doi:https://doi.org/10.15407/emodel.41.02.097

УДК 004.7

В.Ю. Зубок, канд. техн. наук
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України
(Україна, 03164, Київ-164, вул. Генерала Наумова, 15,
тел. (+38044) 4241063, e-mail: vitaly.zubok@gmail.com)

Оцінювання ризику кібератак на глобальну маршрутизацію

Запропоновано нові теоретичні підходи щодо виявлення та оцінки ризику захоплення маршрутів. На основі єдиного методичного підходу [1] проведено систематизацію та класифікацію загроз, спричинених атаками на глобальну маршрутизацію. Запропоновано класичний підхід STRIDE до класифікації загроз безпеці маршрутизації та модель DREAD для оцінки кожної загрози за класифікацією STRIDE. З використанням таких вимірів отримано чисельне подання впливу кожної загрози на агреговану оцінку ризику.

К л ю ч о в і с л о в а: глобальна маршрутизація, перехоплення маршрутів, оцінка ризику, класифікація загроз, кібербезпека.

Актуальність проблеми перехоплення маршртів. Атака на глобальну маршрутизацію здатна завдати шкоди мільйонам мережевих пристроїв та користувачів і коштуватиме набагато менше, ніж відомі DDoS-атаки або здирницькі атаки (ransomware). Оскільки повністю уникнути захоплення маршрутів неможливо, актуальною проблемою є зведення ризику до мінімуму. Глобальна маршрутизація забезпечується десятками тисяч Інтернет-провайдерів. Протокол маршрутизації BGP-4 забезпечує поширення інформації про зв'язності і доступності IP-префіксів. Ця інформація постійно оновлюється в процесі обміну між автономними системами і формує для кожного Інтернет-вузла так звану глобальну таблицю маршрутизації. В результаті кожна підмережа знає (з тим чи іншим ступенем деталізації) як досягти будь-якої ділянки глобальної мережі.

В останні роки все частіше спостерігаються інциденти з так званим перехопленням чи крадіжкою маршрутів, які перетворюються на нову масштабну кіберзагрозу [2]. Ці інциденти за масштабом на кілька порядків перевищують широко відомі атаки класу DDoS і Ransomware, оскільки атака

на глобальну маршрутизацію здатна здійснити шкідливий вплив на мільйони мережевих пристроїв (а також користувачів) значно меншими зусиллями, ніж згадані вище популярні атаки. Наведемо декілька з останніх.

24 квітня 2018 року стався випадок з інфраструктурним IP-префіксом широко відомого хмарного сервісу Amazon AWS, метою якого була фішингова атака на криптовалютний сервіс MyEtherWallet. В ході атаки було «викрадено» префікс, який належить Amazon AWS і до якого прив'язані DNS сервери Amazon AWS. В результаті DNS-запити користувачів, які в якості рекурсивних DNS-резолверів використовували сервери Amazon AWS, було перенаправлено на підмінний DNS-сервер зловмисників, де імена хостів з суфіксом myethewallet.com перетворювались в IP-адреси фішингових сайтів, що працювали по протоколу HTTP. На відміну від HTTPS, в ньому немає автентифікації сервера. За повідомленнями атака тривала кілька годин і зловмисникам вдалося викрасти значну кількість криптовалют завдяки скомпрометованим даним користувачів [3].

12 листопада 2018 року в BGP-маршрутизації стався збій, що вплинув на роботу сервісів Google. Збій торкнувся сервісів G Suite, Google Пошук і Google Аналітика, а також внутрішніх систем компанії і сторонніх сервісів, включаючи Spotify. Винуватцем події став невеликий нігерійський провайдер MainOne Cable Company (AS37282), що анонсував сусіднім провайдерам префікси, які належать дата-центрам Google. За даними аналітичного сервісу BGPmon, який стежить за потоками трафіку в Інтернеті і першим виявив проблему, загалом нігерійський провайдер анонсував для своєї автономної системи 212 префіксів. Невірна інформація поширилася серед інших провайдерів, включаючи державного китайського провайдера China Telecom (AS 4809), який передав транзитом анонси до інших мереж, проте не прийняв (зафільтрував) трафік, що надходив до Google саме цими маршрутами. Аналітики стверджували, що подія мала виражений DoS-ефект щонайменше протягом 74 хв. [4]. Інцидент викликав безліч обговорень серед фахівців. Дослідники з Військово-морського коледжу США і університету у Тель-Авіві звинувачували China Telecom в навмисному улаштуванні BGP-збоїв, нібито китайський державний провайдер багато років некоректно направляє трафік західних країн без будь-яких наявних причин. Пізніше висновки дослідників підтвердили і аналітики компанії Oracle [5].

