mizh-armiyami-nato-ukraina-perevodit-viyskovu-logistiku-z-paperu-na-nativsku-it-sistemu-logfas-naskilki-skladniy-tsey-shlyakh-07092022-8129

УДК 004.056:351.746(043.2)

Кузнєцов І.О., здобувач 3 курсу
спеціальність 125 «Кібербезпека»
Наукові керівники:
Загоруйко Л.В., к.т.н., доцент, доцент кафедри інформаційних технологій
Мартьянова Т.А. к.т.н., ст. викладач кафедри інформаційних технологій

ЕВОЛЮЦІЯ СИСТЕМ УПРАВЛІННЯ КІБЕРПРОСТОРОМ

Донецький національний університет ім. Василя Стуса, м. Вінниця

У роботі розглянуто основні керуючі системи, які відіграють ключову роль в управлінні кіберпростором, виділено структурні елементи кіберпростору та їх взаємозв'язку між собою. Розглянуто регіональні інтернет реєстратори, представлено їх граф зв'язаності.

Розглянуто автономні системи та точки обміну трафіком. Представлені найбільші телекомунікаційні альянси, які впливають на діяльність операторів зв'язку (безпосередньо чи опосередковано) і, зрештою, на одержувані кінцевими споживачами набори ресурсів і послуг, наданих телекомунікаційними операторами.

Ключові слова: кіберпростір, автономна система, управління, інтернет реєстратори, точка обміну трафіком, телекомунікаційні альянси, граф зв'язаності, ICANN.

Вступ

Рушійною силою еволюції систем управління кіберпростором є можливість істотного, а часом і принципового впливу на соціальні, економічні та військово-політичні процеси будь-якого масштабу. У процесі управління кіберпростором задіяна велика кількість учасників з різним ступенем участі та впливу на параметри кіберпростору.

Інтеграція мереж світових операторів зв'язку, інфокомунікаційних систем, систем навігації, моніторингу, інформаційної інфраструктури, інформаційних та телекомунікаційних технологій, технологій їх поєднання та управління тощо, воєдино призвело до формування простору планетарного масштабу – кіберпростору. Використовуючи ресурси кіберпростору, здійснюється управління організаційними та технологічними процесами,

реалізованими в рамках об'єктів та суб'єктів критичної інфраструктури держави, у тому числі банківською системою, логістичними процесами, енергетикою, водопостачанням, медициною, освітою та ін. [1-3]. Використання цих систем, ресурсів та послуг, що надаються кіберпростором, зробило їх мішенню як кіберкомандувань іноземних держав та організованих хакерських угруповань, і одиночних хакерів, які регулярно здійснюють моніторинг і деструктивні програмні атаки на інфраструктуру держав [4-5].

Можливість віддалених деструктивних впливів на критичну інфраструктуру держав дозволяє без фактичного введення збройних сил на територію держави та оголошення війни дестабілізувати її економіку та інфраструктуру.

Керування параметрами кіберпростору можна здійснювати як у спільних інтересах (у рівних частках і пропорціях), так і шляхом зміни параметрів кіберпростору на користь однієї зі сторін.

Єдиного центру управління кіберпростором не існує, але боротьба за кількість параметрів, ступінь управління ними, а також за перенесення каналів управління на певну підконтрольну територію ведеться постійно.

Враховуючи високу складність, динамічність зміни складу, структури та процесів, що протікають у кіберпросторі, безлічі різнорідних, територіально розподілених елементів, що є його складовими, а також розподілений характер його ресурсів, кіберпростір поки не має єдиного центру управління, а сам процес Управління реалізується великою кількістю учасників з різним ступенем участі та впливу на параметри кіберпростору.

Загалом процес управління – це збір інформації про стан керованого об'єкта, ухвалення рішення про бажаний стан та подальшу зміну параметрів, які переводять об'єкт управління у бажаний стан. Відповідно, для здійснення управління кіберпростором необхідно мати доступ до управління ключовими параметрами та здійснювати їх зміну швидше ніж безліч протиборчих сторін.

