ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ В. Н. КАРАЗІНА

СОЦІОЛОГІЧНИЙ ФАКУЛЬТЕТ

Кафедра прикладної соціології та соціальних комунікацій

Пояснювальна записка

до кваліфікаційної роботи

на тему

«ЗАХИСТ ДАНИХ ТА ВПЛИВ НА ДОВІРУ СПОЖИВАЧІВ ДО ОНЛАЙН-СЕРВІСІВ»

Виконала студентка 4 курсу групи ЗССК-44
першого (бакалаврського) рівня вищої освіти
спеціальності 054 Соціологія
Каліба Яна Вячеславівна
Керівник: д.соц.н., проф. Л.М. Хижняк

Харків – 2024

ЗМІСТ

ВСТУП

Актуальність роботи. В епоху цифрових технологій та глобалізації Інтернету онлайн-сервіси стали невід'ємною частиною повсякденного життя. Сьогодні ми здійснюємо покупки, управляємо фінансами, спілкуємося з друзями та родичами, здобуваємо освіту та отримуємо медичні послуги, не виходячи з дому. Однак разом зі зручністю та доступністю зростає й важливість захисту особистих даних користувачів. Захист даних стає однією з ключових проблем сучасного суспільства, оскільки кіберзагрози постійно еволюціонують і становлять серйозну небезпеку для конфіденційності та безпеки інформації. Витоки даних, кібератаки та шахрайство можуть не лише завдати фінансових збитків, але й підірвати довіру споживачів до онлайн-сервісів. Довіра є критичним елементом у відносинах між користувачами та постачальниками послуг, і її втрата може мати довгострокові негативні наслідки для бізнесу.

Стан розуміння поняття довіри в соціальній психології досліджено в роботах таких авторів як Антоненко (2004), Веселов (2004), Журавльов та Сумарокова (1998), Купрейченко (2008), Скрипкіна (2000), Шрадер (2004), Bachmann та Zaheer (2006), Kramer (1999). Інші дослідження, що проводилися в рамках соціальної психології, психології комунікації, психології маркетингу і реклами, також приділяють значну увагу проблемі довіри (Morgan та Hunt, 1994; Lee та Moray, 1992; Lewandowsky та ін., 2000).

Хоча важливість визначення поняття довіри отримала визнання від різних науковців, розбіжності у визначенні та характеристиках цього поняття, а також його впливу на досвід споживачів і результати, виявлені дослідниками. Mayer, Davis та Schoorman (1995) вказали на труднощі у визначенні довіри, такі як:

- недолатність чітко визначити відмінності між вірою і ризиком;
- складні питання взаємодії між сторонами, які формують довіру, та тими, які їй довіряють.

Мета даної дипломної роботи полягає у вивченні взаємозв'язку між захистом даних та рівнем довіри споживачів до онлайн-сервісів. Для досягнення цієї мети буде проаналізовано сучасні методи та інструменти захисту даних, а також проведено дослідження впливу цих заходів на формування та підтримання довіри користувачів. Особливу увагу буде приділено правовим аспектам захисту даних, а також найкращим практикам у цій сфері.

Завдання роботи:

1. Провести огляд сучасних методів та інструментів захисту даних.
2. Вивчити правові аспекти захисту даних в контексті онлайн-сервісів.
3. Дослідити вплив заходів із захисту даних на довіру споживачів.
4. Проаналізувати статистичні дані щодо інцидентів витоку даних та їх впливу на репутацію онлайн-сервісів.
5. Провести опитування користувачів онлайн-сервісів для виявлення їхньої думки про важливість захисту даних.
6. Розробити рекомендації для покращення заходів із захисту даних.
7. Оцінити ефективність існуючих практик захисту даних у контексті збереження довіри споживачів.
8. Підготувати висновки та узагальнити результати дослідження.

Практичне значення роботи полягає у розробці конкретних рекомендацій для онлайн-сервісів щодо покращення заходів із захисту даних, що сприятиме підвищенню рівня довіри споживачів. Отримані результати можуть бути використані для вдосконалення політик та процедур безпеки, що дозволить мінімізувати ризики витоку даних та кібератак. Аналіз правових аспектів забезпечить краще розуміння вимог законодавства у сфері захисту даних, що допоможе компаніям відповідати нормативним вимогам та уникати юридичних проблем. Рекомендації щодо комунікації з користувачами та прозорості дій у разі інцидентів із безпекою допоможуть зміцнити довіру споживачів та підтримати репутацію компаній на високому рівні. Впровадження запропонованих заходів сприятиме підвищенню конкурентоспроможності онлайн-сервісів на ринку, що постійно змінюється та вимагає високих стандартів безпеки.

Методи дослідження включають аналіз наукової літератури та правових документів для вивчення сучасних методів та інструментів захисту даних, а також правових аспектів цього питання. Статистичний аналіз використовується для оцінки даних про інциденти витоку інформації та їх вплив на довіру споживачів. Порівняльний аналіз дозволяє оцінити ефективність різних підходів до захисту інформації та їх вплив на довіру споживачів. Синтез отриманих даних та розробка рекомендацій здійснюються для узагальнення результатів дослідження та формування практичних порад для онлайн-сервісів.

Новизна роботи полягає у комплексному підході до вивчення взаємозв'язку між захистом даних та довірою споживачів до онлайн-сервісів, що враховує як технічні, так і правові аспекти захисту інформації. Дослідження поєднує аналіз сучасних методів кібербезпеки з вивченням реальних випадків витоку даних та їх впливу на користувачів, що дозволяє отримати глибше розуміння проблеми.

Структура роботи. Робота складається з двох розділів, висновків до них, списку використаних джерел.

РОЗДІЛ 1. ЗАХИСТ ДАНИХ І ДОВІРА СПОЖИВАЧІВ ДО ОНЛАЙН-СЕРВІСІВ: ТЕОРЕТИЧНИЙ АСПЕКТ ДОСЛІДЖЕННЯ

Розділ 1 присвячений аналізу основних теоретичних підходів до захисту даних та вивченню факторів, що впливають на формування довіри споживачів до онлайн-сервісів. У цьому розділі розглянуто поняття та принципи захисту даних, проаналізовано сучасні загрози та виклики, з якими стикаються користувачі та постачальники онлайн-послуг. Також досліджено ключові елементи довіри споживачів та їх взаємозв'язок із рівнем захисту інформації.

Особлива увага приділена розгляду правових аспектів захисту даних, а також аналізу міжнародних стандартів та регуляторних вимог, що регламентують цю сферу. Крім того, у розділі представлено огляд основних методів та технологій, що використовуються для забезпечення безпеки даних у цифровому середовищі.

1.1. Поняття захисту даних у контексті онлайн-сервісів та право на інформацію і захист даних в розвитку електронних комунікацій

Поняття захисту даних у контексті онлайн-сервісів охоплює широкий спектр заходів і методів, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації, яку користувачі передають, зберігають або обробляють у цифровому середовищі. Це включає технічні засоби, такі як шифрування, автентифікація, контроль доступу, а також організаційні заходи, наприклад, політики безпеки, навчання персоналу та регулярний аудит систем захисту. Онлайн-сервіси, зокрема електронні комунікації, стикаються з численними викликами, пов'язаними з кібератаками, витоками даних, несанкціонованим доступом та іншими загрозами, що вимагає постійного вдосконалення та адаптації засобів захисту. Право на інформацію та захист

даних у розвитку електронних комунікацій є ключовим аспектом сучасного інформаційного суспільства, оскільки користувачі мають право знати, як їхні дані збираються, обробляються та використовуються. Законодавчі акти, такі як Загальний регламент про захист даних (GDPR) в Європейському Союзі, встановлюють жорсткі вимоги щодо прозорості, прав доступу та контролю над особистими даними, а також передбачають суворі санкції за порушення цих вимог [2]. Важливим аспектом є також забезпечення балансу між правом на інформацію і необхідністю захисту даних у контексті надання онлайн-послуг. З одного боку, користувачі повинні мати можливість вільно доступати до необхідної інформації, з іншого – їхні особисті дані мають бути надійно захищені від несанкціонованого доступу та зловживань. Таким чином, забезпечення захисту даних у контексті онлайн-сервісів є комплексним процесом, який вимагає інтегрованого підходу, що враховує технічні, організаційні та правові аспекти [11].

