DOI https: //doi.org/10.26486/mst2411-2816
DOI (Issue): https: //doi.org/10.26486/mst2411-2816.2022.1(68)

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДЕРЖАВНИЙ НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ

СУЧАСНА СПЕЦІАЛЬНА ТЕХНІКА

НАУКОВО-ПРАКТИЧНИЙ ЖУРНАЛ

№ 1(68), 2022

ВИДАЄТЬСЯ ЩОКВАРТАЛЬНО

ЗАСНОВНИК

Державний науково-дослідний інститут МВС України; Національний авіаційний університет; Національна академія внутрішніх справ

НАКАЗОМ

МОН України від 17.03.2020 № 409 науково-практичний журнал "Сучасна спеціальна техніка" включено до Переліку наукових фахових видань України відповідно до списку згідно з додатком 1 (категорія "Б")

ЗАРЕЄСТРОВАНО

Міністерством юстиції України 13 лютого 2015 року

Свідоцтво – серія КВ № 21221-11021Р

Науково-практичний журнал "Сучасна спеціальна техніка" внесено до переліку міжнародної науковометричної бази

Index Copernicus International Journal Master List

Рекомендовано до друку рішенням Вченої ради ДНДІ МВС України
(протокол від 29.04.2022 № 2)

Науково-практичний журнал посів ІІІ місце в конкурсі на краще наукове періодичне видання в системі МВС України у 2017 році та І місце у 2020 році

Київ 2022

УДК 004.738.2

Задерейко Олександр Владиславович,
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій Національного університету “Одеська юридична академія”, м. Одеса, Україна,
ORCID ID 0000-0003-0497-9861
Трофименко Олена Григорівна,
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій Національного університету “Одеська юридична академія”, м. Одеса, Україна,
ORCID ID 0000-0001-7626-0886
Логінова Наталія Іванівна,
кандидат педагогічних наук, доцент, завідувачка кафедри інформаційних технологій Національного університету “Одеська юридична академія”, м. Одеса, Україна,
ORCID ID 0000-0002-9475-6188
Прокоп Юлія Віталіївна,
кандидат історичних наук, доцент кафедри інформаційних технологій Національного університету “Одеська політехніка”, м. Одеса, Україна, ORCID ID 0000-0002-6608-3668
Кухаренко Сергій Вікторович,
кандидат технічних наук, доцент кафедри кібербезпеки, Національний університет “Одеська юридична академія”, м. Одеса, Україна,
ORCID ID 0000-0001-7100-6408
Дика Анастасія Іванівна,
асистент кафедри інформаційних технологій, Національний університет “Одеська юридична академія”, м. Одеса, Україна, ORCID ID 0000-0002-4196-8734

ЗАХИСТ ДАНИХ КОРИСТУВАЧІВ У ІНФОРМАЦІЙНИХ СИСТЕМАХ

У статті проведено аналіз способів збору даних з інформаційних систем користувачів, представлених пристроями комунікації, під час обміну даними з цифровим простором.

Показано, що провідні світові IT-корпорації фактично монополізували цифровий ринок даних користувачів за рахунок організації процесів їх збору, зберігання та обробки. Це дозволяє формувати необхідні керуючі впливи на користувачів цифрового простору.

Встановлено, що DNS трафік пристрою комунікації (фіксується DNS серверами провайдера, що становить загрозу приватності користувачів. Розроблено комплекс заходів, який дозволяє організувати захист від витоків даних користувачів у інформаційних системах.

***Ключові слова**: DNS запит, DNS сервер, DNS трафік, збір персональних даних, інформаційна зброя, захист персональних даних, блокування витоків даних, фільтрація з'єднань інформаційних систем, модель фільтрації, мережевого трафіку, пристрій комунікації.*

Вступ

Через об'єктивні процеси формування єдиного загальносвітового інформаційного простору відбувається переміщення різних видів соціальної, фінансової, економічної діяльності користувачів у цифровий простір. У сучасному інтернет- просторі циркулюють гігантські обсяги інформації, більшу частину якої становлять дані обміну користувачів унаслідок їхньої взаємодії з різними інтернет-сервісами. Головна небезпека цього процесу полягає в тому, що він сприяє інтенсивному збільшенню обсягу персоналізованих даних користувачів в цифровому просторі. Структуризація та аналіз таких даних дозволяє виявляти приховані, на перший погляд, закономірності, прогнозувати, а за системного підходу d і формувати по- ведінкові тенденції інтернет-аудиторії.

