НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

24 листопада 2023 року

З НАГОДИ 5-Ї РІЧНИЦІ ЗАСНУВАННЯ
ФАКУЛЬТЕТУ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КІБЕРПРОСТІР
В УМОВАХ ВІЙНИ ТА ГЛОБАЛЬНИХ ВИКЛИКІВ XXI СТОЛІТТЯ: ТЕОРІЯ ТА ПРАКТИКА

МАТЕРІАЛИ
МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»
Факультет кібербезпеки та інформаційних технологій
Кафедра кібербезпеки

КІБЕРПРОСТІР В УМОВАХ ВІЙНИ ТА ГЛОБАЛЬНИХ ВИКЛИКІВ XXI СТОЛІТТЯ: ТЕОРІЯ ТА ПРАКТИКА

МАТЕРІАЛИ МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

24 листопада 2023 року, м. Одеса

Одеса, 2023

УДК 340.12:316.3

ББК 67.0

Відповідальній редактор:

О. В. Дикий, декан факультету кібербезпеки та інформаційних технологій,
кандидат юридичних наук, доцент

Матеріали видано в авторській редакції.
Повну відповідальність за достовірність та якість поданого матеріалу
несуть учасники конференції, їхні наукові керівники,
які рекомендували ці матеріали до друку.

Друкується згідно з наказом ректора
Національного університету «Одеська юридична академія»
(№ 3449-62 від 19.10.2023 р.)

Матеріали Міжнародної науково-практичної конференції «Кіберпростір в умовах війни та глобальних викликів XXI століття: теорія та практика» (м. Одеса, 24 листопада 2023 р.). Одеса, 2023. 301 с.

Міжнародна науково-практична конференція «Кіберпростір в умовах війни та глобальних викликів XXI століття: теорія та практика» присвячена 5-ї річниці заснування факультету кібербезпеки та інформаційних технологій.

До участі у конференції запрошені студенти, аспіранти, молоді вчені, викладачі та науковці. Конференція проводиться на базі Національного університету «Одеська юридична академія».

Шановні учасники міжнародної науково-практичної конференції «Кіберпростір в умовах війни та глобальних викликів XXI століття: теорія та практика»!

В епоху стрімких змін та викликів кіберпростір став невід'ємною частиною людського життя, але разом з тим він приносить нові загрози та виклики, особливо в умовах війни та глобальних криз. Він вражає своєю багатогранністю та охоплює не тільки технологічні питання, а й соціально-психологічні, нормативно-правові, управлінські та інші аспекти.

Кожен з напрямів досліджень кіберсередовища є багатовекторним і всі вони є взаємопов'язаними. Кібербезпека та захист інформації є основою сучасного суспільства, адже кібератаки завдають значних збитків, як приватним компаніям, так і державним установам. Тому фахівці у галузі кібербезпеки повинні мати глибокі знання та навички не тільки в сфері технічного захисту інформації, але й в інших областях, таких як: законодавство у сфері кібербезпеки; економіка кібербезпеки; психологія кібербезпеки; організаційні аспекти кібербезпеки.

На рівні суспільства зміни в кіберсередовищі приносять, як користь, виявлену в забезпеченні прав людей на інформацію та задоволенні їхніх інформаційних потреб, так і потенційні ризики, пов’язані з неправомірним використанням інформації та шкодою інформаційним правам та інтересам осіб. У період воєнних дій особливо актуальними стають проблеми вибору достовірної інформації та запобігання неконтрольованому розповсюдженню інформації.

В умовах війни інформаційно-комунікаційні системи також переживають значні трансформації. Особливої уваги заслуговує сегмент Military Technologies, що зосереджується на підсиленні оборонних можливостей нашої держави.

Не менш важливою є роль правових принципів у регулюванні кібернетичного простору, тому актуальним є питання вдосконалення законодавчої бази, що викликає зростаючий інтерес серед юридичної наукової спільноти. Окрім того, кібертехнології мають значний вплив на управлінські процеси, соціальну взаємодію та психологічний стан людей у сучасному світі.

В цілому, більшість сучасних питань прямо чи опосередковано пов’язані з інформаційними технологіями та кіберпростіром. Одеса входить до числа лідерів у цій галузі, маючи всі необхідні умови для розвитку: матеріально-технічну базу, високий науковий потенціал, значний кадровий ресурс та розвинену IT спільноту.

Ми сподіваємося на подальшу плідну роботу, продуктивний обмін знаннями, ідеями та досвідом щодо подальшого розвитку кіберпростору в умовах війни та глобальних викликів сьогодення.

