меМіністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки та захисту
інформації
_____Іван ПАРХОМЕНКО
«___» червня 2025 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)
спеціальність 125 Кібербезпека
(код і назва спеціальності)
освітній ступень бакалавр
освітня програма Кібербезпека
(назва освітньо-професійної програми)
на тему: Механізми виявлення загроз безпеці персональних даних пов'язаних з використанням трекінгових пікселів

Виконавець: студентки IV курсу, групи КБ-42

_____ **Анастасія БОНДАРЕНКО**
(підпис) (ім'я прізвище)

	Прізвище, ініціали	**Підпис**
Керівник	Лариса МИРУТЕНКО	
Нормоконтроль	Сергій ДАКОВ	

Київ 2025

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«29» листопада 2025 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студентці **КБ-42** **Анастасії Олегівні Бондаренко**
(група) (прізвище ім'я по батькові)

Тема кваліфікаційної роботи Механізми виявлення загроз безпеці персональних даних пов'язаних з використанням трекінгових пікселів

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №6 від 28.11.2024 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Технологія трекінгових пікселів у цифровому маркетингу; нормативно-правові акти щодо захисту персональних даних (GDPR, Закон України «Про захист персональних даних»); потенційні загрози, пов'язані з використанням трекінгових пікселів, вимоги до систем виявлення витоків інформації; методи криптографічного захисту даних (псевдонімізація, блокові шифри); практика застосування пікселів у сервісах Google, Meta, TikTok.

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Принципи дії трекінгових пікселів, класифікація та приклади їх використання; законодавчі вимоги щодо конфіденційності даних (GDPR, CCPA, українське законодавство); вектори загроз, пов’язані з використанням пікселів (session hijacking, фішинг, витік IP-адреси, профілювання користувачів); технічні методи виявлення сторонніх пікселів та доменів; вибір криптографічного алгоритму захисту даних (AES, інші блокові шифри); рекомендації для безпечного використання трекінгових пікселів; механізми захисту персональних даних; економічне обґрунтування впровадження заходів безпеки; формулювання висновків і пропозицій щодо політик конфіденційності

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розроблено універсальну багаторівневу методику захисту персональних даних від трекінгових пікселів, що поєднує технічні рішення (CMP, проксі-сервери, Privacy Gateway, маскування та фільтрацію) з організаційними заходами (політики, навчання персоналу, контроль згоди користувачів). Запропоновано механізми, що дозволяють автоматично виявляти й нейтралізувати трекери у вебсередовищі та електронній пошті, забезпечуючи відповідність вимогам законодавства і знижуючи юридичні та репутаційні ризики.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29 листопада 2024 року

Завдання видала	_____	Лариса МИРУТЕНКО
	(підпис)	(ім’я, прізвище)
Завдання прийняла до виконання	_____	Анастасія БОНДАРЕНКО
	(підпис)	(ім’я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі та вибір об'єкта дослідження	29.11.2024 – 15.12.2024	*виконано*
2	Аналіз літератури з теми трекінгових пікселів та безпеки персональних даних	16.12.2024 – 05.01.2025	*виконано*
3	Ознайомлення з правовими аспектами (GDPR, CCPA), формування теоретичної бази	06.01.2025 – 25.01.2025	*виконано*
4	Дослідження механізмів дії трекінгових пікселів та їх взаємодії з іншими технологіями	26.01.2025 – 15.02.2025	*виконано*
5	Аналіз вразливостей і потенційних загроз при використанні трекінгових пікселів	16.02.2025 – 05.03.2025	*виконано*
6	Розробка методичних рекомендацій з моніторингу трекінгу та виявлення аномалій	06.03.2025 – 25.03.2025	*виконано*
7	Розробка рекомендацій щодо захисту персональних даних (криптографія, анонімізація)	26.03.2025 – 15.04.2025	*виконано*
8	Підготовка політики конфіденційності та шаблонів внутрішніх процедур	16.04.2025 – 05.05.2025	*виконано*
9	Оформлення пояснювальної записки	06.05.2025 – 08.06.2025	*виконано*
10	Підготовка до захисту кваліфікаційної роботи	09.06.2024 – 13.06.2025	*виконано*

Завдання видала _____ Лариса МИРУТЕНКО
(підпис) (ініціали, прізвище)

Завдання прийняла до виконання _____ Анастасія БОНДАРЕНКО
(підпис) (ініціали, прізвище)

Термін подання кваліфікаційної роботи до ЕК 13 червня 2025 року

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел та додатків, має 104 сторінки основного тексту, 12 таблиць, 11 рисунків та 4 додатки. Список використаних джерел містить 16 найменувань і займає 2 сторінки.

Метою роботи є впровадження механізмів виявлення загроз безпеці персональних даних пов'язаних з використанням трекінгових пікселів.

У роботі досліджено механізми виявлення загроз безпеці персональних даних, пов'язаних з використанням трекінгових пікселів у цифровому середовищі. Особливу увагу приділено аналізу ризиків, які виникають під час збору, обробки та передачі даних користувачів через технології веб-трекінгу, що застосовуються в маркетингових, аналітичних та рекламних цілях.

Завданнями роботи є дослідження принципів дії трекінгових пікселів, їх класифікація та приклади використання; аналіз законодавчих вимог щодо конфіденційності даних (GDPR, CCPA, українське законодавство); виявлення векторів загроз, пов'язаних з використанням пікселів (session hijacking, фішинг, витік IP-адреси, профілювання користувачів); вивчення технічних методів виявлення сторонніх пікселів та доменів; вибір криптографічного алгоритму захисту даних (AES, інші блокові шифри); розробка рекомендацій для безпечного використання трекінгових пікселів; визначення механізмів захисту персональних даних; економічне обґрунтування впровадження заходів безпеки; формулювання висновків і пропозицій щодо політик конфіденційності.

Об'єктом дослідження є процес обробки персональних даних у вебсередовищі з використанням трекінгових технологій.

Предмет дослідження є механізми виявлення загроз, інструменти моніторингу, технічні та організаційні заходи із захисту персональних даних у контексті використання трекінгових пікселів.

Практичне значення полягає в розробці універсальної багаторівневої методики захисту персональних даних від трекінгових пікселів, яка охоплює технічні рішення

(CMP, проксі, Privacy Gateway, маскування, фільтрація) та організаційні заходи (політики, навчання, контроль згоди). Запропоновані механізми дозволяють автоматично виявляти і нейтралізувати трекери у вебсередовищі та електронній пошті, забезпечуючи відповідність вимогам законодавства і зниження юридичних та репутаційних ризиків.

Методи дослідження: аналіз літератури з питань виявлення цифрових загроз, синтез отриманих відомостей про механізми трекінгових пікселів і результати кіберінцидентів, моделювання потенційних сценаріїв витоку персональних даних.

У роботі розглянуто технічні аспекти функціонування трекінгових пікселів, їхню здатність відслідковувати активність користувачів навіть без прямої згоди, а також ризики, пов’язані з ідентифікацією IP-адрес, побудовою поведінкових профілів та передачею даних на сторонні сервери. Проаналізовано потенційні вектори атак, зокрема фішинг, social engineering, session hijacking.

Розроблено підхід для виявлення загроз персональним даним через трекінгові пікселі. Запропоновано рішення, що дозволяють знаходити приховані елементи стеження на сайтах та в листах, аналізувати їхню поведінку та вчасно реагувати на ризики витоку даних.

Ключові слова: захист персональних даних, трекінгові пікселі, кукі. кібербезпека, GDPR, NIST CSF 2.0, ризики витоку даних.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

CCPA/CPRA	–	California Consumer Privacy Act / California Privacy Rights Act
DPA	–	Data Protection Authority
DPIA	–	Data Protection Impact Assessment
DPO	–	Data Protection Officer
GDPR	–	General Data Protection Regime
HTTP	–	Hypertext Transfer Protocol
NIST CSF 2.0	–	National Institute of Standards and Technology Cybersecurity Framework version 2.0
PDCA	–	Plan–Do–Check–Act
ІС	–	Інформаційна система
НПА	–	Нормативно-правовий АКт

ВСТУП

Актуальність теми роботи обумовлена стрімким розвитком цифрових технологій, що суттєво змінили способи збору, обробки та аналізу інформації про користувачів у мережі Інтернет. Одним із таких інструментів стали трекінгові пікселі — невеликі фрагменти коду, які вбудовуються у вебсторінки або електронні листи для збору даних про поведінку користувача. Їх широке використання у сфері онлайн-маркетингу, електронної комерції, рекламних кампаній та аналітики сприяє ефективному таргетингу та підвищенню взаємодії з аудиторією, проте одночасно породжує серйозні ризики для конфіденційності та безпеки персональних даних.

Загрози, пов’язані з використанням трекінгових пікселів, включають несанкціоноване відстеження користувачів, порушення принципу інформованої згоди, збирання надмірного обсягу інформації без відповідного захисту, а також потенційну можливість доступу до конфіденційних даних зловмисниками. Така ситуація викликає занепокоєння з боку правозахисників, користувачів та регуляторів, зокрема в контексті дотримання вимог міжнародних стандартів, як-от Загального регламенту про захист даних (GDPR) та Національної системи кібербезпеки США (NIST CSF 2.0).

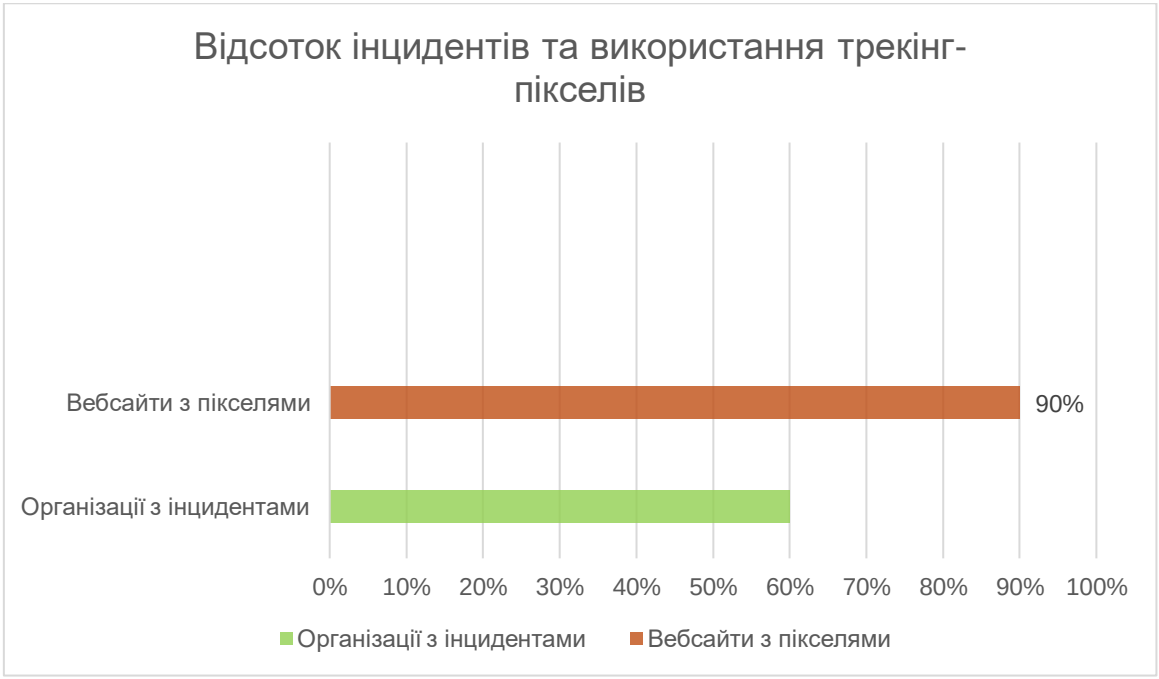

Рисунок 1.1 – Відсоток інцидентів та використання трекінг-пікселів

Статистичні дані (див. Рисунок 1.1) лише підтверджують гостроту проблеми: за даними звіту IAPP (International Association of Privacy Professionals) за 2023 рік, понад 60% організацій стикалися з інцидентами, пов'язаними з порушенням конфіденційності даних, а середня вартість витоку даних зросла до $4,45 млн у 2023 році, згідно з дослідженням IBM Cost of a Data Breach Report. Крім того, згідно з дослідженням Ghostery, до 90% вебсайтів використовують трекінгові пікселі, а в середньому одна вебсторінка містить понад 20 таких елементів, що створює широке поле для потенційного зловживання даними та ускладнює контроль за їх обробкою.

На фоні збільшення кількості інцидентів, пов’язаних з витоками персональних даних, та посилення вимог до прозорості в обробці інформації, актуальним стає завдання виявлення загроз безпеці персональних даних, що виникають у результаті використання трекінгових пікселів. Це включає аналіз методів збору інформації, технічних особливостей їхньої роботи, потенційних векторів атак, а також оцінку відповідності використаних механізмів захисту чинним нормативним вимогам.

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ВИКОРИСТАННЯ ТРЕКІНГОВИХ ПІКСЕЛІВ ТА ЇХ ВПЛИВ НА БЕЗПЕКУ ПЕРСОНАЛЬНИХ ДАНИХ

1.1. Поняття трекінгового пікселя

Трекінговий піксель — це спеціальний код або невелике графічне зображення (зазвичай розміром 1x1 піксель), яке вбудовується у вебсторінки, електронні листи чи інші цифрові ресурси з метою збору інформації про поведінку користувачів. Незважаючи на свою назву, візуально піксель зазвичай є прозорим і невидимим для відвідувачів, однак він виконує потужну функцію — передає дані на сторонній сервер кожного разу, коли користувач відкриває відповідний ресурс або виконує певну дію на ньому [6].

З технічної точки зору, трекінговий піксель — це посилання на зовнішнє зображення або скрипт, що розміщений на сервері компанії-оператора. Коли сторінка або лист завантажуються, браузер користувача надсилає запит на цей сервер [6]. У відповідь сервер фіксує набір даних про користувача: IP-адресу, версію браузера, тип пристрою, роздільну здатність екрана, час і дату доступу, реферер (адресу сторінки, з якої прийшов користувач), мову браузера, операційну систему тощо.

Трекінговий піксель — це інструмент невидимого збору інформації про дії користувача у цифровому середовищі. Він являє собою невеличке графічне зображення, як правило, розміром 1×1 піксель, яке вбудовується у код вебсторінок або електронних листів. Сам піксель є непомітним, оскільки має нульову або майже нульову роздільну здатність та зазвичай приховується стилями CSS (display:none;) [6].

Основне завдання трекінгового пікселя — зафіксувати момент, коли користувач завантажив сторінку, відкрив email або виконав іншу дію. Цей факт використовується для збирання статистики, побудови поведінкових профілів, персоналізації реклами, A/B-тестування тощо [6].

З технічного боку, трекінговий піксель функціонує як тег <img>, у якому джерелом зображення (src) є URL, що вказує на сервер, який отримує запит [5]. Приклад даного коду показано на рисунку 1.2.

```
<img src="https://tracker.example.com/pixel.png" width="1" height="1"
style="display:none;">
```

Рисунок 1.2 – HTML-код прихованого трекінгового пікселя розміром 1×1 піксель (style="display:none;") для таємного збору даних про відвідування

Під час завантаження сторінки браузер автоматично звертається до вказаного серверу, передаючи в заголовках HTTP додаткову інформацію, як-от IP-адресу, тип пристрою, браузер, джерело переходу та інші метадані.

Особливістю трекінгових пікселів є те, що вони часто взаємодіють із cookie-файлами або іншими технологіями відстеження (наприклад, localStorage або device fingerprinting). Це дозволяє зберігати унікальні ідентифікатори користувачів, об'єднувати інформацію з різних сайтів або сесій, а також проводити точне профілювання поведінки відвідувача. Такі технології широко використовуються в онлайн-рекламі, персоналізації контенту, аналітичних системах та у процесах, пов’язаних із UX-дизайном [6, 7].

Найбільш поширеними прикладами трекінгових пікселів є Meta Pixel (Facebook), TikTok Pixel, Google Ads Conversion Pixel, LinkedIn Insight Tag, а також email-пікселі в платформах розсилок (Mailchimp, SendGrid тощо).

Попри ефективність цих інструментів для бізнесу, застосування трекінгових пікселів викликає серйозні занепокоєння з точки зору конфіденційності. Вони дозволяють відстежувати користувача без явної згоди, обходити технічні обмеження браузерів і часто використовуються у спосіб, що суперечить принципам прозорої обробки персональних даних, визначених у міжнародних стандартах, зокрема у GDPR. У багатьох випадках користувач не знає про існування трекінгового пікселя та обсяг інформації, яку той збирає про нього.

Таким чином, поняття трекінгового пікселя охоплює не лише візуальний елемент, а й складний механізм збору, передачі й обробки персональної інформації, що має прямий вплив на безпеку користувачів у цифровому середовищі.

1.2. Принципи роботи трекінгових пікселів

Трекінговий піксель являє собою невеличкий елемент (зображення або фрагмент коду), вбудований у контент сторінки чи листа, який виконує роль «маяка» для збору даних про взаємодію користувача. Коли користувач відкриває веб-сторінку або електронний лист, що містить такий піксель, браузер або поштовий клієнт автоматично надсилає запит на сервер, де зберігається піксельне зображення [6,5]. У відповідь сервер повертає прозоре зображення 1×1 px (яке не впливає на відображення), але водночас реєструє на своїй стороні всю доступну інформацію про взаємодію користувача.

Взаємодію браузера/клієнта з сервером трекінгу можна описати спрощено зазначеними нижче етапами (див. рис. 1.2).

Рисунок 1.3 – Технічна схема роботи трекінгового пікселя на веб-сайті

Як видно з наведеної схеми, при завантаженні пікселя на стороні сервера-відстежувача накопичується інформація про користувача та його сеанс роботи. Серед даних, що автоматично фіксуються, можуть бути: IP-адреса користувача (що дозволяє

визначити його приблизне місцезнаходження), тип пристрою, браузера та операційної системи, час і дата відвідування, роздільна здатність екрану, джерело переходу на сторінку (реферер) тощо [6, 14]. Якщо піксель використовується у веб-аналітиці, також реєструються дії на сайті – переглянуті сторінки, кліки, здійснені покупки або інша взаємодія протягом сесії [9,10]. У випадку пікселів в електронних листах фіксуються факти і час відкриття листа, тривалість перегляду, чи був лист прокручений повністю, на які посилання в листі натиснув отримувач, який пристрій та поштовий клієнт він використовує. Така інформація надзвичайно цінна для маркетингових цілей, оскільки дає змогу оцінити поведінку аудиторії, ефективність рекламних кампаній та персоналізувати контент [6].

Цей механізм дозволяє отримати такі дані: IP-адресу користувача (з якої можна визначити його геолокацію), тип і версію браузера, версію операційної системи, розмір екрану, мову браузера, відвідану URL-сторінку, попередній URL (реферер) та час взаємодії [6,14].

У поєднанні зі збереженими локальними даними браузера трекінговий піксель здатний відстежувати поведінку користувача не лише на одній сторінці, а й між сайтами. Це особливо поширено у випадках із глобальними рекламними мережами, такими як Google Ads, Facebook Ads, LinkedIn та ін [8,9,10,11]. Якщо піксель інтегрований на кількох сайтах, які користуються однією й тією ж рекламною платформою, то її сервер отримує уніфіковану інформацію про активність користувача у різних вебдоменах, що дозволяє будувати детальні поведінкові моделі [9,13].

Деякі трекінгові пікселі функціонують у форматі server-side tracking — коли інформація не лише зчитується з браузера, а й доповнюється даними з серверної частини сайту, наприклад, про дії користувача після авторизації (купівлі, завантаження, залишення коментаря) [6,13]. Це значно розширює обсяг отримуваної інформації.

Таким чином, принцип дії трекінгового пікселя полягає в безперервному відстеженні активності користувача через механізм завантаження зображення або коду, з можливістю збирання великого обсягу персональних і технічних даних, що у

разі неналежного захисту або зловживань може становити серйозну загрозу для конфіденційності особи [6,14].

Робота трекінгового пікселя базується на запиті до сервера. Процес відбувається у кілька етапів [5]:

1. Користувач відкриває сторінку або лист, у якому вбудовано піксель.
2. Браузер виконує HTTP-запит до URL, вказаного в атрибуті src.
3. Сервер отримує запит і фіксує такі дані:
   - IP-адресу користувача — дає змогу орієнтовно визначити місце перебування.
   - User-Agent — містить інформацію про браузер, операційну систему та тип пристрою.
   - Referrer — вказує на попередню сторінку або джерело переходу.
   - Cookies або інші ідентифікатори — дозволяють зв’язати взаємодії користувача з іншими діями на сайті.
   - Час і дата запиту — для вимірювання частоти і динаміки відвідувань.
   - Екранна роздільна здатність і мова браузера — для аналізу технічних параметрів пристроїв [6,14].

Ключовим моментом є те, що весь процес відбувається автоматично і миттєво — користувач не взаємодіє з пікселем напряму [6].

У поєднанні з cookie, локальним сховищем браузера або сторонніми скриптами, трекінговий піксель може створювати повноцінний профіль поведінки користувача, включаючи історію відвіданих сторінок, дії на сайті, повторні відвідування тощо. Якщо користувач залогінений у певну платформу (наприклад, Facebook), ці дані можуть бути зв’язані з його акаунтом [8,13,14].

1.3. Основні види трекерів

На ринку цифрового маркетингу існує велика кількість інструментів відстеження, однак серед них можна виділити кілька найбільш поширених, які використовуються підприємствами по всьому світу для збору, обробки та аналізу даних користувачів. До таких належать: Meta Pixel (Facebook), Google Analytics, TikTok Pixel, LinkedIn Insight Tag, Twitter Pixel та інші. Кожен із них має свої особливості, проте виконує одну спільну функцію — збір даних для аналізу поведінки користувачів і оптимізації контенту або реклами [8,9,10,11,12].

Meta Pixel (раніше Facebook Pixel) — один із найпоширеніших інструментів для відстеження взаємодії користувача з вебресурсами. Він дозволяє компаніям оцінювати ефективність реклами у Facebook та Instagram, здійснювати ретаргетинг, відстежувати конверсії, будувати «аудиторії схожих користувачів» (Lookalike Audiences). Meta Pixel інтегрується на сайт і передає дані про переглянуті сторінки, додані товари в кошик, здійснені покупки тощо [8,13].

Google Analytics (Universal та GA4) — комплексна система веб-аналітики, яка застосовується для збору статистики про відвідуваність сайту, джерела трафіку, взаємодію з контентом. GA4 також дозволяє аналізувати поведінкові шаблони, створювати сегменти користувачів, будувати воронки конверсій. Важливо, що Google може поєднувати ці дані з іншими своїми сервісами (YouTube, Google Ads), створюючи детальні профілі користувачів [9].

TikTok Pixel — піксель, який використовується для аналітики ефективності рекламних кампаній у TikTok. Він дозволяє відстежувати ключові події: завантаження сторінки, додавання до кошика, купівлі, реєстрації тощо. TikTok активно просуває використання свого пікселя для побудови «аудиторій за подіями», що дозволяє оптимізувати кампанії у динаміці [10].

LinkedIn Insight Tag — аналітичний інструмент, який дозволяє вимірювати ефективність реклами в LinkedIn, а також створювати професійно орієнтовані аудиторії. Завдяки LinkedIn Insight Tag можна отримати дані про посади, галузі, компанії користувачів, що взаємодіяли із сайтом [11].

Twitter Pixel (Conversion Tracking) — застосовується для ретаргетингу користувачів у мережі Twitter та аналізу ефективності рекламних оголошень [12].