Це обумовлює потребу в захисті учасників цифрового простору від маніпулятивного впливу з боку IT-корпорацій на користувачів. Користувачі мають право не лише знати, яку саме інформацію про них можуть збирати спеціалізовані інтернет-сервіси, а й мати змогу самостійно обирати рівень приватності в інтернет-просторі. Тим більше, що розробка засобів контролю та управління приватністю даних для запобігання небажаному обробленню персональної ідентифікаційної інформації визначена стандартом ISO/IEC 29100:2011.

Мета статті - на основі аналізу результатів аудиту трафіка класичної інформаційної системи користувача виробити комплекс заходів щодо захисту від витоків даних користувачів у цифровому просторі.

Основна частина

1. Вплив на учасників цифрового простору

Сучасні тенденції несанкціонованого збору, накопичення та оброблення даних з пристроїв комунікації користувачів, підключених до інтернет-простору, обумовлені енергійними зусиллями високотехнологічних IT-корпорацій. Як наслідок, це призводить до формування неофіційного "ринку" персональних даних користувачів, до регулювання якого державні структури більшості країн мають дуже опосередкований стосунок, незважаючи на заходи, що вживаються у вигляді прийняття законів про захист персональних даних на своїх територіях [1, 2]. При цьому регуляторна роль різних державних інститутів у питаннях дотримання прав на приватність життя користувачів, як-от: таємниця листування, інформація про відвідувані адреси, імена і паролі користувачів, пошукові запити, неухильно знижується [3].

Цей процес ускладнюється тим, що енергійні зусилля провідних світових IT-корпорацій, як-от: Google, Microsoft, Amazon, Cloudflare, Facebook, Yandex тощо, вже фактично призвели до розділу й часткової монополізації цифрового ринку даних користувачів [4]. Аналіз даних користувачів, що ґрунтується на організації процесів їх збору, зберігання та оброблення, є основою для вироблення

(персоналізованого або групового) цифрового простору (рис. 1).

певного керівного впливу на учасників

Рис. 1. Процес формування впливу на учасників цифрового простору

Кінцевою метою експансії IT-компаній на цифровий ринок персональних даних користувачів є отримання прибутку від сформованих ними ж фактично необмежених можливостей з негласного вивчення, контролю та управління користувачами цифрового простору.

Іншими словами, IT-корпорації інтегрували в цифрове середовище комплекс засобів впливу (інформаційна зброя), якісним результатом котрого досягається модифікація властивостей інформаційної системи (ІС), під якою зазвичай розуміється об'єкт, що взаємодіє з інформацією - людина з пристроєм комунікації (ПрК), на якому встановлено відповідне програмне забезпечення (ПЗ).

Головний ефект інформаційної зброї полягає в тому, що її застосування неминуче спричиняє зміни у свідомості учасників цифрового простору, перепро- грамування їхньої системи оцінок подій і, як наслідок, повної керованості їхньою поведінкою, особливо у прийнятті потрібних IT-корпораціям рішень [5-7].

Планомірне створення і впровадження IT-корпораціями цифрових інформа-ційно-комунікаційних, теле-, відео-, фото-, радіомовних платформ, інтегрованих

одночасно в людський соціум і цифровий простір, багаторазово підсилюють ефект керуючого і маніпулятивного впливу на масову свідомість цифрової аудиторії [8, 9].

2. Оброблення DNS запитів у доменному просторі

Сучасний цифровий простір забезпечує вільний транскордонний обмін даними між ПрК користувача й хостами різного призначення. Фізичне підключення ПрК користувача (клієнта DNS) до цифрового простору й його подальше звернення до різних ресурсів розпочинаються з відсилання DNS запитів на DNS сервери (рис. 2).