Усвідомлення проблеми BGP сталося досить давно, тому вже існують рекомендовані механізми, які дозволяють автоматично фільтрувати несанкціоновані маршрути, що надходять від провайдерів-сусідів. Нажаль, фільтрацію виконують не всі, є також проблеми з фільтрами навіть у найбільших у світі транзитних операторів. Тому BGP-інци-

денти — це результат не тільки помилки новачка або зловмисної активності атакуючого, але й нездатність великих операторів підтримувати в діючому стані свої фільтри маршрутів.

Швидко вирішити дану проблему неможливо, адже замість єдиного Інтернету існує безліч окремих мереж і у кожної з них є власні настройки BGP-маршрутизації. Оскільки причиною більшості витоків є неправильне налаштування протоколу, єдиним способом вирішення проблеми стає усунення умов, при яких помилки інженерів здатні впливати на інших операторів зв'язку. Потрібно обмежити функціонально BGP, тобто вбудувати в протокол опціональні механізми фільтрації, тим самим збільшивши складність його налаштування.

Низка міжнародних фахівців намагається внести свій внесок у поліпшення технічної складової Інтернету і розвиває ініціативу щодо внесення змін до стандарту протоколу BGP в рамках міжнародної організації IETF (Internet Engineering Task Force) — Інженерної ради Інтернету. Ця організація являє собою велике професійне співтовариство мережевих архітекторів, операторів, вендорів, дослідників з усього світу, які впливають на еволюцію архітектури Інтернету і його функціонування. Розширення BGP, що знаходиться в стадії чернетки стандарту, надасть механізм для автоматичного виявлення BGP-перехоплень і запобігання їх поширенню. Але реалізація цього завдання займе роки навіть в разі повного успіху і прийняття професійним співтовариством. Оскільки потрібно міняти протокол, то, щоб система стала ефективною, відповідні зміни повинні бути впроваджені значним числом операторів у світі. Однак, на жаль, зловмисна активність та її наслідки є реальністю, яку варто враховувати при плануванні своїх ризиків вже зараз.

На основі єдиного методологічного підходу, який викладено в настановах [1], проведемо систематизацію та класифікацію загроз, що з'являються від атак на глобальну маршрутизацію, і розглянемо підхід до оцінювання ризиків, що виникають внаслідок цих загроз.

Деякі методи аналізу загроз і оцінки ризиків. При забезпеченні інформаційної безпеки необхідно дослідити ланцюжок від потенційного зловмисника, наявної вразливості, загрози її використання, безпосередньої дії (атаки) та її наслідків. Класифікація загроз охоплює сукупність можливих варіантів дій джерел загроз, які призводять до реалізації цілей атаки. Мета атаки може не співпадати з метою реалізації загроз і може бути направлена на отримання проміжного результату, необхідного для досягнення надалі реалізації загрози. У разі такого незбігу атака розглядається як етап підготовки до здійснення дій, направлених на реалі-

зацію загрози, тобто як «підготовка до здійснення» протиправної дії. Завдяки такому підходу можна здійснити наступне:

встановити пріоритети цілей безпеки;
визначити перелік актуальних джерел загроз;
визначити перелік актуальних вразливостей;
оцінити взаємозв'язок загроз, джерел загроз і вразливостей;
визначити перелік можливих атак на об'єкт;
описати можливі наслідки реалізації загроз.