Загальною характеристикою усіх вищезгаданих пікселів є їхня здатність до інтеграції у зовнішні ресурси, зв'язок з обліковими записами у рекламних системах та передача детальної інформації про поведінку користувачів. Це відкриває як можливості для точного маркетингу, так і ризики для конфіденційності персональних даних, якщо не дотримано принципів прозорості, згоди та обмеженого збору даних згідно з вимогами GDPR [1,14].

Трекінгові пікселі широко застосовуються і в email-розсилках. Маркетологи вбудовують у тіло електронного листа невидиме зображення (наприклад, файл pixel.png розміром 1×1, колір прозорий), яке завантажується з сервера відправника при відкритті листа. Таким чином фіксується, що лист був відкритий (open rate), а також коли і скільки разів це сталося. За допомогою додаткових параметрів URL пікселя відстежуються кліки по посиланнях у листі та інші дії [5,6]. Наприклад, HTML-код листа може містити рядок зазначений на рисунку 1.4.

```
<img·src="https://track.example.com/open?uid=12345"·width="1"·height="1"·
style="display:none"·alt="."/>¶
```

Рисунок 1.4 – Приклад HTML-коду трекінгового пікселя з унікальним ідентифікатором користувача (uid=12345)

У цьому випадку унікальний ідентифікатор uid=12345 дозволяє відправнику листа (компанії) визначити, який саме отримувач відкрив лист. Візуалізацію роботи пікселя в email можна подати схематично (рис. 1.5).

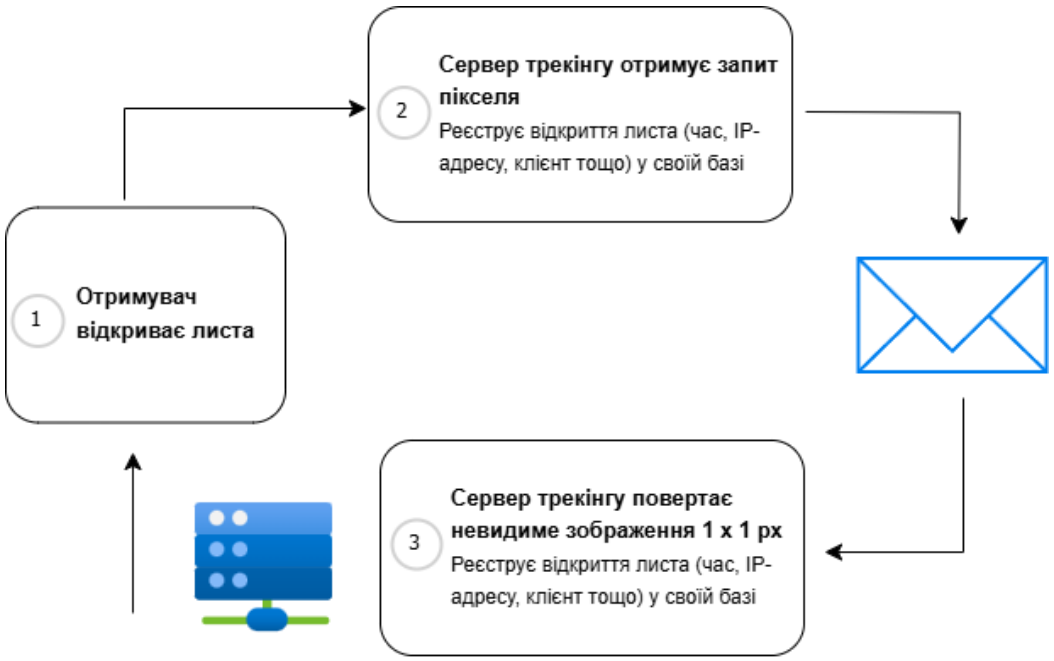

Рисунок 1.5 – Схема дії трекінгового пікселя в електронному листі

1) Отримувач відкриває email → Поштовий клієнт автоматично запитує 1×1 px зображення з сервера відправника.

2) Сервер трекінгу отримує запит пікселя → Реєструє відкриття листа (час, IP-адресу, клієнт тощо) у своїй базі.

3) Сервер трекінгу повертає невидиме зображення 1×1 px назад поштовому клієнту (лист відображається користувачу без видимих змін) [6].

Зібрані таким чином дані дозволяють відправнику оцінити рівень зацікавленості отримувачів: наприклад, можна визначити відсоток тих, хто відкрив лист (метрика *open rate*), час доби коли листи читають найактивніше, які посилання в листі привабили увагу (метрика *click rate*). Це, в свою чергу, допомагає вдосконалювати зміст розсилок і персоналізувати комунікацію з клієнтами [6].

На рис. 1.3 та 1.4 вище проілюстровано базову технічну модель роботи трекінгових пікселів у двох середовищах – на веб-сайті та в електронній пошті. В обох випадках принцип подібний: невидимий код (зображення або скрипт) генерує запит до стороннього сервера, передаючи йому інформацію про користувача та його дії. Цей процес прихований від очей користувача, оскільки піксель має розмір 1×1 і, як правило, стилізований як прозорий або вбудований через скрипт, що не залишає видимих елементів на сторінці [6,14]. Користувач може й не здогадуватися, що його

дія (відкриття сторінки чи листа) спричинила передачу даних про нього третій стороні.

З технічної точки зору, трекінгові пікселі можуть бути впроваджені різними способами: через простий тег <img> як у прикладі вище, через <iframe> або за допомогою JavaScript-коду, який динамічно створює такий образ. Деякі сучасні трекери – це складні скрипти (наприклад, Facebook Pixel кодується як скрипт, що завантажує інші ресурси), але концептуально вони виконують ту саму функцію. Браузер виконує сторонній код і звертається до зовнішнього домену, передаючи туди контекстну інформацію (cookies, параметри URL, заголовки тощо) [5,6,13].

Важливо зазначити, що трекери можуть працювати навіть за умови блокування cookies – на відміну від cookie-файлів, які користувач може легко видалити чи заблокувати через налаштування браузера, піксельні теги майже невидимі та малодоступні для неозброєного ока [6,7].

Тому вони стали популярним засобом обходу обмежень: якщо користувач відхилив файли cookie, то все одно його дії можуть бути відстежені через піксель (адже браузер виконає запит за зображенням, не питаючи додаткового дозволу) [6,14].

Технічно, окрім класичних запитів за тегом <img>, деякі трекери використовують механізм Web Beacon у поєднанні з технологіями Canvas або WebGL, щоб отримувати додаткові характеристики оточення користувача (розмір екрану, встановлені шрифти, графічні можливості) та формувати унікальний “відбиток” пристрою. Цей підхід дозволяє ідентифікувати користувачів навіть у режимі інкогніто чи при регулярній очистці cookies, оскільки дані про конфігурацію апаратури та софту зазвичай залишаються незмінними.

Більш того, сучасні трекінгові рішення інтегрують відправку даних не лише через HTTP GET, а й за допомогою фонових AJAX-запитів і WebSocket-з’єднань, що дозволяє відстежувати події в реальному часі (наприклад, пересування миші, натискання клавіш, прокрутку сторінки) та передавати їх на аналітичні сервери без перезавантаження сторінки. Це значно розширює можливості профілювання та робить виявлення трекерів ще складнішим.

1.4. Правові аспекти використання трекерів

1.4.1. Вимоги GDPR щодо трекінгових пікселів

Загальний регламент із захисту даних (GDPR) – ключовий нормативний акт ЄС, що регулює обробку персональних даних. Його дія поширюється і на технології відстеження в інтернеті. Хоча сам термін “cookies” чи “пікселі” у GDPR прямо не згадано, багато норм GDPR безпосередньо застосовні до збору даних через трекери [1,14]. Розглянемо головні вимоги GDPR, які необхідно врахувати при використанні трекінгових пікселів:

Законність обробки та отримання згоди (ст.6 GDPR). Будь-яка операція з персональними даними має мати правову підставу. Для трекінгових пікселів, що збирають дані з маркетинговою або аналітичною метою, типовою законною підставою є добровільна інформована згода користувача (ст.6(1)(a)). Винятково можлива спроба обґрунтувати обробку “легітимним інтересом” (ст.6(1)(f)), але в контексті сторонніх рекламних трекерів європейські регулятори неодноразово заявляли, що це навряд чи правомірно, адже втручання у приватність значне, а користувачі очікують мати контроль (крім того, діє спеціальна Директива ePrivacy, яка *вимагає згоди* для майже всіх cookies, окрім технічно необхідних)

Отже, отримання явної згоди – де-факто обов’язкова вимога перед активацією пікселя. Згода має відповідати критеріям ст.7 GDPR: бути даною до збору даних, вільною, конкретною, поінформованою і однозначною (як правило, це реалізується через банер з опціями, де користувач активно натискає “Приймаю” для маркетингових/аналітичних cookies). Також повинна бути можливість легко відкликати згоду в будь-який момент (напр., через налаштування cookie або спеціальну сторінку).

Прозорість та інформування суб’єктів даних (ст.12–14 GDPR) [1,14]. Організація зобов’язана чітко повідомляти користувачів про використання трекінгових технологій і пов’язану обробку даних. Це реалізується через Політику конфіденційності та/або повідомлення у cookie-банері. У цій інформації слід вказати,

які дані збираються пікселями, з якою метою (напр., “відстеження конверсій, персоналізація реклами”), хто виступає отримувачем даних (назвати сторонні компанії – Facebook, Google тощо), чи відбувається передача даних за кордон, як довго дані зберігаються, і які права має користувач.

Прозора політика приватності дає користувачу розуміння, що відбувається за лаштунками сайту. GDPR вимагає, аби така інформація була легко доступною, зрозумілою та надавалась у момент збору даних або незадовго після (якщо дані отримано не від суб’єкта). Для трекерів практично це означає: посилання “Політика конфіденційності” та “Політика використання cookies” мають бути на видному місці; в них детально описано про пікселі (які саме ставляться, для чого, як відмовитись). Непрозорість або надто загальні фрази можуть розцінюватися як порушення (ст. 12 – принцип прозорості) [1,14].

Мінімізація даних та обмеження мети (ст.5(1)(c, b) GDPR). За принципом мінімізації, збирати можна лише ті персональні дані, які дійсно необхідні для визначеної мети, і не більше. В контексті трекінгових пікселів це означає, що налаштування пікселя повинні бути консервативними щодо обсягу даних. Наприклад, якщо мета – підрахувати відвідуваність сторінок, достатньо анонімного ідентифікатора; немає потреби відправляти ім’я користувача чи email у систему аналітики.

Якщо мета – рекламний ретаргетинг, може використовуватись хешоване значення email (для зіставлення в аудиторіях Facebook), але тільки за наявності згоди і з дотриманням умов (Meta вимагає щоб email хешувався перед передачею, але навіть хеш згідно GDPR залишається персональними даними, тому це не знімає вимог захисту).

Принцип обмеження мети означає, що дані від пікселя не можна використати на іншу несумісну ціль без отримання нової згоди. Наприклад, якщо ви збирали дані для аналітики по сайту, не можна раптом почати використовувати ті ж дані для емейл-розсилки чи передачі партнерам, якщо про це не було заявлено при зборі.

Захист даних за допомогою технологій (ст.25 GDPR – “Data Protection by Design and Default”). Ця стаття вимагає від контролера впроваджувати підходи, коли

приватність забезпечується “за замовчуванням” ще на етапі розробки системи. По відношенню до трекінгових пікселів це означає, що за замовчуванням налаштування мають бути найбільш сприятливими для приватності.

Наприклад, якщо компанія впроваджує Google Analytics, то за замовчуванням повинна бути увімкнена анонімізація IP-адрес, вимкнені функції “розширеного ремаркетингу” чи обміну даними з іншими сервісами Google, доки користувач не погодиться на додатковий трекінг. Аналогічно, піксель не має спрацьовувати без згоди – це теж принцип “by default”: якщо користувач нічого не обрав, система повинна поводитись, ніби згоди немає (тобто не передавати дані). Реалізація цього принципу часто досягається через використання менеджерів тегів та скриптів, які запускають код пікселя тільки після отримання позитивного сигналу від банеру згоди.

Data Protection by Design також передбачає впровадження технічних заходів для псевдонімізації та шифрування (Recital 78, Art.25 GDPR). Наприклад, дані, що збираються пікселем, можна одразу хешувати або шифрувати перед зберіганням, щоб у разі витоку вони були менш читабельними. Крім того, слід опрацьовувати сценарії, як мінімізувати збиток приватності, якщо користувач відмовився від трекінгу: система повинна все одно коректно працювати, просто без збору маркетингових даних.

Безпека обробки даних (ст. 32 GDPR) [1]. Контролер та процесор зобов’язані впровадити “відповідні технічні та організаційні заходи”, щоб забезпечити рівень безпеки, відповідний ризикам. Для трекінгових пікселів це має декілька рівнів реалізації:

Безпечна передача даних: самі запити пікселя повинні йти по захищених каналах (HTTPS). На щастя, сучасні браузери і сервіси це забезпечують автоматично (Facebook Pixel, GA працюють через HTTPS). Але якщо це власний піксель на внутрішньому сервері, потрібно подбати про наявність TLS-сертифікату і шифрування каналу.

Контроль доступу до даних: зібрані через пікселі дані (наприклад, в аналітичній системі або базі) повинні бути доступні тільки уповноваженому персоналу. Потрібно впровадити аутентифікацію, розмежування прав, журнали доступу. Якщо

використовуються зовнішні сервіси (GA, Meta), треба налаштувати безпечний доступ до їхніх консолей (двохфакторна автентифікація для адміністраторів акаунтів, тощо).

Захист від витоку: дані, що зберігаються, бажано псевдонімізувати. Наприклад, замість зберігати у логах IP-адресу у відкритому вигляді – зберігати тільки частину (анонімізувати останній октет IPv4, що GA Universal Analytics пропонував як опцію), або хеш від неї. Якщо піксель пов'язує дії з конкретним користувачем (напр., ID облікового запису), то у зовнішній системі краще користуватись не реальним ID, а сурогатним ключем, який не дасть зрозуміти особу без окремого довідника (який зберігається в компанії) [1,14]. Також слід встановити політики видалення/очищення даних: не тримати інформацію вічно, а видаляти або агрегувати її після досягнення мети. Google Analytics, наприклад, дозволяє налаштувати період зберігання даних користувацького рівня (від 14 місяців до необмежено) – рекомендується обирати мінімально необхідний (наприклад, 14 або 26 місяців, а не "не закінчується").

Тестування та оцінка ефективності безпеки: ст. 32 також згадує необхідність регулярного тестування захисних заходів. Це може включати аудит налаштувань пікселів, перевірку, чи не збирають вони зайвого; моделювання "атаки" – чи може зловмисник витягти дані з нашої аналітики; чи безпечні API, що приймають дані.

Оцінка впливу на захист даних (DPIA, ст. 35 GDPR) [1]. Якщо використання трекінгових технологій ймовірно призводить до високого ризику для прав і свобод суб'єктів даних, компанія повинна провести DPIA – детальний аналіз ризиків і визначити заходи з їхньої мінімізації. Багато наглядових органів вважають, що системи масового відстеження поведінки користувачів можуть підпадати під критерії "високого ризику" (особливо якщо йдеться про профілювання, відстеження діяльності на різних платформах, обробку чутливих даних).

Наприклад, якщо урядовий веб-сайт хоче встановити трекер від сторонньої компанії, або медичний портал – це точно варто проаналізувати через DPIA. DPIA допоможе формально описати, які є загрози (несанкціонований доступ, порушення прав суб'єктів, міждержавна передача тощо) і які контрзаходи застосовані. Це також спосіб довести відповідність ст. 25 (підхід "by design"), оскільки DPIA часто включає

пошук більш приватних альтернатив (напр., чи можна замість Google Analytics використати self-hosted аналітику з меншим обсягом даних).

Угоди з третіми сторонами і спільна відповідальність (ст. 26, 28 GDPR). Якщо на сайті використовується сторонній трекер, важливо визначити, ким є ця сторона згідно GDPR – контролером чи процесором. Наприклад, Meta заявляє, що отримує дані через Pixel як окремий контролер (оскільки використовує їх для своїх цілей реклами). Google Analytics за умовами – скоріше обробник (процесор), що діє від імені сайту (хоча з нюансами, адже Google теж використовує дані для своїх аналітичних інтересів). У будь-якому разі, письмовий договір або відповідні умови повинні регулювати такі відносини. Якщо третя сторона – процесор, має бути Data Processing Agreement (DPA), який відповідає ст. 28 GDPR (включає зобов'язання щодо безпеки, допомоги контролеру, повідомлення про інциденти тощо). Якщо ж сторони – спільні контролери (як часто буває з соціальними плагінами), доцільно укласти угоду про розподіл відповідальності (хто за що відповідає, хто інформує суб'єктів, і т.д., ст. 26). На практиці великі компанії пропонують приєднатися до стандартних умов – наприклад, Google має "Стандартні положення обробки даних для рекламних продуктів", Meta – "Додаток щодо обробки даних" тощо. Важливо, щоб організація-оператор сайту прийняла ці умови і дотримувалась їх. Крім того, якщо дані йдуть за межі ЄС, мають бути оформлені Standard Contractual Clauses (SCCs) або інші механізми трансферу (ст. 46), хоча, як згадувалось, після Schrems II одних SCC недостатньо без додаткових гарантій.

Права суб'єктів даних (ст. 15–22 GDPR). Використовуючи трекінгові пікселі, організація повинна бути готова виконувати запити користувачів щодо їхніх даних. Наприклад, людина може подати запит: "Надішліть мені копію моїх персональних даних". Потрібно передбачити, що дані з систем аналітики чи маркетингу теж потрапляють під це визначення, якщо вони прив'язані до ідентифікатора [1,14].

Хоч Google Analytics і працює з псевдонімними ID, але якщо ваш сайт може співставити той ID з конкретним користувачем, доведеться надати ці журнали. Те ж стосується права на видалення (якщо користувач вимагає, треба видалити його дані, у т.ч. з логів трекерів). Тому варто заздалегідь продумати механізм пошуку та

вилучення записів про користувача в базах даних, що накопичені пікселями. Це знову ж спонукає до мінімізації – якщо ви не зберігаєте прямі ідентифікатори, а лише сукупну статистику, права суб'єктів менш застосовні. Але якщо, наприклад, e-commerce сайт передає через піксель номер клієнта і покупки, то ці дані потрапляють під GDPR, і треба вміти їх витягти.

Підсумовуючи, GDPR накладає багаторівневі зобов'язання: від організаційних (політики, угоди) до технічних (настройки систем). Використовувати трекінгові пікселі у відповідності до GDPR – можливо, але вимагає ретельного підходу: належним чином отриманої згоди, прозорості для користувача, мінімізації та захисту кожного біту даних, що збирається і передається [1,14].

По-перше, слід впровадити механізми псевдонімізації та шифрування даних у базі ще на етапі їх надходження: наприклад, замість безпосереднього збереження ідентифікатора користувача (який передається через піксель), генерувати одноразовий токен або хеш із солями, що унеможливлює зворотне відновлення особистості без наявності додаткового ключа. Це не лише знижує ризик витоку персональних даних, але й спрощує виконання запитів на видалення або виправлення інформації за запитом суб'єкта даних (право на забуття та виправлення) — достатньо видалити або оновити відповідний токен у сховищі ключів, а не масив усіх записів.

По-друге, необхідно вести аудит та логування всіх операцій із піксельними даними: коли відбулось збереження, доступ або видалення запису; які сервіси обробляли дані; хто і за яким запитом ініціював зміну. Такий підхід забезпечує вимогу GDPR щодо підзвітності (accountability) — організація зможе довести, що всі обробки здійснювалися на підставі законних підстав, а права суб'єктів даних (на доступ, виправлення, видалення) були реалізовані у встановлені строки. Одночасно це дозволяє швидко виявляти та реагувати на аномальні операції, які можуть сигналізувати про несанкціонований доступ чи витік.

1.4.2. Вимоги CCPA/CPRA щодо онлайн-трекінгу

Закон Каліфорнії про захист конфіденційності споживачів (CCPA), що набув чинності у 2020 р., та його оновлення CPRA (з 2023 р.) – це американські нормативні акти, які регулюють збір і продаж персональної інформації споживачів у штаті Каліфорнія. На відміну від GDPR, CCPA не вимагає попереднього отримання згоди на трекінг або використання пікселів. Втім, CCPA дає споживачам право відмовитися від «продажу» їхніх персональних даних третім сторонам [14,15].

Поняття *"продаж"* у CCPA трактується широко і може охоплювати обмін даними з третіми сторонами в комерційних цілях. Отже, якщо веб-сайт передає дані користувача сторонній рекламній мережі (наприклад, через піксель Facebook, який збирає дані для таргетингу реклами), це може розглядатися як продаж персональної інформації, *якщо* за це отримується якась вигода (не обов'язково пряма оплата). В такому випадку компанія повинна надати користувачу можливість *opt-out*, тобто відмовитися від такого обміну (зазвичай реалізується через посилання "Do Not Sell or Share My Personal Information" на сайті).

Ще одне важливе положення CCPA/CPRA – вимога прозорості. Політика конфіденційності компанії має перелічувати категорії персональної інформації, що збираються, і треті сторони, яким ці дані розкриваються, а також цілі такого розкриття. Це безпосередньо стосується трекінгових пікселів: організація повинна у своєму повідомленні про приватність вказати, що вона використовує інструменти відстеження (pixels, cookies, analytics) і що при цьому певні дані (наприклад, ідентифікатор пристрою, історія переглядів сайту, демографічні дані тощо) можуть передаватися, скажімо, компанії Meta або Google. Відомо, що американські компанії іноді нехтували деталізацією цих положень, намагаючись уникнути згадки про "продаж" даних. Однак свіжа судова практика показує, що це небезпечно.

У березні 2025 року федеральний суд Каліфорнії постановив, що передача персональних даних через трекінгові пікселі може розглядатися як "несанкціоноване розголошення" інформації, даючи підстави для судового позову навіть без традиційного витоку даних. Справа *Shah v. Capital One* стосувалася того, що банк

Capital One використовував пікселі аналітики, які передавали дані користувачів стороннім компаніям (на кшталт аналітичних сервісів) [15].

Позивачі заявили, що це порушило їхнє право на конфіденційність. Суддя підтримала цю позицію, дозволивши позов, і зазначила, що навмисна передача персональних даних стороннім через пікселі може вважатися порушенням CCPA – а саме несанкціонованим розголошенням підрозділу 1798.150 CCPA. Раніше приватні позови за CCPA були обмежені випадками витоку даних внаслідок порушення безпеки (злама) – тепер же поле відповідальності розширено. Це рішення *значно підвищує ризики* для бізнесу, адже тепер рутинні практики онлайн-трекінгу можуть спричиняти статутні збитки (штрафні санкції) у розмірі $100–750 за кожного споживача за інцидент [15].

Для великих веб-сайтів з мільйонами користувачів потенційний позов щодо пікселів здатний обернутися багатомільйонними компенсаціями.

Ще один висновок з цієї справи – суд звернув увагу на розбіжності між заявленою політикою конфіденційності і фактичними діями компанії. Зокрема, в політиці Capital One не було чітко сказано про масштаб передачі даних стороннім трекерам, що було розцінено як введення споживачів в оману [15].

Цей прецедент сигналізує усім компаніям: *слід ретельно перевірити зміст своїх Privacy Policy*, щоби вони відверто та точно описували використання пікселів і розкриття даних третім сторонам. Інакше компанія ризикує не тільки порушити сам закон, а й втратити правовий захист (адже неправдива або неповна політика може посилити позиції позивачів у суді).