Залежно від завдань, управління можна розділити на:

Оперативне (поточне) управління – безпосереднє управління, яке здійснюється в поточних умовах та вирішує поточні завдання. Керування простором IP-адрес, керування службою єдиного часу та синхронізації, доменами верхнього рівня, параметрами протоколів тощо.

Середньострокове управління – спрямоване на розв'язання середньострокових завдань. Наприклад, обладнання території щодо зв'язку (створення нових вузлів, вибір оптимальних місць їх розміщення, будівництво регіональної кабельної інфраструктури, переведення інших елементів кіберпростору регіону під свою юрисдикцію), виділення пулів IPадрес, реєстрація автономних систем тощо.

Стратегічне управління – спрямоване на довгострокові цілі та дії. Стратегії розвитку кіберпростору, оснащення території в галузі зв'язку

(будівництво міжконтинентальної кабельної інфраструктури, створення точок обміну трафіком, хостів-реплік *DNS* серверів тощо), розробка нових протоколів, стандартів та обладнання, що дозволяє їх реалізувати, ліцензування, технологічне випередження конкурентів тощо.

ICANN, IANA та кореневі DNS сервери

Основними функціями *ICANN (Internet Corporation for Assigned Names and Numbers)* є регулювання питань, пов'язаних з доменними іменами, *IP*-адресами та іншими аспектами функціонування кіберпростору. Крім цього, *ICANN* координує функції IANA (Internet Assigned Numbers Authority) з управління просторами *IP*-адрес, доменами верхнього рівня та параметрами протоколів, що використовуються в кіберпросторі.

Формально ICANN є незалежною спільнотою зацікавлених сторін-волонтерів з усього світу, головною метою яких є забезпечення стабільності, безпеки та єдності глобального інтернету. Однак питання з незалежністю *ICANN* є досить складним і потребує розгляду історичного аспекту появи *ICANN*.

Враховуючи складність розв'язуваних ICANN завдань, своє функціонування воно здійснює консультаційно у взаємодії:

- з міжнародним союзом електрозв'язку (Inter national Telecommunication Union, ITU) – визначає стандарти в галузі телекомунікацій;

- з всесвітньою організацією інтелектуальної власності (Organisation Mondiale de la Pro periete Intelectuelle, OMPI) – адміністрування міжнародних конвенцій у галузі інтелектуальної власності;

- з організацією економічного співробітництва та розвитку (Organization for Economic Cooperation and Development, OECD) – міжнародна економічна організація розвинених країн. Здійснює аналітичну роботу, виробляє рекомендації для країн-членів і служить платформою для організації багатосторонніх переговорів щодо економічних проблем.

Функціонування в контакті з цими організаціями дозволяє формувати та приймати в якості рекомендацій «зручні» для ICANN стандарти, використовувані протоколи, телекомунікаційне обладнання, визначати порядок його функціонування тощо. Усі елементи телекомунікаційного обладнання своєчасно патентуються, що унеможливлює вихід на ринок «неугодних» виробників, а виробників, що залишилися, змушує купувати патенти. Після чого всі рекомендації, обладнання, протоколи можуть рекомендуватися за допомогою OECD (Organisation for Economic Co-operation and Development) як у країнах, що входять до його складу, так і світовому співтовариству.

Регіональні та локальні інтернет реєстратори

Забезпеченням технічної складової функціонування кіберпростору займається *RIR* (*Regional Internet Registry*) здійснюючи: виділення *IP*-адрес, номерів автономних систем (*Autonomous System, AS*), моніторинг точок обміну

трафіком, статистичний аналіз мереж, що входять до кіберпростору та інших технічних сторін функціонування кіберпростору. Усі *RIR* колективно утворюють *NRO* (*Number Resource Organization*), створену для представлення інтересів *RIR* та їх глобальної взаємодії.

На рис. 1 поданий граф зв'язаності регіональних інтернет-реєстраторів.