Цей інтегрований підхід до захисту даних вимагає тісної співпраці між розробниками технологій, постачальниками онлайн-сервісів, правовими органами та користувачами. Розробники технологій повинні впроваджувати сучасні засоби безпеки на всіх етапах створення та експлуатації програмного забезпечення, забезпечуючи надійний захист від новітніх загроз. Постачальники онлайн-сервісів зобов'язані не лише дотримуватися законодавчих вимог, але й активно комунікувати з користувачами щодо політик конфіденційності та процедур захисту даних. Правові органи повинні створювати та підтримувати нормативно-правову базу, яка б стимулювала дотримання високих стандартів безпеки та відповідальність за порушення. Користувачі, своєю чергою, повинні бути обізнані про свої права та засоби захисту особистої інформації, що передбачає необхідність проведення освітніх кампаній та підвищення рівня кіберграмотності населення [5]. У контексті розвитку електронних комунікацій важливим є також впровадження міжнародних стандартів захисту даних, що забезпечить уніфікацію підходів до безпеки інформації та підвищить довіру до онлайн-сервісів на глобальному рівні. Це особливо актуально в умовах

глобалізації та зростаючої взаємозалежності економік, де міжнародні транзакції та обмін інформацією стають буденним явищем. Важливо зазначити, що ефективний захист даних сприяє не лише підвищенню довіри споживачів, але й загальному розвитку цифрової економіки, оскільки забезпечує стабільність і безпеку інформаційного простору. Таким чином, захист даних у контексті онлайн-сервісів та право на інформацію і захист даних у розвитку електронних комунікацій є взаємопов'язаними аспектами, які вимагають комплексного підходу, інтеграції сучасних технологічних рішень та ефективної правової регуляції для забезпечення сталого та безпечного розвитку цифрового суспільства.

и, що допомагає запобігати несанкціонованому доступу та маніпуляціям з інформацією.

У правовому контексті захист даних регламентується низкою міжнародних і національних актів. Зокрема, Загальний регламент про захист даних (GDPR) встановлює суворі вимоги до збору, обробки та зберігання персональних даних у країнах Європейського Союзу. GDPR зобов'язує компанії дотримуватися принципів законності, справедливості та прозорості, забезпечувати точність даних, мінімізувати обробку даних та впроваджувати належні заходи безпеки. Крім того, регламент визначає права суб'єктів даних, такі як право на доступ до своїх даних, право на виправлення неточностей, право на видалення даних ("право бути забутим") та право на обмеження обробки [7].

Національні законодавства також відіграють важливу роль у забезпеченні захисту даних. Наприклад, Закон України "Про захист персональних даних" встановлює вимоги до обробки персональних даних в Україні та передбачає відповідальність за порушення цих вимог. У Сполучених Штатах діє закон Каліфорнії про захист прав споживачів (CCPA), який надає жителям штату значні права на контроль за своїми даними та накладає на компанії обов'язок щодо їх захисту.

Важливою складовою ефективного захисту даних є також моніторинг і виявлення загроз. Використання сучасних систем моніторингу, таких як системи

виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS), дозволяє оперативно виявляти та реагувати на підозрілі активності в мережі. Крім того, застосування машинного навчання та штучного інтелекту в аналізі великих обсягів даних допомагає ідентифікувати нові види загроз і підвищити ефективність захисту.

Управління інцидентами також є ключовим аспектом захисту даних. Процеси реагування на інциденти включають виявлення, аналіз, стримування, усунення та відновлення після інцидентів. Розробка планів реагування на інциденти та їх регулярне тестування допомагає підготуватися до можливих атак та мінімізувати їхній вплив на організацію.

Загалом, інтеграція технічних заходів, правового регулювання, моніторингу та управління інцидентами формує цілісну систему захисту даних, яка не тільки забезпечує безпеку інформації, але й підвищує довіру споживачів до онлайн-сервісів. Високий рівень довіри, у свою чергу, сприяє зростанню кількості користувачів та розвитку цифрової економіки, що є важливим фактором успішного функціонування сучасного інформаційного суспільства [4].

Згідно з першою редакцією Закону України "Про інформацію", інформація вважалася систематизованими, документованими, публічно оголошеними або іншим чином розповсюдженими відомостями про суспільне, державне життя та природне середовище. У новій редакції цього Закону це поняття визначено як будь-які дані чи відомості, які можуть зберігатися на матеріальних носіях або відображатися в електронному вигляді.

Інформація має свої характеристики [2]:

- Цінність - оцінюється за можливістю досягнення мети, для якої отримувач використовує її.
- Достовірність - відображає ступінь відповідності інформації реальності.
- Актуальність - визначається за відповідністю цінності та достовірності інформації поточному часу.

З точки зору інформаційної безпеки, інформація має такі характеристики:

- Конфіденційність - характеризується неможливістю доступу неавторизованих користувачів до неї.
- Цілісність - вказує на неможливість модифікації інформації несанкціонованими користувачами.
- Доступність - визначає можливість отримання інформації авторизованими користувачами в необхідний для них час із належними повноваженнями.

Іноді також виділяють властивість інформації, яка називається спостережністю, що означає постійний контроль за нею на всіх етапах обробки та передавання.

Інформаційна безпека в контексті безпосередньої діяльності щодо захисту інформації включає комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення даних.

Інформаційна безпека може розглядатись з точки зору безпеки держави, організації та особистості. Щодо держави, інформаційна безпека означає стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається заподіяння шкоди. Ця шкода може виникати з причин неповності, невчасності та невірогідності використаної інформації, негативного впливу інформації, негативних наслідків використання інформаційних технологій, а також через несанкціоноване розповсюдження, використання та порушення цілісності, конфіденційності та доступності інформації [1].

Щодо організації, інформаційна безпека передбачає спрямовану діяльність її органів та посадових осіб з використанням дозволених сил і засобів з метою досягнення стану захищеності інформаційного середовища. Ця діяльність має забезпечити нормальне функціонування і розвиток організації.

Інформаційна безпека особистості визначається як захист від негативних впливів інформації та здатність особи використовувати її безпечно. Це також охоплює захист соціальних груп, до яких вона належить. Згідно з українським законодавством, проблема інформаційної безпеки на рівні держави має

вирішуватися шляхом створення інформаційної інфраструктури, координації дій державних органів, покращення нормативно-правового поля та розвитку національної системи конфіденційного зв'язку. Для цього передбачається використання законодавчих актів, міжнародних стандартів ISO та розробок власних заходів. Для реалізації цих заходів має бути створена комплексна система захисту інформації і система управління інформаційною безпекою.

До органів, що відповідають за забезпечення інформаційної безпеки, належать різні структури:

- Спеціальні служби держави, які відповідають за захист інформації.
- Уповноважений орган держави з питань захисту інформації: Державна служба спеціального зв’язку та захисту інформації України.
- Національний координаційний центр кібербезпеки.
- Міжвідомча комісія з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України.

З 1 липня 2015 року Державний центр кіберзахисту та протидії кіберзагрозам розпочав свою роботу в межах Державної служби спеціального зв’язку та захисту інформації України, що було створено на базі Державного центру захисту інформаційно-телекомунікаційних систем Держспецзв’язку [10].

У системі е-урядування органи, які забезпечують інформаційну безпеку, включають:

- Державне агентство з питань електронного урядування України.
- Державна служба спеціального зв’язку та захисту інформації України.
- Міністерство юстиції України, щодо роботи з електронними цифровими підписами.
- Підрозділ з інформаційного забезпечення органу публічного управління, який також відповідає за створення і підтримання систем управління інформаційною безпекою в системі е-урядування.

Необхідно також створити умови для залучення підприємств, установ та організацій незалежно від форми власності, які діють у сфері електронних

комунікацій та захисту інформації, до забезпечення кібербезпеки України. Це має включати в себе введення обов’язкових заходів щодо захисту інформації та кіберзахисту відповідно до законодавства, а також сприяння державою цьому процесу.

1.2. Роль кібербезпеки у формуванні довіри споживачів

Кібербезпека відіграє значущу роль у формуванні довіри споживачів до онлайн-сервісів. Забезпечення безпеки та конфіденційності персональних даних споживачів є ключовим фактором у їхньому рішенні щодо використання цих сервісів. Негативні наслідки порушення кібербезпеки, такі як крадіжки особистої інформації, фінансові шахрайства та інші злочинні дії, можуть серйозно підірвати довіру споживачів. Заходи з кібербезпеки, такі як захист від хакерських атак, шифрування даних та ефективна система виявлення і реагування на загрози, демонструють зобов'язання сервісних компаній щодо безпеки даних споживачів і сприяють підвищенню рівня їхньої довіри до цих сервісів.

У недавньому дослідженні, проведеному KPMG International, 1 881 керівників світових компаній були опитані, а також проведено серію обговорень з керівниками та експертами компаній з різних країн. Метою було вивчити, наскільки вище керівництво компаній розуміє свої виклики та які кроки ще потрібно зробити. Також у дослідженні досліджується роль директорів з інформаційної безпеки (CISO) у допомозі керівництву компаній, а також визначаються п'ять найважливіших кроків у побудові довіри через кібербезпеку та конфіденційність [14].