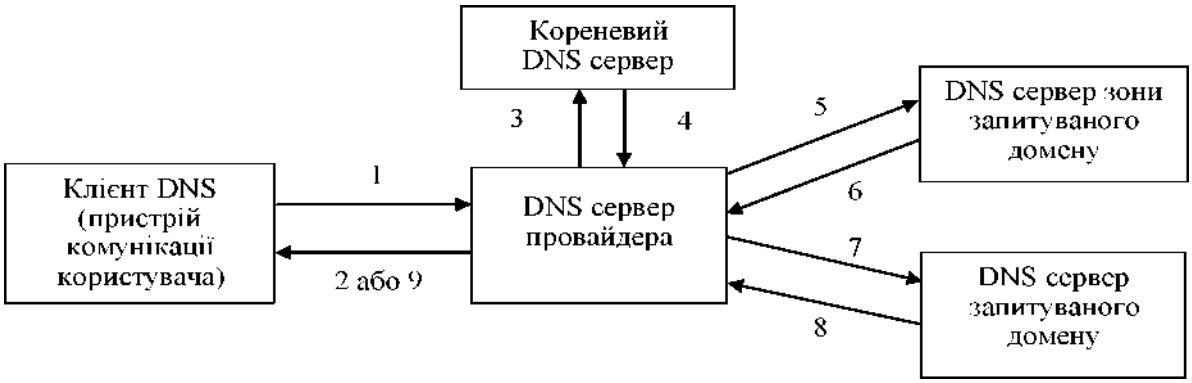

Рис. 2. Схема взаємодії типового клієнта DNS з доменним простором імен інтернету

Оброблення DNS запитів у доменному просторі (рис. 2) виконується в строго визначеному порядку:

1) клієнт DNS формує запит типу “протокол://домен” до DNS сервера провайдера для отримання IP-адреси, хостингу, на якому розташований інтернет-ресурс, відповідний запитуваному домену;

2) DNS сервер провайдера виконує пошук запитуваного домену у своєму журналі, і якщо його знаходить, то повертає клієнту DNS IP-адресу, відповідну виконаному DNS запиту;

3) DNS сервер провайдера звертається до кореневого сервера DNS із запитом IP-адреси DNS сервера, відповідального за доменну зону, відповідну DNS запиту клієнта DNS;

4) кореневий DNS сервер повертає DNS серверу провайдера IP-адресу DNS сервера, відповідального за доменну зону, відповідну DNS запиту клієнта DNS;

5) DNS сервер провайдера звертається до DNS сервера, відповідального за доменну зону, відповідну запиту клієнта DNS, із запитом IP-адреси DNS сервера, відповідального за хостинг домену інтернет-ресурсу, що запитується клієнтом DNS;

6) DNS сервер, відповідальний за доменну зону, відповідну DNS запиту клієнта DNS, повертає IP-адресу DNS сервера, відповідального за хостинг домену, запитуваного клієнтом DNS;

7) DNS сервер провайдера звертається до DNS сервера, відповідального за хостинг домену, запитуваного клієнтом DNS, із запитом IP-адреси хостингу, відповідного домену, запитуваного клієнтом DNS;

8) DNS сервер, відповідальний за хостинг домену, запитаного клієнтом DNS, повертає шукану IP-адресу DNS серверу провайдера;

9) DNS сервер провайдера повертає клієнту DNS IP-адресу, відповідну запитаному домену.

Вивчення схеми обміну даними ПрК (див. рис. 2) дозволяє дійти висновку, що всі запити клієнтів DNS фіксуються в журналах DNS сервера провайдера. їх аналіз дає вичерпну інформацію для провайдера і контролюючих його державних структур про дії користувача або його ПрК в цифровому просторі. Саме ця обставина дозволяє розглядати DNS запити користувачів як дані користувачів, до збирання, зберігання та аналізу яких з кожним роком виявляють дедалі більший інтерес IT-корпорації і спецслужби різного призначення в усіх державах [3].

Не менш важливим аспектом є той факт, що початкова відкритість DNS полегшує моніторинг, перехоплення і підміну даних. DNS запити користувачів передаються у відкритому незашифрованому вигляді за протоколом UDP і TCP (порт 53), що значно спрощує їхню фіксацію або перехоплення не лише провайдерами різного рівня, а й сторонніми особами [10]. Тому для захисту DNS трафіка користувачів від витоків і перехоплення були розроблені і впроваджені протоколи DNS-over-TLS (DoT) і DNS-over-HTTPS (DoH). їх упровадження не вимагає внесення жодних змін у наявну систему доменних імен, але додають захищений спосіб роботи DNS для її клієнтів [11].

Логічним продовженням застосування протоколу DoH у цифровому просторі стало впровадження його більшістю розробників веб-браузерів у свої програмні продукти. На додаток до цього розробники веб-браузерів надали своїм користувачам можливість прямого підключення (в обхід провайдерів) до публічних DNS серверів провідних IT-корпорацій (табл. 1), які також підтримують протокол DoH [12].

Таблиця 1

Веб-браузери з підтримкою DoH і публічних DNS серверів

Веб-браузери	Підтримка DoH	Вбудована підтримка публічних DNS серверів		
		Google	Cloudflare	Cisco
Mozilla	+	+	+	+
Opera	+	+	+	+
Chrome	+	+	+	+
Edge	+	+	+	+
Yandex	+	+	+	+

Отже, користувач ПрК засобами будь-якого веб-браузера може самостійно вибирати DNS сервер й активувати використання протоколу DoH для захищеної передачі своїх даних. Реалізація цих заходів у цифровому просторі вже фактично призвела до:

- неможливості перехоплення і контролю DNS трафіки з боку уповноважених служб і національних відомств держав;
- монополізації збору й аналізу даних про DNS трафік користувачів на користь лідуючих на глобальному цифровому ринку даних IT-корпорацій.