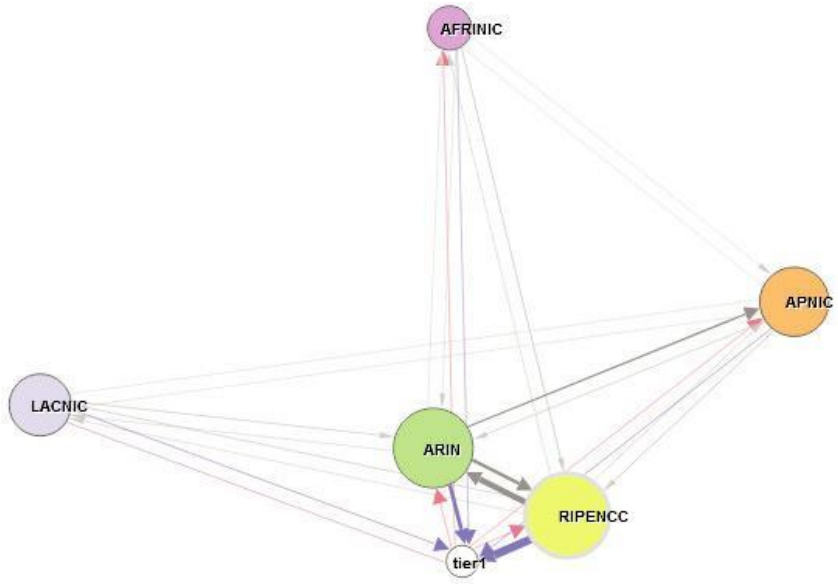

Рис. 1. Граф зв'язаності регіональних інтернет-реєстраторів

Вершинами графа є *RIR*, а ребрами кількість з'єднань між ними, чим товще ребро між вершинами, тим більше з'єднань у ньому проходить. Tier 1 – пірингові оператори. Як видно з рис 1, найбільша кількість з'єднань є між Європою та Україною (*RIPENCC)*, Північною Америкою (*ARIN*) та піринговими операторами, які здійснюють транзит трафіку. Кожен із *RIR* має автономні системи, розташовані в різних країнах.

Таким чином, з першого погляду незалежні телекомунікаційні оператори приймають свої рішення на основі координуючих органів (альянсів), які, в першу чергу, діють у своїх інтересах, і основною метою яких у мирний час є отримання прибутку, та рішення, прийняті - що мають керівництво альянсу, впливають на діяльність операторів зв'язку (безпосередньо чи опосередковано).

Автономні системи та точки обміну трафіком

Автономні системи є одним із ключових елементів у структурі кіберпростору. Згідно з міжнародними рекомендаціями, під автономною системою розуміється сукупність маршрутизованих діапазонів IP-адрес під єдиним адміністративним управлінням із загальною, однозначно визначеною політикою маршрутизації.

Кожна AS має унікальний номер та керує як мінімум одним діапазоном IP-адрес (IPv4, IPv6). Розподіл IP-адрес регулюють RIR (LIR). Для забезпечення коректної маршрутизації трафіку в мережі кожен власник AS зобов'язаний

оперативно вносити зміни до записів бази даних RIR (LIR), які відбивають політику маршрутизації.

Під точкою обміну трафіком розуміється мережева інфраструктура, призначена для оперативної організації з'єднань та між операторського обміну IP-трафіку (пірингу) між незалежними мережами. Учасниками обміну трафіку є організації, які керують автономними системами. Точка обміну трафіком у більшості випадків не є «точкою» у класичному її розумінні, а представляє собою сукупність технологічних майданчиків у межах міста чи країни, з'єднаних між собою високошвидкісними каналами передачі даних. Внутрішня структура точки обміну трафіком прихована від учасників обміну, тому для них вона є «точкою».

Висновок

Управління кіберпростором є вкрай складним процесом, що задіює безліч структур, основною з яких є наднаціональна структура *ICANN*, створена і що знаходиться в США, підпорядкована їхньому законодавству та чинна згідно з моделлю управління, схваленою США. За фактом управління кіберпростором монополізовано *ICANN* та пов'язаними з ним структурами.

В умовах УКРАЇНА фактично виключена з процесу управління кіберпростором, у тому числі і на своїй території (як з географічної точки зору, так і з логічної), а основні канали управління та органи управління знаходяться за межами України.