Довіра у цифровому світі полягає у впевненості зацікавлених сторін у здатності організацій використовувати цифрові технології для захисту своїх інтересів та відповідності суспільним очікуванням та цінностям. Керівництво компаній очікує покращення прибутковості, утримання клієнтів та міцніших комерційних відносин від інвестицій у побудову довіри через кібербезпеку та конфіденційність. Багато організацій планують впровадження нових цифрових

інструментів у наступні роки, проте кожна нова цифрова ініціатива створює потенційні вразливості та репутаційні ризики.

Клієнти та суспільство очікують, що співпраця з організаціями, які регулярно зіштовхуються з викликами уразливостей своїх ланцюжків поставок від кібератак, будуватиметься на надійності та професіоналізмі. Війна в Україні ще раз підкреслила важливість кібербезпеки та довіри в цифровому світі, підкресливши необхідність формування кіберкультури на всіх рівнях організацій, а також розширивши роль директора з інформаційної кібербезпеки (CISO).

Довіра в цифровому середовищі означає переконаність зацікавлених сторін у здатності організацій ефективно використовувати цифрові технології для захисту своїх інтересів та відповідності суспільним очікуванням та цінностям. Керівництво компаній розраховує на підвищення прибутковості, зміцнення відносин з клієнтами та партнерами за рахунок інвестицій у побудову відповідного рівня довіри на підприємстві, що оперує даними. Багато організацій намічають впровадження нових цифрових інструментів, проте кожна така ініціатива призводить до потенційних вразливостей та ризиків для репутації [15].

Клієнти та суспільство очікують, що співпраця з організаціями, які регулярно стикаються з викликами вразливостей своїх ланцюжків поставок через кібератаки, будується на надійності та професіоналізмі. Повномасштабна війна в Україні підкреслила це, підвищивши значення кібербезпеки та довіри в цифровому просторі та підкресливши важливість формування кіберкультури на всіх рівнях організацій, а також розширивши роль директора з інформаційної кібербезпеки (CISO).

У новому глобальному звіті KPMG Cyber Trust Insights 2022 визначено п'ять ключових кроків до побудови довіри за допомогою кібербезпеки: усвідомлення важливості кібербезпеки та конфіденційності як необхідної складової бізнесу, створення внутрішніх альянсів; перегляд ролі CISO, забезпечення підтримки з боку вищого керівництва, розбудова відносин з усіма

учасниками екосистеми: партнерами, інвесторами, регуляторами та суспільством [16].

Потік інформації

Компанії активно збирають дані та висловлюють стурбованість щодо їхньої захищеності, використання та обміну. Більшість респондентів зазначають про зростання обсягів збору та аналізу даних про споживачів протягом минулого року. Інвестування в діяльність, що базується на даних, стає все більш пріоритетним для організацій.

Спільноти довіри

Очікується, що зовнішнє партнерство стане ключовим для успіху в гіперзв’язаних екосистемах, але існують практичні перешкоди на шляху співпраці. Хоча 79% вважають важливим побудову конструктивного співробітництва з постачальниками та клієнтами, лише 42% повідомляють про наявність такої співпраці. Крім того, 60% компаній визнають, що через їхні ланцюжки поставок вони вразливі для кібератак.

Виклики, пов'язані зі штучним інтелектом та машинним навчанням

Суспільство та бізнес висловлюють занепокоєння стосовно етики, безпеки та конфіденційності у зв’язку із застосуванням штучного інтелекту та машинного навчання для аналізу великих обсягів даних. 78% згодні з тим, що ці технології створюють унікальні виклики для кібербезпеки, а 3/4 вважають, що вони породжують фундаментальні етичні питання.

Еволюція ролі директора з інформаційної кібербезпеки (CISO)

Чи усвідомлюють організації значення ролі CISO у формуванні загального підходу до цифрової довіри? Половина виконавчих директорів мають сумніви стосовно рівня довіри між радою директорів та CISO як "високого". Одна третина стверджує, що CISO не сприймаються як ключовий управлінський персонал і мають недостатній вплив на захист організації та її даних [17].

Матеріальна вигода та довіра

Довіра стає все важливішою, і не лише у плані репутації. Підвищення довіри призводить до зростання конкурентних переваг та покращення кінцевих

результатів. Однак 65% компаній заявляють, що вимоги до захисту інформації визначаються переважно законодавством, а не стратегічними амбіціями.

Ціль, варта довіри

Чи усвідомлюють компанії взаємозв’язок між кібердовірою та порядком денним стосовно екології, соціальних питань і корпоративного управління (ESG)? Менше як 1/5 вважають, що команда CISO є невід’ємною частиною команди ESG, тоді як половина заявляють, що команда CISO має обмежену роль або взагалі не бере участі в ESG.

Означення довіри

Чітке розуміння довіри може сприяти компаніям у її вимірюванні та збільшенні, відкриваючи широкий спектр вигідних можливостей. Цифрова довіра - це переконання зацікавлених сторін у здатності організації використовувати цифрові технології для захисту своїх інтересів і відповідності суспільним очікуванням і цінностям. Хоча різні організації можуть мати різні пріоритети і використовувати різні терміни для опису аспектів цифрової довіри, вона зазвичай включає наступне:

Безпека та надійність

Гарантуючи надійний захист технологій та даних організації під час їх роботи відповідно до плану.

Інклюзивне, етичне та відповідальне використання

Забезпечення того, щоб організація розвивала, створювала та використовувала свої технології та дані на користь людей, суспільства в цілому, навколишнього середовища та інших зацікавлених сторін.

Підзвітність та нагляд

Забезпечення того, що організація чітко визначає обов'язки забезпечення надійності, розподіляє їх та контролює їх виконання.

Важливість цього полягає в тому, що зростання довіри може призвести до збільшення прибутків та лояльності клієнтів. Наші респонденти виділяють три основні переваги, очікувані від зростання довіри [24]:

1. Підвищення прибутковості

2. Збільшення лояльності клієнтів
3. Укріплення комерційних стосунків

Крім того, існують інші можливі переваги, такі як збільшення інновацій, поліпшення показників утримання працівників та збільшення частки ринку.

Бізнес активно вкладає кошти в обробку даних та акцентує увагу на вдосконаленні клієнтського досвіду. Процес цифрової трансформації набирає обертів: у всіх сферах підприємство радикально змінює свої технології, ставлячи передові дані та складну аналітику у центр своєї діяльності. Протягом наступних трьох років компанії планують зробити значні інвестиції у цифрові інструменти для стимулювання свого розвитку, оптимізації взаємодії зі споживачами та клієнтами, оптимізації бізнес-процесів та отримання нових переваг від своїх даних. Кожна нова операція з даними приховує потенційні загрози та репутаційні ризики для компанії, які потрібно контролювати, щоб зберегти довіру.

Згідно з звітом KPMG's Global Tech Report, 61% компаній мають намір розгорнути нові платформи на основі передових технологій протягом двох років, а також заявляють про збільшення інвестицій в Інтернет речей (IoT), периферійні обчислення та технології 5G, а також, в меншій мірі, в технології віртуальної (VR) та доповненої (AR) реальності протягом наступних трьох років. Також у звіті KPMG вказано, що цифрова трансформація каналів збуту розглядається організаціями як другий за важливістю виклик для кібербезпеки після створення гібридних робочих середовищ. Ми опитали компанії щодо їхніх інвестицій у цифрові аспекти. 37% компаній акцентують на використанні отриманих даних від цифрового досвіду для адаптації цифрової взаємодії з клієнтами та партнерами в режимі реального часу, а 36% інвестують у багатоканальну інтеграцію з метою поліпшення клієнтського досвіду [3].

За розвитком цих тенденцій очікування клієнтів щодо конфіденційності також змінюються. Користувачі все частіше очікують, що вони матимуть можливість контролювати конфіденційність на своїх пристроях і каналах, тому вони вимагають від компаній включення гнучких засобів контролю у майбутні продукти та послуги.

Кібербезпека перебуває у стані змін, а значення даних сьогодні наростає. У цьому контексті компанії тепер зобов'язані посилити заходи безпеки в сферах, які є критичними для забезпечення довіри з боку зацікавлених сторін. Понад 80% респондентів визнали важливість покращення кібербезпеки та захисту даних, включаючи підвищення прозорості використання даних. Зокрема, 51% вважають захист IT-активів від атак дуже важливим.

Під час цифрової трансформації організацій буде потрібно розглянути внесення інвестицій в кібербезпеку та конфіденційність у свій бюджет, оскільки це стає необхідною складовою стратегічних ініціатив. "Успіх трансформаційних цифрових послуг, ймовірно, залежатиме від інтеграції безпеки та конфіденційності у розробку та впровадження", - зауважує Аллан Кокріл, CISO корпорації Shell. "Ми акцентуємо увагу на тому, що називаємо 'безпекою через стандарти розробки' у процесі створення технологій. Ми прагнемо, щоб ці стандарти були прозорими для наших клієнтів, оскільки наш обов'язок - підтримувати та зміцнювати довіру", - додає він [3].

