МВС України
Харківський національний університет внутрішніх справ
Науковий парк «Наука та безпека»

ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

Збірник матеріалів

Міжнародної науково-практичної конференції

(м. Вінниця, 31 травня 2023 року)

Вінниця

2023

УДК [351.74:004](477)(08)
П83

Друкується згідно з рішенням оргкомітету
за дорученням Харківського національного університету внутрішніх справ
від 18.01.2023 № 3

Протидія кіберзлочинності та торгівлі людьми :
П83 зб. матеріалів міжнарод. наук.-практ. конф. (м. Вінниця, 31 трав. 2023 р.) / МВС України, Харків. нац. ун-т внутр. справ, Наук. парк «Наука та безпека». – Вінниця : ХНУВС, 2023. – 176 с.

У матеріалах конференції окреслено найбільш актуальні проблеми протидії кіберзлочинності та торгівлі людьми на сучасному етапі; проаналізовано питання правового та організаційного забезпечення протидії кіберзлочинності та торгівлі людьми; кримінально-правові, процесуальні та криміналістичні аспекти протидії цьому негативному явищу; розглянуто відповідний міжнародний досвід, а також кадрове забезпечення правоохоронних органів. Досліджено використання інформаційних технологій і технічних засобів у протидії кіберзлочинності та торгівлі людьми.

УДК [351.74:004](477)(08)

Матеріали викладено в авторській редакції з незначними коректорськими правками. За достовірність наукового матеріалу, професійного формулювання, фактичних даних, цитат, власних назв, географічних назв, а також за розголошення фактів, що не належать відкритому друку, тощо відповідають автори публікацій та їх наукові керівники.

Електронна копія збірника розміщується у відкритому доступі на сайті Харківського національного університету внутрішніх справ (http://www.univd.edu.ua) у розділі «Наука», сторінка «Конференції, семінари та круглі столи», а також у репозитарії ХНУВС (http://dspace.univd.edu.ua/xmlui/).

ЗМІСТ

Вирішення поставленого оптимізаційного завдання підвищення оперативності передачі даних можна здійснити завдяки вдосконаленню алгоритму управління чергами. В основу розглянутого вдосконаленого алгоритму управління чергами покладено спосіб розрахунку віртуального часу обслуговування інформаційних пакетів. Цей спосіб відрізняється від уже відомих обліком фактору передачі сигнальних даних із комп'ютерних мереж у хмарні антивірусні системи. При цьому зазначені сигнальні дані отримують найвищий пріоритет обробки у вузлах комутації.

На першому кроці вдосконаленого алгоритму управління чергами з інформаційного потоку вибирається перший еталонний пакет з деяким Nпр, а також значенням віртуального часу обслуговування в черзі – VFT.

З іншого боку, здійснюється порівняння «еталонного» інформаційного пакета з пакетами в інший момент часу. При цьому рішення про присвоєння «еталонного» пріоритету інформаційному пакету приймається за такими критеріями:

1) мінімальне значення віртуального часу обслуговування в черзі;

2) належність інформаційного пакету до черги з максимальним пріоритетом.

При цьому друга умова присвоєння «еталонного» пріоритету виконується не в повному обсязі, а з деякими винятками, що визначаються показником імовірності присвоєння пріоритету, який задається адміністратором комп'ютерної мережі шляхом відповідних налаштувань інтелектуальних вузлів комутації. Одним із невирішених питань у цьому випадку залишається завдання оптимального розподілу обчислювальних та інформаційних ресурсів (наприклад, смуги пропускання), що дозволяє мінімізувати час виявлення шкідливого програмного забезпечення.

Це завдання можливо вирішити за допомогою імітаційного моделювання. Імітаційне моделювання можна провести з використанням типових і критичних параметрів телекомунікаційної системи.

Одержано 17.04.2023

УДК 341.01

БІГДАН Михайло Євгенович,
курсант 1 курсу факультету № 4
Харківського національного університету внутрішніх справ;
ВОЙЦІХОВСЬКИЙ Андрій Васильович,
кандидат юридичних наук, доцент,
професор кафедри конституційного
і міжнародного права факультету № 4
Харківського національного університету внутрішніх справ
https://orcid.org/0000-0001-5629-8852

ДІЯЛЬНІСТЬ НАТО ІЗ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Питання забезпечення інформаційної безпеки набуло пріоритетного напрямку в діяльності Організації Північноатлантичного договору (НАТО). З розмаїттям способів можливого застосування інформаційно-комунікаційних технологій, особливо у військовій сфері, перед НАТО постало завдання вироблення мінімальних стандартів щодо протидії будь-яким загрозам в інформаційному просторі.

Питання забезпечення захисту інформації входять до юрисдикції Комітету внутрішньої безпеки НАТО (NSC), який є дорадчим органом Північноатлантичної ради з питань, що стосуються безпеки НАТО. Головою Комітету є директор Служби безпеки НАТО (NOS), яка надає підтримку Комітету з боку Міжнародного секретаріату НАТО. NSC підпорядкована Робоча група з питань гарантування безпеки автоматичної обробки даних [1, с. 321].

Нова Стратегічна концепція оборони та безпеки держав-членів НАТО, що була схвалена главами держав та урядів під час Лісабонського саміту держав-членів НАТО в 2010 р., фактично прирівняла загрози в інформаційному просторі до воєнних загроз, що, у свою чергу, передбачає можливість застосування у відповідь національні збройні сили.

Така позиція Альянсу була підтверджена в Декларації Чиказького саміту, що була схвалена главами держав та урядів на засіданні Північноатлантичної ради в 2012 р. (м. Чикаго, США). Зокрема в п. 49 Декларації йдеться про готовність НАТО співпрацювати з іноземними партнерами для організації адекватних відповідей на будь-які загрози в інформаційному просторі.

