналіз відкритих літературних джерел і визначені загрози та ризики глобальної маршрутизації, їх особливості та взаємозв'язки, розроблена класифікація загроз глобальній маршрутизації, показано, що порушення безпеки глобальної ма-

ршрутизації становить глобальну загрозу в сучасному кіберпросторі, з якою пов'язані ризики, що мають тенденцію до зростання.

Ризики глобальної маршрутизації можуть мати негативний вплив на бізнес- процеси і спілкування в мережі, особливо, якщо постачальники мережевих послуг (постачальники підключень, хмари та мережі доставки контенту) не приділяють достатньо уваги захисту процесів маршрутизації, не впроваджують новітні методи безпеки маршрутизації. Оскільки нормативні документи наявні тільки для протоколів маршрутизації, то єдиним способом запобігти ризикам глобальної маршрутизації на даний час є приєднання до спільноти MANRS [1], дотримання і популяризація її рекомендацій, застосування новітніх способів маршрутизації [6, 8].

Список літератури:

1. MANRS: Protect the Internet URL: https://www.manrs.org/

2. Зубок В.Ю. Оцінювання ризиків глобальної маршрутизації // Електронне моделювання. – 2019. – Т.41. – №2. – С.97-109. URL: https://www.emodel. org.ua/images/em/41-2/Zubok.pdf

3. Зубок В.Ю. Мохор В. В. Кібербезпека топології INTERNET : монографія. – К. : ІПМЕ ім. Г.Є.Пухова, 2022. – 191 с. URL: https://ipme.kiev.ua/ wp-content/ uploads/ 2022/07/ Zubok_Mokhor_Kiberbezpeka_ Topologii_Internet.pdf

4. Jiajia L., Yih-Chun H., Mingwei X., Jianping W. BGP with BGPsec: Attacks and Countermeasures // IEEE Network. – 2019. – Vol. 33. – Issue 4. – PP. 194-200, URL: https://ieeexplore.ieee.org/document/ 8594708;

5. Lakshmanan R. Researchers Uncover New BGP Flaws in Popular Internet Routing Protocol Software. URL: https://thehackernews.com/ 2023/05/ researchers-uncover-new-bgp-flaws-in.html

6. Чакрян В.Х. Моделі та методи маршрутизації трафіку в телекомунікаційних мережах з урахуванням вимог інформаційної безпеки. – Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня кандидата технічних наук (доктора філософії) за спеціальністю 05.12.02 «Телекомунікаційні системи та мережі» (172 – Телекомунікації та радіотехніка). – Харківський національний університет радіоелектроніки, Харків, 2017. URL: https://nure.ua/wp-content/uploads/2018/Dissertation /diss_Chakryan.pdf

7. ДСТУ ISO/IEC 27005:2023 (ISO/IEC 27005:2022, IDT). Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки. URL: https://online.budstandart.com/ru/catalog/doc-page?id_doc=104400

8. Патент України №107617 H04L 12/00, МПК (2016.01). Спосіб маршрутизації трафіку за допомогою протоколу EIGRP з урахуванням вимог інформаційної безпеки / Снігуров А.В., Чакрян В.Х.; власник Харківський національний університет радіоелектроніки. – № u201600667; заявл. 27.01.2016; опубл. 10.06.2016, бюл. № 11

УДК 004.056.52:53

РОЗРОБКА КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ РЕЖИМНО-СЕКРЕТНОГО ВІДДІЛУ МОРСЬКОГО ПОРТУ

Автор: *Харченко М.С., магістрант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Науковий керівник: *Нужний С.М., к.т.н., доцент, зав. каф. КТІБ, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв, Україна*

Анотація

Забезпечення інформаційної безпеки держави стоїть на одному рівні із захистом територіальної цілісності України та захистом суверенітету, як найважливішими функціями держави. Державна політика забезпечення інформаційної безпеки України є невіддільною частиною державної політики у сфері національної безпеки і оборони України. Інформаційна безпека полягає в аналізі загроз, які можуть виникнути в інформаційній сфері, і створенні умов для запобігання їхньому виникненню.

Аналіз, оцінка та використання позитивних здобутків країн ЄС та НАТО мають важливе значення при розбудові системи забезпечення інформаційної безпеки України, адже нині наша країна стикається з новими викликами та загрозами в інформаційній сфері та перебуває на

ЗМІСТ

Наукове видання

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

СПІБТ–2023

XI Всеукраїнська науково-технічна конференція
з міжнародною участю

23–24 листопада 2023 року

Національний університет кораблебудування
імені адмірала Макарова
Навчально-науковий інститут автоматики та електротехніки
просп. Центральний, 3, м. Миколаїв

МАТЕРІАЛИ КОНФЕРЕНЦІЇ

(*українською мовою*)

Відповідальна за випуск В. В. Трибулькевич