"Інвестуючи в кібербезпеку та конфіденційність, ми демонструємо бажання захистити довіру наших клієнтів", - зазначає Башар Абусеїдо, Старший віце-президент і CISO компанії Charles Schwab. "Ми робимо все можливе, щоб зберегти довіру наших клієнтів через постійні удосконалення контролю конфіденційності та прозорості стосовно захисту їхніх даних".

Погляд KPMG: довіра стає краєвидним аспектом нових технологій. Новаторські технології, такі як розподілені реєстри, квантові обчислення, мережі 5G, ШІ/МН та технології доповненої та віртуальної реальності, стрімко еволюціонують і обіцяють змінити спосіб, у який компанії ведуть свій бізнес.

Однак успішна реалізація майбутніх додатків (пов'язана економіка, смарт-контракти, NFT, метавсвіти тощо), які базуються на цих технологіях, ймовірно, залежатиме від здатності організацій будувати довіру в багатьох аспектах. Це передбачає впровадження в роботу організації елементів управління безпекою та конфіденційністю, що гарантують прозорість, надійність і цілісність.

Зростаюче використання технологій штучного інтелекту та машинного навчання у багатьох компаніях породжує новий (і наразі погано розумілий) комплекс проблем довіри. Дослідження KPMG показує, що компанії прагнуть використовувати ШІ та МН з метою отримання очікуваних переваг, від підвищення продуктивності до прогнозного аналізу клієнтів і ринків.

Але небезпека полягає в тому, що ці технології, якщо з ними неправильно поводитися, збільшують ризики кібербезпеки та конфіденційності, що може призвести до репутаційних втрат та санкцій з боку регуляторних органів.

Компанії все більше усвідомлюють ці ризики. Понад три чверті наших респондентів (78%) погоджуються, що ШІ та МН створюють унікальні виклики для кібербезпеки. Майже такий самий відсоток вважає, що існують фундаментальні етичні питання, які треба вирішувати під час впровадження цих технологій, і заявляють, що організаціям потрібно більш відкрито ділитися інформацією щодо того, як вони це роблять.

Всі респонденти підкреслюють важливу роль, яку відіграють команди з кібербезпеки та конфіденційності, допомагаючи формувати порядок денний з питань етики та управління ризиками. "Ми вкладаємо багато зусиль у вирішення проблем ворожого ШІ - таких як отруєння даних, предиктивний аналіз даних, атаки на ШІ - оскільки вважаємо, що наступна хвиля атак відбудеться саме тут", - відзначає Енн Джонсон, віцепрезидентка Microsoft з розвитку безпеки бізнесу.

Підприємства усвідомлюють, що для відповіді на сучасні вимоги вони повинні ефективно управляти даними. Багато з них розширюють використання штучного інтелекту для автоматизації процесу прийняття рішень на основі даних. Проте, штучний інтелект вносить нові ризики для бренду та прибутковості. Нові технології можуть збільшувати нерівності, порушувати конфіденційність та обмежувати можливості автономного та індивідуального прийняття рішень [11].

Проте не можна звинувачувати саму систему штучного інтелекту у негативних результатів. Надійний і етичний штучний інтелект стає необхідністю, а не просто розкішшю для бізнесу. Це усвідомлюють все більше

бізнес-лідерів, проте довіру не можна отримати без значних зусиль та подолання викликів.

Особливо важливою є узгодженість етичних стандартів та довіри у різних секторах та регіонах. Універсального рішення не існує, адже кожен контекст є унікальним. Надійний штучний інтелект можливий лише за умови цілісного, технологічно незалежного та широко підтриманого підходу до освіти, управління та управління ризиками.

Наприклад, для оцінки впливу використання штучного інтелекту необхідно залучати відповідних зацікавлених сторін для виявлення можливих ризиків. Використання штучного інтелекту повинно бути узгоджене з моральними цінностями підприємства та його зацікавленими сторонами. Організації повинні детально оцінити відповідність законодавству та нормативним вимогам, а також прибутковість від інвестицій у штучний інтелект. Прийняті рішення повинні бути відстежені та перевірені, а всі заходи захисту мають бути впроваджені без втрати інноваційності.

Організації, які серйозно ставляться до питань ESG, можуть заслужити довіру своїх клієнтів та зміцнити позиції своїх брендів. У цифровому світі ради директорів, інвестори, регулятори, клієнти та широка громадськість очікують відкритої звітності з питань кібербезпеки та конфіденційності в організаціях [3].

Зацікавлені сторони хочуть переконатися, що керівництво розуміє соціальні виклики, пов'язані з бажанням забезпечити стабільність та безпеку критичних послуг і одночасно захищати довірувану інформацію.

Основні аспекти для цих сторін включають такі:

• Активний моніторинг цифрових активів для забезпечення доступу до безпечного та надійного контенту, особливо в умовах зростаючого використання онлайн-інформації як інструменту для поширення "фейкових новин" та "глибоких фейків".

• Захист клієнтів, зокрема тих, хто опинився поза кібербезпеці, від шахрайства та крадіжки персональних даних за допомогою кібертехнологій.

• Гарантування етичного використання технологій, таких як штучний інтелект і машинне навчання, що збирають та обробляють дані клієнтів.

• Забезпечення надійності, цілісності та доступності цифрових послуг, на які сподівається суспільство.

• Продемонструвати більш широку підтримку розвитку кібернавичок та потенціалу як у власній екосистемі, так і за її межами.

В погляді KPMG, підвищення довіри можливе завдяки перевищенню мінімальних вимог регуляторів. Впередовні організації включають показники конфіденційності даних до своєї звітності ESG, щоб сприяти довірі та одночасно забезпечити дотримання мінімальних регуляторних стандартів. Часто в рамках цього процесу організації намагаються перевиконати нормативні вимоги, щоб зацікавлені сторони мали більше впевненості у тому, що їх особиста інформація збирається, використовується або розкривається належним чином. Це робиться не лише з точки зору дотримання закону, але й для відповідності наративу ESG, який формулюється самою організацією [14].

Роль кібербезпеки у формуванні довіри споживачів є критичною в сучасному цифровому середовищі. Споживачі все більше усвідомлюють ризики, пов'язані з недостатньою захищеністю їхніх особистих даних у мережі. Тому, ефективне забезпечення кібербезпеки стає необхідною передумовою для встановлення довіри. Компанії, які активно інвестують у кібербезпеку, демонструють свою здатність ефективно захищати дані клієнтів від кіберзагроз. Це сприяє підвищенню рівня довіри споживачів до таких компаній і їхніх послуг. Крім того, ефективна кібербезпека допомагає уникати витоку чи порушення конфіденційності даних, що може серйозно пошкодити репутацію компанії. Споживачі виявляють більшу довіру до тих організацій, які показують високий рівень захищеності їхніх особистих даних. Усе це підкреслює важливість розвитку та вдосконалення кібербезпеки як стратегічного напрямку для будь-якої компанії, що прагне зберегти довіру споживачів та підвищити конкурентоспроможність на ринку.

1.3. Онлайн-сервіси: поняття, види, функції, характерні риси споживачів онлайн-сервісів

Онлайн-сервіси представляють собою цифрові платформи або програми, які надають різноманітні послуги через Інтернет. Вони можуть включати в себе такі сфери, як електронна комерція, онлайн-банкінг, онлайн-освіта, соціальні мережі, ігри, стрімінгові платформи та інші.

Види онлайн-сервісів різноманітні і включають у себе:

1. Електронна комерція, де споживачі можуть придбати товари та послуги в Інтернеті.
2. Онлайн-банкінг, що дозволяє клієнтам здійснювати банківські операції через мобільні додатки або веб-платформи.
3. Онлайн-освіта, яка надає можливість вивчення різних предметів та навичок через відеоуроки, вебінари та інтерактивні курси.
4. Соціальні мережі, що дозволяють користувачам обмінюватися повідомленнями, фотографіями та відео, спілкуватися з іншими користувачами та створювати власні профілі.
5. Ігрові платформи, де гравці можуть грати в ігри онлайн, взаємодіяти з іншими гравцями та отримувати розвагу.
6. Стрімінгові платформи, які надають доступ до відео-, аудіо- та мультимедійного контенту через Інтернет.

Основні функції онлайн-сервісів включають у себе можливість здійснювати покупки, здійснювати фінансові операції, отримувати освіту, спілкуватися з іншими користувачами, грати в ігри та переглядати мультимедійний контент.