Президент Національного університету
“Одеська юридична академія”,
академік НАПрН України, академік НАПН України
доктор юридичних наук, професор,
Заслужений юрист України *Сергій КІВАЛОВ*

Секція 2. ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ В УМОВАХ ВІЙНИ

АНАЛІЗ ПОТЕНЦІЙНИХ ВИТОКІВ ДАННИХ В ПРИСТРОЯХ КОМУНІКАЦІЇ

Задерейко Олександр

доцент кафедри інформаційних технологій, факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія», кандидат технічних наук, доцент

Логінова Наталія

завідувач кафедри інформаційних технологій, факультету кібербезпеки та інформаційних технологій Національного університету «Одеська юридична академія», кандидат педагогічних наук, доцент

Троянський Олександр

директор інституту інформаційної безпеки, радіоелектроніки та телекомунікацій Національного університету «Одеська політехніка», кандидат технічних наук, доцент

Переважна більшість користувачів не можуть відмовитися від використання засобів комунікації інтегрованих в глобальну мережу Інтернет. Внаслідок цього, повністю виключити витоки конфіденційних даних користувачів не є можливим. Найбільш поширеним способом запобігання витоків конфіденційних даних користувачів є різні способи моніторингу і подальшого контролю мережевого трафіку пристроїв комунікації.

Тому актуальним завданням є виявлення ймовірних витоків конфіденційних даних, заснованих на методиках (алгоритмах) їх виявлення і подальшого блокування. Рішення цього завдання може бути реалізовано з використанням моніторингу всього мережевого трафіку пристроїв комунікації користувачів і подальшому виявленні в ньому даних, які можна віднести до конфіденційних (або надлишкових) і даних, що передаються в незашифрованому вигляді [1].

На практиці організація моніторингу мережевого трафіку пристроїв комунікації може бути виконана з використанням спеціалізованого програмного забезпечення – сніферів [2]. Реалізація такого підходу дозволяє виконувати детальний аналіз протоколів мережевого трафіку (на рівні пакетів) пристроїв комунікації на предмет наявності з'єднань, які можуть призвести до потенційних витоків даних, керуючись нижче наведеною методикою (рис. 1).

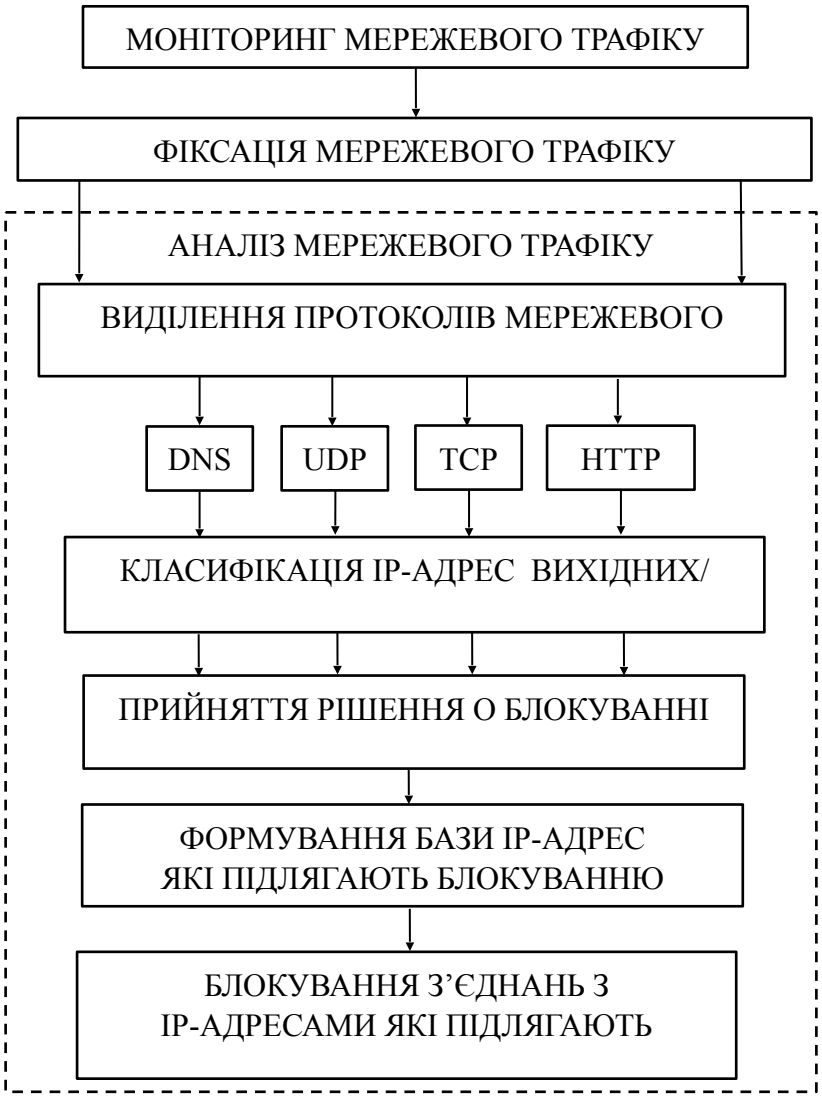

Рис. 1. Методика захисту пристроїв комунікації від потенційних витоків конфіденційних даних.