Отже, хоча CCPA/CPRA і не забороняють прямо трекінгові пікселі, вони встановлюють певні обов’язки для компаній-користувачів таких технологій:

- забезпечити можливість відмови від передачі даних (opt-out) для каліфорнійських споживачів, якщо піксель ділиться даними з третіми сторонами для реклами;
- чесно повідомити користувача про всі такі практики в політиці приватності;

- вживати заходів для захисту даних (бо CCPA дає право позову у випадку *«невжиття розумних заходів безпеки»*, що призвело до несанкціонованого доступу або розголошення даних – тепер, як бачимо, і піксель може підпасти під це визначення).

Насамкінець, на рівні федерації США відсутній єдиний “американський GDPR”, проте активно діють Федеральна комісія з торгівлі (FTC) та суди. FTC уважно стежить за питаннями онлайн-трекінгу і видає рекомендації та приписи. У 2023 р. FTC вперше оштрафувала компанії за порушення Health Breach Notification Rule – у випадках, коли цифрові сервіси здоров’я передавали чутливі дані користувачів (наприклад, про ліки чи психічне здоров’я) через трекери на кшталт Google і Facebook без згоди клієнтів. Одна телемедична компанія заплатила $1,5 млн штрафу за неповідомлення користувачів про такий витік даних на сторонні платформи, інша – онлайн-сервіс психологічної допомоги – була оштрафована на $7,8 млн та заборонена до передачі даних на рекламні платформи за аналогічне порушення. Ці випадки підкреслюють: використання пікселів без достатнього аналізу ризиків може призвести до юридичних наслідків навіть у США, особливо якщо йдеться про чутливі категорії інформації [14,15].

1.4.3. Закон України «Про захист персональних даних» і трекінгові технології

В Україні основним актом, що регулює обробку персональних даних, є Закон України «Про захист персональних даних» №2297-VI від 01.06.2010 (з численними змінами) [4]. Цей закон установлює загальні вимоги до будь-якої операції з персональними даними – збору, зберігання, використання, поширення тощо – і спрямований на захист фундаментальних прав людини на невтручання в особисте життя. Хоча закон було прийнято раніше появи GDPR, за духом він близький до європейських норм, оскільки був розроблений на основі Конвенції №108 Ради Європи [4].

Закон визначає персональні дані як відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути ідентифікована. Таким чином, IP-адреса користувача, файли cookie, ідентифікатор його пристрою чи браузера можуть вважатися персональними даними, якщо існує можливість ідентифікувати конкретну особу через них. У контексті трекінгових пікселів, якщо збирається хоча б IP-адреса чи унікальний ID, прив'язаний до користувача, український закон розглядає це як обробку персональних даних і вимагає дотримання відповідних правил [4].

Обробка персональних даних дозволена лише за згодою суб'єкта або в інших визначених законом випадках (наприклад, коли обробка необхідна для виконання договору, в життєво важливих інтересах суб'єкта, для здійснення повноважень держоргану тощо). Очевидно, що використання пікселя для маркетингу не підпадає під спеціальні виключення, отже необхідно отримувати згоду користувача на таку обробку. Відповідно до закону, згода має бути інформованою та добровільною. На практиці реалізація цього принципу аналогічна до підходів GDPR – через явне погодження (галочку, натискання кнопки) після надання чіткої інформації про збір даних [1,4,14].

Ст.12 закону вимагає повідомляти суб'єкта про включення його даних до бази, мету збору, третіх осіб, яким передаються дані, його права тощо. У випадку трекінгу це може тлумачитись як необхідність вказувати інформацію про використання пікселів у політиці конфіденційності (або іншому документі), доступному користувачу. Тобто український користувач також має право знати, що його дані (навіть технічні) передаються, скажімо, компанії Facebook для цілей реклами, і сам факт такої передачі має бути зафіксований у документах компанії [4].

Володілець персональних даних (тобто компанія, що збирає дані через піксель) зобов'язаний вживати технічних і організаційних заходів захисту даних від несанкціонованого доступу, втрати, перекручення тощо. Це означає, що якщо дані користувачів зберігаються або передаються, вони мають бути належно захищені – використання шифрування, контроль доступу, тощо. Наприклад, якщо українська компанія використовує власний трекінг-піксель і зберігає зібрані дані в базі, вона повинна забезпечити їх захищеність (щоб сторонні не отримали до них доступ). В

контексті сторонніх пікселів (як-от Facebook) компанія має впевнитись, що сам постачальник пікселя (Facebook) дотримується стандартів безпеки – за українським законом, відповідальність за передачу даних третій особі частково лежить і на тому, хто ці дані зібрав.

Закон передбачає, що передача персональних даних іноземним суб'єктам може відбуватись лише до країн, які забезпечують належний захист персональних даних, або за наявності окремої згоди суб'єкта на таку передачу. Тому, коли трекінговий піксель відправляє дані на сервери, скажімо, у США чи інші країни, теоретично компанія повинна переконатися, що або країна-отримувач входить до переліку належного захисту (встановлюється законодавством чи міжнародними договорами), або ж отримати від користувача пряму згоду на те, що його дані можуть бути передані за кордон. На практиці ці норми в Україні часто ігноруються через недосконалий механізм контролю, але формально вони є.

Станом на 2025 р., українське законодавство продовжує адаптуватися до європейських вимог. Готується нова редакція закону «Про захист персональних даних», ближча до положень GDPR, яка ймовірно введе чіткіші вимоги щодо згоди на cookies і трекери. Вже зараз багато українських компаній, орієнтованих на ринок ЄС, добровільно впроваджують банери згоди на використання cookies/пікселів, щоб відповідати міжнародним стандартам [1.4,14].

Висновок до розділу 1

У цьому розділі було проведено аналіз теоретичних основ використання трекінгових пікселів у цифровому середовищі та визначено їхній вплив на безпеку персональних даних. Розкрито сутність трекінгового пікселя як інструменту прихованого збору інформації про дії користувачів у вебпросторі та електронній пошті. Детально описано технічний механізм функціонування трекінгових пікселів, способи їхньої інтеграції у вебсторінки та листи, а також ті дані, які можуть автоматично передаватися і накопичуватися на сторонніх серверах, включаючи IP-адреси, інформацію про пристрої, дії користувачів і технічні характеристики

браузерів. Проаналізовано основні різновиди трекерів, зокрема Meta Pixel, Google Analytics, TikTok Pixel, а також специфіку їхнього застосування у сучасному маркетингу, веб-аналітиці та email-розсилках. Встановлено, що широке використання трекінгових пікселів суттєво підвищує ризики для конфіденційності та безпеки персональних даних користувачів, оскільки дозволяє створювати детальні поведінкові профілі без явної поінформованої згоди.

Особлива увага була приділена аналізу правових аспектів використання трекінгових пікселів у контексті сучасних міжнародних і національних стандартів захисту персональних даних. Було системно розглянуто вимоги GDPR щодо законності обробки, необхідності отримання добровільної інформованої згоди, забезпечення прозорості для суб'єктів даних, обмеження обсягу зібраної інформації, впровадження принципів "Privacy by Design and Default", захисту даних на всіх етапах обробки, а також виконання прав користувачів щодо доступу, виправлення, видалення і обмеження обробки даних. Досліджено ключові положення американського законодавства CCPA/CPRA, які регламентують права споживачів щодо відмови від передачі даних третім сторонам, прозорості у політиках конфіденційності, а також судову практику, що посилює відповідальність бізнесу за неналежне інформування користувачів та передачу персональних даних через трекінгові пікселі.

РОЗДІЛ 2 АНАЛІЗ ЗАГРОЗ БЕЗПЕЦІ ПЕРСОНАЛЬНИХ ДАНИХ ПРИ ВИКОРИСТАННІ ТРЕКІНГОВИХ ПІКСЕЛІВ

Використання трекінгових пікселів несе значний ризик для безпеки персональних даних, оскільки збір інформації відбувається без відома користувача, передача даних здійснюється через сторонні сервери, а обробка персональних ідентифікаторів дозволяє будувати цілісні поведінкові профілі.[6,14]

У цифровому середовищі можна виокремити основні типи загроз:

– Збір та передача ідентифікаторів без згоди користувача. Це включає IP-адресу, дані геолокації, час перебування на сторінці, навігаційні дії. Часто ця інформація передається третім сторонам, не зазначеним у політиках конфіденційності.[6,14]

– Session hijacking. [6] За умови, якщо трекінговий піксель записує унікальний ідентифікатор користувача, є ймовірність перехоплення даних сесії, зокрема через маніпуляції з cookie чи localStorage.

– Фішинг на основі поведінкових шаблонів. Комбінування даних трекінгу дозволяє зловмисникам створювати персоналізовані фішингові атаки на основі інтересів користувача.[6,15]

– Обхід cookie-згоди. Пікселі можуть працювати через серверні механізми (server-side tracking), що уникає обмежень браузера щодо cookies.[6,16].

Крім технічного аналізу, було досліджено відповідність практики використання пікселів основним принципам GDPR [1,14,16]. Виявлено, що більшість сервісів, зокрема Meta, TikTok, Google, використовують системи трекінгу без забезпечення повної прозорості, а багато сайтів мають неактивні або надто загальні банери cookie-згоди.[8,9,10]

Для візуалізації ризиків було побудовано матрицю ризиків витоку персональних даних, яка ґрунтується на ймовірності події та рівні впливу (див. Таблиця 2.1).

Таблиця 2.1

Матриця ризиків витоку персональних даних

Потенційна загроза	Ймовірність	Вплив	Рівень ризику
Збір IP-адреси без згоди	Висока	Середній	Високий
Поведінковий профайлінг	Висока	Високий	Високий
Session hijacking	Середня	Високий	Високий
Cross-site tracking	Висока	Середній	Високий
Використання 3rd party трекерів	Висока	Середній	Високий
Server-side tracking без cookies	Висока	Низький	Середній

На підставі виявлених ризиків та невідповідностей запропоновано такі заходи:

Використання криптографічних методів (AES, блокові шифри) для захисту даних, що передаються [2,3];

Застосування механізмів детектування активності сторонніх доменів через DNS-запити [6,7];

Впровадження системи моніторингу аномалій у HTTP/HTTPS-запитах [2];

Формалізація Політики конфіденційності, яка прямо вказує на використання трекінгових технологій [6,4,14] (Розроблений шаблон такої політики наведено в Додатку А.)

2.1. Особливості збору персональних даних за допомогою трекінгових пікселів

Трекінгові пікселі (англ. *tracking pixels*) — це невеликі прозорі зображення (зазвичай розміром 1×1 піксель), які вбудовуються у вміст вебсторінок, електронних листів або рекламних оголошень і завантажуються з серверів третіх сторін [5,6]. Основною метою їх використання є прихований збір інформації про дії користувача

з метою аналітики, таргетингу або поведінкового профілювання. Попри свою просту структуру, трекінгові пікселі є ефективним інструментом стеження за активністю користувачів, часто без їх прямої обізнаності.

Коли користувач відкриває вебсторінку або електронний лист, що містить такий піксель, браузер автоматично надсилає запит до сервера, на якому зберігається це зображення. Разом із запитом передаються різноманітні метадані, які сервер може обробити та зберегти. Ці дані можуть включати, але не обмежуються:

– IP-адресу користувача, яка дозволяє встановити його приблизне географічне розташування;

– тип браузера та операційної системи, що допомагає адаптувати вміст до пристрою користувача;

– час та дата перегляду сторінки, що використовується для аналізу поведінки користувачів у реальному часі;

– URL сторінки, з якої завантажується піксель, що дозволяє відстежити, на якому ресурсі відбувається взаємодія;

– джерело трафіку (referrer), що показує, з якого сайту чи платформи користувач потрапив на сторінку;

– взаємодія з елементами сторінки (кліки, перегляд відео, прокручування) [6] у випадках, коли піксель інтегровано з JavaScript або іншими скриптами.

Особливо небезпечною [6] є можливість ідентифікації користувачів шляхом поєднання цих даних із іншими інформаційними слідами, наприклад, за допомогою device fingerprinting або cookie-механізмів. У багатьох випадках трекінгові пікселі працюють у тандемі з куками, що дозволяє збирати довгострокові профілі поведінки користувачів навіть при відвідуванні різних сайтів (так званий *cross-site tracking*).

Варто зазначити, що сучасні аналітичні системи, такі як Facebook Pixel, Google Analytics 4, TikTok Pixel або LinkedIn Insight Tag, активно застосовують піксельні механізми. Наприклад:

– Facebook Pixel дозволяє відстежувати дії користувачів після перегляду реклами у Facebook (наприклад, покупки або реєстрації на сайті).

– Google Analytics використовує трекінгові пікселі для аналізу поведінки користувачів на сайті, формування демографічного профілю, визначення конверсій.

– TikTok Pixel виконує схожі функції у межах своєї рекламної екосистеми, збираючи детальні поведінкові дані для оптимізації кампаній.

Ці платформи декларують відповідність міжнародним вимогам щодо захисту персональних даних, однак на практиці не завжди забезпечують прозорість у тому, які саме дані збираються, як довго вони зберігаються та кому можуть передаватися [1,8,9,10,11,14]. Таким чином, користувачі, взаємодіючи з вебресурсами, часто не усвідомлюють повного обсягу збору своїх даних, що порушує принципи прозорості та інформованої згоди, закріплені, зокрема, в статті 5 GDPR.

У підсумку, трекінгові пікселі становлять важливий об'єкт аналізу в контексті інформаційної безпеки, оскільки їх використання прямо пов’язане з можливими ризиками витоку, несанкціонованого доступу або вторинного використання персональних даних без згоди суб’єкта.

2.2. Методи обходу згоди користувача та порушення принципів GDPR

Однією з ключових вимог Загального регламенту про захист даних (GDPR) є забезпечення прозорого та законного оброблення персональних даних. Згідно зі статтями 6 та 7 GDPR, для обробки персональних даних зазвичай необхідна чітка, добровільна, інформована та недвозначна згода суб’єкта даних. У випадку з трекінговими пікселями, дотримання цього принципу є надзвичайно складним завданням, що часто свідомо ігнорується операторами вебсайтів та рекламними платформами.

Один з найпоширеніших способів обходу згоди — це приховане вбудовування трекінгових пікселів у контент вебсторінок або HTML-тіла електронних листів. У таких випадках пікселі завантажуються автоматично після відкриття сторінки чи листа, ще до того, як користувач має змогу взаємодіяти з банером згоди на cookies або надати згоду на обробку персональних даних [1,14,16]. Це суперечить вимогам

GDPR, де чітко визначено, що жодна обробка даних не повинна здійснюватися до отримання згоди (виняток — правова підстава, яка має бути належно обґрунтована).

Ще один метод — використання загального банера згоди [14], який не деталізує специфіку трекінгових технологій. У таких випадках користувач може погодитися лише на використання cookies, не будучи інформованим про присутність трекінгових пікселів, JavaScript-компонентів або інших інструментів моніторингу. Це порушує принцип прозорості, визначений у статті 5 GDPR.

Окрему небезпеку становить використання «темного дизайну» (dark patterns) — елементів інтерфейсу, які психологічно підштовхують користувача до натискання кнопки «Погоджуюсь», уникаючи перегляду або зміни налаштувань конфіденційності. Деякі банери спеціально ховають або ускладнюють доступ до опцій «Відмовитися» або «Налаштувати», що викривлює реальну свободу вибору.

Нерідко зустрічаються і гібридні методи збору даних, коли трекінг здійснюється пікселями від імені сторонніх рекламних партнерів, і ці партнери не зазначаються у політиці конфіденційності основного вебресурсу [16]. Таким чином, суб’єкт даних не має змоги реалізувати своє право на доступ, виправлення чи видалення даних згідно зі статтями 15–17 GDPR, адже він навіть не знає, хто є контролером цих даних.

Також слід звернути увагу на техніки обфускації (приховування) коду пікселів, які ускладнюють виявлення трекінгу засобами блокування реклами або сканерами конфіденційності [6,7]. Це дозволяє операторам сайтів приховано збирати дані навіть у користувачів, які активно намагаються захистити свою приватність.

Нарешті, використання трекінгових пікселів у розсилках електронної пошти без попереднього інформування користувача є прямим порушенням GDPR, оскільки такі листи не мають відповідного банера згоди. У момент відкриття листа персональні дані (зокрема IP, геолокація, пристрій, час перегляду) автоматично потрапляють до стороннього аналітичного сервісу — без жодної інформованої дії з боку користувача.

Таким чином, методи обходу згоди користувача при використанні трекінгових пікселів становлять серйозну загрозу дотриманню прав суб’єктів персональних даних. Вони не лише підривають довіру до цифрового середовища, а й можуть стати

підставою для накладення значних штрафів з боку наглядових органів, як це передбачено у статті 83 GDPR.

2.3. Аналіз прикладів витоків даних, пов'язаних з трекінгом

Реальні інциденти, пов'язані з використанням трекінгових пікселів, демонструють, що ці технології, якщо не контролюються належним чином, можуть стати джерелом масових витоків персональних даних. Нижче наведено найбільш резонансні приклади, які висвітлюють уразливості систем трекінгу та показують, як саме такі інструменти можуть порушувати конфіденційність.

Витік даних пацієнтів через Meta Pixel на сайтах NHS (Велика Британія) [15]. У 2023 році виявлено, що близько 20 медичних закладів британської Національної служби здоров'я (NHS) розмістили на своїх веб-сайтах трекінговий піксель Facebook (Meta Pixel), який таємно передавав Meta дані про відвідувачів цих сайтів. Серед переданих даних були подробиці про переглянуті сторінки, натиснуті кнопки, здійснені пошуки на медичних порталах – наприклад, сторінки, що стосуються ВІЛ, онкології, питань гендерної ідентичності, ментального здоров'я тощо. Ця інформація, у поєднанні з IP-адресою та (як з'ясувалося) даними облікового запису Facebook користувача, дозволяла Meta ідентифікувати конкретну особу і знати про її медичні запити.

Це кричуще порушення конфіденційності: лікарняні сайти обіцяли пацієнтам зберігати їх дані в таємниці, а натомість автоматично надсилали їх третьій стороні без будь-якої згоди. Після розголосу цього скандалу більшість шпиталів поспішно відключили пікселі та принесли вибачення пацієнтам. Даний інцидент продемонстрував, наскільки небезпечним може бути бездумне впровадження маркетингових інструментів у чутливих сферах.

Навіть якщо метою було, скажімо, відстеження ефективності рекламних кампаній для набору персоналу чи благодійних програм (як заявили деякі з NHS-трастів), результатом стало масове порушення приватності мільйонів пацієнтів. В юридичній площині, у Великій Британії (і ЄС) такі дії порушують GDPR, а також

принцип довірчості відносин лікар-пацієнт. Розпочато розслідування і можливі колективні позови від імені пацієнтів.

Використання пікселів на медичних сайтах США (Advocate Aurora Health та інші). Подібні історії трапилися у США [16]: низка великих медичних мереж (Advocate Aurora Health, Novant Health та ін.) повідомили про витік персональних медичних даних сотень тисяч пацієнтів через пікселі Facebook і Google на їхніх сайтах. Зокрема, в жовтні 2022 р. система Advocate Aurora (що обслуговує ~3 млн пацієнтів) зізналася, що інтеграція Meta Pixel у її портал для пацієнтів призвела до відправки Facebook деталей про відвідування пацієнтами сторінок з результатами аналізів, записами на прийом тощо – без належного дозволу.

Це було кваліфіковано як *витік* (breach) відповідно до законів США [16], і постраждалим розіслали повідомлення про порушення. На хвилі цих новин у США було подано декілька колективних позовів проти медичних закладів та проти компанії Meta, звинувачуючи їх у незаконному зборі даних про здоров'я (порушення конфіденційності, вторгнення в приватне життя, порушення різних актів про захист даних). Ці справи досі розглядаються, але вже очевидно, що репутаційні втрати для лікарень величезні, не кажучи про мільйонні витрати на судові процеси та можливі компенсації.

Для Meta цей скандал теж став серйозним – проти неї об'єднуються численні позови з різних штатів. Хоча Facebook захищається, вказуючи що його умови забороняють передавати *чутливі дані* через піксель, ці інциденти показали, що на практиці багато хто не дотримується цих умов, а сама компанія не змогла запобігти збору такої інформації.

Витік даних з урядових сайтів. Окрім комерційних компаній, під роздачу потрапляють і державні органи. У 2022 році з'ясувалося, що веб-сайти деяких урядових установ та міських рад (наприклад, в Австралії, Данії) мали вбудовані трекери Facebook/Google, які відстежували дії відвідувачів навіть на сторінках, де ті подавали особисту інформацію або здійснювали оплати. Це означало, що потенційно дані про користування державними послугами (штрафи, комунальні платежі тощо) могли стати відомі третім сторонам. Такі випадки отримали широкий розголос, і

органи поспіхом видаляли трекери, визнаючи, що їхні диджитал-відділи “не подумали” про наслідки. Ці інциденти, хоч і менш гучні, додатково підтверджують: проблема пікселів є всюдисущою, охоплюючи навіть ті сфери, де приватність мала б бути особливо захищеною.

Неочевидний трекінг користувачів без згоди [14,16]. Іноді трекінгові пікселі опиняються на сайтах несподівано для самих власників ресурсу – як результат вставлення сторонніх віджетів або коду. Наприклад, у 2021 р. у Франції штрафували кілька компаній за те, що на їхніх сайтах працювали *вбудовані сторонні елементи (відеоплеєри, соціальні кнопки)*, які встановлювали трекери без відома користувачів і без відображення в політиці конфіденційності.

Регулятор (CNIL) розцінив це як ненавмисне, але порушення: компанії зобов’язані контролювати весь код на своєму сайті і забезпечити, щоб жоден трекер не запускався без згоди. Це показує ще один ризик: відсутність належного аудиту сторонніх скриптів може призвести до “прихованого” встановлення пікселів. Після того випадку європейські організації почали уважніше перевіряти, які скрипти і пікселі присутні на їхніх сторінках, та включати відповідні положення до договорів з постачальниками веб-сервісів.

Фішингові атаки з відстеженням відкриття листів [6,7]. З боку кібербезпеки можна згадати приклад кампанії з використанням пікселів для цілеспрямованого шпигунства. У 2022–2023 рр. фіксувались фішингові розсилки на керівників компаній, де зловмисники вкладали невидимий піксель у перший лист. Ті, хто відкрив лист, потім отримували другий – вже з більш переконливим контентом (бо атакери знали, що адресат читав їхній попередній лист, і, отже, зацікавлений).

Деякі такі атаки навіть намагалися збирати *таймлайн активності* – піксель повідомляв, скільки разів і коли лист відкривали, що дозволяло припустити, наскільки уважно жертва читає повідомлення. Подібні епізоди засвідчили: трекінгові пікселі – це не лише про маркетинг, а й про кіберрозвідку. Для захисту від цього великі поштові сервіси (Gmail, Apple Mail) почали впроваджувати захисні заходи: приміром, Gmail з 2014 р. став проксувати зображення через свої сервери (частково це нейтралізує трекінг, приховуючи реальний IP користувача), а Apple в 2021 р.

запровадила функцію Mail Privacy Protection, яка завантажує всі зображення листів у фоновому режимі через анонімний проксі – тим самим *збиваючи точність* пікселів (відправнику завжди здається, що лист відкритий, але насправді це зробив Apple-проксі, а не сам користувач). Ці технічні заходи хоч і знижують ефективність email-трекінгу, але поки що не стали повсюдним стандартом.

Висновок до розділу 2

У цьому розділі було проведено детальний аналіз сучасних загроз безпеці персональних даних, які виникають унаслідок використання трекінгових пікселів у цифровому середовищі. Описано ключові ризики, зокрема прихований збір та передача ідентифікаторів без згоди користувача, побудову поведінкових профілів, можливість захоплення сесії, обходу обмежень cookie-згоди, а також створення персоналізованих фішингових атак. Проаналізовано практичні приклади інцидентів у медичній, державній та комерційній сферах, що підтвердило серйозність і багатовимірність проблеми — від втрати приватності до юридичних і репутаційних наслідків для організацій.