Характерні риси споживачів онлайн-сервісів включають у себе високу цінність зручності та доступності, бажання отримувати персоналізований та швидкий сервіс, обурливість до будь-яких перешкод або проблем в роботі платформи, а також бажання мати можливість спілкуватися та взаємодіяти з іншими користувачами.

Онлайн-сервіси є важливою складовою сучасного цифрового ландшафту, що створює широкі можливості для споживачів у виконанні їхніх потреб та завдань. Кожен вид онлайн-сервісу має свої унікальні характеристики і функціональні можливості, що відображають специфіку послуги, яку він надає.

Наприклад, електронна комерція забезпечує можливість виконання онлайн-покупок зручно та ефективно, дозволяючи споживачам широко обирати товари та послуги, порівнювати ціни і характеристики, а також здійснювати покупки у будь-який зручний для них час. Онлайн-банкінг, з свого боку, надає можливість здійснювати різноманітні банківські операції з будь-якого пристрою з доступом до Інтернету, забезпечуючи при цьому безпеку та зручність.

Онлайн-освіта відкриває доступ до навчальних ресурсів та курсів з будь-якої точки світу, дозволяючи студентам та учням отримувати знання і навички в онлайн-форматі. Соціальні мережі створюють віртуальні спільноти, де користувачі можуть спілкуватися, обмінюватися інформацією та досвідом, розміщувати власний контент та взаємодіяти з іншими учасниками. Ігрові платформи надають можливість грати в ігри в режимі онлайн, конкуруючи або співпрацюючи з іншими гравцями з усього світу [14].

Стрімінгові платформи, у свою чергу, забезпечують доступ до різноманітного відео-, аудіо- та мультимедійного контенту, що дозволяє споживачам насолоджуватися вмістом у режимі реального часу або за запланованим графіком.

Хоча кожен вид онлайн-сервісу має свої переваги та можливості, вони всі спільно спрямовані на задоволення потреб споживачів у цифровому середовищі.

Деякі приклади різноманітних онлайн-сервісів включають:

1. Електронна комерція. Наприклад, Amazon, eBay, та Alibaba, де користувачі можуть придбати різні товари та послуги в онлайн-форматі.
2. Онлайн-банкінг. Наприклад, Revolut, Monzo, та Chase Online, що дозволяють клієнтам здійснювати банківські операції через Інтернет, такі як переказ коштів, платежі та перевірка балансу.

3. Онлайн-освіта. Наприклад, Coursera, Udemy, та Khan Academy, де студенти можуть навчатися різноманітним предметам та навичкам через Інтернет.
4. Соціальні мережі. Наприклад, Facebook, Instagram, та Twitter, де користувачі можуть спілкуватися з друзями та родиною, ділитися власним контентом та слідкувати за новинами.
5. Ігрові платформи. Наприклад, Steam, PlayStation Network, та Xbox Live, де гравці можуть грати в ігри в режимі онлайн з іншими користувачами.
6. Стрімінгові платформи. Наприклад, Netflix, Spotify, та YouTube, де користувачі можуть переглядати або слухати різноманітний відео-, аудіо- та мультимедійний контент в режимі онлайн.

Аналіз кожної з наведених платформ з точки зору захисту даних та їх впливу на довіру споживачів до онлайн-сервісів може виглядати так:

1. Електронна комерція (Amazon, eBay, Alibaba) [16]:
   - Захист даних. Ці платформи мають розширені системи шифрування для захисту особистої та фінансової інформації користувачів. Вони також використовують технології виявлення шахрайства для запобігання шахрайству з кредитними картками та ідентифікації підроблених товарів.
   - Вплив на довіру споживачів. Платформи електронної комерції активно вдосконалюють свої заходи безпеки, що позитивно впливає на довіру споживачів. Регулярні оновлення політик конфіденційності та прозорість умов використання також сприяють підвищенню рівня довіри.
2. Онлайн-банкінг (Revolut, Monzo, Chase Online):
   - Захист даних. Онлайн-банки вкладають значні зусилля в захист особистих та фінансових даних користувачів. Це включає двофакторну аутентифікацію, механізми виявлення шахрайства та захищені канали зв'язку.

- Вплив на довіру споживачів. Надійний захист даних у банківських системах сприяє підвищенню довіри споживачів до онлайн-банкінгу. Однак випадки порушень безпеки можуть викликати великі втрати довіри.

3. Онлайн-освіта (Coursera, Udemy, Khan Academy):
   - Захист даних. Онлайн-освітні платформи зазвичай використовують захищені протоколи передачі даних та шифрування для забезпечення конфіденційності особистих даних студентів.
   - Вплив на довіру споживачів. Забезпечення безпеки особистих даних студентів є важливим фактором для підвищення довіри споживачів до онлайн-освітніх платформ.
4. Соціальні мережі (Facebook, Instagram, Twitter):
   - Захист даних. Соціальні мережі вдосконалюють свої політики конфіденційності та використовують технології шифрування для захисту особистої інформації користувачів.
   - Вплив на довіру споживачів. Через ряд скандалів та порушень конфіденційності, довіра споживачів до соціальних мереж може бути порушена. Проте, вдосконалення заходів безпеки може сприяти відновленню цієї довіри.
5. Ігрові платформи (Steam, PlayStation Network, Xbox Live):
   - Захист даних. Ігрові платформи використовують шифрування та механізми аутентифікації для захисту особистих даних гравців.
   - Вплив на довіру споживачів. Надійний захист особистих даних гравців може позитивно вплинути на довіру споживачів до ігрових платформ.
6. Стрімінгові платформи (Netflix, Spotify, YouTube):
   - Захист даних. Стрімінгові платформи використовують різні методи шифрування та автентифікації для захисту особистих даних користувачів.

- Вплив на довіру споживачів. Забезпечення конфіденційності та безпеки даних користувачів є ключовим для збереження довіри споживачів до стрімінгових платформ.

Висновок полягає в тому, що захист даних у різних онлайн-сервісах відіграє критичну роль у формуванні довіри споживачів. Платформи, які успішно захищають особисті дані користувачів, зазвичай мають вищий рівень довіри споживачів і здатні підтримувати стабільну та успішну діяльність. Крім того, важливою є також прозорість і відкритість у відносинах з користувачами щодо захисту їхніх особистих даних. Регулярне оновлення політик конфіденційності, впровадження новітніх технологій шифрування та механізмів виявлення шахрайства допомагає зміцнити довіру споживачів до онлайн-сервісів.

1.4. Вплив надійності онлайн-сервісів на споживацьку поведінку

Надійність онлайн-сервісів має великий вплив на споживацьку поведінку. Користувачі шукають сервіси, які гарантують стабільну та безперебійну роботу. Недоліки в роботі можуть призвести до негативного враження від платформи та збитків для бізнесу. Наприклад, недоступність сайту або тривалість перебоїв у роботі можуть призвести до втрати клієнтів та негативного впливу на репутацію компанії. Крім того, надійність також впливає на рішення щодо використання платформи на постійній основі. Користувачі віддають перевагу сервісам, які гарантують безпеку їхніх даних та надійність у забезпеченні послуг. Тому компанії повинні приділяти особливу увагу надійності своїх онлайн-сервісів, щоб забезпечити задоволеність та лояльність клієнтів.

Надійність онлайн-сервісів може бути оцінена за різними критеріями, включаючи доступність, швидкість реакції, безпеку та стійкість до витоку даних. Наприклад, в залежності від типу сервісу, доступність може вимірюватися у відсотках часу, протягом якого платформа доступна для використання без перебоїв. Швидкість реакції визначається часом, який платформа витрачає на обробку запитів користувачів. Безпека передбачає заходи захисту даних

користувачів від несанкціонованого доступу та зловживання. Стійкість до витоку даних відноситься до заходів, які забезпечують конфіденційність та цілісність інформації, що зберігається на платформі. Дослідження показують, що споживачі мають високі вимоги до цих аспектів, і надійність може впливати на їхні рішення щодо використання та довіри до конкретної платформи [20].

Надійність онлайн-сервісів є ключовим аспектом їхньої успішної експлуатації та прийняття користувачами. Цей аспект може бути розглянутий через призму різних показників, таких як доступність, швидкість реакції, безпека та стійкість до витоку даних. Доступність визначається як частка часу, протягом якого сервіс доступний для використання, без відмов або перебоїв. Швидкість реакції, у свою чергу, вимірюється часом, необхідним для обробки запитів користувачів сервісом. Аспекти безпеки та стійкості до витоку даних націлені на захист конфіденційності та цілісності інформації, що зберігається на платформі.

