УДК 343.2/.7(477)
DOI https://doi.org/10.24144/2307-3322.2024.84.3.38

ПРОБЛЕМА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В КІБЕРПРОСТОРІ

Аніщук В.В.,
кандидат юридичних наук, доцент, завідувач кафедри права
факультету бізнесу та права
Луцького національного технічного університету
ORCID: 0000-0002-9854-4932
e-mail: viktoriya.anishchuk@ukr.net

Аніщук В.В. Проблема захисту персональних даних в кіберпросторі.

У сучасному цифровому світі, де обсяг інформації, яка зберігається та обробляється в кіберпросторі, невпинно зростає, питання захисту персональних даних набуває все більшої актуальності. Персональні дані, такі як фінансова інформація, медичні записи, а також дані соціальних мереж, є цінним ресурсом, який може бути використаний як в легітимних цілях, так і для зловмисних дій. Незважаючи на постійне вдосконалення технологій безпеки, зростаюча складність кіберзагроз та еволюція методів кібератак створюють нові виклики для захисту персональної інформації.

У зв'язку з цим виникає необхідність аналізу сучасних проблем захисту персональних даних, зокрема правових, технічних та етичних аспектів цього питання.

Забезпечення безпеки персональних даних залишається актуальною проблемою сьогодення, адже дедалі більше людей користуються. Мережею Інтернет, проходять авторизацію на різних ресурсах, використовуючи для цього свої персональні дані, а також дедалі більше різних установ створюють своєрідні бази даних, не завжди дбаючи про їх схоронність. Недостатня міра забезпечення безпеки персональних даних у кіберпросторі призводить до надмірної активності кібератак та вчинення різних махінацій із персональними даними. Актуальність теми захисту персональних даних в кіберпросторі обумовлена кількома важливими факторами, які мають значний вплив на сучасне суспільство, економіку та безпеку. Основні аспекти, що підкреслюють актуальність цього питання: зростання цифровізації; кіберзагрози; законодавчі вимоги; соціальна відповідальність і довіра; економічні наслідки; технологічні виклики; міжнародні відносини та геополітика. Таким чином, актуальність теми захисту персональних даних в кіберпросторі зумовлена складністю та глобальним характером цього питання, а також його важливістю для збереження приватності, безпеки та довіри в цифровому світі.

Дана стаття спрямована на дослідження ключових викликів у сфері захисту персональних даних в кіберпросторі, а також надання рекомендацій щодо підвищення рівня безпеки та мінімізації ризиків витоку інформації.

Ключові слова: персональні дані, Мережа Інтернет, кіберпростір, безпека, кібератака.

Anishchuk V.V. The Problem Of Personal Data Protection In Cyber Space.

In today's digital world, where the amount of information that is stored and processed in cyberspace is constantly growing, the issue of personal data protection is becoming more and more relevant. Personal data, such as financial information, medical records, and social media data, is a valuable resource that can be used for both legitimate and malicious purposes. Despite the continuous improvement of security technologies, the growing complexity of cyber threats and the evolution of cyber attack methods create new challenges for the protection of personal information.

In this connection, there is a need to analyze the modern problems of personal data protection, in particular the legal, technical and ethical aspects of this issue.

Ensuring the security of personal data remains an urgent problem today, because more and more people use it. On the Internet, they pass authorization on various resources, using their personal data for this purpose, and more and more different institutions create peculiar databases, not always taking

care of their safety. The insufficient measure of ensuring the security of personal data in cyberspace leads to excessive activity of cyberattacks and the commission of various manipulations with personal data. The relevance of the topic of personal data protection in cyberspace is due to several important factors that have a significant impact on modern society, economy and security. The main aspects that emphasize the relevance of this issue: the growth of digitalization; cyber threats; legal requirements; social responsibility and trust; economic consequences; technological challenges; international relations and geopolitics. Thus, the relevance of the topic of personal data protection in cyberspace is due to the complexity and global nature of this issue, as well as its importance for preserving privacy, security and trust in the digital world.

This article is aimed at researching key challenges in the field of personal data protection in cyberspace, as well as providing recommendations for increasing the level of security and minimizing the risks of information leakage.

Key words: personal data, Internet, cyberspace, security, cyber attack.

Постановка проблеми. В умовах сучасності, використання Мережі Інтернет, різних застосунків та ведення електронних комп'ютерних баз даних є дуже зручним. Ви можете оперативно знайти потрібну інформацію, здійснити онлайн-шопінг, скористатися різними освітніми та іншими послугами тощо. Проте, необхідно дотримуватися певних правил поводження із персональними даними, аби забезпечити їх безпеку та схоронність. Персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [1].