Ще одним важливим фактом є те, що широкий спектр даних про ПрК користувача та його дії у цифровому просторі збирається кожним хостом (інтернет-ресурсом), що в переважній більшості підключені їх власниками до сервісів збору й аналізу даних Google Analytics, Yandex Metrika, Liveinternet тощо [13]. Це, у свою чергу, призводить до безапеляційної монополізації процесу збору Інкорпораціями даних про користувачів (рис. 3).

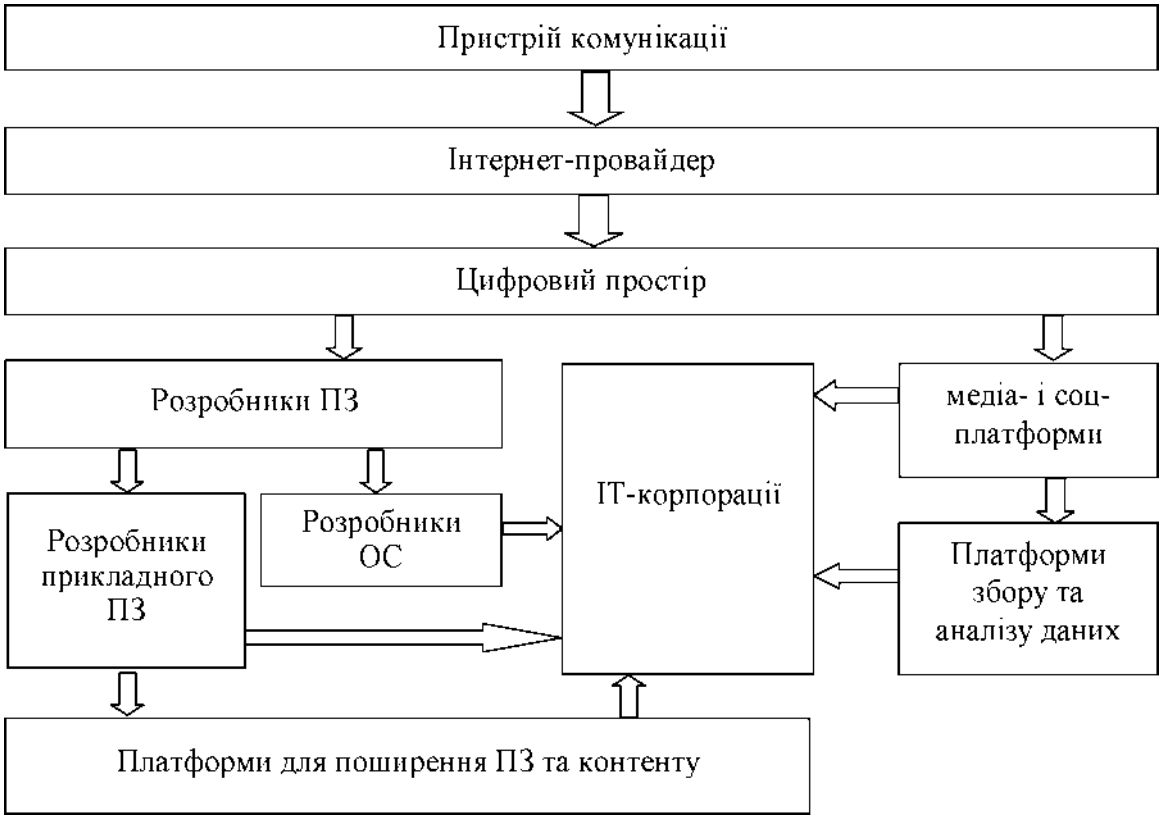

Рис. 3. Схема збору даних з пристрою комунікації користувача

3. Комплекс заходів для захисту від витоків даних в ІС

Результати схеми збору даних з ПрК та проведеного аналізу з'єднань інформаційних систем із цифровим простором [3] зумовлюють актуальність розробки комплексу заходів для захисту користувачів від збору їх даних, що дозволить підвищити їхню приватність і знизити можливості впливу IT-корпорацій на цифрову аудиторію.