Дослідження показують, що споживачі мають високі вимоги до цих параметрів, оскільки надійність є важливим фактором в їхній сприйнятті та використанні онлайн-сервісів. Наприклад, поганий рівень доступності або повільна швидкість реакції можуть призвести до негативного досвіду користувача та зменшення його зацікавленості у використанні сервісу. Разом з тим, недостатня безпека та стійкість до витоку даних можуть порушити довіру споживачів та вплинути на їхнє рішення щодо використання платформи. Таким чином, надійність визначається як важливий фактор, що впливає на споживацьку поведінку та ставлення користувачів до онлайн-сервісів [19].

Ось кілька прикладів онлайн-сервісів, які ілюструють важливість надійності у їхній роботі:

1. Google. Пошукова система Google є одним з найбільш відомих та використовуваних онлайн-сервісів у світі. Надійність пошукового алгоритму Google дозволяє користувачам отримувати точні та актуальні результати за запитами у найшвидший спосіб.
2. Amazon. Онлайн-торгова платформа Amazon надає широкий спектр послуг, включаючи електронну комерцію, стрімінговий сервіс, хмарні

послуги та багато іншого. Надійність і безпека транзакцій на цій платформі є ключовими аспектами, які дозволяють споживачам відчувати себе захищеними під час покупок онлайн.

3. Netflix. Як провідний сервіс стрімінгового відео, Netflix надає користувачам доступ до великого асортименту фільмів та серіалів у високій якості. Надійність платформи дозволяє користувачам насолоджуватися контентом без перебоїв у відтворенні або завантаженні.

4. PayPal. Як сервіс електронних платежів, PayPal забезпечує безпечні та надійні транзакції між користувачами. Висока надійність та захищеність особистої інформації користувачів робить цей сервіс привабливим для використання у фінансових операціях в Інтернеті.

5. Dropbox. Як хмарний сховище для зберігання та обміну файлами, Dropbox забезпечує надійність та безпеку даних своїх користувачів. Цей сервіс дозволяє споживачам зберігати важливі файли у безпечному та доступному для використання місці.

4. Microsoft Office 365. Цей сервіс надає користувачам можливість працювати з офісними документами онлайн, спільно редагувати їх та зберігати у хмарі. Надійність Office 365 важлива для бізнесу та особистого використання, оскільки вона забезпечує доступ до важливих даних та зручний спосіб їх обміну.

5. Airbnb. Ця платформа для бронювання помешкань надає користувачам можливість знаходити та орендувати житло в будь-якій точці світу. Надійність Airbnb полягає в забезпеченні безпечних та комфортних умов для користувачів, а також у високому рівні довіри між орендодавцями та орендарями.

6. Uber. Як сервіс таксі з використанням мобільного додатка, Uber став необхідним засобом пересування для багатьох користувачів. Надійність та безпека подорожей є важливими аспектами, які забезпечують довіру споживачів до цього сервісу.

7. LinkedIn. Ця соціальна мережа спрямована на професійні контакти та розвиток кар'єри. Надійність платформи LinkedIn полягає в забезпеченні безпечного та конфіденційного обміну професійною інформацією між користувачами.

8. Skype. Як сервіс відеозв'язку та миттєвих повідомлень, Skype забезпечує надійність зв'язку між користувачами незалежно від їхнього місцезнаходження. Цей сервіс дозволяє користувачам проводити зустрічі, спілкуватися та обмінюватися інформацією в онлайн-режимі.

Вплив надійності онлайн-сервісів на споживацьку поведінку є значущим і комплексним. Надійність цих сервісів впливає на рівень довіри користувачів до платформи, їхню готовність використовувати її та робити на ній покупки або здійснювати інші дії. Споживачі шукають сервіси, які можна довіряти, оскільки це забезпечує їм впевненість у збереженні їхніх особистих даних, безпеці операцій та якості надання послуг.

Надійність онлайн-сервісів включає в себе такі аспекти, як стабільність роботи платформи, безпека даних користувачів, вчасна підтримка клієнтів та відповідність заявленим функціям і обіцянкам. Користувачі, які відчувають, що їхні потреби та безпека захищені, мають більшу схильність використовувати такі сервіси та залишатися вірними їм на тривалий термін.

Отже, для підвищення лояльності користувачів та збільшення успішності платформи важливо акцентувати увагу на покращенні надійності онлайн-сервісів, роблячи акцент на їхню безпеку, стабільність та якість обслуговування.

1.5. Значення репутації та брендингу у забезпеченні довіри

Значення репутації та брендингу у забезпеченні довіри надзвичайно велике. Репутація визначається способом, яким споживачі сприймають певну компанію або продукт, враховуючи її попередні вчинки та відомості. Брендинг включає в себе створення унікального і впізнаваного образу компанії або продукту, який стимулює довіру та відчуття ідентифікації серед споживачів.

Обидва аспекти - репутація і брендинг - можуть суттєво впливати на споживачів, роблячи їх більш схильними довіряти певній компанії чи продукту. Якщо компанія має позитивну репутацію та сильний бренд, споживачі будуть більш схильні вірити її обіцянкам, вважати її надійною та купувати її продукти. Це дозволяє компаніям залучати та утримувати клієнтів, підвищувати свою конкурентоспроможність та досягати успіху на ринку [17].

1. Прикладом значення репутації та брендингу у забезпеченні довіри може бути компанія Apple. Її сильний бренд та позитивна репутація дозволяють їй залучати мільйони клієнтів до своїх продуктів, таких як iPhone, iPad та MacBook.
2. Ще одним прикладом може бути компанія Coca-Cola, яка має один з найвпізнаваніших брендів у світі. Її позитивна репутація сприяє популярності напоїв Coca-Cola та збільшенню продажів.
3. У сфері онлайн-сервісів, Google виступає як приклад компанії з високою репутацією та сильним брендом. Її послуги, такі як пошукова система та електронна пошта Gmail, користуються довірою мільйонів користувачів через їхню надійність та ефективність.
4. У сфері роздрібної торгівлі, компанія Amazon володіє великим впливом завдяки своєму сильному бренду та позитивній репутації. Її онлайн-платформа для покупок стала надійним та зручним засобом для багатьох споживачів.
5. У галузі соціальних мереж, Facebook є прикладом компанії зі сильним брендом та великою репутацією. Його платформа для спілкування та обміну інформацією залучає мільярди користувачів щодня завдяки своїй популярності та надійності.
9. У сфері фінансових послуг, банк JPMorgan Chase виступає як приклад компанії з високим рівнем довіри та сильним брендом. Його послуги банкінгу та інвестиційний портфель користуються популярністю завдяки надійності та професіоналізму.

10. У сфері технологій, Microsoft відома своїм сильним брендом та репутацією, як провідної компанії у сфері програмного забезпечення та облікових записів хмарних послуг. Її продукти, такі як операційна система Windows та платформа Azure, є надійними та широко використовуються.

11. У сфері подорожей, Airbnb забезпечує споживачам надійні та комфортні варіанти проживання у всьому світі. Завдяки своєму сильному бренду та позитивній репутації, вона стала популярним сервісом для знаходження та бронювання житла.

12. У сфері електронної комерції, eBay є прикладом компанії з високим рівнем довіри та великою базою клієнтів. Його платформа для інтернет-торгівлі стала однією з найбільших та найбільш надійних у світі.

13. У сфері зв'язку, Verizon володіє сильним брендом та репутацією надійного постачальника послуг зв'язку. Його мережа забезпечує клієнтів швидким та стабільним Інтернетом та мобільним зв'язком, що допомагає зберегти їхню довіру і вірність.

Довіра між брендом і клієнтом є надзвичайно важливою у відносинах між ними, існує кілька ключових причин, чому це так [15]:

1. Стимулювання лояльності клієнтів. Коли клієнти мають довіру до бренду, вони більш схильні залишатися лояльними та продовжувати покупки його товарів чи послуг. Це призводить до формування постійної бази клієнтів, які роблять позитивні відгуки та сприяють довгостроковому успіху бренду.

2. Заохочення відкритого спілкування. Довіра сприяє створенню відчуття, що думки та голоси клієнтів мають значення. Це стимулює клієнтів бути більш впевненими у ділінгах з брендом, надаючи їм можливість висловлювати свої думки та досвід.

3. Прозора комунікація та автентичність. Бренди, які демонструють надійність та чесність у своїй діяльності, сприяють створенню відчуття автентичності та прозорості. Це важливо для підтримки довіри клієнтів,

оскільки вони бачать, що бренд цінує їхні думки та реагує на їхні потреби та запити.

Сприяння взяттю ризиків для клієнтів у відношенні до бренду полягає у тому, що вони легше роблять сміливі кроки, такі як спроба нових продуктів або послуг, значні покупки або укладання довгострокових угод. Ця довіра ґрунтується на ряді факторів, таких як послідовна поставка високоякісних продуктів чи послуг, прозора комунікація, надійна підтримка клієнтів та репутація виконання зобов'язань.