Регулятори, найбільші споживачі ресурсів та послуг кіберпростору (у тому числі силові відомства, елементи критичної інфраструктури тощо) позбавлені можливості керування українським сегментом кіберпростору та діють на правах споживачів. При цьому вони зобов'язані надавати інформацію, що характеризує стан елементів кіберпростору, цілих сегментів (наприклад, *AS*) іноземним органам управління.

Україні необхідно здійснювати боротьбу за управління кіберпростором, причому як з точки зору прибутку (якщо говорити про конкуренцію телекомунікаційних операторів), так і з точки зору національної безпеки.

Розглянута структура управління кіберпростором на даному рівні деталізації дозволила виділити такі ключові елементи кіберпростору: кореневі *DNS* сервери; хости-репліки; автономні системи; точки обміну трафіком.

Список використаних джерел

1. Стародубцев Ю.І., Закалкін П.В., Іванов С.А. Техносферна війна як основний спосіб вирішення конфліктів за умов глобалізації // Військова думка. 2020. № 10. С.16-21.

2. Зарудницький В.Б. Характер та зміст військових конфліктів у сучасних умовах та доступній для огляду перспективі // Військова думка. 2021. №1. С.34-44.

3. Жіленков А.А., Чорний С.Г. Система безаварійного управління критично важливими об'єктами за умов кібернетичних атак // Питання кібербезпеки. 2020. № 2 (36).

4. Ромашкіна Н.П. Глобальні військово-політичні проблеми міжнародної інформаційної безпеки: тенденції, загрози, перспективи// Питання кібербезпеки. 2019. № 1 (29).

5. Котенко І.В., Крибель А.М., Лаута О.С., Саєнко І.Б. Аналіз процесу самоподібності мережевого трафіку як підхід до виявлення кібератак на комп'ютерні мережі // Електрозв'язок. 2020. № 12. С.54-59.

УДК 004.056.5:621.397.12

Кунцов М.С., здобувач 3 курсу
спеціальність 125 «Кібербезпека»
Наукові керівники:
Загоруйко Л.В., к.т.н., доцент, доцент кафедри інформаційних технологій
Мартьянова Т.А. к.т.н., ст. викладач кафедри інформаційних технологій

СТАТИСТИЧНИЙ СТЕГАНОАНАЛІЗ ФОТОРЕАЛІСТИЧНИХ ЗОБРАЖЕНЬ

Донецький національний університет ім. Василя Стуса, м. Вінниця

В результаті дослідження експериментально здійснено підбір оптимальних, параметрів алгоритму знаходження градієнтних шляхів. Отримано та проаналізовано результати застосування моделей машинного навчання, визначено оптимальний масштаб ядра *SVM*-регресора. Розраховано час обчислення векторів ознак, навчання моделі, розпізнавання контейнерів. Показано, що вектор ознак на основі градієнтних шляхів доцільно використовувати для вирішення завдань, де необхідно варіювати точність виявлення вкладення в залежності від навантаження на систему стеганоаналіті, оскільки цей вектор ознак дозволяє визначити співвідношення розмірність/точність. Також шляхом експерименту підібрано комплексний вектор з кількох одновимірних кількісних стеганодетекторів і вектора ознак на основі градієнтних шляхів, ефективність якого можна порівняти з вектором ознак *SPAM*.

Ключові слова: вектор ознак, градієнт яскравості, стеганодетектор, машинне навчання, регресія, машина опорних векторів, просторова область зображення, найменш значні біти, сегментація бітової площини за складністю.

Вступ

Основою статистичного стеганоаналізу зображень є факт порушення певних закономірностей зображення, спричинений реалізацією стегановкладення. Одна з класифікацій існуючих методів стеганоаналізу (сигнатурні, статистичні, евристичні) дозволяє віднести до групи статистичних методи, які ґрунтуються на зіставленні характеристик узагальнених порожнього і заповненого зображень, іншими словами, оцінюють близькість досліджуваного зображення до реального.