Результати проведення оцінки і аналізу можуть бути використані при виборі адекватних оптимальних методів протидії загрозам, а також при аудиті реального стану інформаційної безпеки об'єкту для його страхування.

При визначенні актуальних загроз експертно-аналітичним методом визначаються об'єкти захисту, вразливі до дії тієї або іншої загрози, характерні джерела цих загроз і уразливості, які сприяють їх реалізації. За результатами аналізу складається матриця взаємозв'язку джерел загроз і вразливостей, за якою визначаються можливі наслідки реалізації загроз (атак), і обчислюється коефіцієнт небезпеки цих атак як добуток коефіцієнтів небезпеки відповідних загроз і джерел загроз, визначених раніше.

Аналіз потенційно можливих загроз інформації є одним з перших і обов'язковим етапом розробки будь-якої захищеної інформаційної системи. При цьому складається якомога повніша сукупність загроз, аналізується ступінь ризику при реалізації тієї або іншої загрози, після чого визначаються напрями захисту інформації в конкретній системі. Краще за все аналізувати наслідки реалізації загроз ще на стадії проектування локальної мережі, робочого місця або інформаційної системи, для того щоб заздалегідь визначити потенційні втрати і встановити вимоги до заходів забезпечення безпеки. Вибір захисних і контрольних заходів на ранній стадії проектування системи вимагає набагато менших витрат, ніж виконання подібної роботи на діючій системі.

Модель STRIDE (за першими буквами назв категорій) розроблена фірмою Microsoft і майже 20 років успішно застосовується для визначення та «зважування» загроз [6]. Вона заснована на класифікації загроз безпеці за наступними категоріями:

1. Підміна мережевих об'єктів (Spoofing identity). Атаки такого типу дозволяють зловмисникові видавати себе за іншого користувача або підміняти справжній сервер підробленим. Приклад підміни особи користувача — використання чужих автентифікаційних даних (імені користувача, пароля) для атаки на систему.

2. Модифікація даних (Tampering with data). Атаки цього типу порушують цілісність даних, що зберігаються, обробляються чи передаються.

Приклади: несанкціоновані зміни даних (наприклад, що зберігаються в базі даних).

3. Відмова від авторства (Repudiation). Легальний користувач може виконати певну операцію і відмовитися від її «авторства», а адміністраторові не вдасться нічого довести в разі відсутності чи несправності механізмів аудиту та протоколювання дій користувачів.

4. Розголошування інформації (Information disclosure). Розкриття інформації особам, яким заборонено доступ до неї, тобто порушення конфіденційності.

5. Відмова в обслуговуванні (Denial of service). В атаках такого типу зловмисник намагається позбавити доступу до сервісу правомочних користувачів, наприклад, зробивши веб-сервер тимчасово недоступним або непридатним для роботи.

6. Підвищення привілеїв (Elevation of privilege). Непривілейований користувач дістає привілейований доступ, що дозволяє йому «проникнути» в систему, а саме отримати конфіденційну інформацію, підмінити чи впровадити власний програмний код або знищити систему.

У табл. 1 наведено методи, які застосовуються для боротьби з небезпеками, описаними в моделі STRIDE. Основні запропоновані засоби боротьби з загрозами наступні:

автентифікація користувачів;
розподіл повноважень (авторизація);
захист від несанкціонованого доступу;
аудит;
фільтрація.

У 2003 році запропоновано спосіб оцінки ризиків DREAD [7], який також засновано на класифікації загроз безпеці за наступними категоріями (перші букви п’яти категорій):

1. Потенційний збиток (Damage potential). Це міра реального збитку від успішної атаки. Найвищий ступінь небезпеки означає практично безперешкодний злом засобів захисту і виконання практично будь-яких операцій. Підвищенню привілеїв зазвичай привласнюють оцінку 10. У інших ситуаціях оцінка залежить від цінності даних, які захищають.