Стан опрацювання проблематики. Проблеми захисту персональних даних в кіберпросторі досліджували багато науковців з різних дисциплін, включаючи інформатику, право, соціологію та етику. Ось кілька відомих дослідників і їхній внесок у цю сферу:

1. Брюс Шнайєр. Один із провідних експертів у галузі криптографії та комп'ютерної безпеки. Його праці стосуються питань захисту даних, приватності та кібербезпеки, зокрема, проблеми управління ризиками та захисту від кібератак.
2. Даніель Солове. Професор права в Університеті Джорджа Вашингтона, відомий своїми дослідженнями у сфері конфіденційності та захисту персональних даних. Його роботи аналізують правові та соціальні аспекти приватності в цифрову еру.
3. Гелен Ніссенбаум. Вчена з філософії та етики, яка досліджує питання конфіденційності та етики в інформаційному суспільстві. Вона ввела концепцію «контекстуальної цілісності», яка пояснює, як контекстуальні норми впливають на очікування приватності.
4. Рос Андерсон. Професор безпеки в комп'ютерних системах в Кембриджському університеті. Його дослідження охоплюють широкий спектр питань кібербезпеки, включаючи захист персональних даних та розробку безпечних систем.
5. Шошана Зубофф. Професорка Гарвардської бізнес-школи, авторка книги «Епоха спостережуваного капіталізму». Її дослідження зосереджені на впливі великих даних та цифрових технологій на приватність і соціальне життя.

Ці науковці зробили значний внесок у розуміння проблем захисту персональних даних в кіберпросторі, їхні дослідження є важливим джерелом для подальших розробок у цій галузі. Серед українських науковців також є фахівці, які досліджують питання захисту персональних даних у кіберпросторі. Ці науковці роблять важливий внесок у розвиток наукових досліджень з проблем захисту персональних даних в Україні та мають великий вплив на формування національної політики в галузі кібербезпеки, серед них:

1. Володимир Горбулін. Академік Національної академії наук України, відомий своїми дослідженнями у сфері національної безпеки, зокрема в контексті кібербезпеки та захисту інформаційних ресурсів. Він також є автором численних публікацій з питань кіберзагроз і захисту критичної інформаційної інфраструктури.
2. Олександр Шульга. Доктор технічних наук, професор, фахівець у галузі інформаційної безпеки. Його дослідження зосереджені на питаннях криптографії, захисту інформаційних систем та захисту персональних даних в умовах кіберзагроз.
3. Ірина Прозорова. Доктор юридичних наук, професор, спеціаліст у галузі права інформаційних технологій. Вона досліджує правові аспекти захисту персональних даних, зокрема законодавче регулювання та міжнародний досвід.

4. Валентин Петрук. Доктор технічних наук, професор, спеціалізується на кібербезпеці та захисті інформації. Його праці присвячені питанням захисту персональних даних, особливо в контексті захисту від внутрішніх загроз і розробки політик безпеки.

5. Олександр Карпенко. Кандидат юридичних наук, доцент, який займається дослідженням правових аспектів кібербезпеки та захисту персональних даних. Його роботи стосуються правового регулювання кіберпростору, зокрема в українському контексті.

Мета статті. Дана стаття спрямована на дослідження ключових викликів у сфері захисту персональних даних в кіберпросторі, а також надання рекомендацій щодо підвищення рівня безпеки та мінімізації ризиків витоку інформації.

Виклад основного матеріалу. З появою всесвітньої мережі з'явились і проблеми захисту інформації в ній, адже Інтернет та інформаційна безпека несумісні за своєю природою. Відомо, що чим легший доступ в мережу, тим гіршою є її інформаційна безпека. Користувач може навіть не дізнатися, що його дані були скопійовані, змінені або навіть зіпсовані [2]. Недостатня міра забезпечення безпеки розробниками різних інтернет-ресурсів, відсутність необхідного рівня обізнаності користувачів та навпаки обізнаність шахраїв стають прямими передумовами порушення безпеки персональних даних користувачів.