Остаточне визнання Альянсом інформаційного простору в якості операційної «території» для ведення бойових дій відбулось за результатом саміту держав-членів НАТО, що проходив в 2016 р. (м. Варшава, Польща).

З метою протидії загрозам в інформаційному просторі в 2011 р. у НАТО виникла ідея щодо формування Групи швидкого реагування. Фахівці цієї Групи є відповідальними за надання допомоги державам-членів, які звертаються за нею в разі здійснення нападу в інформаційному просторі національного значення.

Технічний центр Сил реагування НАТО на комп'ютерні інциденти (NATO Computer Incident Response Capability, NCIRC) став мозковим вузлом Альянсу з протидії загрозам в інформаційному просторі (м. Монс, Бельгія). NCIRC відповідає за захищеність усіх інформаційних ресурсів НАТО [2].

Будь-яка держава-член НАТО, яка потерпіла атаки в інформаційному просторі, може звернутися до Альянсу по допомогу. Такий запит розглядає Комісія з менеджменту кіберзахисту (Cyber Defence Management Board, CDMB). Прохання про допомогу, які надходитимуть від держав – не членів НАТО, затверджуються Північноатлантичною радою Організації.

НАТО розробляє вимоги до своїх держав-членів щодо інформаційної безпеки та здійснює відповідну підтримку, зокрема у сфері професійної підготовки. У структурі Альянсу діє низка спеціалізованих структур:

– Спільний центр передового досвіду кіберзахисту (Cooperative Cyber Defence Centre of Excellence, CCDCOE) – здійснює співпрацю та обмін інформацією в НАТО з питань кібероборони шляхом навчання, наукових досліджень та розвитку, узагальнення отриманих практичних результатів та проведення консультацій (м. Таллінн, Естонія);

– Школа комунікаційних та інформаційних систем (Communications and Information Systems School, CIS School) - здійснює офіційну технічну підготовку щодо певних комунікаційних та інформаційних систем НАТО, розгорнутих на операціях або навчаннях Альянсу. Школа діє як навчальна установа для стратегічних командувань НАТО (м. Латина, Італія);

– Центр стратегічних комунікацій (Strategic Communications Centre of Excellence, StratCom) - сприяє покращенню стратегічних комунікаційних можливостей в НАТО, проводить дослідження з пошуку практичних рішень існуючих проблем, забезпечує підготовку інформаційних операцій Альянсу (м. Рига, Латвія).

До основних завдань НАТО щодо співробітництва між державами-членами, з державами-партнерами та іншими державами у сфері забезпечення інформаційної безпеки в умовах порушення Російською Федерацією міжнародного правопорядку шляхом розв'язання агресивної війни проти України відносяться: підтримка безпечного рівня діяльності об'єктів критичних інформаційно-комунікаційних інфраструктур; розробка дієвих заходів з протидії загрозам в інформаційному просторі; надання допомоги державам у відновленні нормального функціонування відповідної інфраструктури внаслідок вчинення зовнішніх атак в інформаційному просторі; функціонування системи оперативного реагування на будь-які загрози в інформаційній сфері держав [3, с. 517-519].

Список використаних джерел

1. Основні комітети НАТО та інститути співпраці, партнерства і діалогу // NATO. URL: https://www.nato.int/docu/other/ukr/handbook/2001/pdf/287-327.pdf (дата звернення: 08.04.2023).

2. NATO Cyber Security Centre // NATO. URL: https://www.ncirc.nato.int/ (дата звернення: 08.04.2023).

3. Войціховський А. В. Міжнародне право : підручник. МВС України, Харків. нац. ун-т внутр. справ. Харків, 2020. 544 с.

Одержано 10.04.2023

УДК 351.817:004:343.33:343.97(477)(470+571)

БУРАК Марія Василівна,
кандидат юридичних наук, старший науковий співробітник
наукової лабораторії з проблем протидії злочинності
Національної академії внутрішніх справ
https://orcid.org/0000-0002-1099-2096

КІБЕРАТАКИ РОСІЇ У ВІЙНІ ПРОТИ УКРАЇНИ: ШЛЯХИ ПРОТИДІЇ

З початку війни Україна стала ціллю чисельних кібератак, які охопили державні установи, приватні організації та громадян. Ті підприємства, які є частиною критичної інфраструктури, зокрема енергетичні, телекомунікаційні, медіа та фінансові компанії, також мають бути у режимі підвищеної готовності, оскільки саме ці галузі часто вважаються пріоритетними цілями у період війни. Бізнес, у свою чергу, має бути напоготові протидіяти цим викликам – компанії повинні оцінити свою готовність до кіберінцидентів і свою здатність відновити діяльність.

Так, напередодні повномасштабного російського вторгнення та з початком війни в Україні чисельність та потужність кібератак зросла в кілька разів. Масовані кібератаки проти державних структур України та бізнесу були 13-14 січня, 15-16 лютого і в ніч з 23 на 24 лютого 2022 року. Ці кібератаки були зумовлені тим, щоб паралізувати роботу наших стратегічних об'єктів. До прикладу, за даними Держспецзв'язку в період з середини лютого до початку березня 2022 року

Наукове видання

ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ
ТА ТОРГІВЛІ ЛЮДЬМИ

Збірник матеріалів
Міжнародної науково-практичної конференції
(31 травня 2023 року, м. Вінниця)

Відповідальні за випуск: *О. В. Манжай*
Комп'ютерне верстання: *А. О. Зозуля*

Формат 60х84 1/8. Ум. друк. арк. 20,53. Обл.-вид. арк. 11,93