2. Відтворюваність (Reproducibility). Це міра можливості реалізації загрози. Деякі вразливості доступні постійно, інші — тільки залежно від ситуації, і їх доступність непередбачувана, тобто не можна напевно знати, наскільки успішною виявиться атака. Наприклад, вразливості, знайдені у типовому програмному забезпеченні, характеризуються високою відтворюваністю.

3. Легкість організації атаки (Exploitability). Це є міра зусиль і кваліфікації, необхідних для проведення атаки. Якщо її може реалізувати не-

досвідчений програміст на домашньому комп'ютері — оцінка небезпеки 10, якщо для її проведення треба витратити 100 млн. доларів, — оцінка 1. Атака, для якої можна створити алгоритм (а отже, розповсюдити у вигляді сценарію серед любителів), також оцінюється у 10 балів. Слід враховувати необхідний для атаки рівень автентифікації і авторизації в системі. Наприклад, якщо це доступно будь-якому видаленому анонімному користувачеві, подібна небезпека оцінюється у 10 балів.

4. Коло користувачів, що потрапляють під удар (Affected users) — частка користувачів, робота яких порушується внаслідок успішної атаки. Оцінка виконується на основі процентної частки: 100% користувачів відповідає оцінка 10 балів, а 10% — 1 бал. Іноді небезпека стає реальною тільки в системі, яка конфігурована особливим чином.

Таблиця 1

Тип загрози	Засіб боротьби
Підміна мережевих об'єктів (S)	Надійний механізм автентифікації
	Захист секретних даних
	Відмова від зберігання секретів
Модифікація даних (T)	Надійний механізм авторизації
	Використання хеш-кодувань
	MAC-коди
	Цифрові підписи
	Протоколи, що запобігають прослуховуванню трафіка
Відмова від авторства (R)	Цифрові підписи
	Мітки дати і часу
	Контрольні сліди
Розголошування інформації (I)	Авторизація
	Протоколи з посиленим захистом від несанкціонованого доступу
	Шифрування
	Захист секретів
	Відмова від зберігання секретів
Відмова в обслуговуванні (D)	Надійний механізм автентифікації
	Надійний механізм авторизації
	Фільтрація
	Управління числом вхідних запитів
	Якість обслуговування
Підвищення рівня привілеїв (E)	Виконання з мінімальними привілеями

5. Важкість виявлення (Discoverability) — наскільки швидко і чи взагалі можна виявити факт реалізації загрози. Ця оцінка вважається найскладнішою для визначення.

Інтегральний ризик R в методиці DREAD оцінюється за формулою

$$R = \frac{R_{\text{Dam}} + R_R + R_E + R_A + R_{\text{Dis}}}{5},$$

де R_{Dam} і R_{Dis} — чисельні оцінки відповідних типів ризику. Подекуди в методику DREAD включають ще один показник, а саме витрати на усунення наслідків успішної атаки, який умовно названо X (eXpense). Таким чином, для кількісної оцінки ризику використовується модель DREADX і сумарна DREADX-оцінка дорівнює сумі всіх оцінок, поділеній на шість.

Ризик перехоплення маршруту в термінах ISO/IEC 73:2009. У роботі [8] сформульовано поняття ризику, описано причетні сторони та ознаки, за якими можна ідентифікувати ризики, а саме:

джерелами виникнення ризику обов'язково є інші суб'єкти глобальної маршрутизації;

події, які спричиняють ризик, є джерелом несанкціонованих змін в глобальній таблиці маршрутизації чи її інтерпретації на інших суб'єктах глобальної маршрутизації;

наслідками цих подій є несанкціонована зміна напрямку проходження мережевого трафіку.

Опишемо ризики, які виникають внаслідок загроз глобальній маршрутизації, по методу DREAD. Міра (межа) потенційного збитку (damage potential) може бути дуже високою внаслідок того, що вона впливає на всі аспекти інформаційної безпеки. Відтворюваність (reproducibility), тобто можливість використати вразливість «типовими» засобами, які не потрібно розробляти під конкретну атаку, є також високою. Для проведення атаки з перехопленням маршруту використовуються стандартні засоби керування глобальною маршрутизацією.