В Україні питання захисту персональних даних регулюється низкою нормативно-правових актів. Закон України «Про захист персональних даних» від 1 червня 2010 року є ключовим нормативним актом, що регулює обробку персональних даних в Україні. Він визначає права та обов'язки суб'єктів і контролерів даних, процедури збору, зберігання, використання та розповсюдження персональних даних, а також вимоги до їх захисту. Закон також передбачає адміністративну та кримінальну відповідальність за порушення законодавства у сфері захисту персональних даних. Конституція України у статті 32 гарантує право на недоторканність приватного життя, захист особистої та сімейної таємниці, а також забороняє збирання, зберігання, використання та поширення конфіденційної інформації без згоди особи. Цивільний кодекс України у статтях 301 та 302 визначає право особи на захист своєї особистої інформації та передбачає право на ознайомлення з інформацією про себе, яка збирається іншими особами. Кримінальний кодекс України у статті 182т встановлює кримінальну відповідальність за незаконний збір, зберігання, використання або поширення конфіденційної інформації про особу без її згоди. Закон України «Про інформацію» від 2 жовтня 1992 року визначає правові основи інформаційних відносин і захисту інформації в Україні. Закон встановлює права на доступ до інформації, її захист, а також порядок доступу до персональних даних. Закон України «Про доступ до публічної інформації» від 13 січня 2011 року регулює питання доступу до публічної інформації, яка знаходиться у володінні органів державної влади та місцевого самоврядування. При цьому, закон передбачає захист персональних даних, які можуть міститися в публічних реєстрах. Закон України «Про електронні довірчі послуги» від 5 жовтня 2017 року регулює надання електронних довірчих послуг, включаючи електронний підпис і електронну ідентифікацію, які мають важливе значення для захисту персональних даних в електронному середовищі. Розпорядження Кабінету Міністрів України від 14 грудня 2016 р. № 920-р «Про схвалення Концепції розвитку кібербезпеки України» визначає стратегію розвитку кібербезпеки в Україні, включаючи захист персональних даних від кіберзагроз. Постанова Кабінету Міністрів України від 25 травня 2011 р. № 616 «Про затвердження Порядку здійснення державного контролю за додержанням законодавства про захист персональних даних» встановлює порядок здійснення державного контролю за додержанням законодавства у сфері захисту персональних даних. Ці нормативні акти разом утворюють основу для захисту персональних даних в Україні, регулюючи як права суб'єктів даних, так і обов'язки осіб, що обробляють ці дані.

Актуальною на наш погляд, в умовах сьогодення є проблема безпеки персональних даних при використанні інтернет-банкінгу. Користувачам слід частіше змінювати паролі до застосунків банку, не повідомляти його нікому, не переходити ні за якими посиланнями, якщо їх надіслав не офіційний представник банку, а також утримуватися від прив'язування банківських карт до різних застосунків. Проте, й самі банківські установи інколи збирають надлишкову інформацію про клієнта.

Ще однією площиною кіберпростору, яка вимагає забезпечення безпеки персональних даних є різноманітні реєстри та бази даних. На нашу думку, вони повинні мати досконалу систему захисту від зовнішнього втручання, яка складається із кількох етапів, лише так вони можуть гарантувати інформаційну безпеку та уникати несанкціонових втручань, і як наслідок – витоку інформації.

Забезпечення безпеки особистості – досить актуальне завдання для держави й суспільства. Це завдання загострюється у зв'язку із внутрішніми та зовнішніми обставинами [3]. В умовах сьогодення, на нашу думку, питання забезпечення схоронності персональних даних в кіберпросторі постає досить гостро, в тому числі внаслідок російської агресії проти України. В зв'язку із цим, не рекомендовано відвідувати будь-які інтернет-ресурси країни-агресора, а також не користуватися застосунками вказаного вище розробника, адже агресія росії проявляється не лише у яскраво виражених воєнних діях на території України, а й у значних кібератаках.

Щодня, в світі, в силу його шаленого темпу розвитку, з'являється дуже багато різних можливостей у кіберпросторі, більшість із них, відповідно потребують збору та обробки ваших персональних даних. Варто зауважити, що ні приписи норм законодавства, ні інші важелі суспільного впливу не зможуть забезпечити абсолютну безпеку ваших персональних даних у кіберпросторі, адже витік інформації може статися навіть тоді, коли ви про це не здогадуєтеся.

Потрібно стежити за своїми персональними даними і дотримуватися певних правил при користуванні мережею Інтернет:

1. Уважно вивчати угоди про обробку персональних даних на сайтах, якими користуєтеся.
2. Не довіряти важливу інформацію сайтам, які не містять угоди про обробку персональних даних.
3. Не прив'язувати банківську карту до платіжної системи сайту при користуванні послугами електронної комерції.
4. Обов'язково звертатися до відповідних контролюючих органів при виявленні порушень законодавства в сфері захисту персональних даних [4].