У ході дослідження встановлено, що на практиці сучасні трекінгові інструменти часто використовуються із порушенням принципів прозорості та інформованої згоди, закріплених у GDPR, CCPA/CPRA та українському законодавстві. Виявлено типові методи обходу законодавчих вимог — від маскування коду пікселів до маніпуляцій інтерфейсом згоди та використання сторонніх партнерських трекерів без належного повідомлення користувача. Наведені реальні кейси витоків даних демонструють, що ризики стосуються не лише звичайної аналітики, а й охоплюють найчутливіші сфери — медицину, державне управління, комунікації.

Відзначено, що недостатня увага до налаштувань трекінгових систем, відсутність належного аудиту і контролю за впровадженням сторонніх скриптів можуть призвести до непередбачуваних наслідків, у тому числі масштабних витоків персональної інформації.

РОЗДІЛ 3 РОЗРОБКА МЕХАНІЗМІВ БЕЗПЕКИ ПЕРСОНАЛЬНИХ ДАНИХ У КІБЕРПРОСТОРІ З ВИКОРИСТАННЯМ ТРЕКІНГОВИХ ПІКСЕЛІВ

3.1 Модель загроз і ризиків, пов'язаних з трекінговими пікселями

Головним цінним активом, на який посягають трекінгові пікселі, є *персональні дані користувачів* – інформація про особу, її поведінку, вподобання, здоров'я тощо. Ці дані можуть перебувати як на боці користувача (у його браузері/пристрої), так і на боці організації (в базах даних сайту або маркетингових сервісів). Крім того, зачіпається такий нематеріальний актив як *право на приватність* та довіра користувача до системи.

Суб'єкти загроз:

– Зовнішні трекери-рекламні мережі: великі компанії (Meta, Google та інші), що надають код пікселя. Вони отримують дані і використовують їх у власних цілях – тут існує ризик, що ці дані будуть використані не лише для заявленої аналітики, а й для профілювання, передачі іншим стороннім, чи можуть стати об'єктом витоку. Мотив – комерційна вигода від накопичення даних.

– Недобросовісні або скомпрометовані сторонні провайдери: якщо компанія користується послугами маловідомого трекера, є ризик, що той може навмисно збирати зайве (шпигунство) або бути зламаним, і дані витечуть до зловмисників.

– Кіберзлочинці (хакери): можуть використовувати пікселі як інструмент атаки (наприклад, у фішингу, для визначення активності цілі). Також вони можуть впровадити свій трекер шляхом атаки типу XSS чи шляхом компрометації стороннього віджета на сайті, аби красти дані користувачів (наприклад, відома схема атак Magecart – коли шкідливий код вбудовується в сайт для крадіжки даних карт; теоретично схожа схема може бути застосована для піксель-трекінгу, щоб потай зливати дані сесії користувача на сервер зловмисника).

– Несвідомі внутрішні співробітники: маркетологи чи розробники компанії, які можуть додати на сайт трекінговий код, не провівши оцінку ризиків. Це *внутрішня загроза* не навмисна, але дуже поширена – через необережність або недостатню кваліфікацію працівники самі можуть відкрити ворота для витоку даних (як у випадку з NHS, де команди веб-розробників впровадили піксель, мабуть, не усвідомлюючи наслідків).

Можливі вразливості системи включають (не обмежуючись):

– Відсутність контролю за вмістом сайту (поганий інвентаризаційний контроль скриптів) – на сторінках присутні сторонні скрипти/пікселі, про які IT-безпека може не знати.

– Немає механізмів перевірки чи моніторингу вихідного трафіку з сайту – тобто, *невидимі запити* пікселів не фіксуються і не аналізуються.

– Відсутність політик і процедур щодо додавання трекінгових інструментів – відсутній процес оцінки впливу на приватність (PIA) перед впровадженням нового трекера.

– Недостатнє навчання персоналу щодо конфіденційності – маркетингова команда зосереджена на KPI, але не навчена розглядати приватність як важливий фактор.

– Невикористання технічних засобів захисту – таких як Content Security Policy (CSP) або сканери, що могли б попередити про підозрілі підключення.

– Збереження отриманих через пікселі даних у незахищеному вигляді – наприклад, якщо дані, зібрані маркетинговою командою, зберігаються на локальному сервері без шифрування і резервної копії, це робить їх легкою здобиччю у випадку інциденту.

Потенційні загрози та атаки: У Додатку Б наведено *матрицю загроз*, що показує взаємозв’язок між типами загроз, векторами атак через трекінгові пікселі та наслідками для безпеки даних.

У наведеній розроблені матриці видно, що загрози мають як технічний, так і правовий/етичний вимір. З одного боку – витоки даних, фішинг, хакерські прийоми, з іншого – порушення законів і довіри. Багато загроз тісно пов’язані: наприклад,

невідповідність політики може вилитись у судовий позов і штраф, а зовнішній витік через піксель – одночасно кіберінцидент і порушення закону про дані.

Оцінка ризиків. Ризик кожної загрози можна оцінити за двома параметрами: ймовірність та потенційний вплив. Наприклад, для середньостатистичного e-commerce сайту:

Неправомірний збір даних (через інтегровані пікселі соцмереж) – ймовірність висока (майже всі сайти їх мають), вплив середній (штрафи можливі, але низька ймовірність інциденту, якщо все робити по правилах).

Фішинг через email-піксель – ймовірність для конкретного сайту невисока (цілеспрямовано атакують не всіх), вплив може бути високим для окремих осіб (втрата даних).

Вбудовування зловмисного пікселя – ймовірність середня (залежить від захищеності сайту та використання зовнішніх скриптів), вплив високий (витік клієнтських даних, репутаційні втрати).

Накопичення даних без захисту – ймовірність, на жаль, часто висока (не всі середні компанії впроваджують шифрування), вплив дуже високий (витік мільйонів записів).

Невідповідність політики – ймовірність висока (багато хто недописує деталі), вплив зріс (як показує кейс із CCPA, можливі позови на великі суми).

Переслідування користувачів – ймовірність відносно низька для законослухняного бізнесу, але вплив етично негативний (втрата лояльності, відтік користувачів, якщо вони дізнаються про таке стеження).

Пониження продуктивності – ймовірність залежить від числа піксельних інтеграцій, вплив може бути помірний (повільніший сайт = менше конверсій).

Враховуючи оцінки, пріоритетними для захисту є загрози з високою ймовірністю та високим впливом: зокрема, несанкціонована передача чутливих даних, зловмисне вбудовування пікселя, а також комплаєнс-ризики, які можуть матеріалізуватися у вигляді штрафів. На щастя, багато з заходів захисту, про які піде

мова нижче, мають комплексний характер – тобто знижують ризик одразу декількох загроз.

Механізми виявлення загроз трекінгових пікселів. Важливою частиною моделі є розуміння того, як виявляти факт наявності або діяльності трекінгових пікселів, особливо якщо вони діють без дозволу. Основні напрямки:

Моніторинг мережевого трафіку: на рівні корпоративної мережі чи сервера можна відстежувати вихідні запити до зовнішніх доменів. Якщо, наприклад, помітно багато запитів на домени типу facebook.com або невідомі домени, це привід перевірити, що їх викликає. Спеціалісти з безпеки можуть налаштувати *SIEM* чи *DNS-логування*, які сигналізуватимуть про звернення до підозрілих URL (особливо з параметрами, що схожі на ідентифікатори). Наприклад, якщо з офісної мережі компанії йдуть GET-запити на attacker.com/track?uid=..., це повинно бути виявлено і розслідувано.

Аналіз коду та контенту сторінок: регулярний аудит веб-сторінок на предмет наявності <img> з дуже малими розмірами, прихованих <iframe>, підозрілих JavaScript-фрагментів. Це можна робити вручну або за допомогою сканерів безпеки/приватності. До прикладу, існують інструменти, що можуть автоматично сканувати сайт і видавати звіт про всі сторонні ресурси (скрипти, зображення) на кожній сторінці. Це дозволяє виявити “зайві” інтеграції. Також браузерні розширення на кшталт Ghostery, uBlock, NoScript можуть бути використані для тестування – вони часто показують список трекерів на сторінці.

Інструменти для кінцевих користувачів: є спеціальні утиліти, що прямо зазначають наявність пікселів у листах. Наприклад, розширення *Ugly Email* для Gmail позначає вхідні листи, які містять трекери, і може їх блокувати. З точки зору компанії, заохочення використання таких інструментів співробітниками може захистити від витоку інформації через, скажімо, прочитання конфіденційного листа із шпигунським пікселем.

Кореляція подій: якщо піксель спрацював, за ним може послідувати інша активність. Наприклад, у випадку фішингу – після відкриття листа і зливу даних може прийти більш таргетований лист. Аналітики безпеки повинні навчитися зв’язувати

такі події: *“лист X був відкритий, пішов запит на domainY, а через годину з цього domainY надійшов наступний лист”*. Це дає змогу зрозуміти, що domainY належить зловмисникам, і внести його до блокування.

Засоби захисту, вбудовані в клієнт: як вже згадано, сучасні email-сервіси (Apple) та браузери (Safari, Firefox) додають опції блокування трекерів. В корпоративному середовищі адмін може увімкнути відповідні налаштування політик, аби за замовчуванням вимикати завантаження віддалених зображень у пошті або накладати контент-фільтри на веб-трафік.

Оцінка і контроль постачальників: метод більш стратегічний – перевіряти усіх сторонніх постачальників скриптів/пікселів на відповідність політикам. Проводити *третьосторонній ризик-аналіз*: які скрипти запускаємо, що вони роблять з даними, які ризики несуть. Це виявляє потенційно небезпечних партнерів і дозволяє відмовитися від них або обмежити їх доступ.

Виявлення – це перший крок. Другий – реагування та усунення загрози: якщо знайдено неавторизований піксель, його негайно прибирають, проводять розслідування (як потрапив, які дані злив), повідомляють за потреби регулятора та суб’єктів (щоб виконати законні вимоги, як, наприклад, правило про повідомлення про витік даних). Якщо виявлено, що легітимний піксель збирає більше даних, ніж очікувалося, – наприклад, передає деталі форм, – теж вживаються заходи: переналаштування або відключення такого пікселя, переговори з постачальником про зміну конфігурації.

Таким чином, *ефективна модель протидії трекінговим загрозам* повинна включати постійний моніторинг, аудит, використання автоматизованих рішень (напр. системи типу Jscrambler Webpage Integrity, що відстежують активність скриптів на клієнтській стороні) і організаційні процеси перевірки/дозволу на впровадження нових трекерів. На цьому підґрунті далі сформульовано конкретні рекомендації щодо захисту.

3.2. Універсальна методика підвищення захисту персональних даних від трекінгових пікселів для малих та середніх організацій

Спираючись на принципи та рекомендації, розглянуті у розділі 1, було сформовано універсальну поетапну методику, яка допоможе організації комплексно підійти до захисту персональних даних при використанні трекінгових пікселів. Ця методика призначена для застосування в організаціях будь-якого типу – від державних установ до комерційних підприємств та онлайн-сервісів – і враховує як випадок, коли організація виступає контролером даних (власник сайту чи сервісу, що інтегрує пікселі), так і коли вона є обробником (наприклад, виконує розсилку з пікселем від імені іншого контролера).

Методика носить універсальний характер і може бути адаптована під конкретні потреби. Її ключова особливість – процесний підхід: передбачено послідовні етапи від планування і аудиту до впровадження технічних рішень і подальшого контролю. Також методика враховує *privacy by design*: впровадження захисту даних відбувається на архітектурному рівні системи, а не лише як додаток.

Нижче наведено основні етапи методики (таблиця 10), загальну архітектурну схему рішення (рис. 1) та опис робочого процесу захисту на кожному кроці (рис. 2). Окремо надано рекомендації щодо застосування цієї методики в популярних сценаріях (Google Analytics, Meta Pixel, email-маркетинг, мобільні додатки).

3.2.1. Етапи методики та їх зміст

Для систематизації підходу методика розбита на шість основних етапів. Додаток Г підсумовує ці етапи, їхню суть та ключові дії в рамках кожного.

Таблиця окреслює універсальний план дій. Звісно, для кожної організації деталі можуть різнитися: десь більше технічних заходів, десь акцент на юридичних нюансах. Але загалом ці 6 етапів охоплюють повний життєвий цикл впровадження захисту даних при використанні трекінгових пікселів – від виявлення проблем до сталого вдосконалення.

3.2.2 Архітектурна схема рішення

Для наочності розглянемо спрощену архітектурну схему (див. рисунок 3.1), яка відображає, як можуть бути інтегровані компоненти захисту даних навколо трекінгових пікселів. Нижче описано основні елементи такої схеми і їх взаємодію:

Користувач (браузер / пристрій) – відвідує веб-сайт або користується застосунком. При першому відвідуванні користувач бачить CMP Банер згоди, який є частиною фронтенду сайту.

Consent Management Platform (CMP) – відображає інтерфейс вибору згод, зберігає вибір користувача (наприклад, у cookie “consent=yes/no” або локальному сховищі) і має логіку керування скриптами. CMP взаємодіє з тегами пікселів: якщо користувач не погодився, CMP блокує виклики до зовнішніх трекерів. Після згоди – навпаки, запускає їх.

Веб-сервер/Додаток організації – бекенд, що генерує сторінки або відповіді. Він завантажує CMP і також може вбудовувати спеціальні посилання.

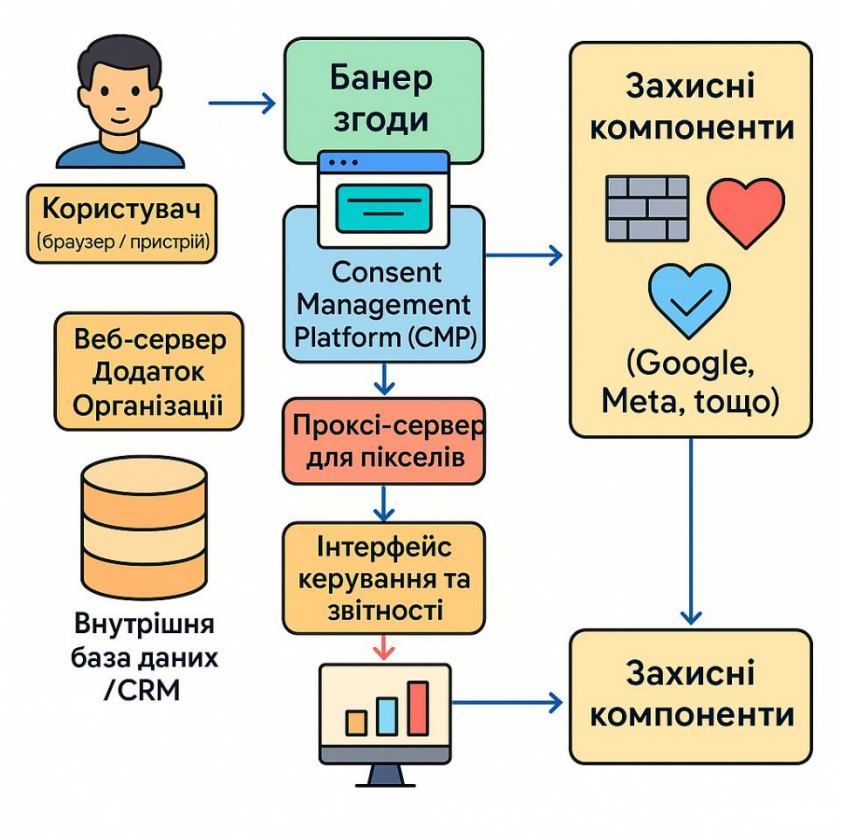

Рисунок 3.1 – Архітектурна схема інтеграції трекінгових пікселів з контролем приватності

Проксі-сервер для пікселів (опціонально) – розміщується в інфраструктурі організації (див. рисунок 3.1). Його роль – отримувати дані від браузерів замість прямих запитів до сторонніх серверів. Проксі може знаходитися під тим же доменом, що і сайт (щоб уникнути блокування).

Він приймає, наприклад, виклик https://analytics.mycompany.com/pixel?... замість Google-адреси, і вже на сервері пересилає на Google, попередньо відфільтрувавши або анонімізувавши дані (як IP). Проксі також може логувати мінімальну інформацію для контролю.

Сторонні сервери трекінгу (Google, Meta, тощо) – кінцеві точки, куди мають потрапити певні дані (за згодою користувача). В ідеалі, через проксі вони отримують лише необхідний набір (наприклад, знеособлений ID та подію “click”), і не бачать прямих ідентифікаторів користувача.

Внутрішня база даних / CRM – якщо організація зберігає частину трекінгової інформації (наприклад, історію дій авторизованого користувача, з’єднану з його

аккаунтом), то ця база теж включена в схему. Вона повинна бути підключена до механізму видалення (щоб, якщо користувач попросив, можна було знайти його дані і стерти).

Інтерфейси керування та звітності – це панелі для адміністраторів/DPO. Через них можна: переглянути журнал отриманих згод (для доказу), ініціювати пошук і видалення даних користувача (за запитом), налаштувати політику CMP (наприклад, додати новий категорію трекера). Також тут можна побачити зведення метрик (скільки % користувачів погодились і т.д.).

Захисні компоненти – до архітектури також належать: *Firewall/Web Application Firewall*, що захищає від зовнішніх атак; *бібліотеки шифрування*, задіяні для конфіденційності; *моніторингова система*, що перевіряє відправки даних.

У підсумку, архітектура будується за принципом *“вбудованого захисту”*: між користувачем і зовнішніми трекерами стоять наші контролюючі компоненти (CMP на фронтенді і, опціонально, проксі на бекенді). За лаштунками все пов’язано з внутрішніми системами управління даними і безпекою. Це ілюструє реалізацію Privacy by Design: захист “вбудований” у сам процес відправлення трекінгових даних.

3.2.3. Проксі-сервер із фільтрацією запитів до зовнішніх піксельних трекерів

Впровадження корпоративного або локального HTTP(S) проксі-сервера, який аналізує та блокує запити до доменів трекінгових систем (наприклад, facebook.com/tr, google-analytics.com/collect, tiktok.com/pixel, тощо). Проксі-сервер застосовує список дозволених і заборонених доменів, фільтрує запити за User-Agent, Referer і Content-Type, і перешкоджає витоку ідентифікаторів користувачів та cookies.

Проксі-сервер із фільтрацією запитів до зовнішніх трекінгових систем — це проміжна ланка між пристроєм користувача та зовнішнім інтернетом, яка забезпечує контроль над тим, які саме запити надсилаються з браузера або застосунку до сторонніх аналітичних сервісів (див. рисунок 3.2). Його головна мета — запобігти

передачі ідентифікаторів, cookies та інших персональних даних до трекінгових платформ (таких як Google Analytics, Facebook Pixel, TikTok Pixel тощо) без згоди користувача або поза політикою приватності організації.

Такий проксі-сервер працює як центральна точка перевірки всіх вихідних HTTP(S) запитів. Він розміщується у внутрішній мережі компанії або в хмарному середовищі, через яке проходить увесь трафік користувачів. Проксі аналізує кожен запит на основі кількох параметрів — наприклад, адреси призначення (домену), типу запиту (методу), заголовків (User-Agent, Referer, Content-Type), а також вмісту самого запиту, якщо він не зашифрований. Якщо запит відповідає критеріям для блокування — наприклад, якщо він спрямований до відомого трекера або містить заборонені типи даних — проксі або повністю зупиняє його, або змінює вміст, наприклад, підмінюючи IP-адресу на анонімізовану, видаляючи cookies чи видаляючи заголовки, що дозволяють сторонньому сервісу відстежити користувача.

У випадках, коли йдеться про HTTPS-з'єднання, проксі може бути налаштований на розшифрування зашифрованого трафіку за допомогою SSL-інспекції. Це потребує встановлення довіреного сертифіката у браузерах або пристроях користувачів, але дозволяє повністю бачити вміст шифрованих запитів і застосовувати ті самі правила фільтрації, що й до звичайного HTTP.

Особливістю цього підходу є його повна прозорість для кінцевого користувача. Йому не потрібно змінювати налаштування браузера, встановлювати розширення чи вручну контролювати трекери — усе здійснюється автоматично на рівні мережевої інфраструктури. Це також дозволяє компанії централізовано керувати політиками фільтрації, оновлювати списки заборонених трекерів, а також забезпечувати аудит доступу до даних — наприклад, логувати всі запити, які були заблоковані або пропущені, і проводити аналіз у разі інцидентів.

Крім того, проксі-сервер може бути інтегрований із внутрішніми системами безпеки та управління ризиками, такими як SIEM або DLP, і виступати частиною загальної архітектури захисту персональних даних. Таким чином, він не лише блокує небажані трекінгові запити, а й дозволяє організації дотримуватись принципів GDPR

(зокрема статей 25 і 32 — Privacy by Design і Security of Processing), забезпечуючи технічні та організаційні заходи для захисту приватності користувачів.

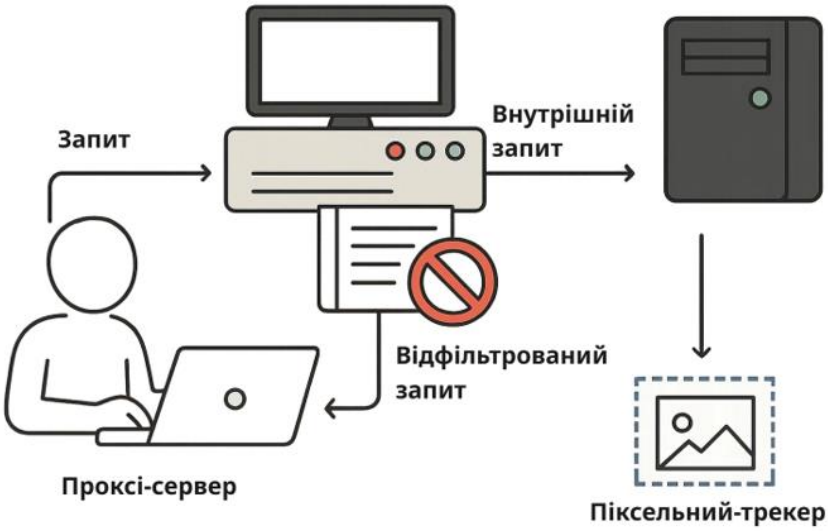

Рисунок 3.2 – Проксі-сервер із фільтрацією запитів до зовнішніх піксельних трекерів

Загалом, фільтраційний проксі є ефективним інструментом контролю за цифровими слідами користувачів, особливо у великих організаціях або системах з підвищеними вимогами до конфіденційності, таких як медичні установи, державні сервіси або корпоративні інфраструктури.

3.2.4. Інтеграція Privacy Gateway + Тег-менеджера з інструментами маскування

У межах реалізації підходу «Privacy by Design» усе більше організацій переходять від прямого збору і передачі користувацьких даних до моделі з використанням Privacy Gateway — проміжного серверного компонента, що поєднується із системою керування тегами (Tag Management System, TMS), як-от Google Tag Manager або Matomo Tag Manager, а також із технологіями маскування, хешування та псевдонімізації даних (див. рисунок 3.3).

Принцип дії такої інтеграції полягає у наступному. На фронтенді вебсайту користувач взаємодіє із сторінкою, а вбудовані в неї скрипти тег-менеджера відстежують події — наприклад, перегляд сторінки, клік на кнопку, додавання товару

до кошика. У звичайному сценарії ці події надсилаються безпосередньо до аналітичних або маркетингових сервісів. Проте в запропонованій архітектурі передача даних відбувається не напряму, а через Privacy Gateway — спеціалізований сервер, розгорнутий на боці компанії або в ізольованому хмарному середовищі.