Складність організації атаки на практиці умовно має три рівні:

найнижчий — атаку може здійснити будь-який користувач;

середній — атаку може здійснити тільки користувач з професійними навичками та інструментами;

найвищий — атакувати може лише освічений спеціаліст рівня розробника.

Попри те, що багато атак типу перехоплення маршруту відбувається помилково, через низьку кваліфікацію чи брак досвіду, атаку може виконати лише професіонал з навичками та інструментами. «Область ураження», коло користувачів, які опиняться під впливом перехоплення маршруту, є потенційно надзвичайно великим і зазвичай перевищує кількість

уражених від більш типових атак DDoS з використанням виснаження ресурсів [1].

За показником складності виявлення (discoverability) атаки перехоплення маршруту є такими, виявити які найпростіше. З перелічених інцидентів всі атаки і їхні джерела були виявлені протягом декількох годин. Проте лишається відомий інцидент з крадіжкою криптовалют у 2014 р., коли підміною маршрутів зловмисники досягали своїх цілей протягом чотирьох місяців [1].

Класифікація загроз глобальній маршрутизації. Атака класу BGP-hijacking має кілька варіантів реалізації:

1. Захоплення префіксу, коли вузол анонсує у якості джерела адресний простір, який йому не належить. При виборі маршруту BGP віддасть перевагу більш короткому маршруту, вимірюваному числом мереж між джерелом і одержувачем. Цей маршрут конкуруватиме з істинним [2, рис. 1]. Така атака може бути швидко виявлена, бо у глобальній маршрутизації наявність двох джерел в одного префікса є помилкою.

2. Захоплення маршруту, в якому вузол ретранслює легально отриманий анонс чужого адресного простору, пропонуючи транзит через себе. Цей маршрут буде також конкурувати з істинним, проте, на відміну від попереднього випадку, джерело не підмінюється і виявити такий інцидент значно складніше.

3. Захоплення підмереж через анонсування більш специфічних префіксів. При виборі маршруту BGP обирає той, який вказано більш специфічним префіксом, і таким чином атакуючий виграє, незважаючи на топологічну віддаленість. За відсутності конкуруючих префіксів такого ж розміру захоплення має глобальний ефект [2, рис. 2].

4. Захоплення нерозподіленого або невикористаного адресного простору. Анонсований префікс не зустрічає конкуренції і має високі шанси поширення по всьому Інтернету.

5. Перенаправлення трафіку. Трафік доставляється коректному одержувачу, але передається шляхом, відмінним від істинного.

Наслідки атак на глобальну маршрутизацію можуть бути різними. Захоплення маршруту призводить до перетягування трафіку, призначеного для захопленої мережі, який зазвичай потім відкидається. Така стратегія має назву створення «чорної діри» (blackholing) — мережеві пакети проходять хибним маршрутом та «зникають». Таким чином відбувається DoS-атака на всі сервіси мережі. У цю категорію атак потрапляє більшість помилок конфігурації маршрутизаторів.

Якщо при атаці анонсується фрагмент адресного простору, який досі не використовувався (так звані «нічиї мережі», можливо, нерозподілений

адресний простір), вона може бути використана для короткострокової генерації не просто трафіку, а для доставки шкідливого контенту, тобто елементарно — для розсилки спаму.

Інший варіант стратегії — перенаправлення трафіку. Трафік йде не в чорну діру, а перехоплюється і аналізується. Іноді атака ще більш глибока, і перехоплений трафік не тільки не йде в чорну діру і аналізується, але після перехоплення повертається знову в Інтернет, щоб бути доставленим істинному одержувачу. Таку атаку важче виявити. Метою може бути не тільки підслуховування, але і модифікація переданих даних. У більш витонченому вигляді захоплення маршруту може бути спрямоване на захоплення деякого інформаційного ресурсу, наприклад веб-сайту, з наданням користувачам підробленого сайту.

Проведемо класифікацію цих загроз відповідно до моделі STRIDE.