Одним з ефективних і широко застосовуваних способів блокування витоків даних користувачів є організація на програмному або апаратному рівнях ІС фільтрації з'єднань системного і прикладного ПЗ ПрК із цифровим простором (рис. 4).

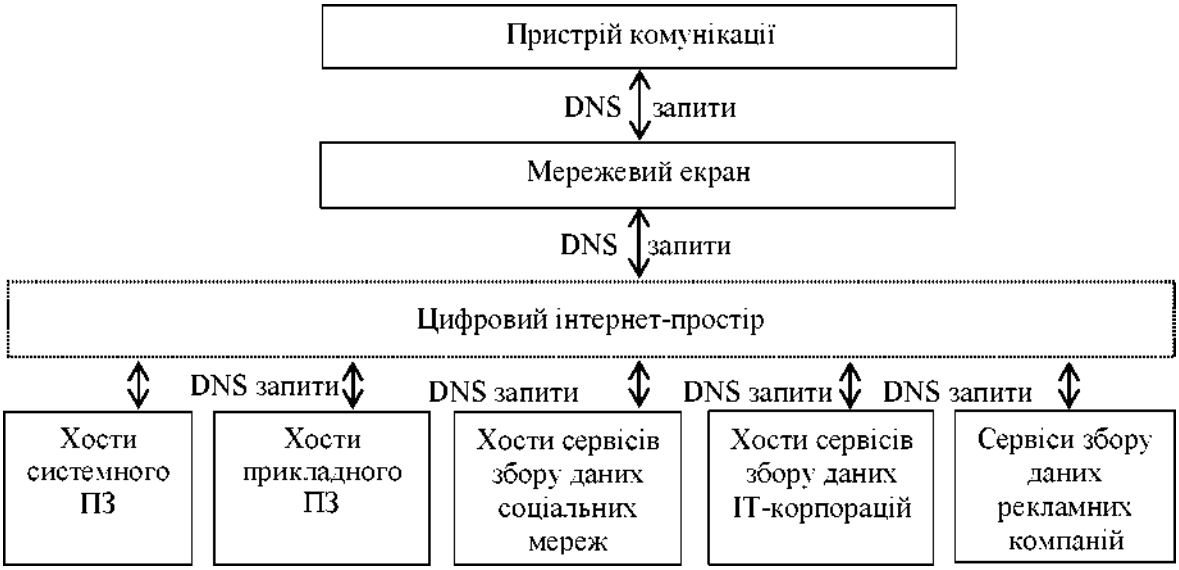

Рис. 4. Організація захисту ІС від збору і витоків даних

Для досягнення поставленої мети дослідження було організовано процес фільтрації мережевого трафіка ІС, відповідальних за:

- збір даних прикладним ПЗ;
- збір даних системним ПЗ;
- збір даних користувача спеціалізованими сервісами.

Для практичної реалізації фільтрації мережевого трафіка були використані міжмережеві екрани. Вони працюють на мережному пакетному рівні, що дозволяє виконувати блокування всіх вхідних і вихідних з'єднань ІС, і відповідають:

- IP-адресам/доменам стороннього трафіка системного і прикладного ПЗ;
- IP-адресам/доменам сервісів збору даних.

Для фільтрації трафіка ІС у дослідженні використовували три різні моделі захисту ІС від збору даних.

Першу модель реалізували на базі програмної організації фільтрації з'єднань ІС засобами спеціалізованого прикладного ПЗ для ПрК (рис. 5):

- для ОС Android було використано мережевий екран No Root Firewall [14];
- для сімейства ОС Windows було застосовано розширення вбудованого мережевого екрану Windows Firewall Control [15].

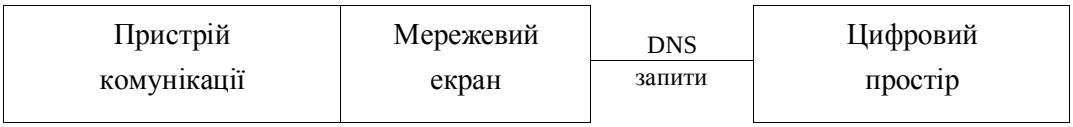

Рис. 5. Програмна організація захисту ІС від збору даних

Другу модель реалізовували на основі апаратної організації фільтрації з'єднань ІС за допомогою налаштувань вбудованого мережевого екрану апаратного мережевого обладнання організації: роутера, маршрутизатора, сервера тощо (рис. 6).