Перед тим як дані надсилаються із тег-менеджера до Privacy Gateway, відбувається первинна фільтрація відповідно до політики згоди користувача, отриманої через CMP (Consent Management Platform). Тільки якщо користувач дав згоду на аналітичні або маркетингові трекери, дані переходять на наступний рівень обробки.

У межах Privacy Gateway діє механізм маскування (data masking) або хешування (hashing). Наприклад, унікальні ідентифікатори користувача (таких як user_id, client_id, session_id, email) перетворюються або на псевдоніми, або на односторонні хеші (наприклад, з використанням SHA-256 + salt). Усі IP-адреси або геолокаційні дані обрізаються до рівня країни або регіону, а cookie ID — або видаляються, або підмінюються випадковими, неприв'язаними до реальної особи значеннями. Завдяки цьому сторонні сервіси отримують лише технічно необхідну статистику — наприклад, кількість переглядів, послідовність кліків чи конверсії — без будь-яких елементів, які дозволили б ідентифікувати конкретного користувача.

Перевагою такої моделі є також гнучка архітектура керування даними: конфігурація Gateway може містити окремі правила обробки для кожного типу тегів — аналітичних, маркетингових, функціональних, або спеціальних (наприклад, для A/B-тестування).

Це дозволяє відповідно до GDPR дотримуватися принципу data minimization (мінімізації обробки) та обмежувати передачу даних тільки тим, що необхідно для визначеної мети.

Крім того, у разі використання серверного тег-менеджера (наприклад, Google Tag Manager Server-Side) компанія отримує можливість повного логування запитів, аудиту подій, налаштування TTL збереження даних, та автоматичного видалення або обмеження доступу до них.

Рисунок 3.3 – Інтеграція Privacy Gateway + Тег-менеджера з інструментами маскування

Таким чином, інтеграція Privacy Gateway із тег-менеджером та механізмами маскування створює повноцінний технологічний шар захисту приватності, вбудований у саму логіку збору і передачі даних. Це не лише відповідає статтям 5, 25 та 32 Регламенту GDPR, але й суттєво знижує ризики витоку або несанкціонованого аналізу персональних даних у випадку компрометації зовнішніх сервісів. Водночас така модель зберігає цінність аналітики для бізнесу, не порушуючи прав користувачів на конфіденційність.

3.3. Механізми захисту від витоку персональних даних через трекінгові пікселі

Трекінговий піксель – це прозоре зображення розміром часто 1×1 піксел, вбудоване у HTML-код листа чи сторінки. При завантаженні такої картинки браузер чи поштова програма робить запит до сервера (зазвичай стороннього) і таким чином передає йому інформацію про користувача. Це можуть бути IP-адреса, тип та версія браузера/ПЗ, операційна система, розмір екрану, реферер тощо.

Тобто один трекінговий піксель може передати безліч персональних даних. При цьому такі пікселі зазвичай повністю невидимі (скриті у коді, 1×1 px) і їх неможливо «побачити» при звичайному перегляді повідомлення або сторінки. Завдання – автоматизовано виявити й нейтралізувати такі пікселі до того, як вони збиратимуть дані.

Нижче запропоновано два інноваційні методи: один для перехоплення у вхідних листах, другий – при завантаженні веб-сторінок. Обидва підходи можуть бути реалізовані на стороні користувача (наприклад, у поштовому клієнті або браузері) або на стороні адміністратора (поштовому сервері чи проксі).

3.3.1. Фільтрація трекерів у вхідних email

Цей метод працює за принципом аналізу та зміни HTML-коду вхідного повідомлення (у клієнті або на сервері).

Схема отримує HTML-повідомлення (наприклад, через IMAP чи SMTP-фільтр) і виконує його парсинг. Далі перевіряються всі вбудовані елементи <img> та інші потенційні трекери. Для виявлення пікселів використовуються такі критерії:

Розмір зображення 1×1 або дуже малий (ширина чи висота ≤1).

URL-адреса зовнішнього ресурсу (img src з домену, відмінного від відправника), часто з унікальними параметрами запиту.

Відомі домени трекерів або підозрілі ключові слова у URL (наприклад, track, pixel, mail, analytics тощо).

Білі списки/чорні списки джерел. Можна використовувати публічні фільтри (як-от списки трекерів з uBlock Origin) або корпоративні бази.

На додачу до простих правил пропонується навчальний блок (машинне навчання) або статистичний аналіз. Система може збирати ознаки кожного зображення (розмір, метадані, структура URL, час завантаження) і застосовувати класифікацію. Наприклад, використовувати модель ML, навчену на відомих трекерах, щоб виявляти схожі нові патерни.

Така модель (див. рисунок 3.4) буде стійкою до маніпуляцій (наприклад, заміни розміру чи назви) та зменшить хибні спрацьовування. Крім того, можливе впровадження «проксі-завантажувача» всіх картинок: система могла б попередньо завантажити зображення через власний сервер з «загальним IP», як це робить Proton Mail, щоб перевірити, чи викликає завантаження зовнішній запит із ідентифікацією.

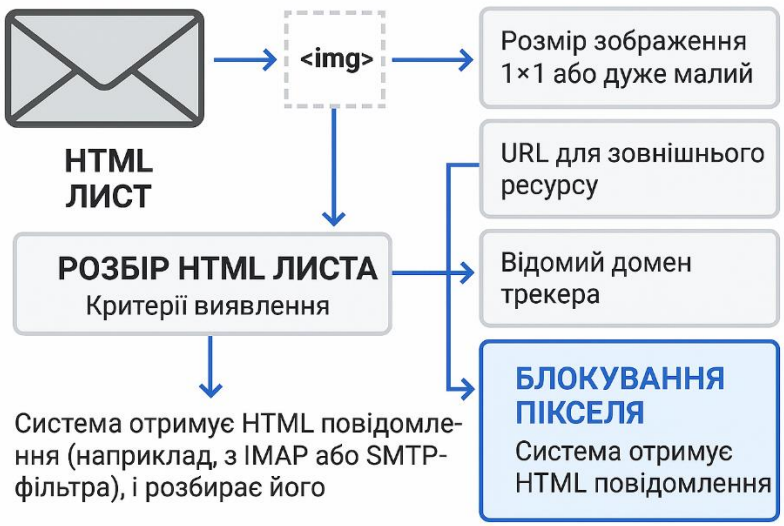

Рисунок 3.4 – Ілюстрація виявлення та блокування трекінгового пікселя у HTML-листі

Якщо виявлено трекер, посилання замінюється на порожній або локальний піксель. Таким чином закладається клієнтська анонімізація (приховування реальних даних) та блокування самого трекера.

Кроки фільтрації (приклад):

1. Отримання та парсинг повідомлення: витягнути HTML-текст з листа.

2. Аналіз зображень: для кожного тегу <img> перевірити атрибути width/height і src.

3. Виявлення трекерів: якщо зображення має розмір 1×1 або домен не належить довіреному відправнику – позначити як потенційно шкідливе. Також перевірити URL по чорному списку трекерів.

4. Нейтралізація: видалити або замінити <img>-тег трекера (наприклад, на локальний пустий піксель або просто видалити тег).

5. Логування та сповіщення: зберегти інформацію про заблоковані трекери і, за потреби, показати користувачу повідомлення про їх наявність.

```
from bs4 import BeautifulSoup

html_content = get_email_html()  # Отримуємо HTML текст листа
soup = BeautifulSoup(html_content, 'lxml')
for img in soup.find_all('img'):
    # Отримуємо розміри (якщо вказані) та URL зображення
    width = int(img.get('width', 0))
    height = int(img.get('height', 0))
    src = img.get('src', '')
    # Простий критерій: якщо зображення мікроскопічне або URL підозрілий – видаляємо
    if (width <= 1 and height <= 1) or is_known_tracker(src):
        img.decompose()  # Видалення тега з DOM
# Повертаємо відфільтрований HTML-лист
clean_html = str(soup)
deliver_email(clean_html)
<div id="k"></div>
```

Рисунок 3.5 – Python-код для автоматичного видалення мікропікселів із HTML-листа

На рисунку 3.5 функція is_known_tracker(src) може перевіряти наявність домену у чорному списку або збіг з регулярними виразами, характерними для трекерів. При бажанні її можна замінити на виклик ML-моделі, що класифікує URL за ознаками.

Метод 1 можна реалізувати як плагін у поштовому клієнті (наприклад, у Thunderbird через API), так і як серверний фільтр (наприклад, Python-модуль у поштовому проксі або MTA). Він автоматично виявляє та блокує 1×1-пікселі у вхідних листах, що ефективно запобігає відправці особистих даних трекерам.

Принцип роботи: при завантаженні веб-сторінки (усередині браузера чи на сервері-видавачі) система перехоплює HTML-код і фільтрує його. Це може бути

реалізовано як проміжне програмне забезпечення (middleware) у веб-фреймворку або як браузерне розширення. Суть – проглянути всі вставлені картинки (<img>, CSS-фони, навіть iframe) та виявити серед них трекінгові пікселі, застосовуючи аналогічні критерії (розмір, відмінний домен, підозрілі параметри).

3.3.2. Інтерцепція трекерів при завантаженні сторінок

Крім звичайного видалення картинок, пропонується проксирування контенту (див. рисунок 3.6). Унікальна ідея – замість повного блокування картинок взагалі (що порушує вигляд сторінки), маршрутизувати усі зовнішні ресурси через безпечний проксі-сервер. Наприклад, для кожного <img src="http://tracker.example.com/pixel?id=123"> підставляти <img src="/proxy?url=http://tracker.example.com/pixel?id=123">. Тоді сервер проксі завантажує контент від імені користувача: він може маскувати IP (як робить ProtonMail) і фільтрувати запит. Якщо виявлено, що URL – це трекер, проксі просто поверне пустий респонс або прозоре зображення, не дозволивши передачі даних. Такий підхід дає повний контроль над всіма зображеннями, а також дозволяє централізовано оновлювати правила (якщо з’явилися нові схеми трекерів).

Рисунок 3.6 – Схема роботи системи трекінгу

Кроки роботи рішення (наприклад, Middleware):

Перехоплення відповіді сервера: у функції after_request (Flask/Django) чи аналогі у веб-сервері отримати HTML-контент перед відправкою.

Парсинг HTML: знайти всі теги <img>, CSS-фони, посилання на зовнішні зображення.

Виявлення трекерів: як і в першому методі – перевірити атрибути width/height, домен і URL. Можна також аналізувати параметри запиту (наприклад, багато трекерів додають у URL унікальні ідентифікатори).

Проксірування або видалення: для безпечних зображень (локальних або безпечних сервісів) залишати посилання неторканими. Для підозрілих – замінювати на внутрішній шлях проксі, що блокує запит.

Оновлення правил: система може автоматично підвантажувати чорні списки трекерів або аналітичні сигнатури (наприклад, з відкритих фільтрів uBlock) для актуальності.

```python
from bs4 import BeautifulSoup
from flask import Flask, request, Response
import requests
from urllib.parse import quote, urlparse

app = Flask(__name__)

@app.after_request
def filter_tracking_pixels(response):
    # Обробляємо тільки HTML-сторінки
    if response.content_type == 'text/html':
        html = response.get_data(as_text=True)
        soup = BeautifulSoup(html, 'lxml')
        for img in soup.find_all('img'):
            src = img.get('src', '')
            # Якщо це абсолютна адреса і не на нашому домені
            if src.startswith('http'):
                # Простий детектор трекера
                if is_tracking(src):
                    # Замінюємо на локальний прозорий pixel (або видаляємо)
                    img['src'] = '/proxy?url=' + quote(src, safe='')
                # Інакше – перевести через проксі для анонімізації
                else:
                    img['src'] = '/proxy?url=' + quote(src, safe='')
```

Рисунок 3.7 – Flask-хук для перехоплення HTML-відповідей і фільтрації зовнішніх трекінг-пікселів через проксі

На рисунках 3.7-3.8 всі зовнішні зображення переправляються через маршрут /proxy?url=.... Якщо функція is_tracking(target) повертає True (за критеріями трекера), проксі повертає порожню відповідь – і відвідувач не передає жодних даних трекеру.

Якщо ж ресурс безпечний, проксі-клієнт (сервер) отримує картинку та віддає її користувачу, при цьому оригінальний трекер бачить лише IP проксі, а не користувача (анонімізація). Такий підхід можна реалізувати як на стороні сайта (власне сайти почнуть служити проксі для зовнішніх ресурсів), так і в локальному проксі (наприклад, розширення браузера, яке змінює всі src на локальні).

3.4. Рекомендації щодо виявлення та нейтралізації загроз длля малих та середніх організацій

3.4.1. Забезпечення принципів GDPR при використанні трекінгових пікселів

GDPR встановлює сім базових принципів обробки персональних даних (ст.5 GDPR): законність, справедливість і прозорість; обмеження цілей; мінімізація даних; точність; обмеження зберігання; цілісність і конфіденційність; а також принцип «accountability» (підзвітності), який покладає на контролера відповідальність за дотримання решти принципів. У контексті трекінгових пікселів кожен з цих принципів набуває практичного вираження у вигляді конкретних вимог та контрольних заходів. Нижче наводяться детальні рекомендації щодо виконання кожного принципу при зборі та використанні даних за допомогою пікселів. Для наочності рекомендації згруповані у таблиці за відповідними категоріями контролю.

3.4.2. Законність і прозорість

Законність означає, що будь-яка обробка персональних даних повинна здійснюватися на законних підставах, визначених ст.6 GDPR (наприклад, за згодою

суб’єкта або на основі легітимного інтересу), та не порушувати інших норм права. Прозорість вимагає від контролера відкритості й чесності перед суб’єктом даних: людина має точно знати, які її дані збираються, як, з якою метою і ким вони обробляються. У випадку трекінгових пікселів принципи законності і прозорості тісно пов’язані, адже збір даних відбувається приховано. Тому ключовим завданням є отримати явну інформовану згоду користувача на таке відстеження та належно поінформувати його про всі аспекти обробки.

Рекомендації: На практиці забезпечення законності та прозорості при використанні пікселів включає реалізацію прозорих повідомлень для користувачів і впровадження механізму згоди до активації пікселя. В Додатку Б наведено конкретні кроки та заходи.

Як видно з наведеного, законність реалізується переважно через механізм явної згоди (або іншу належну правову підставу), а прозорість – через належне інформування. У результаті користувач отримує можливість зробити свідомий вибір, а організація – виконати вимоги GDPR щодо чесної та відкритої обробки даних. Важливо зауважити, що у деяких випадках власники сайтів намагалися обґрунтовувати використання аналітичних пікселів на основі *легітимного інтересу*. Однак регулятори ЄС (і Європейська рада з захисту даних) займають позицію, що будь-яке нестатистичне відстеження поведінки в онлайні, яке не є строго необхідним, вимагає згоди згідно з ePrivacy та GDPR. Тому рекомендація – отримувати саме явну згоду у більшості сценаріїв використання трекінгових пікселів.

3.4.3. Обмеження цілей

Принцип обмеження цілей (purpose limitation) передбачає, що персональні дані повинні збиратися визначеними, чіткими і законними цілями та не оброблятися надалі несумісним з ними способом. Практично це означає: перед тим як впровадити трекінговий піксель, організація повинна точно визначити і задокументувати мету його використання (наприклад, “відстеження конверсій реклами для оптимізації

маркетингової кампанії” або “зібрання статистики відвідувань сайту для поліпшення UX”). Заборонено використовувати дані, зібрані пікселем, для будь-яких інших цілей, не сумісних з початковою, без отримання нової згоди від суб’єкта.

Рекомендації: Для дотримання принципу обмеження цілей слід впровадити внутрішні процедури контролю за тим, з якою метою збираються дані трекінговими пікселями і як вони використовуються надалі. Таблиця 3.1 містить рекомендації щодо цього аспекту.

Таблиця 3.1.

Рекомендації для забезпечення обмеження цілей обробки

Рекомендований захід	Пояснення щодо реалізації принципу цільового обмеження
Чітко визначити та задокументувати мету збору даних кожним пікселем.	Перед запуском трекінгового пікселя опишіть його призначення: які показники він збирає і для чого (вимірювання конверсій, аналітика користувацької поведінки, ремаркетинг тощо). Це слід відобразити у внутрішніх документах (реєстрі обробки даних) і в зовнішніх політиках для користувачів. Наявність чітко сформульованої мети відповідає вимозі GDPR збирати дані для *«встановлених, явних і законних цілей»*, а також запобігає «зайвому» використанню даних.
Застосувати механізм зв'язування згоди з конкретною метою.	Якщо один і той самий сайт використовує кілька видів трекінгових пікселів для різних потреб (напр., один – для аналітики, інший – для реклами), у банері згоди варто надати користувачу окремі опції: наприклад, "Я погоджуюся на аналітичні cookies/pixel" і "Я погоджуюся на рекламні трекери". Це забезпечує *специфічність* згоди під кожну ціль та відповідає вимозі, щоб згода була "конкретною" (specific). Користувач може погодитися на одне і відмовитись від іншого, що гарантує обмеження використання даних лише заявленими цілями.
Не використовувати дані пікселів для нових цілей без повторної згоди.	Зібрані за допомогою пікселя дані не можна просто брати і застосовувати для будь-яких інших задач, не сумісних з початковою метою. Наприклад, якщо піксель збирав email-адреси для розсилки повідомлень про статус замовлення, компанія не має права без окремої згоди

Продовження Таблиці 3.1.

	використовувати ці адреси для маркетингових розсилок. У разі потреби змінити мету – необхідно або *анонімізувати* дані (щоб вони перестали бути персональними) або запитати у суб'єкта нову згоду на нову мету. Це запобігає «функціональному зсуву» (function creep) – непередбаченому розширенню використання даних поза межами первинних цілей.
Обмежити доступ до даних відповідно до цілей.	Практичний спосіб підтримувати цільове обмеження – це розмежувати доступ до даних, зібраних пікселями, між підрозділами компанії. Наприклад, дані веб-аналітики (поведінкові патерни) доступні лише відділу, що займається UX/UI чи маркетингом, і не передаються іншим, хто не має чіткої потреби. Так само інформація з маркетингових пікселів (конверсії реклам) не повинна використовуватися, скажімо, HR-відділом. Це організаційна міра, що гарантує: кожен використовує дані тільки за призначенням, відповідно до визначеної мети збору.
Регулярно перевіряти сумісність обробки з заявленою метою.	Під час аудитів приватності або перегляду налаштувань трекінгових пікселів варто оцінювати: чи не використовується деінде випадково (або навмисно) інформація, зібрана пікселем, для інших цілей. Якщо виявлено нові способи застосування даних – перевірити їхню законність, сумісність з початковою метою або отримати окрему згоду. Такий контроль допомагає підтримувати принцип обмеження цілей на постійній основі.

Дотримання принципу обмеження цілей дозволяє уникнути ситуацій, коли персональні дані, зібрані під одним приводом, починають використовуватися у зовсім іншому руслі, що могло б порушити довіру користувачів і вимоги GDPR. Наприклад, якщо сайт декларує, що піксель збирає дані *"для поліпшення роботи сайту"*, а сам потім передає ці дані партнерській рекламній мережі – це було б порушенням принципу цільового обмеження та прозорості. Тому організація повинна забезпечити чіткий зв'язок "мета – дані – згода", задокументувати його і дотримуватися його надалі.

3.4.4. Мінімізація даних

Принцип мінімізації даних означає, що слід збирати і обробляти тільки ті персональні дані, які дійсно необхідні для досягнення заявленої мети, і не більше. Стосовно трекінгових пікселів цей принцип можна сформулювати як вимогу: *збирати найменший обсяг інформації про користувача, достатній для цілей відстеження*. На практиці трекери часто "навішують" багато зайвих параметрів (наприклад, повний IP-адрес, детальний цифровий відбиток пристрою тощо), хоча для агрегованої аналітики це не конче потрібно. З точки зору GDPR, зайві дані підвищують ризики для приватності і тому їх збір невиправданий.

Рекомендації: Для забезпечення мінімізації слід налаштувати трекінгові пікселі та суміжні інструменти таким чином, щоб обмежити обсяг зібраних даних. У табл.3.2 наведено заходи, які сприяють виконанню цього принципу.

Таблиця 3.2

Рекомендації для забезпечення мінімізації даних

Рекомендований захід	Деталі реалізації та виправдання мінімізації
Вимкнути збір непотрібних даних у налаштуваннях пікселя.	Багато популярних піксельних сервісів надають опції конфігурації, які слід використати для зниження обсягу збираних даних. Наприклад, у Google Analytics передбачено функцію анонімізації IP-адрес – її треба увімкнути, аби не зберігати повний IP користувача (останній октет обнуляється). Так само у Facebook Pixel (Meta Pixel) можна обмежити автоматичний збір детальної інформації про користувача, якщо вона не потрібна. Встановивши відповідні прапорці або параметри API, контролер гарантує, що піксель працює “у щадному режимі”, збираючи тільки те, що потрібне для заявленої мети.
Не збирати чутливі дані через пікселі.	Категорично не рекомендується передавати трекінговим пікселям будь-які спеціальні категорії даних (ст.9 GDPR) – такі як інформація про здоров’я, релігійні переконання, тощо. Також слід уникати в URL сторінок, де розміщено піксель, параметрів, що містять персональні дані (наприклад, email або ім’я в відкритому вигляді). Були випадки, коли медичні веб-сайти мали пікселі, що надсилали інформацію про відвідувача і переглянуті ним симптоми третім сторонам – це грубе порушення приватності.

Продовження Таблиці 3.2

Обмежити кількість сторонніх трекерів до необхідного мінімуму.	Мінімізація стосується не лише полів даних, а й кількості самих пікселів. Рекомендується провести аудит і “причесати” свій сайт: вилучити всі трекери, які не приносять суттєвої користі або дублюють функції одне одного. Наприклад, якщо організація користується Google Analytics, можливо, їй не потрібен додатковий піксель Yandex Metrica чи іншої системи одночасно. Менше пікселів = менше точок збору даних = нижчі ризики. В таблиці 4.4 Lockton прямо радить: *“Проредіть зайві трекери, переконайтесь, що всі вони мають необхідну мету”*.
Використовувати агреговані дані замість персоналізованих, де можливо.	Піксельні служби іноді дозволяють задавати рівень деталізації даних. Наприклад, у аналітичних звітах можна знеособити окремих користувачів і дивитись тільки агрегати (кількість відвідувачів на день, конверсії тощо). Якщо є можливість *не отримувати персональних профайлів*, слід налаштувати саме такий режим. Крім того, варто очищати дані після збору: видаляти полішники (точні мітки часу, детальні ідентифікатори), залишаючи тільки те, що необхідно для аналітики. Це перетворює деякі дані на неперсональні і знижує ризики витоку приватної інформації.
Реалізувати server-side proxy для посередництва в зборі даних.	Сучасним підходом до мінімізації (та до захисту в цілому) є використання проксі-сервера між користувачем і стороннім трекером. Замість того, щоб браузер користувача напряму звертався до Facebook чи Google, запит на піксель надходить

Продовження Таблиці 3.2.

спершу на сервер контролера, де можна “відфільтрувати” дані: напр., відкинути або замінити останні цифри IP, видалити або захешувати ідентифікатор користувача. Лише після цього сервер контролера передає інформацію далі сторонньому сервісу. Таким чином організація контролює, що *мінімум даних* покидає її периметр. Цей метод складніший у реалізації, проте значно підвищує відповідність принципу мінімізації та конфіденційності за замовчуванням.