Завдання аналізу і класифікації трафіку, який може бути віднесений до конфіденційних даних з пристрою комунікації слід вирішувати, ґрунтуючись на таких критеріях [3]:

1. Заборону вихідних/вхідних з'єднань з сервісами інтернет статистики [4];

2. Заборону незахищених вихідних/вхідних з'єднань системного і прикладного програмного забезпечення, що здійснюються через всі порти, крім 443 (з обов'язковою перевіркою збереження його функціональності, після блокування);

3. Заборону вихідних/вхідних з'єднань необхідно виконувати на (L4) і (L7) рівнях моделі OSI (табл. 1) [5].

Таблиця 1. Модель OSI з розкладкою протоколів за рівнями

Рівень (L)	Назва	Протоколи
1	Application	SSH, HTTP, FTP, LPD, SMTP, TELNET, TFTP, EDI, POP3, IMAP, SNMP, NNTP, S-RPC, SET
2	Presentation	Encryption protocol types and format, such as ASCII, EBCDICM, TIFF, JPEG, MPEG, MIDI
3	Session	SMB, RPC, NFS, SQL
4	Transport	SPX, SSL, TLS, TCP, UDP
5	Network	ICMP, RIP, OSPF, BGP, IGMP, IP, IPSec, IPX, NAT, SKIP
6	Data link	ARP, SLIP, PPP, L2F, L2TP, PPTP, FDDI, ISDN
7	Physical	EIA/TIA-232, EIA/TIA-449, X. 21, HSSI, SONET, V. 2.4, V. 35, BLUETOOTH, 802.11, ETHERNET

Практична реалізація заборони вихідних/вхідних з'єднань повинна бути здійснена з використанням стандартних міжмережевих екранів і/або міжмережевих екранів нового покоління класу NGFW [6]. Такі міжмережеві екрани, дозволяють здійснювати глибоку фільтрацію трафіку, засновану на роботі засобів аналізу на рівні додатків (L7), таким чином, що "вміст" кожного пакета аналізується, починаючи від рівня L3 та закінчуючи рівнем L7 моделі OSI, у тому числі пакети, що містять зашифрований SSL(TLS) трафік.

Висновки

Апробація запропонованого підходу заснованого на аналізі мережевого трафіку на різних стаціонарних і мобільних пристроях комунікації дозволила ефективно виявляти і блокувати збір конфіденційних даних користувачів, що дозволило знизити ймовірність витоку їх конфіденційних даних.

Список використаних джерел:

1. ACSAC '10: Proceedings of the 26th Annual Computer Security Applications Conference. December 2010. Pages 261–269. DOI: https://doi.org/10.1145/1920261.1920300.
2. Pughazhendhi K. Amutha N. Packet sniffer. URL: https://www.irjmets.com/uploadedfiles/paper/issue_3_march_2023/35048/final/fin_irjmets1680097820.pdf/. (Дата звернення 6.11.2023).
3. Задерейко О.В., Трофименко О.Г., Прокоп Ю.В., Логінова Н.І., Кухаренко С.В. Аналіз витоків даних у інформаційних системах. Сучасна спеціальна техніка. № 3 (66), 2021, С. 16-30. URL: http://dspace.onua.edu.ua/handle/11300/23298.

4. Zadereyko O., Trofymenko O., Prokop Y., Loginova N., Dyka A., Kukharenko S. Research of potential data leaks in information and communication systems. Radioelectronic and Computer Systems. 2022. No 4. P.64-84. DOI: https://doi.org/10.32620/reks.2022.4.05. URL: https://dspace.onua.edu.ua/bitstream/handle/11300/23361/doslidjena_potenciynuh_vutokiv_danuh.pdf.
5. Задерейко О.В., Трофименко О.Г., Прокоп Ю.В., Логінова Н.І., Кухаренко С.В. Дика А.І. Захист даних користувачів в інформаційних системах. Сучасна спеціальна техніка. № 1 (68), 2022, С. 23-33. URL: https://hdl.handle.net/11300/23313.
6. Know, what you need to. "Defining the Next-Generation Firewall." (2009). URL: https://media.paloaltonetworks.com/documents/Gartner-NGFW-Research-Note.pdf. (Дата звернення 6.11.2023).

Ключові слова: пристрої комунікації, аналіз протоколів мережевого трафіку, аналіз пакетів мережевого трафіку, аналіз витоків даних, конфіденційні дані користувачів, моніторинг мережевого трафіку, міжмережевий екран, міжмережевий екран NGFW, глибока фільтрація трафіку, база конфіденційних даних, база IP адрес, блокування з'єднань
Keywords: communication devices, network traffic protocol analysis, network traffic packet analysis, data leak analysis, confidential user data, network traffic monitoring, firewall, NGFW firewall, deep traffic filtering, confidential data database, IP address database, connection blocking

ЗМІСТ

КІБЕРПРОСТІР В УМОВАХ ВІЙНИ ТА ГЛОБАЛЬНИХ ВИКЛИКІВ ХХІ СТОЛІТТЯ: ТЕОРІЯ ТА ПРАКТИКА

МАТЕРІАЛИ МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

24 листопада 2023 року
м. Одеса

Відповідальній редактор: О.В. Дикий

Дизайн та верстка:
М.Ю. Овчинников