Загроза підміни мережевих об'єктів притаманна атакам на глобальну маршрутизацію. Механізм реалізації загрози наступний:

1) IP-адреси мережі жертви присвоюються іншим мережевим пристроям, розташованим під керуванням зловмисника;

2) зловмисник анонсує IP-адреси жертви так, щоб новий хибний маршрут мав вищий пріоритет порівняно з істинним маршрутом;

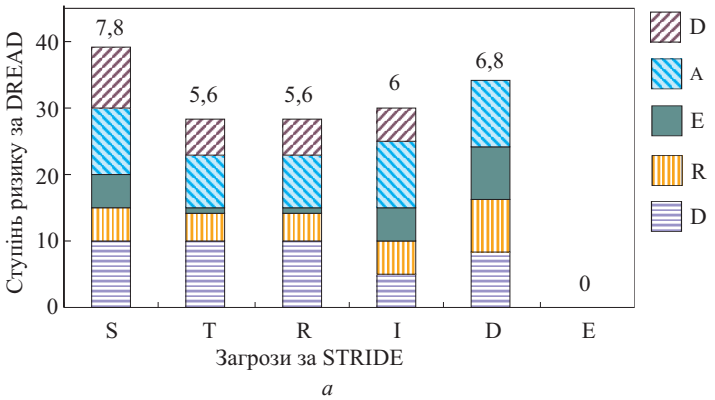
3) зловмисник набуває можливості створювати мережеву активність (навіть ініціювати та приймати повноцінні сеанси клієнт-сервер) з власних мережевих пристроїв, видаючи їх за пристрої жертви.

Реалізація атаки за таким сценарієм лежить в основі наступних загроз.

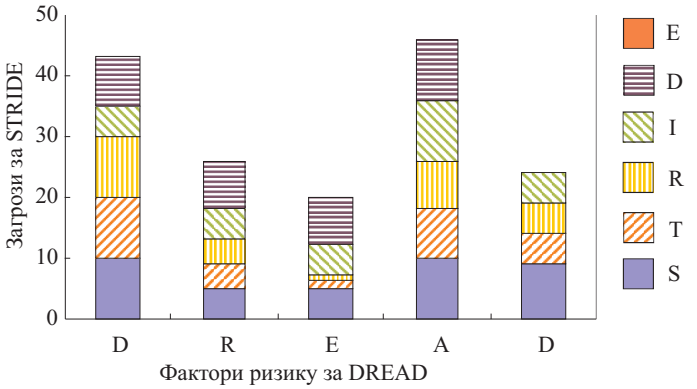
Загроза модифікації даних, або порушення цілісності даних, є реальною в разі, коли перехоплений зловмисником завдяки хибному анонсу трафік повертається зловмисником знову в Інтернет, щоб бути достав-

Таблиця 2

Тип загрози	R_{Dam}	R_R	R_E	R_A	R_{Dis}	Інтегральний ризик R
S	10	5	5	10	9	7,8
T	10	4	1	8	5	5,8
R	10	4	1	8	5	5,8
I	5	5	5	10	5	6
D	8	8	8	10	0	6,8
E	0	0	0	0	0	0
Сума по категоріях	43	26	20	46	24	32,2



а



б

Діаграми оцінки загроз від атак по методу STRIDE за факторами ризику DREAD (*а*) та вага загроз STRIDE в оцінці різних типів ризику (*б*)

леним істинному одержувачу. Така атака може відбуватись з підміною мережевих об'єктів або без неї.

Загроза відмови від авторства також є можливою в ході атаки разом із з підміною мережевих об'єктів.

Загроза розголошування інформації внаслідок перехоплення трафіку є однією з найсуттєвіших. Порушення конфіденційності є можливим в разі виконання атаки методом перехоплення трафіку та повернення його в мережу, бо це часто є необхідною умовою з урахуванням особливостей побудови мережевих протоколів рівня застосувань.