Принцип мінімізації, втілений на практиці, не тільки знижує ризики порушення GDPR, а й зменшує можливий збиток у разі витоку чи неправомірного доступу до даних. Адже якщо з самого початку збирати менше – то й розкрити можна менше. Особливо це стосується технічних і організаційних заходів, таких як регулярний аудит трекерів: компанія повинна періодично переглядати перелік активних пікселів і відключати все зайве. Як вказує практика, з часом у коді сайтів накопичуються скрипти і пікселі, що вже не використовуються чи встановлені “про запас” – їх потрібно видаляти. Мінімізація – це процес постійний, а не одноразова дія.

3.4.5. Точність

Точність (accuracy) – принцип GDPR, що вимагає підтримувати персональні дані в актуальному і точному стані; у разі неточностей – виправляти або видаляти їх. На перший погляд, застосування цього принципу до трекінгових пікселів не таке очевидне, адже пікселі зазвичай збирають *автоматичні дані* (время відкриття листа, кліки, технічні параметри) і не завжди прив’язують їх до імені чи профілю користувача. Проте, якщо компанія агрегує з пікселів якусь інформацію про користувача (наприклад, історію його покупок чи реакцію на розсилки) – ця інформація має бути точною і оновлюватися при потребі.

Рекомендації: Забезпечити точність даних, зібраних через пікселі, можна шляхом коректного з’єднання їх з основними даними користувача та надання самому користувачу механізмів коригування або принаймні видалення таких даних. Таблиця 3.3 пропонує кроки для виконання принципу точності.

Таблиця 3.3

Рекомендації для забезпечення точності даних

Рекомендований захід	Як це сприяє точності даних
Зв’язати трекінгові дані з відповідним користувачем (за потреби).	Якщо бізнес-логіка передбачає, що дані від пікселя асоціюються з конкретним користувачем (наприклад, email-розсилка: відкриття листа записується в профіль адресата в CRM), важливо забезпечити правильне співставлення. Помилки у відповідності “дані – особа” призводять до неточностей. Наприклад, якщо трекінг кліків прив’язався до неправильного користувача через схожий ідентифікатор – це порушення точності. Тому системи повинні однозначно і коректно ідентифікувати суб’єкта даних, використовуючи унікальні ключі (email, ID) без колізій.
Надавати користувачу спосіб виправити або оновити свої дані.	Хоча безпосередньо “виправити” дані трекінгу (такі як час відкриття листа) користувач не може, він може впливати на пов’язані дані. Наприклад, якщо система профілює інтереси користувача на основі його кліків по пікселю, то користувач повинен мати змогу змінити налаштування інтересів чи відмовитися від профілювання. Крім того, якщо трекінгові дані виявилися помилковими (скажімо, помилково зарахувалося, що користувач здійснив дію, якої не було), компанія на запит повинна скоригувати або видалити такі записи. GDPR

	гарантує суб’єктам право на виправлення неточних даних, тож процеси повинні це враховувати.

Продовження Таблиці 3.3

Використовувати актуальні довідники і геобази.	Деякі дані, що отримуються пікселем, опосередковано залежать від зовнішніх довідників – наприклад, визначення геолокації за IP-адресою або ідентифікація браузера/пристрою. Щоб ця інформація була точною, потрібно регулярно оновлювати відповідні бази (географічні бази IP, списки агентів браузера тощо). Інакше система може приписувати користувача до невірного міста (неточна геолокація) або плутати тип пристрою, що порушуватиме принцип точності в контексті аналітичних висновків.
Автоматично видаляти або архівувати застарілі трекінгові дані.	Дані, зібрані пікселями, з часом можуть втрачати актуальність. Наприклад, історія кліків річної давнини може більше не відповідати поточним уподобанням користувача. Якщо ці застарілі дані продовжують використовуватись, висновки можуть бути неточними. Тому рекомендується через певний період архівувати або анонімізувати старі трекінгові записи (скажімо, старші 1–2 років), залишаючи в оперативній базі тільки актуальну інформацію. Таким чином підтримується “свіжість” даних, що підлягають обробці та аналізу.
Верифікувати та очищати дані, отримані від третіх сторін.	Якщо організація отримує результати трекінгу від зовнішнього партнера (наприклад, звіти від рекламної мережі про конверсії за пікселем), варто проводити верифікацію даних: чи немає дублікатів, аномалій, помилок. Будь-які виявлені неточності (наприклад, неправдоподібно багато кліків від одного користувача за нереальний проміжок часу) слід

	уточнювати або фільтрувати. Це елемент контролю якості даних, що забезпечує більш високу точність аналітики і відповідність принципу точності GDPR.

У контексті GDPR точність часто розглядається стосовно персональних даних, що явно ідентифікують особу (ім’я, адреса, контактна інформація). Однак і поведінкові дані, зібрані через пікселі, можуть впливати на користувача (скажімо, якщо на їх основі йому показуються певні рекламні пропозиції або приймаються рішення). Тому важливо, щоб ці дані були настільки точними, наскільки це практично можливо. Наприклад, якщо алгоритм рекомендацій помилково відніс користувача до неправильної категорії – це неточність, яку слід виправляти.

Організація повинна бути готовою реалізувати право суб’єкта на виправлення або видалення його даних, отриманих в результаті трекінгу. Хоча може бути складно видалити точково всі сліди відстеження (особливо якщо дані анонімні), мінімум – це припинити подальший збір (відключити піксель для конкретного користувача) та знищити раніше зібрані ідентифіковані дані на запит.

3.4.6. Обмеження зберігання

Згідно з принципом обмеження строку зберігання (storage limitation), персональні дані повинні зберігатися у формі, що дозволяє ідентифікацію суб’єктів, не довше, ніж це необхідно для зазначених цілей обробки. Іншими словами, GDPR вимагає видаляти або анонімізувати персональні дані, щойно відпала потреба у їх ідентифікації. Для трекінгових пікселів цей принцип означає, що організація не повинна зберігати зібрані через пікселі дані нескінченно довго “про всяк випадок”. Натомість слід визначити обґрунтовані періоди зберігання (наприклад, 14 місяців для аналітичних даних) і по закінченні цього терміну дані автоматично очищуються.

Рекомендації: Забезпечення обмеження строків зберігання включає як політичні рішення (визначення строків у політиці компанії), так і технічні налаштування (конфігурування автоматичного видалення даних). Основні кроки наведено у таблиці 3.4.

Таблиця 3.4

Рекомендації для забезпечення обмеження строку зберігання даних

Рекомендований захід	Застосування та наслідки
Встановити чіткий період зберігання даних, зібраних пікселем.	Проаналізуйте, скільки часу вам дійсно потрібні трекінгові дані для досягнення мети. Наприклад, для веб-аналітики часто досить мати дані за останні 12–24 місяці для річного порівняння. Встановіть політику: дані пікселя зберігаються не довше N місяців, після чого видаляються або агрегуються. Важливо прописати це як у внутрішніх процедурах, так і в зовнішній політиці конфіденційності (щоб виконати прозорість).
Налаштувати автоматичне видалення/анонімізацію у службах аналітики.	Більшість аналітичних платформ мають опції data retention. У Google Analytics 4, наприклад, можна обрати максимальний строк зберігання даних користувача – 14 місяців (за замовчуванням). У Universal Analytics раніше можна було задавати від 14 місяців до “не обмежувати” – звісно, слід обирати не безстрокове зберігання, а мінімально необхідне (наприклад, 14 місяців). У налаштуваннях також варто вимкнути опцію “reset on new activity” (щоб кожен новий візит не продовжував нескінченно життя користувацького ідентифікатора). Таким чином сервіс самостійно буде стирати старі записи, забезпечуючи виконання політики зберігання.

Продовження Таблиці 3.4

Передбачити різні строки для різних категорій даних.	Не всі дані однаково цінні однаково довго. Наприклад, детальні логи відвідувань зі зв'язкою до cookie ID можуть бути потрібні лише кілька місяців, а агреговані звіти (без ідентифікації особи) можна зберігати довше, бо вони вже не містять персональних даних. Тому в рамках методики зберігання даних слід класифікувати: персонально ідентифікуючі дані трекінгу – видаляти раніше (або деперсоналізувати), а загальну статистику – можна архівувати на довший термін. Це узгоджується з GDPR, який дозволяє довше зберігати дані для архівних, наукових чи статистичних цілей за умови належних заходів безпеки.
Забезпечити видалення даних на вимогу користувача.	Якщо суб'єкт даних реалізує своє право на видалення (право бути забутим), контролер повинен видалити і дані, зібрані трекінговими пікселями, що можуть його ідентифікувати. Тому потрібно мати процедуру: по запиту користувача знаходити всі його ідентифікатори в системах трекінгу (cookie ID, email у списках розсилки, тощо) і видаляти або анонімізувати відповідні записи. Це частина як принципу обмеження зберігання, так і дотримання прав суб'єктів. Якщо прямий пошук неможливий (наприклад, дані в Google Analytics анонімні), користувачу слід роз'яснити, що особистих даних там не зберігається або вони не пов'язані персонально.

Продовження Таблиці 3.4

Контролювати зберігання даних у сторонніх піксельних сервісах.	Дані, що збираються трекінговими пікселями, часто потрапляють на сервери сторонніх компаній (Google, Meta). Контролер має поцікавитися і задокументувати, як довго партнер зберігає ці дані. Бажано в налаштуваннях акаунтів обрати найкоротші строки зберігання, які пропонує сервіс, та укласти з постачальником трекера угоду, що зобов'язує його видаляти дані після закінчення наданого періоду. Наприклад, якщо email-маркетинговий сервіс збирає статистику відкриттів листів, варто налаштувати автоматичне очищення цих логів після, скажімо, 6 місяців. Це продемонструє дотримання принципу minimisation & storage limitation у випадку перевірки.

Правильне керування строками зберігання даних приносить двояку користь. По-перше, воно мінімізує обсяг інформації, який перебуває “в обороті” і може бути скомпрометований у разі інциденту (чим менше зберігаємо – тим менше може витекти). По-друге, виконання цього принципу – один з показників accountability: компанія демонструє, що вона усвідомлено керує життєвим циклом даних і не зберігає їх довше, ніж треба. Багато організацій зіштовхуються з тим, що історично накопичили гори старих даних з трекерів. GDPR стимулює навести тут лад: провести ревізію і позбавитися зайвого. Врешті, це й економічно вигідно – менші обсяги даних знижують витрати на їх хостинг і обробку.

3.4.7. Цілісність і конфіденційність

Останній з принципів, перелічених у ст.5(1) GDPR – цілісність і конфіденційність – вимагає забезпечити належну безпеку персональних даних, включно із захистом від несанкціонованої чи незаконної обробки, випадкової втрати, знищення чи пошкодження, шляхом відповідних технічних і організаційних заходів. У контексті трекінгових пікселів це означає, що зібрані через пікселі персональні дані повинні бути надійно захищені на всіх стадіях: під час передачі від користувача до сервера, при зберіганні у базах, при передаванні третім сторонам. Також слід забезпечити цілісність даних – захистити від непомітної модифікації чи підробки (наприклад, щоб ніхто не міг внести зміни до аналітичних даних).

Рекомендації: Забезпечення принципу конфіденційності та цілісності для трекінгових пікселів включає широкий спектр заходів кібербезпеки та управління доступом. У таблиці 3.5 наведено ключові рекомендації.

Таблиця 3.5

Рекомендації для забезпечення цілісності та конфіденційності даних

Рекомендований захід	Як захищає дані від пікселів
Передавати дані пікселів лише через захищені з'єднання (HTTPS).	Переконайтеся, що URL трекінгового пікселя використовує HTTPS-протокол. У сучасному вебі більшість легітимних пікселів і так працюють через HTTPS, але важливо це проконтролювати. Шифрування трафіку гарантує, що дані (такі як ідентифікатор сесії, параметри браузера, IP) не будуть перехоплені зловмисником по дорозі від браузера до сервера трекера. Це базовий технічний захід для забезпечення конфіденційності під час передачі.
Обмежити доступ до зібраних даних всередині організації.	Персональні дані, отримані з трекінгових пікселів (наприклад, списки емейлів, які відкрили лист, або логи активності користувачів сайту), повинні бути доступні лише уповноваженим особам. Необхідно впровадити систему розмежування доступу: наприклад, маркетинговий відділ може переглядати агреговані звіти, але доступ до сирих логів має лише адміністратор аналітики; або ж для доступу до деталей конкретного користувача потрібен окремий дозвіл. Це запобігає ситуаціям, коли хтось з співробітників без потреби переглядає персональні трекінгові дані, і тим самим зменшує ризик людського фактора (витоку, зловживання).

Продовження Таблиці 3.5

Укласти договори з третіми сторонами та переконатися в їх надійності.	Оскільки трекінгові пікселі часто належать зовнішнім постачальникам (Google, Meta та ін.), важливо мати з ними договір про обробку даних (DPA), що передбачений ст.28 GDPR. У такому договорі компанія-постачальник зобов'язується забезпечувати конфіденційність та безпеку даних, діяти лише за інструкціями контролера тощо. Також варто пересвідчитись, що у постачальника є належні сертифікати безпеки (наприклад, ISO 27001) та позитивна репутація щодо захисту даних. Це організаційний захід, що зменшує ризик несанкціонованого використання чи компрометації даних на стороні партнера.
Шифрувати персонально ідентифікуючі дані, що зберігаються.	Якщо трекінгові дані зберігаються у власних базах компанії і містять ідентифікатори (напр. адреси електронної пошти, номери телефонів, cookie-ID, прив'язані до осіб), бажано застосувати шифрування для таких полів у стані спокою (*at rest*). Наприклад, хешувати email перед збереженням у журнал відкриття листів. Тоді навіть якщо база даних буде зламана, зловмисник не отримає прямий доступ до PII. Так само резервні копії цих даних повинні зберігатися у зашифрованому вигляді.
Застосувати контроль цілісності для критичних даних.	Щоб гарантувати, що дані трекінгу не були потай змінені, можна впровадити контрольні механізми: логи діяльності повинні бути захищені від редагування (наприклад, експортувати їх у систему, де записи незмінні, або використовувати хешування/цифрові підписи для верифікації цілісності). Це особливо важливо, якщо дані можуть стати

Продовження Таблиці 3.5

	предметом перевірки чи розслідування (наприклад, у випадку інциденту або запиту суб'єкта – чи справді саме такі дії він зробив). Забезпечення цілісності є частиною принципу безпеки і підзвітності: компанія повинна мати можливість довести, що дані не були маніпульовані.
Виявляти та запобігати зловмисному використанню пікселів.	Необхідно врахувати, що трекінгові пікселі можуть використовуватись не лише вами, а й потенційно зловмисниками (наприклад, у фішингових листах для збору інформації про те, хто відкрив лист). Для захисту користувачів і власної інфраструктури варто налаштувати фільтри безпеки: відслідковувати, чи не вбудував хтось сторонній свій піксель на ваш сайт через уразливість, контролювати, які домени отримують виклики з вашого сайту (CSP – Content Security Policy може заборонити несподівані зовнішні звернення). Також бажано інформувати користувачів (особливо внутрішніх, співробітників) про ризики відкриття неочікуваних зображень у листах. Це радше превентивні заходи, але вони вписуються в комплекс захисту конфіденційності.

Дотримання принципу конфіденційності та цілісності суттєво знижує технічні ризики при роботі з трекінговими даними. Як було зазначено в Jscrambler, компанії, що використовують пікселі, повинні не лише отримувати згоду, а й гарантувати безпеку зібраних даних. Реалізація згаданих заходів – шифрування, контроль доступу, безпечна передача, договори з обробниками – демонструє відповідальне ставлення до даних і відповідність ст.32 GDPR (вимоги до безпеки обробки). Не менш важливою є й культурна складова: навчання співробітників правилам роботи з такими даними, періодичні перевірки систем безпеки, тестування на уразливості.

3.4.8. Права суб'єктів даних

GDPR надає фізичним особам – суб'єктам персональних даних – широкий спектр прав щодо їхніх даних. Найважливіші з них: право на доступ до своїх даних, право на виправлення, право на видалення (бути забутим), право на обмеження обробки, право на перенесення даних, право на заперечення проти обробки, а також право не підлягати автоматизованим рішенням, що мають істотні наслідки (профілювання) – ст. 15–22 GDPR. У випадку трекінгових пікселів забезпечити реалізацію цих прав часто складніше, оскільки збір даних відбувається автоматично і непомітно. Тим не менш, організація–контролер зобов'язана бути готовою виконати вимоги суб'єкта щодо даних, отриманих шляхом трекінгу, так само, як і будь-яких інших даних.

Право на доступ. Користувач може запросити в компанії копію своїх персональних даних або інформацію, які саме дані про нього збираються. Потенційно це включає й дані трекінгових пікселів – наприклад, записи про його дії на сайті, історію відкриттів email, IP-адреси, зафіксовані при його візитах тощо. Контролер повинен надати цю інформацію у зрозумілій формі (звичайно, що агреговану аналітику без прив'язки до особи можна не включати). На практиці це може вимагати вибірки з логів по ідентифікаторах користувача (cookie ID, email). Якщо дані анонімні і контролер не може їх пов'язати з конкретним індивідом, треба пояснити це заявнику.

Право на видалення. Як зазначалося, суб’єкт може вимагати видалити всі свої персональні дані. Для трекінгових даних це означає: знайти всі ідентифіковані записи (наприклад, всі події, зв’язані з його email чи іншим ID) і або стерти їх, або безповоротно деперсоналізувати. Якщо дані передані третім сторонам, треба повідомити їх про запит на видалення (якщо це технічно можливо). Важливо мати процедури, як це зробити, особливо якщо дані розпорошені між різними системами (CRM, аналітика, email-сервіс).

Право на заперечення. GDPR окремо гарантує суб’єкту право заперечити проти обробки його персональних даних в певних випадках (ст.21), зокрема проти обробки для цілей прямого маркетингу. Це безпосередньо стосується трекінгових пікселів, які використовуються для маркетингу і реклами – якщо людина заявляє заперечення, контролер зобов’язаний припинити таке відстеження щодо цієї особи. На практиці це може бути реалізовано через механізм відмови (opt-out): напр., якщо користувач вимкнув рекламні cookie або натиснув “не продавати мої дані” (для CCPA, але в ЄС аналог – “не використовувати мої дані для таргетингу”), то потрібно відключити пікселі маркетингових платформ для цього користувача. Право на заперечення не потребує обґрунтування з боку суб’єкта, особливо коли йдеться про маркетинг – компанія має безумовно виконати.

Права на виправлення і обмеження. У контексті трекінгу вони менш явно проявляються, але, приміром, право на обмеження може застосовуватися, якщо суб’єкт оскаржує точність даних або законність обробки – тоді компанія мусить призупинити використання трекінгових даних (не видаляючи їх) на час розгляду. Право на перенесення щодо трекінгових даних, імовірно, мало буде застосоване (воно стосується даних, що надані самим користувачем і обробляються автоматично за згодою чи контрактом), хоча теоретично користувач може попросити передати йому його поведінкові дані в зручному вигляді.

Рекомендації: Таблиця 3.6 підсумовує кроки для забезпечення прав суб’єктів даних у аспекті трекінгових пікселів.

Таблиця 3.6

Рекомендації для забезпечення прав суб'єктів даних

Рекомендований захід	Як сприяє виконанню прав суб'єктів
Запровадити прозорий механізм opt-out (відмови від трекінгу).	Користувачам має бути легко доступна функція відключення трекінгових пікселів. Це може бути посилання *"Відмовитися від відстеження"* на сайті (яке встановлює cookie, що блокує пікселі), або налаштування в профілі користувача *"Не відстежувати мою активність"*. У email-розсилках варто, окрім кнопки "Відписатися", додати примітку про використання трекінгу і можливість його вимкнути, перейшовши за спеціальним посиланням. Надання такої опції демонструє повагу до права на заперечення та права не бути відстежуваним для маркетингу. За даними UpGuard, можливість відмовитися від пікселів допомагає зберегти довіру користувачів.
Налагодити процес обробки запитів доступу/видалення щодо трекінгових даних.	Внутрішня команда (відповідальна за GDPR) повинна знати, де і як шукати дані трекінгу по конкретному користувачу. Необхідно скласти алгоритм: по запиту "надайте мені мої дані" – перевірити CRM, бази веб-аналітики (за clientID, IP), бази email-маркетингу (за email) тощо, зібрати відомості: коли і які дії фіксувались. Так само на випадок запиту на видалення – визначити, у яких системах є ідентифіковані сліди користувача, і видалити їх. Це може потребувати функцій пошуку в журналах

Продовження Таблиці 3.6

	або API від сторонніх сервісів (Google, наприклад, має інструмент видалення даних користувача з аналітики). Головне – визначити відповідальних і задокументувати процедури, щоб не діяти спонтанно.
Інформувати користувачів про їхні права в контексті трекінгу.	У політиці конфіденційності або на сторінці з налаштуваннями приватності слід прямо написати, що користувач має право вимагати припинення відстеження, видалення отриманих даних тощо. Також можна додати розділ FAQ: “Як дізнатися, чи відстежується моя активність?” – з поясненнями про трекінгові пікселі на сайті. Виконання обов’язку за ст.13–14 GDPR (інформаційні повідомлення) має включати згадку про трекінгові технології та права, пов’язані з ними. Це забезпечує прозорість і допомагає користувачу реалізувати свої права усвідомлено.
Відслідковувати звернення користувачів щодо трекінгу і реагувати на них.	Якщо користувачі починають скаржитись (наприклад, пишуть: “Я відмовився від cookie, а ви все одно відстежуєте”), треба оперативно це виправляти – можливо, технічна проблема. Або якщо користувач питає: “Я хочу, щоб ви не збирали про мене нічого” – йому варто надати інструкцію (як мінімум, як відключити трекінг) чи застосувати внутрішній прапорець “не трекати”. В цілому, усі запити, що стосуються трекінгових даних, мають оброблятися так само ретельно, як і запити щодо основних персональних даних. Для відстеження статусу таких звернень може

Продовження Таблиці 3.6

	використовуватися спеціальний журнал (щоб не загубити і виконати вчасно протягом 1 місяця, як вимагає GDPR).
У випадку сумнівів – надавати більше контролю користувачу.	Якщо певний аспект прав важко прямо реалізувати (наприклад, право на перенесення – немає стандартизованого формату для поведінкових даних), можна запропонувати альтернативу: надати користувачу CSV-файл з його логами або просто повідомити йому основні показники. Головне – не ігнорувати запити. Так само з профілюванням: якщо сайт використовує піксель для автоматизованого прийняття рішень (скажімо, вирішує, яку знижку показати постійному клієнту на основі трекінгу), то потрібно дати можливість відмовитися від такого профілювання. Загальне правило – ставити інтереси і права користувача на перше місце, навіть якщо технічно це створює певні складнощі для бізнесу.

Таким чином, забезпечення прав суб'єктів даних при використанні трекінгових пікселів зводиться до надання прозорих опцій контролю (opt-in, opt-out), готовності надати звіт користувачу про зібрані про нього дані, а за потреби – видалити або передати ці дані. Це тісно переплітається з попередньо розглянутими принципами (прозорість, обмеження зберігання) і фактично є продовженням їхньої реалізації з акцентом на індивідуальні запити. Організації повинні пам'ятати: навіть якщо трекінгові дані на перший погляд *не ідентифікують прямо* людину, але якщо існує шлях пов'язати їх з конкретним користувачем (напряму чи опосередковано), цей користувач має права на ці дані за GDPR.

3.4.9. Обробка на основі згоди

Хоча отримання згоди вже згадувалось у контексті законності (розділ 1.1), важливо окремо розглянути вимоги до обробки персональних даних на підставі згоди в контексті трекінгових пікселів. Справа в тому, що для більшості сценаріїв використання пікселів у веб-середовищі згода суб'єкта є основною (а часто єдиною легально допустимою) підставою, з урахуванням вимог не лише GDPR, а й Директиви про ePrivacy. Згода повинна відповідати суворим критеріям GDPR: бути *свідомою, конкретною, вільно наданою та недвозначно вираженою* шляхом активної дії.