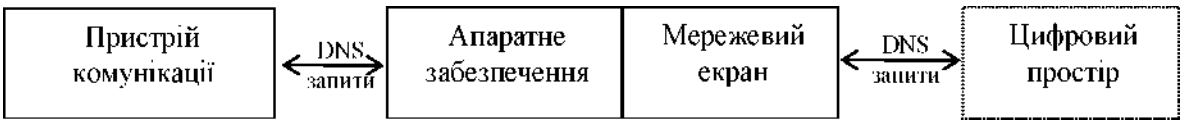

Рис. 6. Апаратний захист ІС від збору даних

Третя модель реалізовувалася на базі комбінованого застосування програмної та апаратної фільтрації з'єднань ІС (рис. 7).

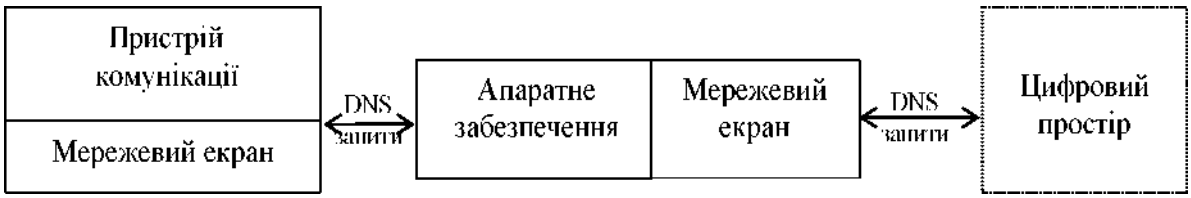

Рис. 7. Програмно-апаратний захист ІС від збору даних

Експериментальна перевірка запропонованих моделей захисту ІС показала, що апаратна фільтрації з'єднань інформаційної системи не повинна виключати програмну фільтрацію, реалізовану безпосередньо на самому ПрК або навпаки. З іншого боку, застосування комбінованого підходу (третя модель) фільтрації мережевого трафіка ІС дозволяє краще позбавитись від витоків даних користувачів. Ефективність третьої моделі захисту ІС обумовлюється тим, що в ПрК під управлінням мобільної ОС Android спостерігається мимовільне вимикання мережевого екрану [3]. Це стається через несумісність деяких версій ОС Android із поточною версією мережевого екрану.

Висновки

Розроблено комплекс заходів, який дозволяє організувати захист від витоків даних користувачів в інформаційних системах. У основу його реалізації покладено використання мережевого екрану, який здійснює блокування визначених експериментальним шляхом функціональних і сторонніх з'єднань системного і прикладного ПЗ ПрК.

Запропоновано моделі програмної та апаратної організації захисту даних користувачів від витоків в ІС. Виконано експериментальну перевірку запропонованих моделей організації захисту даних. Дослідним шляхом встановлено, що найбільш ефективною є модель, заснована на одночасному використанні програмної та апаратної реалізації захисту даних користувачів.

Практичне застосування запропонованих моделей захисту даних від витоків дозволить користувачам ПрК:

- підвищити приватність у цифровому просторі;
- знизити точність цифрового профілювання ПрК користувача;
- зберегти функціональність і працездатність системного і прикладного ПЗ ПрК;
- скоротити трафік з цифровим простором інтернет, що зменшить витрати на оплату послуг мобільних провайдерів;
- запобігти збору даних ІТ-корпораціями;
- знизити ймовірність маніпулятивних впливів з боку ІТ-корпорацій на рішення, що приймаються.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. General Data Protection Regulation (EU GDPR). URL: https://gdpr-text.com/ (дата звернення: 12.03.2022).
2. Закон України "Про захист персональних даних". URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 12.03.2022).
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.* 2021. № 3(66). С. 16-30. DOI: 10.36486/mst2411-3816.2021.3(66).2.
4. *Праневич А.А.* Монополизация глобального цифрового пространства: растущие угрозы для развивающихся стран и возможности их преодоления. Вестник Тверского государственного университета. Серия: Экономика и управление. 2020. № 4. С. 149-157.
5. *Новиков В.К.* Информационное оружие - оружие современных и будущих войн. М.: Горячая линия-Телеком, 2018. 287 с. ISBN 978-5-9912-0502-3.
6. *Корсаков Г.Б.* Информационное оружие супердержавы. *ИМЭМО РАН.* 2012. №1 (42). URL: https://cyberleninka.rU/article/n/informatsionnoe-oruzhie-superderzhavy (дата звернення: 12.03.2022).
7. *Трофименко О.Г., Дубовой Я.В.* Еволюція поглядів на інформаційні війни в епоху інформаційного суспільства. Порівняльно-аналітичне право: електронне наукове фахове видання. 2017. № 1. С. 189-192.
8. Google: a sinister trait. URL: https://eurasia.film/2019/08/google-v-tvoej-golove/ (дата звернення: 12.03.2022).
9. *Esteve A.* The business of personal data: Google, Facebook, and privacy issues in the EU and the USA. International Data Privacy Law. 2017. Vol. 7(1). P. 36-47. DOI: 10.1093/idpl/ipw026.
10. *Belyavsky D.* DNS: those who didn't hide are to blame. *Internet in Numbers.* 2015. Vol. 1(21). P. 74-77.
11. *Bumanglag K., Kettani H.* On the Impact of DNS Over HTTPS Paradigm on Cyber Systems. *3rd International Conference on Information and Computer Technologies (ICICT),* San Jose, CA, USA. 2020. P. 494-499. DOI: 10.1109/ICICT50521.2020.00085.
12. *Charanjeet S.* How to Enable DNS Over HTTPS in Chrome, Firefox, Edge, Brave & More? *Fossbytes.* 2020. URL: https://fossbytes.com/how-to-enable-dns-over-https-on-chrome-firefox- edge-brave (дата звернення: 12.03.2022).
13. *Zadereyko O., Prokop Y., Trofymenko O., Loginova N., Plachinda O.* Development of an algorithm to protect user communication devices against data leaks. *Eastern-European Journal of Enterprise Technologies.* 2021. Vol. 1/2 (109). P. 24-34. DOI: 10.15587/1729-4061.2021.225339.
14. NoRoot Firewall. URL: https://play.google.com/store/apps/details?hl=en&id=app.greyshirts.firewall (дата звернення: 12.03.2022).
15. Windows Firewall Control. URL: https://binisoft.org/wfc (дата звернення: 12.03.2022).