Відмова в обслуговуванні є найчастішим наслідком перехоплення маршрутів. Створення чорної діри, в яку потрапляє частина трафіку, що адресовано мережі жертви, не потребує отримання та аналізу трафіку.

Загроза підвищення рівня привілеїв не властива атакам з захопленням префіксу, оскільки керування глобальною маршрутизацією не має ієрархії повноважень.

Оцінювання ризику атак на глобальну маршрутизацію. З урахуванням пояснень до оцінки ризиків DREAD та запропонованої класифікації конкретних загроз глобальній маршрутизації, побудуємо матрицю ризиків, поєднуючи класифікації загроз STRIDE та оцінки ризиків DREAD. Як запропоновано в моделі DREAD, оцінки для кожної загрози будуть від 0 до 10. При цьому 10 означатиме високу вірогідність настання певного наслідку від реалізації даної загрози, а 0 — або відсутність наслідку або невластивість подібної загрози при атаках типу перехоплення маршруту.

Приклад такої оцінки наведено в табл. 2 і на рисунку, де застосовано оцінки, отримані в результаті аналізу відомих інцидентів безпеки в глобальній маршрутизації. Ці результати візуалізовано у вигляді двох діаграм, де показано, на які ризики впливає певний тип загрози (рис. 1, *а*) і які загрози є складовими в оцінці певного фактору ризику (рис. 1, *б*).

Для оцінювання впливу загроз потрібно мати чітке уявлення про природу походження загрози, а саме про її джерело, об’єкти впливу, способи реалізації. Адекватність такого оцінювання має базуватись на розумінні теоретичних основ та сучасних практик імплементації протоколу глобальної маршрутизації BGP-4 при побудові зв’язків між Інтернет сервіс-провайдерами.

Висновки

Інциденти з перехопленням маршрутів в глобальній Інтернет-маршрутизації — це результати помилки новачка, нездатність великих операторів підтримувати в актуальному стані свої фільтри маршрутів, та, безумовно, результати кібератак. Попри те що IETF ініціює внесення змін до стандарту протоколу BGP, відповідні зміни повинні бути впроваджені значним числом операторів у світі, а це відтерміновує впровадження змін на невизначений термін. Запропонована двовимірна модель оцінки ризиків на основі класифікації загроз і поєднання добре відомих моделей STRIDE та DREAD дає змогу визначити стратегію поводження з ризиками атак на глобальну маршрутизацію. Результат дозволяє отримати кількісну оцінку ризику кожної загрози глобальній маршрутизації в мережі Інтернет.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. *Risk Management* — Vocabulary (ISO Guide 73:2009, IDT) : ДСТУ ISO Guide 73:2013. [Чинний від 2014—07—01]. Київ : Мінекономрозвитку України, 2014, 13 с. (Національні стандарти України).
2. *Зубок В.Ю.* Визначення напрямків протидії кібератакам на глобальну маршрутизацію в мережі Інтернет // Електрон. моделювання, 2018, **40**, №5, с. 67—76.
3. *История одного* BGP hijack, или необходимо ли фильтровать full-view от аплинков. [Електронний ресурс] Режим доступу: https://nag.ru/articles/article/101232/istoriya-odnogo-bgp-hijack-ili-neobhodimo-li-filtrovat-full-view-ot-aplinkov.html. Дата звернення: Січ. 20, 2019.
4. *Internet Vulnerability* Takes Down Google. [Електронний ресурс] Режим доступу: https://blog.thousandeyes.com/internet-vulnerability-takes-down-google/. Дата звернення: Січ. 20, 2019.
5. *China Telecom's* Internet Traffic Misdirection. [Електронний ресурс] Режим доступу: https://internetintel.oracle.com/blog-single.html?id=China+Telecom%27s+Internet+Traffic+Misdirection. Дата звернення: Січ. 15, 2019.
6. *Kohnfelder L., Garg P.* The threats to our products. [Електронний ресурс] Режим доступу: https://adam.shostack.org/microsoft/The-Threats-To-Our-Products.docx. Дата звернення: Лют. 21, 2019.
7. *Howard M., LeBlanc D.* Writing Secure Code, 2nd edition. Microsoft Press, 2003, 768 p.
8. *Зубок В.Ю., Мохор В.В.* Дослідження зв'язку між топологією та ризиком внаслідок кібератак на глобальну маршрутизацію // Моделювання та інформаційні технології, 2018, Вип. 85, с. 23—26.