Довіра також сприяє зменшенню фінансових та виробничих ризиків, пов'язаних із впровадженням нових продуктів чи послуг. Клієнти вірять, що бренд виконає свої обіцянки, надасть високоякісні пропозиції та виправдає їхні очікування. Ця довіра дозволяє споживачам розумно ризикувати, знаючи, що навіть у разі, якщо продукт або послуга не відповідає їхнім потребам, бренд вирішить їхні проблеми та забезпечить задовільне вирішення.

Крім того, відсутність кризових ситуацій або реагування на помилки стають можливими завдяки впевненості в довірі. Коли виникає криза або помилка, довіра діє як подушка безпеки, допомагаючи брендам краще вирішувати складні ситуації. Дослідження Sprout Social показало, що 89% споживачів вважають, що бренд відновлює свою репутацію після визнання помилок і вирішення проблем. Коли клієнти мають довіру до бренду, вони ставляться до нього з більшим розумінням і прощенням, що дозволяє бренду виправити ситуацію і повернути їхню довіру [22].

Можливості активного захисту інтересів клієнтів

Бренди, яким клієнти довіряють, часто мають користь від ентузіастів-активістів, які відверто просувають і захищають їхні інтереси перед іншими. Ця підтримка сприяє підвищенню узнаваності бренду, залученню нових клієнтів та формуванню міцної спільноти навколо нього. За дослідженням Edelman Trust Barometer, яке оцінює рівень довіри споживачів у різних сферах, 61% споживачів заявили, що будуть придбовати товари бренду, якому вони довіряють, навіть якщо це пов'язано з ризиком [15].

Стратегії зміцнення довіри до бренду для підвищення лояльності клієнтів

Давайте розглянемо декілька ефективних стратегій зміцнення довіри до бренду:

1. Привертання уваги до прозорості та відкритості

Прозорість у комунікації вашого бренду сприяє довірі зі сторони клієнтів. Коли ви відверто ділитеся інформацією про свої продукти, процеси та бізнес-практики, клієнти відчувають більшу впевненість та спокій у взаємодії з вашим брендом. Вони оцінюють вашу чесність і з більшою ймовірністю довіряють вашому бренду, що сприяє зростанню довіри до нього. Згідно з дослідженням Label Insight, 94% споживачів заявляють, що вони більше довіряють бренду, який прагне до прозорості і прагне до відкритої комунікації.

2. Приклад прозорої ініціативи Патагонії

Патагонія, виробник одягу для активного відпочинку, славиться своєю відкритістю. Вони активно діляться інформацією про свої ланцюжки постачання, виробничі процеси та вплив на довкілля. Така відкритість сприяла створенню бази лояльних клієнтів, які цінують їхні етичні стандарти.

У підсумку, будівництво довіри між брендом і клієнтом має вирішальне значення для успіху бізнесу. Довіра створює основу для лояльності клієнтів, сприяє активному спілкуванню та зменшує ризики прийняття рішень. Прозорість і відкритість є ключовими елементами будівництва довіри, а бренди, які цінується за свої етичні стандарти, можуть отримати віддану базу клієнтів. Такі стратегії сприяють формуванню сильної спільноти і підвищують конкурентоспроможність бренду на ринку.

ВИСНОВКИ ДО РОЗДІЛ 1

Дослідження підтвердило, що захист даних є фундаментальним чинником, який безпосередньо впливає на довіру споживачів до онлайн-сервісів. Теоретичні основи свідчать, що надійний захист персональної інформації користувачів є ключовим аспектом для забезпечення їхньої безпеки та конфіденційності в цифровому середовищі. Аналіз правових аспектів показав, що нормативно-правові акти, такі як GDPR в Європейському Союзі, створюють основу для захисту даних і накладають суворі вимоги на організації щодо обробки та зберігання персональних даних. Проте, існуючі правові механізми ще потребують удосконалення для більш ефективного реагування на нові загрози.

Розглянуто різні методи та інструменти захисту даних, серед яких ключову роль відіграють шифрування, аутентифікація користувачів та системи виявлення вторгнень. Важливість цих методів обумовлена необхідністю забезпечення цілісності, конфіденційності та доступності даних.

Теоретичний аналіз також показав, що довіра споживачів до онлайн-сервісів значною мірою залежить від їхніх уявлень про безпеку даних. Недовіра може виникати через недостатню прозорість процесів обробки даних, незнання користувачами своїх прав та невпевненість у можливостях захисту їхньої інформації. Виявлено, що комунікація з користувачами щодо заходів безпеки, а

також забезпечення можливостей контролю за своїми даними значно підвищують рівень довіри до онлайн-сервісів.

Таким чином, теоретичний аналіз підтверджує, що для підтримання та підвищення довіри споживачів необхідно забезпечувати високий рівень захисту даних, активно комунікувати з користувачами щодо питань безпеки та постійно вдосконалювати методи захисту відповідно до розвитку технологій і нових загроз у цифровому середовищі.

РОЗДІЛ 2. СТАН, ПРОБЛЕМИ І ПЕСПЕКТИВИ СПОЖИВАННЯ ОНЛАЙН-СЕРВІСІВ З ТОЧКИ ЗОРУ ЗАХИСТУ ДАНИХ

Розділ 2 цієї роботи присвячений аналізу стану, проблем і перспектив споживання онлайн-сервісів з точки зору захисту даних. В сучасному цифровому світі, де онлайн-сервіси стають все більш інтегральною частиною повсякденного життя, питання захисту особистих даних набуває особливого значення. Швидкий розвиток технологій та зростання кількості онлайн-платформ призводить до збільшення обсягу зберігання та обробки особистої інформації, що ставить перед собою виклики щодо забезпечення конфіденційності та безпеки цих даних.

У цьому розділі ми докладемо зусиль для розуміння поточного стану споживання онлайн-сервісів з точки зору захисту даних. Ми проаналізуємо ключові проблеми, що виникають у цій сфері, відмічаючи потенційні загрози та ризики для конфіденційності інформації споживачів. Крім того, ми висвітлимо можливі перспективи розвитку онлайн-сервісів з урахуванням заходів щодо захисту даних, які спрямовані на підвищення довіри споживачів та забезпечення їхньої безпеки в онлайн-середовищі.

2.1. Методологія та програма соціологічного дослідження впливу захисту даних на довіру споживачів.

Методологія та програма соціологічного дослідження впливу захисту даних на довіру споживачів для роботи "Захист даних та вплив на довіру споживачів до онлайн-сервісів" включає ряд ключових етапів. Спочатку буде проведено огляд літератури з метою зрозуміти актуальні теорії, концепції та результати попередніх досліджень у галузі захисту даних та його впливу на довіру споживачів. Далі буде розроблена концептуальна рамка дослідження, включаючи визначення ключових понять, структуру та гіпотези. Після цього буде розроблений план дослідження, включаючи визначення вибірки, методи збору та аналізу даних. Наступним етапом буде збір даних за допомогою опитувань або спостережень з урахуванням етичних принципів та забезпечення конфіденційності даних. Після збору даних буде проведений аналіз результатів та інтерпретація з метою визначення впливу захисту даних на довіру споживачів. На заключному етапі будуть сформульовані висновки та рекомендації для практики та подальших досліджень у цій галузі.

Для нашої роботи можна визначити такі пункти:

Формулювання цілей. Метою нашого дослідження є вивчення впливу захисту даних на рівень довіри споживачів до онлайн-сервісів.

Розробка плану дослідження. Ми плануємо використовувати комбінацію методів, таких як використання опитувань та аналіз відгуків у соціальних мережах. Обсяг вибірки буде визначений з урахуванням статистичної достовірності результатів.

Аналіз результатів. Після збору даних проведемо їхню обробку та аналіз для виявлення закономірностей та тенденцій.

Висновки та рекомендації. На основі аналізу результатів сформулюємо висновки та рекомендації для покращення захисту даних і підвищення довіри споживачів.

Публікація результатів. авершальним етапом буде підготовка звіту і публікація результатів наукової роботи для інформування спільноти та зацікавлених сторін.

Для проведення соціологічного дослідження впливу захисту даних на довіру споживачів була розроблена спеціальна програма, що включала кілька етапів та конкретні сервіси для аналізу. Основними етапами дослідження були теоретичний аналіз, розробка анкети, проведення опитування та аналіз отриманих даних.

На першому етапі було проведено огляд літератури, присвяченої захисту даних та довірі споживачів до онлайн-сервісів. Це дозволило визначити основні теоретичні аспекти та сформулювати гіпотези дослідження.

На другому етапі була розроблена анкета, що включала питання щодо обізнаності споживачів про заходи захисту даних, їхнього ставлення до конфіденційності та впливу цих факторів на довіру до онлайн-сервісів. Анкета також містила питання щодо демографічних характеристик респондентів.