Методика отримання та управління згодою користувачів на трекінг є критичною. Помилки на цьому етапі знецінюють усі інші заходи: якщо згоди не було, то вся подальша обробка є незаконною, навіть якщо дані захищені чи мінімізовані. Тому організаціям слід приділити максимальну увагу правильній реалізації consent management.

Рекомендації: Зведемо основні правила і поради щодо отримання та використання згоди у таблиці 3.7.

Таблиця 3.7

Рекомендації щодо обробки на основі згоди (Consent Management)

Рекомендований захід	Детальний опис
Отримувати згоду шляхом явного “opt-in” дії.	Будь-які трекінгові пікселі повинні завантажуватися тільки після того, як користувач *активно погодився*. Найкраща практика – банер з опціями, де за замовчуванням відстеження вимкнене, і користувач мусить натиснути “Я згоден” для увімкнення. Неприпустимі попередньо відмічені галочки або завантаження пікселів до згоди (навіть якщо потім є можливість відмовитися – це пізно). Згода фіксується тоді, коли користувач, наприклад, проставив прапорці “аналитичні cookies” і “маркетингові cookies” самостійно. Це відповідає вимозі недвозначності та активності дії.
Збирати окрему згоду на різні категорії трекінгу.	Як згадувалось, якщо на сайті є різні цілі трекінгу, згода має бути специфічною. Практично – кілька чекбоксів/кнопок: *“Погоджуюся на аналітику”*, *“Погоджуюся на персоналізовану рекламу”* тощо. Це не тільки виконує GDPR-вимогу специфічності, а й робить згоду більш усвідомленою: користувач може вирішити, що для статистики він згоден ділитися даними, а для реклами – ні.
Надати можливість легко відкликати згоду.	Важливий аспект – *ревокабельність* згоди. Користувач повинен у будь-який момент мати змогу змінити свій вибір. Реалізувати це можна через постійно доступну кнопку на сайті (наприклад, значок “Налаштування приватності”), де він може відкликати згоду на трекінг. В електронних листах – через посилання типу “Відмовитися від відстеження” або налаштування в акаунті. GDPR прямо вимагає, щоб відкликання згоди було так само простим, як і надання. Після відкликання всі небажані пікселі мають бути негайно відключені, а подальші дані – не збиратися.

Продовження Таблиці 3.7

Вести журнал (лог) отриманих згод.	Принцип підзвітності (ст.5(2) GDPR) зобов'язує контролера довести, що він отримав згоду належним чином. Тому слід зберігати докази згоди: наприклад, записувати у лог файл або в базу даних факт, що користувач X (ідентифікатор cookie або аккаунту) у такий-то час натиснув "Прийняти трекінг". Якщо використовуються Consent Management Platform (CMP), вона зазвичай це робить автоматично, генеруючи унікальний ID згоди (consent ID) і зберігаючи його разом з відмітками, на що саме дано згоду. У разі аудиту або розслідування скарги компанія зможе пред'явити ці записи як підтвердження дотримання ст.7(1) (умови згоди).
Перевіряти вік та дієздатність суб'єкта для згоди.	Якщо аудиторія сайту може включати дітей до 16 років (а в деяких країнах ЄС – до 13 років), необхідно врахувати вимоги щодо батьківської згоди (ст.8 GDPR). Тобто для неповнолітніх користувачів згода на трекінг має надаватися або схвалюватися їхнім представником. Технічно це складно перевірити, але хоча б слід попередити: "особам до 16 років відстеження не застосовується без дозволу батьків" і при виявленні – не ставити пікселі. Це тонкий момент, який у роботі варто згадати, демонструючи комплексність підходу до згоди.
Регулярно оновлювати отримані згоди (re-consent).	Згода не є безстроковою, особливо якщо обставини змінились (нові пікселі, нові цілі). Рекомендується періодично (скажімо, раз на рік) запитувати у постійних користувачів повторне підтвердження згоди на трекінг – особливо якщо у практики відстеження були внесені зміни. Також при істотному оновленні політики (наприклад, додали нову категорію трекінгу) – показати банер знову і отримати згоду. Це гарантує актуальність згоди і відповідність її інформованості.

Правильне управління згодою – це свого роду фундамент законності обробки. Без нього решта заходів можуть виявитися марними з правової точки зору. Варто зазначити, що у деяких випадках організації намагаються обґрунтовувати використання трекінгу на інших підставах (наприклад, *легітимний інтерес* для базової аналітики). Однак після рішення Суду ЄС по Schrems II і роз'яснень EDPB стає зрозуміло, що для більшості трекерів немає альтернативи згоді, оскільки вони не є суто необхідними для надання запитуваної послуги користувачу. Отже, акцент має бути на тому, щоб згода збиралась коректно.

З практичної точки зору, для реалізації всіх цих правил доцільно застосувати спеціалізовану Consent Management Platform (CMP). CMP – це інструмент (власний або сторонній), який відображає банер, записує вибір користувача, автоматично блокує/дозволяє скрипти відповідно до вибору і зберігає докази згоди. В сучасних умовах використання CMP є мало не обов'язковим для сайтів з кількома трекерами, адже вручну відслідкувати, щоб ніякі пікселі не проскочили без згоди, дуже складно.

3.4.10. Передача даних третім сторонам

Трекінгові пікселі майже завжди пов'язані з передачею даних третім сторонам – бо самі пікселі зазвичай належать зовнішнім сервісам (Google, Meta, рекламні мережі, провайдери аналітики тощо). Тому окремо слід розглянути контроль за тим, як дані, зібрані пікселем, передаються і хто їх отримує. Під "передачею третім сторонам" у контексті GDPR можна розуміти дві речі: передачу даних *всередині ЄЕП іншим контролерам/обробникам* та трансфер даних за межі ЄЕП (в треті країни). Обидва аспекти актуальні для трекінгових пікселів.

Особливо гостро стоїть питання трансферу даних в США, оскільки багато популярних трекерів надсилають дані на сервери у США. Після скасування угоди Privacy Shield (рішення "Schrems II" 2020 року) такі передачі вважаються незаконними, якщо не забезпечені інші гарантії. Як згадано у вступі, австрійський та французький регулятори визнали використання Google Analytics та Facebook Pixel

порушенням саме через передачу персональних даних (IP, ідентифікатори) на сервери в США, де до них можуть отримати доступ спецслужби. Тож контролерам потрібно або впровадити додаткові заходи, або обрати європейські альтернативи, або користуватися новими механізмами (як-от “Data Privacy Framework”, прийнятим в 2023 році для США, якщо він буде чинним).

Рекомендації: В таблиці 3.8 представлені кроки щодо належного контролю передачі даних трекінгових пікселів третім сторонам.

Таблиця 3.8

Рекомендації щодо передачі даних третім сторонам при використанні пікселів

Рекомендований захід	Як реалізувати і чому це важливо
Інвентаризувати всіх третіх сторін, що отримують дані через пікселі.	Перший крок – точно знати, *кому* йдуть дані з вашого сайту чи додатку. Складіть перелік всіх трекінгових пікселів і їхніх одержувачів: напр., Google (Analytics, Tag Manager), Meta (Facebook Pixel), Hotjar, Mailchimp (піксель розсилки) тощо. Для кожного – вкажіть, чи виступає ця сторона обробником ваших даних (діє за вашим дорученням, напр. аналітика) чи спільним контролером (як у випадку Meta, що може використовувати дані для власних цілей). Така інвентаризація допоможе визначити, які договори і гарантії потрібні.
Укласти необхідні договори (DPA, Standard Contractual Clauses).	Якщо третя сторона – обробник (processor) вашої інформації, обов'язково укладіть договір про обробку (Data Processing Agreement), як вимого ст.28 GDPR. Типово великі постачальники мають готові DPA (їх треба прийняти). Цей договір зобов'язує їх захищати дані і діяти тільки згідно з вашими інструкціями. Якщо ж відбувається передача за кордон, і країна не має рішення про адекватність, слід укласти стандартні договірні положення (SCC) з додатками щодо захисту. Наприклад, якщо використовується піксель компанії з США, треба підписати з нею SCC (багато хто включає це в DPA).

Продовження Таблиці 3.8

Оцінити законність трансферів даних та застосувати додаткові заходи.	Після Schrems II просто наявності SCC може бути недостатньо, якщо у країні-одержувача (США) закони дозволяють уряду доступ до даних. GDPR вимагає провести *Transfer Impact Assessment* – оцінити, чи забезпечені дані адекватним захистом. Для трекінгових пікселів можна застосувати додаткове шифрування даних перед відправкою (якщо можливо) – так, щоб третя сторона не могла прочитати особисту інформацію. Наприклад, обрубати IP або хешувати ідентифікатори на своєму боці (як згадувався проксі-сервер). Це згадується серед рішень, які EDPB пропонує для нових методів відстеження, щоб обійти ризики. Якщо такі заходи не можуть усунути ризик – можливо, варто відмовитися від конкретного пікселя або використовувати його тільки за умов явно вираженої згоди на міжнародний трансфер (і повідомити про можливі ризики).
Використовувати європейські або самостійно розгорнуті рішення, де можливо.	Один із шляхів зменшити ризики передачі – локалізувати обробку даних. Наприклад, замість Google Analytics використати європейський аналог (Matomo On-Premises, Plausible Analytics), який працює на серверах в ЄС або навіть на ваших серверах. Для email-розсилок – обрати провайдера з Європи, який не передає дані за океан. Якщо цінність трекінгу не переважає ризики – подекуди взагалі відмовитися: наприклад, вирішити не вставляти пікселі в листи, а оцінювати успішність розсилки іншими способами. Таким чином, дані не виходитимуть до третіх сторін, отже мінімізуються юридичні проблеми.

Продовження Таблиці 3.8

Прозоро повідомляти користувачів про передачу даних третім сторонам.	GDPR (ст.13, 14) вимагає інформувати суб'єкта, *кому* передаються його дані. У політиці слід перерахувати всіх партнерів/отримувачів даних від пікселів (назви компаній) і мету передачі. Окремо, якщо є трансфери за межі ЄС – вказати країни (наприклад: "Дані веб-аналітики можуть передаватися на сервери в США (Google) згідно з стандартними положеннями про захист даних") і згадати наявність/відсутність рішення про адекватність, а також *можливі ризики*. Це не тільки вимога регуляції, а й елемент довіри: користувач, бачачи такий рівень прозорості, розуміє, що компанія відповідально ставиться до питання.
Моніторити оновлення законодавства та позиції регуляторів.	Сфера трансграничних передач даних наразі дуже динамічна. Наприклад, у 2023 році ЄС затвердив нову рамкову угоду з США (EU–US Data Privacy Framework) для відновлення трансферів. Компанії, що підпадають під неї, можуть вважатися безпечними отримувачами. Потрібно стежити, чи ваші постачальники сертифікувалися за цією програмою. Якщо так – можна спиратися на це як на підставу передачі. Якщо ж знову якісь рішення скасовуються – треба оперативно реагувати (наприклад, німецький DPA може заборонити конкретний сервіс – тоді варто його відключити, щоб не отримати штраф). Постійне відстеження новин від EDPB, національних регуляторів та юристів у сфері privacy – важлива частина відповідального підходу до передач даних.

У підсумку, контроль над передачами даних третім сторонам при трекінгу зводиться до трьох основних речей: юридичне оформлення відносин (договори, умови трансферу), технічний захист переданих даних (мінімізація перед тим, як відправити; шифрування) та осмислений вибір партнерів (краще ті, що дають гарантії захисту або взагалі уникнення певних передач).

Реальні кейси – як-то рішення проти Meta Pixel – показують, що ігнорувати це питання не можна: включення стороннього пікселя може зробити ваш сайт співвідповідальним за *передачу даних користувачів у США без належного захисту*, що є порушенням ст.44 GDPR. Тому при розробці методики захисту (розділ 2) ми врахуємо цей аспект, зокрема, рекомендуватиметься по можливості використовувати європейські рішення або проксування, а якщо ні – то чітко інформувати і отримувати явну згоду на міжнародні передачі.

3.5 Шаблон політики конфіденційності з врахуванням трекінгових пікселів

Представлений шаблон (Див. Додаток А) відображає ключові аспекти: пояснюється на зрозумілій мові, що таке пікселі і навіщо вони компанії (у даному випадку, ми говоримо про релевантність даного шаблону для мали та середніх організацій); перелічуються конкретні пікселі і їх постачальники (це важливо для прозорості та відповідності вимогам – користувача інформують, хто саме отримує дані і для чого); описуються категорії даних; надаються способи відмови і відкликання згоди; згадується правова основа і міжнародні передачі, права користувача. Такий рівень деталізації допомагає користувачеві зробити свідомий вибір і водночас захищає компанію від звинувачень у приховуванні інформації.

3.6 Інструкція із захисту персональних даних для малих та середніх організацій

Для впровадження вищеописаних рекомендацій на практиці, нижче пропонується стислий план (інструкція) для малих та середніх організацій, що використовують трекінгові пікселі. Ця інструкція складається з двох частин: технічні заходи та організаційні заходи. Вона може слугувати внутрішнім документом компанії, що встановлює правила і відповідальність щодо захисту персональних даних.

Технічні заходи захисту:

– Інвентаризація трекерів: Відповідальний за веб-сайт (СТО або адміністратор) веде актуальний список всіх трекінгових скриптів і пікселів, впроваджених на сайті та в email-розсилках. Будь-який новий трекер повинен бути погоджений і доданий до цього списку.

– Налаштування безпеки веб-додатка: Впровадити Content Security Policy, що обмежує домени: дозволити лише очікувані домени (наприклад, *.facebook.com, *.google-analytics.com) для завантаження ресурсів. Включити режим report-uri для отримання сповіщень про порушення CSP.

– Шифрування даних: Усі персональні дані користувачів, що зберігаються на серверах вашої компанії (наприклад, у базах даних або аналітичних системах), мають бути зашифровані. Варто використовувати надійний алгоритм AES-256 для шифрування баз даних та їх резервних копій. Ключі шифрування зберігайте у спеціальному менеджері секретів, доступ до якого мають лише декілька довірених співробітників.

– Анонімізація аналітики: Налаштуйте сторонні сервіси трекінгу таким чином, щоб вони збирали якомога більше знеособлених даних. Наприклад, завжди анонімізуйте або маскуйте IP-адреси користувачів. Ніколи не передавайте email-адреси у відкритому вигляді через такі сервіси. Для корпоративної пошти розгляньте використання проксі-сервера для email-зображень, щоб приховувати реальні IP-адреси ваших співробітників при відкритті листів.

– Моніторинг логів: Організуйте централізований збір логів з ваших веб-серверів та мережевих пристроїв. Це дозволить вам швидше виявляти підозрілу активність. Впровадьте базові правила для системи SIEM (Security Information and Event Management), навіть якщо це буде простий моніторинг ключових подій. Наприклад, відстежуйте:

o сповіщати, якщо з сервера сайту йде звернення на невідомий домен;

o сповіщати про масові звернення на домени трекерів поза робочим часом (можливий аномальний трафік);

o виявляти шаблони фішингу (якщо після відкриття листа з корпоративної пошти йдуть запити на незнайомі хости).

Відповідальний аналітик SOC переглядає такі сповіщення щоденно.

Використання веб-безпек рішень: Розгорнути на сайті рішення типу Web Application Firewall (WAF) з правилами проти відомих шкідливих доменів/скриптів. Розглянути впровадження клієнтського моніторингу (як Jscrambler) для відстеження цілісності контенту та скриптів на сторінках.

Безпечна розробка: При розробці нового функціоналу сайту інтегрувати принципи Security & Privacy by Design. Будь-який код, що додає нові підключення або збирає дані, проходить рев'ю на предмет приватності та безпеки. Застосовувати статичний аналіз коду для виявлення вставок зовнішніх URL.

Організаційні заходи захисту:

Призначення відповідальних осіб: Призначити посадову особу, відповідальну за захист персональних даних (DPO). DPO разом з IT-безпекою контролює дотримання політик щодо трекінгових пікселів.

Політика використання трекерів: Видати внутрішню політику, що забороняє встановлення будь-яких трекінгових кодів на платформи компанії без письмового погодження з DPO та відділом безпеки. У політиці прописати процедуру оцінки впливу (PIA) – маркетинг- або IT-відділ заповнює коротку форму аналізу ризиків, DPO її затверджує.

Навчання персоналу: Проводити раз на півріччя тренінги для співробітників, особливо маркетологів, розробників, контент-менеджерів, щодо:

- вимог законів GDPR/ЗУПД про згоду та прозорість;
- кращих практик збору даних (мінімізація, анонімність);
- реальних історій інцидентів (щоб підкреслити важливість дотримання правил).

Також навчити всіх співробітників основам розпізнавання фішингу та небажаного трекінгу (наприклад, не відкривати підозрілі листи, вимикати автозавантаження зображень).

Документообіг та згода користувачів: Забезпечити, щоб відділ по роботі з клієнтами та юридичний відділ підтримували в актуальному стані публічну Політику конфіденційності (див. пункт 3.3). При будь-яких змінах у використанні трекерів оновлювати політику та комунікувати зміни користувачам. Отримувати необхідні згоди (впровадити банери та механізми відмови, якщо ще не зроблено).

Договори з третіми сторонами: Переглянути всі діючі договори з постачальниками маркетингових та аналітичних послуг. Включити туди положення про захист даних (якщо їх нема) або укласти окремі DPA. Перевірити сертифікації цих постачальників (наприклад, чи є у них відповідність ISO 27701, чи не було витоків даних у минулому).

Відстеження законодавчих змін: DPO моніторить новини щодо регуляцій. У разі прийняття нового закону або рішення (наприклад, судового прецеденту, як у випадку Capital One) – ініціює внутрішню перевірку: чи відповідає практика компанії вимогам, що потрібно змінити. Наприклад, рішення суду про розкриття даних через пікселі підпадає під CCPA – компанія, хоч і не з Каліфорнії, бере це до уваги і коригує свою політику, щоб уникнути подібних проблем.

План дій при інциденті: Створити робочу групу реагування (інцидент-респонс команда), яка у разі виявлення витоку через піксель одразу збирається. План: ізолювати проблему (відключити піксель, наприклад, через тег-менеджер швидко), дослідити масштаби (подивитись логи, що саме передалось), за потреби – повідомити

користувачів і відповідні органи (Уповноваженого з захисту даних). Провести після інциденту ретроспективу: чому сталося, як запобігти надалі, оновити процедури.

Інструкція вище окреслює конкретні кроки, які має зробити компанія, щоб інтегрувати питання безпеки пікселів у свою щоденну діяльність. Виконання цих кроків перетворить теоретичні рекомендації з таблиці 2 на практичні дії, закріплені на рівні компанійних процесів.

Таким чином, впроваджені заходи комплексно підвищують рівень захищеності персональних даних та зменшують ризики, пов’язані з сучасними трекінговими технологіями.

Висновок до розділу 3

У цьому розділі було комплексно розглянуто сучасні загрози, пов’язані з використанням трекінгових пікселів, а також надано практичні методи їх виявлення та мінімізації ризиків для персональних даних користувачів. Проведений аналіз показав, що трекінгові пікселі є одним з найпоширеніших інструментів збору даних у цифровому середовищі, що створює значні виклики як у технічній, так і у правовій площині.

Визначено основні джерела ризиків — як зовнішні (маркетингові платформи, рекламні мережі, кіберзлочинці), так і внутрішні (недостатня обізнаність співробітників, відсутність контролю за скриптами). Деталізовано вразливості інформаційних систем, які часто залишаються поза увагою через складність виявлення невидимих елементів стеження. Наведена оцінка ризиків доводить: ключовими для захисту є впровадження технічних та організаційних заходів, спрямованих на попередження несанкціонованої передачі та обробки персональних даних.

У роботі запропоновано універсальну багаторівневу методику, що охоплює етапи від ідентифікації та інвентаризації трекерів до архітектурних рішень (CMP, проксі-сервери, Privacy Gateway), інтеграції маскування та фільтрації, а також організаційної роботи із політиками, навчанням персоналу і контролем згод

користувачів. Розроблено окремі механізми для автоматичного виявлення та нейтралізації пікселів у пошті й на веб-сайтах, включаючи алгоритмічні рішення та варіанти використання проксі.

Впровадження зазначених механізмів дозволяє не лише вчасно виявляти і блокувати потенційно небезпечні трекінгові елементи, а й забезпечує відповідність вимогам міжнародного та національного законодавства у сфері захисту персональних даних. Застосування даного підходу сприяє підвищенню рівня довіри користувачів до цифрових сервісів і мінімізує репутаційні та юридичні ризики для компаній.

ВИСНОВКИ

У ході виконання кваліфікаційної роботи було проведено комплексне дослідження механізмів виявлення загроз безпеці персональних даних, пов’язаних з використанням трекінгових пікселів. Тема дослідження є актуальною з огляду на стрімкий розвиток цифрового маркетингу, широке впровадження засобів невидимого збору даних про користувачів та зростання кількості кіберінцидентів, пов’язаних із порушенням конфіденційності.

Проаналізовано технічні аспекти роботи трекінгових пікселів, зокрема механізми їх вбудовування у веб-ресурси, передачу метаданих, взаємодію з cookies, веб-маяками та іншими технологіями онлайн-відстеження. Наведено типові приклади використання пікселів компаніями Meta, TikTok, Google та іншими, а також виявлено потенційні вектори атак, що можуть виникнути внаслідок використання таких технологій (social engineering, session hijacking, deanonymization тощо).

У процесі дослідження оцінено основні ризики витоку персональних даних, створено матрицю ризиків відповідно до вимог Загального регламенту захисту даних (GDPR), побудовано модель загроз і модель потенційного порушника. Також досліджено відповідність практик обробки персональних даних стандартам безпеки, зокрема GDPR та NIST CSF 2.0. Встановлено, що в багатьох випадках веб-ресурси збирають дані без достатньої прозорості та інформованої згоди користувача, що є порушенням міжнародних норм.

На основі проведеного аналізу розроблено Рекомендації для організацій, які впроваджують або використовують трекінгові технології. Запропоновано технічні та організаційні заходи щодо обмеження впливу трекінгових пікселів, серед яких: впровадження криптографічних методів захисту, обмеження скриптів сторонніх розробників, застосування інструментів аналізу трафіку, реалізація політик прозорості та контролю згоди, а також регулярний аудит використання пікселів у веб-інфраструктурі.

Завершальним етапом роботи стало формування шаблону Політики конфіденційності персональних даних, що відповідає вимогам GDPR та містить положення про використання трекінгових пікселів, права суб'єктів даних, механізми відкликання згоди та методи контролю за обробкою інформації.