Отримано 11.03.19

REFERENCES

1. Risk Management — Vocabulary (ISO Guide 73:2009, IDT): DSTU ISO Guide 73:2013, Kyiv, Minekonomrozvytku Ukrainy, 2014.
2. Zubok, V. (2018), "Determining the ways of counteraction to cyberattacks on the Internet global routing", *Elektronne modelyuvannya*, Vol. 40, no. 5, pp. 67-76.
3. "History of some BGP hijack, or whether it is necessary to filter fill-view from uplinks", available at: https://nag.ru/articles/article/101232/istoriya-odnogo-bgp-hijack-ili-neobhodimo-li-filtrovat-full-view-ot-aplinkov.html (accessed January 21, 2019).
4. "Internet Vulnerability Takes Down Google", available at: https://blog.thousandeyes.com/internet-vulnerability-takes-down-google/ (accessed January 20, 2019).
5. "China Telecom's Internet Traffic Misdirection", available at: https://internetintel.oracle.com/blog-single.html?id=China+Telecom%27s+Internet+Traffic +Misdirection (accessed January, 2019).
6. Kohnfelder, L. and Garg, P. (1999), "The threats to our products", available at: https://adam.shostack.org/microsoft/The-Threats-To-Our-Products.docx (accessed January 20, 2019).
7. Howard, M. and LeBlanc, D. (2003), Writing Secure Code, 2nd edition, Microsoft Press, Redmond, USA.
8. Zubok, V. and Mokhor, V. (2018), "Exploring the relations between topology and security risk of cybernetic attacks on global Internet routing", *Modelyuvannya ta informatsiyni teckhnologii*, Vol. 85, pp. 23-26.

Received 11.03.19

В.Ю. Зубок

ОЦЕНИВАНИЕ РИСКА КИБЕРАТАК
НА ГЛОБАЛЬНУЮ МАРШРУТИЗАЦИЮ

Предложены новые теоретические подходы к выявлению и оценке риска захвата маршрутов. На основе единого методического подхода, изложенного в [1], проведена систематизация и классификация угроз глобальной маршрутизации. Предложен классический подход STRIDE для классификации угроз безопасности маршрутизации, а также модель DREAD для оценки каждой угрозы по классификации STRIDE. С использованием этих двух измерений получено численное выражение влияния каждой угрозы на общую оценку риска.

К л ю ч е в ы е с л о в а: глобальная маршрутизация, перехват маршрутов, оптимизация связей, кибербезопасность.

V.Yu. Zubok

GLOBAL INTERNET ROUTING
CYBERATTACKS RISK ASSESSMENT

Attacking global routing is capable of harming millions of network devices (and also users) with much less effort than the well-known DDoS or ransomware attacks. Since route hijacking can't be fully mitigated, minimizing the risk is an actual problem. Relying on actual world practices of risk management, in this paper author offers some new theoretical approaches of identification and evaluation of route hijacking risk. Earlier, we have proceeded through ISO Guide 73:2009 "Risk Management – Vocabulary" to tie-up to the commonly used methodical approach for risk management. In this paper we provide a classic STRIDE approach to routing security threats classification, and DREAD model to assess each threat of STRIDE acronym. Using such two-dimensional measuring, we achieved a numerically expressed impact of each threat on aggregated risk evaluation.

K e y w o r d s: global routing, route hijacking, cyberattack, risk assesment, threats evaluation.

ЗУБОК Віталій Юрійович, канд. техн. наук, ст. наук. співр. Ін-ту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. У 1994 р. закінчив Київський політехнічний ін-т. Область наукових досліджень — глобальні інформаційні мережі, Інтернет, теорія складних мереж.