Крім вказаного вище, вважаємо, що необхідно повністю виключити використання безоплатного, незахищеного паролем Wi-Fi, оскільки є великі ризики несанкціонованого втручання у ваш пристрій, що може мати дуже негативні наслідки, починаючи з зараження вашого пристрою різноманітними вірусами і закінчуючи викраденням ваших даних, розповсюдженням конфіденційної інформації тощо. Також, на усіх можливих ресурсах, де ви реєструєтесь, слід встановлювати надійні паролі, використовувати двофакторну автентифікацію, бути уважними при наданні своїх персональних даних, не відкривати сумнівних повідомлень та не переходити за підозрілими посиланнями, використовувати надійне антивірусне забезпечення, створювати резервні копії даних.

Захист персональних даних вимагає комплексного підходу, який охоплює як технічні, так і організаційні заходи. До основних шляхів забезпечення захисту персональних даних можна віднести:

1. Технічні заходи:

- Шифрування: Використання криптографічних алгоритмів для захисту даних під час їх передачі та зберігання, що робить їх недоступними для сторонніх осіб у разі перехоплення.
- Аутентифікація та авторизація: Впровадження системи багатофакторної аутентифікації (MFA) для забезпечення доступу до даних лише уповноваженим користувачам. Авторизація визначає, які дії можуть виконувати користувачі з даними.
- Захист мережі: Використання міжмережевих екранів (фаєрволів), системи виявлення та запобігання вторгненням (IDS/IPS), а також VPN для захисту мережевих комунікацій.
- Моніторинг і аудит: Впровадження систем моніторингу для відстеження підозрілої активності та проведення регулярних аудитів безпеки для виявлення та усунення потенційних вразливостей.
- Резервне копіювання: Регулярне створення резервних копій даних, щоб забезпечити їх збереження у випадку атаки, збою чи втрати інформації.

2. Організаційні заходи:

- Політики безпеки: Розробка та впровадження внутрішніх політик захисту персональних даних, які включають правила поводження з даними, інструкції щодо зберігання та обробки, а також процедури у разі витоку інформації.
- Навчання персоналу: Проведення регулярного навчання для працівників щодо важливості захисту персональних даних і методів запобігання витокам, зокрема через соціальну інженерію та фішингові атаки.
- Контроль доступу: Обмеження доступу до персональних даних тільки тим працівникам, які мають відповідні повноваження, а також регулярний перегляд і оновлення прав доступу.
- Відповідність законодавству: Забезпечення дотримання міжнародних та національних стандартів і норм захисту персональних даних (наприклад, GDPR у Європейському Союзі) для мінімізації правових ризиків.

• Управління ризиками: Виявлення, оцінка та управління ризиками, пов'язаними з обробкою персональних даних, з метою зниження ймовірності витоку або втрати даних.

3. Етичні та правові заходи:

• Прозорість: Забезпечення прозорості в обробці персональних даних, щоб користувачі знали, які дані збираються, з якою метою і як вони будуть використовуватися.

• Згода користувача: Отримання чіткої і однозначної згоди від користувачів на обробку їхніх даних, з можливістю відкликання цієї згоди в будь-який момент.

• Право на забуття: Забезпечення права користувачів на видалення їхніх даних з бази, якщо ці дані більше не потрібні для обробки або користувач відкликав свою згоду.

• Оцінка впливу на приватність: Проведення оцінки впливу на приватність (Privacy Impact Assessment) при впровадженні нових технологій або зміні процесів обробки даних.

Застосування цих заходів у комплексі може значно підвищити рівень захисту персональних даних і допомогти мінімізувати ризики витоку або несанкціонованого доступу.

Висновок. Таким чином, вживаючи самостійно ряд заходів для забезпечення безпеки ваших персональних даних у кіберпросторі, ви тим самим забезпечуєте безпеку своєї особистості, фінансів та репутації від неправомірних посягань на скільки це можливо.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.
2. Землянська О.В., Праховнік Н.А., Ковтун А.І., Ковтун М.А. Безпека в Інтернеті та захист персональних даних. *Збірник Всеукраїнської науково-практичної конференція «Безпека життя і діяльності людини: теорія та практика»*, 28.04.2022. Полтава, 2022. С. 62–64.
3. Зелений Б. Р. Безпека особистості в умовах глобалізації. *Безпека життя і діяльності людини: теорія та практика : збірник наук. праць Всеукр. наук.-практ. конф., присвяченої Всесвітнім Дням цивільної оборони та охорони праці*. Полтава : ПНПУ імені В.Г. Короленка, 2020. С. 165–168.
4. Воловик Б.П., Томчук М.А.. Безпека персональних даних в мережі інтернет. *Матеріали науково-практичної конференції «Якість і безпека. Сучасні реалії»,* ВНТУ, 2019. С. 11–13.