Таким чином, реалізація запропонованих підходів дозволяє підвищити прозорість, зменшити ризики витоку персональних даних та забезпечити відповідність сучасним міжнародним вимогам у сфері кібербезпеки та конфіденційності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. General Data Protection Regulation (GDPR), Regulation (EU) 2016/679 of the European Parliament and of the Council, 27 April 2016 [Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

2. NIST Cybersecurity Framework (NIST CSF) Version 2.0 [Електронний ресурс]. – Режим доступу: https://www.nist.gov/cyberframework

3. ISO/IEC 27001:2022 – Information Security Management [Електронний ресурс]. – Режим доступу: https://www.iso.org/standard/82875.html

4. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17

5. Mozilla Developer Network. HTML <img> tag. https://developer.mozilla.org/en-US/docs/Web/HTML/Element/img

6. Cloudflare. What is a Tracking Pixel? https://www.cloudflare.com/learning/privacy/what-is-a-tracking-pixel/

7. Electronic Frontier Foundation. Privacy Badger. https://privacybadger.org/

8. Meta Business Help Center. Meta Pixel Setup Guide. https://www.facebook.com/business/help/742478679120153

9. Google Support. Set up Analytics for a website and/or app. https://support.google.com/analytics/answer/9304153

10. TikTok Ads Help Center. How to Use TikTok Pixel. https://ads.tiktok.com/help/article?aid=100006197819

11. LinkedIn Marketing Solutions. Insight Tag Help. https://www.linkedin.com/help/lms/answer/a427660

12. Twitter for Business. Conversion Tracking for Websites. https://business.twitter.com/en/help/campaign-measurement-and-analytics/conversion-tracking-for-websites.html

13. Trackify Blog. How to Set Up Your Facebook Pixel. https://trackifyapp.com/blogs/news/how-to-set-up-your-facebook-pixel

14. GDPR.eu. A Practical Guide to GDPR. https://gdpr.eu

15. StatNews. Facebook is receiving sensitive medical information from hospital websites. https://www.statnews.com/2022/06/16/hospitals-facebook-tracking-tool-sensitive-health-data/

16. Politico Europe. Ad industry trade body IAB Europe hit with GDPR fine. https://www.politico.eu/article/europe-digital-advertising-iab-europe-gdpr-privacy/

ДОДАТКИ

ДОДАТОК А
ПОЛІТИКА КОНФІДЕНЦІЙНОСТІ ТА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Акціонерне товариство

«Назва Компанії»

ЗАТВЕРДЖУЮ

Генеральний директор _____

_____

«_____» _____ 2024 р.

ПОЛІТИКА
КОНФІДЕНЦІЙНОСТІ ПЕРСОНАЛЬНИХ ДАНИХ

«Назва Компанії»

м.Київ 2025

Продовження додатку А

Політика конфіденційності та захисту персональних даних

1. Загальні положення

Ця Політика визначає принципи, підходи та вимоги до обробки персональних даних у межах діяльності Організації. Компанія поважає права користувачів на конфіденційність та зобов'язується забезпечити їх захист при взаємодії з інформаційними системами компанії, включно з використанням трекінгових пікселів.

Організація повинна розглядати захист персональних даних як ключову складову корпоративної культури.

Організація зобов’язується дотримуватись принципів законності, прозорості, мінімізації, точності, обмеження мети та строку зберігання персональних даних.

Політика розроблена відповідно до Закону України «Про захист персональних даних», GDPR (EU 2016/679), ePrivacy та галузевих стандартів.

Політика поширюється на всі інформаційні системи, співробітників, підрядників, клієнтів і партнерів, які обробляють або мають доступ до персональних даних, включаючи дані, отримані з трекінгових пікселів.

2. Ролі та обов’язки

Компанія повинна призначити відповідальну особу (Data Protection Officer), яка здійснюватиме контроль за дотриманням політики конфіденційності та законодавчих вимог.

DPO зобов’язаний проводити аудит, консультувати, навчати персонал і моніторити дотримання законодавчих та корпоративних вимог щодо персональних даних.

Продовження додатку А

Політика конфіденційності та захисту персональних даних

IT-відділ Організації повинен впроваджувати технічні та організаційні заходи безпеки, зокрема для трекінгових пікселів (наприклад, контроль доступу, шифрування, моніторинг логів).

Всі працівники зобов’язані дотримуватися правил обробки персональних даних згідно цієї Політики.

Суб'єкти даних мають право на доступ, виправлення, обмеження обробки, а також на видалення своїх даних.

Кожен співробітник зобов’язаний негайно повідомляти про будь-які інциденти безпеки DPO.

Кожен працівник повинен проходити навчання щодо правил захисту персональних даних щонайменше один раз на рік.

3. Обсяг і мета обробки персональних даних

Компанія повинна обробляти персональні дані лише в обсязі, необхідному для конкретної, визначеної, законної мети. Дані можуть включати IP-адресу, cookie, ідентифікатори пристроїв, інформацію про поведінку користувача на сайті. Забороняється обробка надлишкових або чутливих даних без окремої письмової згоди.

Компанія обробляє лише ті дані, які надаються суб'єктами добровільно або отримуються в результаті технічного аналізу дій на сайті (через пікселі, cookie тощо):

- IP-адреса;
- браузер і операційна система;
- поведінка на сторінках сайту;
- тривалість сесії, джерела переходів.

Метою обробки є покращення користувацького досвіду, аналітика, таргетинг реклами, забезпечення безпеки сервісів.

Продовження додатку А

Політика конфіденційності та захисту персональних даних

4. Взаємодія з третіми сторонами

Передача даних третім сторонам (аналітичні платформи, рекламні партнери) дозволена лише за наявності правової підстави (угода, згода суб'єкта, DPA).

Організація повинна укладати договір про обробку даних (Data Processing Agreement, DPA) з усіма контрагентами, які мають доступ до персональних даних.

Передача даних дозволена лише у разі впровадження адекватних технічних та організаційних заходів безпеки.

Організація повинна вести реєстр всіх третіх сторін, яким передаються дані, з обґрунтуванням цілей і гарантіями захисту.

5. Захист даних і безпека

Організація повинна впровадити багаторівневі заходи захисту даних:

- Шифрування даних у транзиті та при зберіганні (наприклад, AES-256)
- Використання firewall, IDS/IPS, DLP
- Аутентифікація користувачів з MFA
- Сегментація мереж і обмеження доступу за ролями

Для трекінгових пікселів та cookie має використовуватись механізм попередньої згоди (cookie-банер) з можливістю вибору типу трекерів.

Організація повинна проводити регулярний аудит інформаційної безпеки та тестування на проникнення.

Всі інциденти безпеки реєструються, аналізуються та розслідуються відповідальною особою.

Продовження додатку А

Політика конфіденційності та захисту персональних даних

6. Термін зберігання

Компанія повинна зберігати персональні дані протягом терміну, необхідного для досягнення мети обробки або виконання вимог закону. Після закінчення цього терміну дані підлягають знищенню або деперсоналізації згідно з протоколом знищення.

7. Права суб'єктів персональних даних

Компанія повинна забезпечити реалізацію прав суб'єктів персональних даних, а саме:

- право на доступ до своїх персональних даних;
- право на їх виправлення;
- право на відкликання згоди;
- право на обмеження або заборону обробки;
- право на видалення даних («право бути забутим»);
- право на звернення до Уповноваженого ВРУ або суду.

8. Безпека використання трекінгових пікселів та файлів cookie

Організація повинна використовувати трекінгові пікселі лише з легітимною метою, дотримуючись принципу прозорості.

Всі трекінгові пікселі (наприклад, Google Analytics, Meta Pixel, TikTok Pixel, Hotjar) повинні бути активовані лише після явної згоди користувача.

Користувач має право в будь-який момент відкликати згоду на обробку даних трекінговими пікселями.

Не допускається використання трекінгових пікселів, що передають персональні дані третім сторонам без згоди користувача.

Організація повинна вести реєстр активних трекінгових пікселів і регулярно його оновлювати.

Використання трекінгових пікселів повинно бути чітко описано у політиці cookie та розкрито у політиці конфіденційності.

9. Маскування персональних даних

Компанія повинна впровадити механізми маскування персональних даних у середовищах тестування, аналітики та при взаємодії з підрядниками. \

Застосовуються такі методи маскування:

- псевдонімізацію (заміна реальних значень на умовні);
- генерацію тестових даних;
- часткове приховування значень (наприклад, номерів телефонів або ідентифікаторів).

Масковані дані не дозволяють ідентифікувати користувача без доступу до ключа або додаткової інформації.

10. Підтримка, оновлення та розповсюдження

Компанія повинна переглядати цю Політику щонайменше один раз на рік або у разі змін у законодавстві, технологіях чи структурі компанії. Актуальна версія політики повинна бути опублікована на внутрішньому порталі та доступна для всіх співробітників.

ДОДАТОК Б

МАТРИЦЯ ЗАГРОЗ, ПОВ'ЯЗАНИХ З ТРЕКІНГОВИМИ ПІКСЕЛЯМИ, ТА ЇХНІ ПОТЕНЦІЙНІ НАСЛІДКИ

Загроза / Вектор атаки	Опис і розвиток атаки	Наслідки
Неправомірний збір даних третіми сторонами (privacy breach)	Легітимний піксель (Facebook, Google) збирає дані про користувачів без їх інформування чи згоди.	Порушення приватності, можливі штрафи за GDPR/ЗУПД, втрата довіри користувачів.
Несанкціонована передача чутливих даних	Піксель на сайті передає сторонньому серверу медичні, фінансові або інші чутливі дані (напр. через URL).	Ризик витоку конфіденційної інформації, порушення законів (HIPAA, та ін.), судові позови.
Фішинг-розвідка через email-піксель	Зловмисник надсилає email з пікселем, відстежує відкриття і характеристики системи жертви.	Отримання розвідданих для подальшої атаки, підвищення ефективності фішингу.

Продовження Додатку 1

Матриця загроз, пов’язаних з трекінговими пікселями, та їхні потенційні наслідки

Вбудовування зловмисного пікселя (XSS/скрипт)	Хакер компрометує сайт або сторонній віджет, вставляє свій піксель, який збирає дані про користувачів.	Непомітний витік персональних даних до атакера, можливо – крадіжка облікових даних, сесій.
Накопичення даних без належного захисту	Компанія збирає великі обсяги даних через пікселі, але не шифрує і не обмежує доступ до них належним чином.	Масштабний витік даних у разі інциденту (зламу), фінансові та репутаційні втрати.
Невідповідність заявленій політиці (комплаєнс-ризик)	Компанія декларує одне (не продаємо дані), а пікселі роблять інше (діляться з третіми особами).	Регуляторні санкції (як у випадку Capital One), судові позови, втрати довіри.
Переслідування/ідентифікація користувачів	Дані пікселя використовуються для надмірного профілювання, злиття онлайн-даних з реальними особами.	Порушення анонімності, можливе небажане стеження за окремими людьми або групами (риск зловживань).
Пониження продуктивності і безпечності сайту	Надмірна кількість пікселів на сторінці сповільнює завантаження, створює більше цілей для атак (скрипти).	Гірший користувацький досвід, більша поверхня атаки (багато сторонніх підключень).

ДОДАТОК В

РЕКОМЕНДАЦІЇ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЗАКОННОСТІ ТА ПРОЗОРОСТІ

Рекомендований захід	Пояснення і обґрунтування
Отримати явну згоду користувача перед увімкненням пікселя.	До завантаження трекінгових пікселів необхідно запитати у користувача дозвіл (наприклад, через банер файлів cookie або інший інтерфейс згоди). Відповідно до GDPR, трекінгові пікселі можуть використовуватися лише за умови, що користувач дав явну згоду на таке відстеження. Якщо ж згоди немає або вона відкликана, сайт повинен блокувати завантаження пікселя. Такий підхід забезпечує як законність (наявність правової підстави – згоди), так і прозорість (користувач усвідомлює факт і обсяг трекінгу).
Надати зрозуміле повідомлення (банер) про використання пікселів.	Інформація про те, які трекінгові технології застосовуються на сайті, має бути донесена до користувача простою мовою. На банері або спливаючому вікні слід прямо зазначити, що сайт використовує cookies та пікселі для відстеження дій, пояснити мету (аналітика, маркетинг) та запропонувати вибір – прийняти чи відхилити такі трекери. Наявність чіткої попередньої інформації є вимогою принципу прозорості та чесної обробки.

Продовження Додатку 2

Рекомендації для забезпечення законності та прозорості

Оновити політику конфіденційності, включивши розділ про трекінгові пікселі.	Privacy Policy (політика конфіденційності) або політика використання файлів cookie повинна містити вичерпні відомості про використання трекінгових пікселів: які саме сторонні сервіси залучені (Google, Facebook тощо), які дані збираються через пікселі, з якою метою, протягом якого часу зберігаються, кому передаються. Рекомендується навести перелік конкретних третіх сторін і цілей збору. Це забезпечує вимогу прозорості (користувач може детально ознайомитися, що відбувається з його даними).
Не примушувати до згоди та забезпечити справедливість обробки.	Згода має бути добровільною: користувач повинен мати справжній вибір. Неприпустимо вимагати прийняти трекінгові пікселі як умову користування сервісом (заборона на “прив’язування” згоди до послуги). Також слід уникати *«темних шаблонів»* (інтерфейсних рішень, що маніпулюють вибором). Принцип справедливості означає, що обробка даних через пікселі не повинна вводити користувача в оману чи несприятливо для нього відбиватися.
Надати контактні дані для запитань щодо приватності.	В рамках принципу прозорості GDPR вимагає, щоб суб’єкт даних міг легко зв’язатися з контролером. Тому у повідомленні про конфіденційність варто зазначити контакти (email DPO чи відповідальної особи), за якими користувач може звернутися з питаннями про трекінгові технології на сайті. Це підвищує довіру та демонструє відкритість компанії.

ДОДАТОК Г

РЕКОМЕНДАЦІЇ ЩОДО ЗАХИСТУ ДАНИХ ПРИ ВИКОРИСТАННІ ТРЕКІНГОВИХ ПІКСЕЛІВ

Етап	Зміст етапу та ключові заходи
1. Інвентаризація та оцінка (виявлення трекерів)	На цьому початковому етапі проводиться повний аудит використання трекінгових пікселів в діяльності організації. Складається список всіх веб-сайтів, сторінок, застосунків, email-розсилок, де впроваджено трекінгові пікселі або схожі технології. Включаються як власні ресурси, так і сторонні (наприклад, пікселі в рекламних оголошеннях).Для кожного виявленого пікселя ідентифікується, яка третя сторона його обслуговує (Google, Meta, тощо), які дані він збирає (типові параметри або щось специфічне) та з якою метою використовується.Виконується оцінка правових підстав: чи є згода для кожного пікселя? якщо ні – чи можлива інша законна підстава (як правило, ні для ненеобхідних трекерів)? Визначаються потенційні ризики та невідповідності: напр., піксель X збирає дані без згоди, або передає дані в США без належних гарантій – ці моменти відразу фіксуються для усунення. Залучаються всі релевантні сторони: IT-відділ (для технічного переліку скриптів), маркетинг (для розуміння мети), юристи/DPO (для правової оцінки). Результатом етапу є карта трекінгових потоків даних і список проблем, що потребують вирішення.

2. Планування та дизайн рішення (розробка політики та архітектури)	На основі аудиту формується план впровадження контролів і дизайн архітектурного рішення. Розробляється або оновлюється Політика використання трекінгових технологій: документ, що описує, які трекери і для чого будуть використовуватись, як забезпечуються принципи GDPR, які права мають користувачі. Ця політика буде основою як для внутрішніх дій, так і для зовнішніх Privacy Notice.Проектується архітектура інтеграції пікселів з урахуванням приватності. Зокрема: вирішується, чи буде впроваджено CMP; чи потрібен проксі-сервер для зменшення передачі даних; де будуть точки контролю (на рівні фронтенду чи бекенду).Визначаються технічні вимоги: які налаштування внести (анонімізація IP, наприклад), яку платформу обрати (можливо, перейти на іншу аналітику), як зберігати згоди. Якщо організація – обробник (наприклад, розробник SaaS, що вбудовує свої пікселі клієнтам), то також враховується розмежування ролей: де відповідальність компанії, а де – її клієнтів-контролерів, і як їм надавати інструменти виконання GDPR.Встановлюються метрики успіху: як будемо вимірювати, що захищеність зросла? (напр., очікується, що 100% трекерів працюватимуть тільки після згоди; що час зберігання скоротиться до N; що проведено DPIA і ризики оцінено як прийнятні).

3. Впровадження технічних та організаційних заходів (реалізація контролів)	Це основний етап, де задумане перетворюється на практику. Він охоплює: Налаштування Consent Management Platform (CMP): вибір або розгортання CMP, конфігурація банерів згідно з розробленою політикою. Інтеграція CMP з сайтом/додатком, тестування, що до надання згоди пікселі не грузяться, а після надання – працюють. Встановлення ведення журналу згод. Конфігурація самих трекерів: у кожному залученому сервісі (GA, Facebook, тощо) вмикаються налаштування приватності – анонімізація IP, відключення збір гео/демографії, скорочені періоди зберігання, відмова від data sharing з іншими продуктами (наприклад, Google Ads), якщо такі опції є. Також реалізується механізм миттєвого відключення трекера при відкликанні згоди (через API CMP або свій код).Розгортання проксі/серверних компонентів (якщо передбачено дизайном): налаштовується сервер-посередник. Наприклад, ставиться власний endpoint, що імітує роботу пікселя, приймає дані від браузерів, а далі передає на сторонній API вже із очищеними даними. Це потребує розробки/налаштування, перевірки коректності відправки даних (щоб статистика не зламалася).Покращення безпеки: впроваджуються технічні засоби, описані в розділі 1.6: шифрування баз даних, оновлення політик безпеки на серверах, налаштування Content Security Policy для веб-сайту (дозволити звернення тільки до відомих доменів пікселів), встановлення

	контролю доступу співробітників до аналітичних систем (через IAM).Організаційні заходи: проводиться навчання персоналу (маркетингу, аналітики, розробників) новим політикам – як тепер додаємо пікселі тільки через погоджений процес, як реагувати на запити користувачів, що змінилося у щоденній роботі. Також укладаються/оновлюються договори з постачальниками (DPA, SCC) як було заплановано, готуються текстові оновлення Privacy Policy для публікації.Етап 3 є найбільш ресурсоємним, він часто розбивається на під-етапи за напрямками: фронтенд-розробка, бекенд, документи, навчання. Після завершення всіх робіт проводиться рев'ю: чи всі пікселі тепер працюють через новий механізм, чи нема лазівок.
4. Тестування та перевірка відповідності (аудит впровадження)	Після реалізації контролів необхідно пересвідчитись, що вони ефективні і нічого не пропущено. В рамках цього етапу виконується:Технічне тестування: інженери і/або зовнішні аудитори перевіряють сайт/додаток, використовуючи інструменти типу *CookieServe, trackers scanner*, щоб переконатися: жоден трекер не активується без згоди, усі призначені для блокування скрипти реально блокуються CMP. Перевіряються різні сценарії: новий користувач (без згоди), користувач, що дав часткову згоду, користувач, що відкликав згоду і т.д. Також перевіряється, що дані, які відправляються на зовнішні сервери, відповідають

	очікуванням (наприклад, IP прихований). У разі виявлення невідповідностей – повернення до етапу 3 для доопрацювання. Перевірка документів і прозорості: юридична команда оцінює, чи оновлена політика конфіденційності відповідає реальній практиці (наприклад, чи всі треті сторони згадані, чи правильні контактні дані DPO, чи описаний механізм згоди). Також проводиться “таємна” перевірка користувацького досвіду – чи зрозумілий банер згоди, чи легко знайти інформацію про права.Внутрішній аудит на відповідність GDPR: проводиться повторне зіставлення з контрольним списком GDPR-принципів (законність, мінімізація, та ін. – фактично перевірка розд.1). Наприклад: чи тепер усі цілі задокументовані? чи дані мінімізовані – що кажуть інженери? які строки зберігання встановлено – чи вписується в policy? чи закрито питання міжнародного трансферу – наявні SCC/шифрування? якщо все так – ставиться “галочка” про вирішення знайдених проблем з етапу 1.Data Protection Impact Assessment (DPIA) (при необхідності): якщо використання трекінгових пікселів вважалося високоризиковою обробкою (наприклад, масове відстеження поведінки користувачів), проводиться або оновлюється DPIA. У ній фіксуються впроваджені заходи зниження ризику і оцінюється залишковий рівень ризику. Якщо ризик все ще високий – консультуються з наглядовим органом.

5. Експлуатація та моніторинг (нагляд за дотриманням)	Коли нова система захисту запущена, важливо підтримувати її ефективність на постійній основі. Цей етап – безперервний процес, що включає: Моніторинг роботи пікселів: налаштовуються регулярні сканування або моніторингові скрипти, які сповіщають, якщо на сайті раптом з'явився новий трекер або існуючий працює не по правилам (напр., спробував установити cookie до згоди). Таким чином, організація буде одразу знати про відхилення і зможе реагувати.Обробка інцидентів та запитів: якщо станеться витік даних, пов'язаних з трекінгом, чи виявиться зловживання – включається процедура реагування (повідомлення DPA, користувачів тощо згідно ст.33-34 GDPR). Також відслідковуються запити суб'єктів: скільки надійшло, скільки виконано вчасно, чи не повторюються скарги на щось – це індикатор, що десь проблеми. Регулярний перегляд налаштувань: наприклад, раз на квартал або при оновленні SDK/скриптів трекерів, переглядаються налаштування – чи не додали провайдери нових функцій (які варто вимкнути), чи все ще оптимально наші параметри. Так само перегляд строків зберігання – чи не потрібно зменшити ще, чи виконується автолаяв. Підтримка актуальності знань серед персоналу: проводяться періодичні тренінги для нових співробітників і refresh для існуючих щодо правил роботи з трекінговими даними, нагадування про політики. Також KPI для відповідальних

	осіб можуть включати відсутність порушень процесу (наприклад, щоб маркетинг не додав новий піксель без погодження з DPO).Актуалізація згідно з новими вимогами: якщо змінюється законодавство або виходять нові керівні роз'яснення (від EDPB чи національних органів) щодо трекінгу, методика оперативно переглядається. Наприклад, впровадження підтримки Global Privacy Control (спеціального сигналу браузера про відмову від трекінгу) – якщо стане стандартом, то інтегруємо підтримку його в CMP. В результаті етапу 5 забезпечується сталий рівень захищеності і відповідності: захист даних стає не одноразовим проектом, а частиною повсякденної практики.
6. Оцінка ефективності та вдосконалення (цикл PDCA – план/дій/перевірки/корекції)	Цей заключний (і безперервний) етап зорієнтований на постійне покращення. Він включає: Вимірювання показників захищеності: компанія встановлює метрики (деякі були задані на етапі 2) і регулярно їх вимірює. Наприклад: частка користувачів, що дали згоду (і динаміка – чи не падає залученість через це), середній час життя даних (чи справді видаляємо за 14 міс.), кількість інцидентів чи скарг, результати періодичного аудиту (скільки невідповідностей знайдено). Такі показники можна звести у дашборд приватності. Порівняння "до і після": проводиться аналіз, наскільки знизилися ризики у порівнянні з початковим станом. Це і є відповідь на запитання про ефективність: наприклад, ризик витоку

	даних тепер оцінюється як низький замість високого; або рівень відповідності GDPR-принципам зріс з 50% до 95% (якісна оцінка, підтверджена чеклістом). У розділі 4 і 5 буде детальніше показано, як виміряти та виразити в відсотках покращення захищеності. Збір фідбеку та коригування: збирається зворотний зв'язок – як від внутрішніх команд (чи не надто ускладнилось їм життя, можливо є ідеї оптимізації), так і від користувачів (через опитування або аналіз поведінки – чи не надто багато відмов через банер, можливо варто покращити його UX). На основі цього вносяться зміни у методику: наприклад, спрощується текст повідомлень, додаються нові опції для гнучкості згоди, чи впроваджуються нові технології (скажімо, аналітика без cookie – у майбутньому, якщо дозволить функціонал, перейти на такий підхід, щоб менше залежати від згод).Звітність керівництву: результати виконання методики та покращення показників оформлюються у вигляді регулярних звітів (наприклад, раз на рік). У звіті можна відзначити, що, скажімо, ризик штрафу знизився на X%, довіра клієнтів зросла (якщо є такі дані), і що компанія знаходиться на високому рівні зрілості приватності. Етап 6 фактично "замикає коло", повертаючи нас до можливо нового циклу: знову оцінка ризиків, нові цілі і покращення. Методика таким чином стає циклічною (PDCA – Plan-Do-Check-Act).