REFERENCES

1. General Data Protection Regulation (EU GDPR). URL: https://gdpr-text.com/ (Date of Application: 02.02.2022) [in English].
2. Law of Ukraine "On Protection of Personal Data". URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (Date of Application: 12.03.2022) [in Ukrainian].
3. *Zadereyko, O., Trofymenko, O., Prokop, Yu., Loginova, N., Kukharenko, S.* (2021) Analysis of data leaks in information systems. *Modern Special Technics.* Vol. 3 (66), pp. 16–30. DOI: 10.36486/mst2411–3816.2021.3(66).2 [in Ukrainian].
4. *Pranevich, A. (*2020) Global digital space monopolization: growing threats to the developing countries and the ways for its overcoming. *Vestnik Tverskogo gosudarstvennogo universiteta. Seriya: Ekonomika i upravlenie.* Vol. 4. P. 149–157 [in Russian].
5. *Novikov, V.K.* (2018) Information weapons – weapons of modern and future wars. M.: Goriachaia Liniia. 287 p. ISBN 978-5-9912-0502-3 [in Russian].
6. *Korsakov, G.* (2012) Information weapon of a superpower. *IMEMO RAN.* Vol. 1(42). 26 p. URL: https://cyberleninka.ru/article/n/informatsionnoe-oruzhie-superderzhavy (Date of Application: 04.02.2022) [in Russian].
7. *Trofymenko, O., Dubovoy, Y.* (2017) Evolution of glances at information changes in the era of information support. *Comparative Analytical Law.* Vol. 1. P. 189–192 [in Ukrainian].
8. Google: a sinister trait. URL: https://eurasia.film/2019/08/google-v-tvoej-golove/ (Date of Application: 04.02.2022) [in English].

9. *Esteve, A.* (2017) The business of personal data: Google, Facebook, and privacy issues in the EU and the USA. *International Data Privacy Law.* Vol. 7(1). P. 36-47. DOI: 10.1093/idpl/ipw026. [in English].
10. *Belyavsky, D.* (2015) DNS: those who didn't hide are to blame. *Internet in Numbers.* Vol. 1(21). P. 74-77 [in English].
11. *Bumanglag, K., Kettani, H.* (2020) On the Impact of DNS Over HTTPS Paradigm on Cyber Systems. *3rd International Conference on Information and Computer Technologies (ICICT),* San Jose, CA, USA. P. 494-499. DOI: 10.1109/ICICT50521.2020.00085. [in English].
12. *Charanjeet, S.* How to Enable DNS Over HTTPS in Chrome, Firefox, Edge, Brave & More? Fossbytes (2020) URL: https://fossbytes.com/how-to-enable-dns-over-https-on-chrome-firefox- edge-brave/ (Date of Application: 04.01.2022) [in English].
13. *Zadereyko, O, Prokop, Y., Trofymenko, O, Loginova, N., Plachinda, O.* (2021) Development of an algorithm to protect user communication devices against data leaks. *Eastern-European Journal of Enterprise Technologies.* Vol. 1/2 (109). P. 24-34. DOI: 10.15587/1729-4061.2021.225339. [in English].
14. NoRoot Firewall. URL: https://play.google.com/store/apps/details?hl= en&id=app. greyshirts.firewall (Date of Application: 04.01.2022) [in English].
15. Windows Firewall Control. URL: https://binisoft.org/wfc (Date of Application: 04.01.2022) [in English].

