

Основні зміни, спричинені GDPR:

- Явна згода. Компанії тепер зобов'язані отримувати явну, інформовану та однозначну згоду користувачів на обробку їхніх персональних даних для цілей таргетованої реклами. Це означає, що користувачі повинні активно вибрати варіант "так", а не просто прокручувати сторінку нижче.
- Прозорість. Компанії повинні надавати користувачам чітку та зрозумілу інформацію про те, які персональні дані збираються, з якою метою, як довго зберігаються і кому передаються.
- Право на забуття. Користувачі мають право вимагати видалення своїх персональних даних.
- Обмеження цілей. Компанії можуть обробляти персональні дані лише для конкретних, явно визначених і законних цілей.
- Безпека даних. Компанії зобов'язані вживати технічних і організаційних заходів для захисту персональних даних від несанкціонованого доступу, втрати, знищення або пошкодження.
- Відповідальність. Компанії несуть відповідальність за дотримання GDPR. За порушення регламенту передбачені значні штрафи [2, с. 12].

Все це вплинуло на таргетовану рекламу загалом тим що тепер компанії змушені збирати менше персональних даних, що ускладнює створення детальних профілів користувачів. Компанії шукають нові способи таргетингу, які не вимагають такого великого обсягу персональних даних. Наприклад, все більше уваги приділяється контекстній рекламі та інтересам користувачів, які виявляються через їхню поведінку в мережі [3].

GDPR став значним кроком у напрямку захисту персональних даних користувачів у Європі. Хоча він створив нові виклики для компаній, що займаються таргетованою рекламою, він також сприяв підвищенню прозорості та відповідальності в цій галузі. Очікується, що в майбутньому ми побачимо подальший розвиток законодавства в області захисту даних, що ще більше вплине на практику таргетованої реклами та вирішить проблеми приватності та збору даних користувачів.

Список використаної літератури:

1. Чи має GDPR відношення до Вас? Основні правові аспекти, які необхідно знати: 2019. URL: <https://www.de-jure.ua/imeet-li-gdpr-otnoshenie-k-vam-osnovnye-pra/>
 2. Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation): 2019. URL: <http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf>.
 3. Артем Козлюк. GDPR – нові правила обробки персональних даних у Європі для міжнародного IT-ринку: 2018. URL: <https://habr.com/ua/company/digitalrightscenter/blog/344064/>
- Науковий керівник: Фроленкова Н.А., к.е.н., доцент.**

Мар'яновський В. А., к.т.н.

Фесан А.О., студент

***Київський національний університет
імені Тараса Шевченка***

vitalik_m@univ.kiev.ua, fesanartem@knu.ua

ПЕРЕШКОДИ ШИРОКОГО ВПРОВАДЖЕННЯ АДРЕСАЦІЇ IPv6 В УКРАЇНІ

Значна частка розвинених країн досягла широкого впровадження адресації IPv6 відповідно до статистики розрахованої компанією Google [1]. Основними факторами, які збільшують необхідність впровадження IPv6 є постійно зростаюча кількість пристроїв в мережах, які потребують публічної

адресації, серед яких: обладнання інтернету речей, автоматизовані системи спостереження та контролю доступу, зростаюча кількість електронного обладнання, яке містить елементи штучного інтелекту. Наведені фактори є прямою ознакою необхідності та важливості протоколу IPv6 для глобальної мережі Інтернет. Ключовими рушіями впровадження даного протоколу є великі постачальники контенту, ресурсів, сервісів та провайдери мережі Інтернет всіх рівнів. Для пришвидшення розгортання даного протоколу в Україні, важливим фактором є вивчення обмежень на його використання. До найбільш розповсюджених причин відсутності протоколу IPv6 відносять:

- 1) Однією з ключових проблем впровадження протоколу IPv6 є необхідність впровадження великої кількості змін на всіх рівнях ієрархічної моделі побудови мережі. Основним методом роботи протоколу IPv6 є одночасна робота протоколів IPv4 та IPv6 [2]. Такий метод потребує повного циклу розгортання мережі на рівні з попередньою версією протоколу з урахуванням особливостей роботи двох версій протоколу одночасно. Наведена причина вимагає значних додаткових часових витрат інженерів по впровадженню змін в роботу мережі.
- 2) Необхідність підтримки протоколу IPv6 на обладнанні рівня агрегації, ядра та периметру мережі. Дана вимога обмежує можливість використання застарілого обладнання та вимагає заміни обладнання, яке по іншим критеріям ще може експлуатуватись значний проміжок часу. Оновлення програмного забезпечення в застарілому обладнанні в більшості випадків не вирішує проблему по причині відсутності підтримки виробниками нових технологій в обладнанні, яке зняте з виробництва. Враховуючи також фактор короткотривалого періоду, зазвичай 3-5 років, випуску певної лінійки обладнання багатьма виробниками, що призводить до необхідності заміни апаратного забезпечення. У більшості виробників, ключовий підхід випуску оновлень програмного забезпечення є виправлення проблем та недоліків в роботі, а не додавання нових технологій та розширення можливостей обладнання. Наведена причина вимагає значних фінансових витрат, які зумовлені зміною найбільш коштовних компонентів мережі, якщо вони застарілі для використання протоколу IPv6.
- 3) Основний шлях впровадження протоколу IPv6 є не заміна протоколу IPv4, а забезпечення роботи в режимі Dual Stack. Використання такого підходу є єдиним правильним рішенням, яке експоненційно збільшує складність мережі в подальшій підтримці, що в свою чергу збільшує час на виправлення проблем в її роботі. Наведена причина зменшує надійність мережі по причині збільшення часу на пошук несправностей.
- 4) Протокол IPv6 був розроблений не лише з метою збільшення адресного простору, але й з метою виправлення значної частини недоліків попередньої версії. Наслідком даних змін є більш висока складність протоколу IPv6, що вимагає впровадження та розробки нових підходів до підтримки мереж та доопрацювання або заміни існуючих систем керування, систем відслідковування роботи та контролю доступу до мереж. Наведена причина вимагає додаткових фінансових витрат на оновлення існуючих систем або придбання нових.
- 5) Протокол IPv6 технологічно суттєво відрізняється від попередньої версії [3]. Зміни в протоколі враховують недоліки IPv4, що призвело до технологічного ускладнення та суттєвих відмінностей в протоколі IPv6. Тому виникає необхідність більш кваліфікованих інженерів для підтримки мережі чи додаткового тривалого навчання вже існуючих. Наведені особливості призводять до збільшення витрат на оплату праці та додаткові часові витрати на навчання. Описані причини є додатковим фактором передачі обслуговування мережі стороннім організаціям [4] та ускладнює задачу впровадження протоколу IPv6 в мережах малого розміру. В мережах малого розміру більше обмежень на утримання кваліфікованих мережеских інженерів з вузькою спеціалізацією.
- 6) Додатковим стримуючим фактором є низька вартість послуг підключення до мережі Інтернет. Як наслідок, відсутність можливості провайдерів мережі Інтернет використовувати сучасне обладнання. За рахунок фінансової обмеженості більш популярним є вибір застарілого

обладнання, яке відповідає більшості вимог за виключенням: відсутності оновлень програмного забезпечення, відсутність підтримки нових технологій (в тому числі і останніх RFC для протоколу IPv6), більш низька надійність за рахунок значного зносу апаратної частини. Впровадження протоколу IPv6 учасниками мережі (різноманітними компаніями та організаціями) Інтернет на пряму залежить від підтримки даної технології провайдерами мережі Інтернет.

- 7) Найменш значущим, але також важливим фактором є ускладнена підтримка служби DNS, що вимагає роботи з довгими та складними до візуального сприйняття адресами. Наведена причина призводить до збільшення навантаження на підтримку мережі та збільшує вплив “людського фактору” при обслуговуванні служби DNS, яка є однією з найбільш критичних служб роботи IP-мереж.

З наведених причин, при впровадженні протоколу IPv6, слідують наступні обмежуючі фактори: необхідність більш кваліфікованих мережевих інженерів, додаткові фінансові витрати, зменшення надійності роботи мережі, необхідність підтримки протоколу провайдерами мережі Інтернет, необхідність значних робіт по впровадженню. Шляхи вирішення обмежуючих факторів потребують додаткового вивчення та врахування можливостей регулятора (держави) в кожній окремій країні. На даний момент відсутні спроби вплинути на ситуацію зі сторони регулятора в Україні.

Список використаних джерел

1. Google IPv6 Country Rank. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.aelius.com/njh/google-ipv6/>.
2. Li, K.-H.; Wong, K.-Y. Empirical Analysis of IPv4 and IPv6 Networks through Dual-Stack Sites. Information 2021, 12, 246. <https://doi.org/10.3390/info12060246>
3. Igulu, K., Onuodu, F., Singh, T.P. (2024). IPV6: Strengths and Limitations. In: Prasad, A., Singh, T.P., Dwivedi Sharma, S. (eds) Communication Technologies and Security Challenges in IoT. Internet of Things. Springer, Singapore. https://doi.org/10.1007/978-981-97-0052-3_8
4. Forough Karimi-Alagheband, Suzanne Rivard, IT outsourcing success: A dynamic capability-based model. The Journal of Strategic Information Systems, Volume 29, Issue 1, 2020. <https://doi.org/10.1016/j.jsis.2020.101599>

*Онiщенко Д. С., магістрант,
здобувачка 6 курсу гр. ІІІІ-601 спеціальності «8i09»
Київський національний економічний університет
імені Вадима Гетьмана
diana29.oni2@gmail.com*

VISA ACQUIRER MONITORING PROGRAM ЯК ДРАЙВЕР ВПРОВАДЖЕННЯ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ ШАХРАЙСТВА В ОНЛАЙН-ПЛАТЕЖАХ

У 2022 році глобальні втрати від шахрайства в онлайн-платежах сягнули \$41 мільярда, а до кінця 2023-го ця цифра, зросла до \$48 мільярдів. Через такі масштабні ризики протидія платіжному шахрайству стала одним із пріоритетів для бізнесу. Visa та її клієнти мають спільне завдання - захистити від шахрайства всіх учасників платіжного процесу.

Тож, починаючи з 1 квітня 2025 року, Visa запускає вдосконалену програму VAMP (Visa Acquirer Monitoring Program). З цим оновленням VAMP запроваджує метрику ризику та її порогові