UDC 004.738.2

Zadereiko Oleksandr,
Cand. Sci. (Engineering), Associate Professor, Docent
at the Department of Information Technology,
National University "Odessa Law Academy", Odesa, Ukraine,
ORCID ID 0000-0003-0497-9861
Trofymenko Olena,
Cand. Sci. (Engineering), Associate Professor, Associate professor
at the Department of Information Technology,
National University "Odessa Law Academy", Odesa, Ukraine,
ORCID ID 0000-0001-7626-0886
Lohinova Nataliia,
PhD, Associate professor at the Department of Information technology,
National University "Odessa Law Academy", Odesa, Ukraine,
ORCID ID 0000-0002-9475-6188
Prokop Yuliia,
PhD, Associate Professor, Docent at the Department
of Software Engineering of the Odessa Polytechnic National University,
Odesa, Ukraine,
ORCID ID 0000-0002-6608-3668
Kukharenko Serhii,
Cand. Sci. (Engineering), Associate professor at the Department
of Information Technology of the National University "Odessa Law Academy", Odesa, Ukraine,
ORCID ID 0000-0001-7100-6408
Dyka Anastasiia,
Assistant at the Department of Information Technology,
National University "Odessa Law Academy", Odesa, Ukraine,
ORCID ID 0000-0002-4196-8734

PROTECTION OF USERS' DATA IN INFORMATIONAL SYSTEMS

Research article analyzes the methods of data collection from users' information systems represented by communication devices when performing data exchange with digital space.

The study shows that the world's leading IT corporations have actually monopolized the digital market of user data by organizing the processes of their collection, storage, and processing. This makes it possible to form the required control actions on users of the digital space.

It has been established that the provider's DNS servers record the DNS traffic of the communication device. This poses a threat to users' privacy. We developed a set of measures to organize protection against user data leaks in information systems.

Research article proposes models of software and hardware organization of users' data protection from leaks in information systems. Experimental verification of the proposed models of data protection organization was carried out. The use of the proposed data protection models against leaks allowed users to increase privacy when interacting with the digital space.

We experimentally established that the most effective data protection against leaks is provided by a model based on the simultaneous use of software and hardware data protection. We experimentally confirmed that with the practical implementation of simultaneous software and hardware organization of data protection, the functionality and operability of the system and application software of the communication device is preserved. The study shows that the implementation of the proposed data protection models against unauthorized leaks by the user will significantly reduce the volume of network traffic of the communication device.

Keywords: DNS query, DNS server, DNS traffic, personal data collection, information weapon, personal data protection, blocking data leaks, filtering connections of information systems, network traffic filtering model, communication device.

Отримано 09.02.2022

DOI (Issue): https: //doi.org/10.36486/mst2411–3816.2022.1(68) Issue 1(68)2022

СУЧАСНА СПЕЦІАЛЬНА ТЕХНІКА

Modern Special Technics

НАУКОВО-ПРАКТИЧНИЙ ЖУРНАЛ

Scientific and Practical Journal

Випусковий редактор
Лелет С.М.

Редакційна група:
Алєксєєва О.В.,
Якубчик Т.В.

Комп'ютерна верстка
Мухіна Т.М.

Issuing Editor
Lelet Serhii

Editorial Group
Alieksieieva Olha,
Yakubchyk Tetiana

Makeup
Mukhina Tetiana

Адреса редакції:
01011, м. Київ, пров. Євгена Гуцала, 4-а
Телефон: (044) 254-95-21
Факс: (044) 280-01-84
E-mail: dndi@mvs.gov.ua
Сайт: http://suchasnaspetstehnika.com/

Підписано до друку 29.04.2022.
Формат 60х80 1/8. Гарнітура Petersburg. Друк офсетний. Папір офсетний. Ум.-друк. арк. 6,3.
Наклад 50 прим.

Видавець ФОП Горбенко Ю.В.
м. Харків, вул. Ахсарова, 3, корп. В, кв. 168.
Дата та номер запису в ЄДР
01.08.2017 № 24800000000198912.