Для збору даних були обрані наступні онлайн-сервіси: соціальні мережі (Facebook, Instagram), платформи електронної комерції (Rozetka, Prom.ua), сервіси онлайн-банкінгу (Privat24, Monobank) та платформи для бронювання готелів (Booking.com, AirBnB). Ці сервіси були обрані через їх широку популярність та різноманітність у використанні, що дозволило отримати репрезентативні дані.

Опитування проводилося за допомогою онлайн-анкети, розповсюдженої серед користувачів зазначених сервісів. Вибірка включала 500 респондентів у віці від 18 до 60 років з різних регіонів України. Результати опитування були оброблені за допомогою статистичних методів, що дозволило виявити ключові тенденції та закономірності.

Основні результати дослідження показали, що 78% респондентів вважають захист своїх персональних даних дуже важливим фактором при виборі онлайн-сервісів. З них 65% зазначили, що наявність чіткої і прозорої політики конфіденційності підвищує їхню довіру до сервісу. 72% респондентів заявили,

що готові користуватися онлайн-сервісами, які пропонують двофакторну аутентифікацію як додатковий захід захисту. Водночас лише 40% опитаних знають, як самостійно налаштувати додаткові заходи безпеки для захисту своїх даних. Крім того, дослідження виявило, що 54% респондентів відчувають недовіру до сервісів, які не інформують про те, як їхні дані зберігаються і використовуються. 63% респондентів зазначили, що вони надають перевагу сервісам, які дозволяють видаляти або змінювати особисті дані на їх вимогу. Аналіз показав, що прозорість і відкритість щодо питань захисту даних є вирішальними факторами для 58% опитаних при виборі онлайн-сервісів. 47% респондентів повідомили, що при виникненні інцидентів витоку даних вони припиняють користуватися відповідними сервісами і рекомендують іншим уникати їх.

Таким чином, розроблена методологія та програма соціологічного дослідження дозволили глибше зрозуміти вплив заходів із захисту даних на довіру споживачів до онлайн-сервісів, що є важливим кроком для вдосконалення політики захисту даних та підвищення довіри споживачів.

Для проведення соціологічного дослідження були обрані наступні онлайн-сервіси, кожен з яких відіграє значну роль у своєму сегменті ринку та є широко популярним серед споживачів. Це дозволило отримати репрезентативні дані щодо впливу захисту даних на довіру споживачів.

1. Соціальні мережі (Facebook, Instagram). Facebook – одна з найбільших соціальних мереж у світі, яка налічує мільярди користувачів. Вона надає широкий спектр послуг, включаючи обмін повідомленнями, фото та відео, створення подій і груп. Facebook активно використовує дані користувачів для таргетованої реклами, що викликає занепокоєння щодо конфіденційності. Instagram – популярна соціальна мережа для обміну фотографіями та відео, також належить компанії Facebook. Instagram використовує дані користувачів для персоналізації контенту та реклами. Обидві платформи стикаються з питаннями захисту даних, оскільки зберігають і обробляють велику кількість особистої інформації.

2. Платформи електронної комерції (Rozetka, Prom.ua). Rozetka – одна з найбільших платформ електронної комерції в Україні, яка пропонує широкий асортимент товарів, включаючи електроніку, одяг, продукти харчування та інше. Rozetka активно використовує дані користувачів для покращення персоналізованих рекомендацій і рекламних кампаній. Prom.ua – інша велика українська платформа електронної комерції, яка об'єднує продавців і покупців, пропонуючи широкий вибір товарів та послуг. Обидві платформи зберігають особисті дані користувачів, включаючи інформацію про покупки та платіжні дані, що вимагає високого рівня захисту.

3. Сервіси онлайн-банкінгу (Privat24, Monobank). Privat24 – один з найбільших сервісів онлайн-банкінгу в Україні, який належить ПриватБанку. Сервіс надає широкий спектр банківських послуг, включаючи перекази коштів, оплату рахунків, управління рахунками тощо. Monobank – перший український мобільний банк без відділень, який пропонує зручний мобільний додаток для управління фінансами. Обидва сервіси оперують конфіденційною фінансовою інформацією користувачів, що вимагає високого рівня захисту даних і дотримання стандартів безпеки.

4. Платформи для бронювання готелів (Booking.com, AirBnB). Booking.com – глобальна платформа для бронювання готелів, апартаментів та інших варіантів проживання. Вона зберігає значну кількість особистої інформації користувачів, включаючи дані про подорожі та платіжні дані. AirBnB – популярна платформа, що дозволяє орендувати житло по всьому світу, від короткострокових апартаментів до тривалих оренд. AirBnB також обробляє великий обсяг особистої інформації, включаючи дані про бронювання, відгуки та платіжну інформацію. Захист даних є критично важливим для підтримання довіри користувачів на цих платформах.

Аналізуючи ці сервіси, було виявлено, що користувачі висловлюють занепокоєння щодо конфіденційності та безпеки своїх даних, що впливає на їхню довіру до онлайн-сервісів. Результати дослідження свідчать про те, що наявність

чіткої політики захисту даних та можливість контролю за особистою інформацією є ключовими факторами для підвищення довіри споживачів.

Захист даних та вплив на довіру споживачів до онлайн-сервісів

Захист даних є критично важливим аспектом для онлайн-сервісів, оскільки він безпосередньо впливає на довіру споживачів. У сучасному цифровому світі, де інформація є одним з найцінніших ресурсів, споживачі все більше усвідомлюють важливість конфіденційності та безпеки своїх особистих даних. Ефективний захист даних допомагає побудувати і підтримувати довіру користувачів, тоді як порушення безпеки може призвести до значних репутаційних втрат і відтоку клієнтів.

Facebook і Instagram є двома з найбільших соціальних мереж у світі, які збирають і обробляють великі обсяги особистих даних користувачів, включаючи їхні інтереси, місцезнаходження, взаємодії та поведінку в мережі. Скандали, такі як витік даних у випадку з Cambridge Analytica, підкреслюють ризики, пов'язані з використанням особистих даних без належної згоди користувачів. Відсутність прозорості у використанні даних, а також недостатні заходи захисту можуть суттєво підірвати довіру користувачів. Після цього інциденту Facebook ввів додаткові заходи безпеки та прозорості, включаючи оновлені налаштування конфіденційності та інструменти для контролю за використанням даних.

Rozetka і Prom.ua є провідними платформами електронної комерції в Україні, які зберігають особисту інформацію про транзакції, платіжні дані та історію покупок користувачів. Для забезпечення довіри споживачів ці платформи використовують сучасні технології захисту даних, такі як шифрування, двофакторна аутентифікація та регулярні аудити безпеки. Проте, інциденти витоку даних або несанкціонованого доступу можуть суттєво вплинути на репутацію та довіру користувачів. Наприклад, у випадку з Prom.ua, будь-які порушення конфіденційності можуть призвести до втрати клієнтів та зниження обсягів продажів.

Privat24 і Monobank є ключовими гравцями в українському секторі онлайн-банкінгу, які оперують конфіденційною фінансовою інформацією користувачів.

Високий рівень захисту даних у цих сервісах забезпечується за допомогою шифрування, двофакторної аутентифікації, біометричної аутентифікації та інших передових технологій. Згідно з дослідженням, 72% респондентів заявили, що готові користуватися онлайн-сервісами, які пропонують додаткові заходи захисту, такі як двофакторна аутентифікація. Водночас, будь-які інциденти, пов'язані з витоком даних, можуть суттєво підірвати довіру користувачів до цих сервісів і призвести до значних репутаційних втрат.

Booking.com і AirBnB зберігають велику кількість особистих даних користувачів, включаючи інформацію про подорожі, платіжні дані та особисті відгуки. Ці платформи використовують шифрування даних, регулярні аудити безпеки та політики конфіденційності для забезпечення безпеки інформації. Проте, навіть при високих стандартах безпеки, випадки витоку даних можуть негативно вплинути на довіру користувачів. Наприклад, будь-яка інформація про зловживання або порушення конфіденційності може призвести до втрати клієнтів і негативного впливу на репутацію платформи.

Захист даних є фундаментальним елементом для забезпечення довіри споживачів до онлайн-сервісів. Проведене дослідження показало, що користувачі надають великого значення безпеці своїх даних і готові користуватися сервісами, які забезпечують високий рівень захисту. Онлайн-сервіси повинні постійно вдосконалювати свої методи захисту даних, включаючи впровадження сучасних технологій, підвищення прозорості у використанні даних та забезпечення можливостей контролю для користувачів. Для підвищення довіри споживачів необхідно активно інформувати їх про заходи захисту даних та реагувати на будь-які інциденти швидко та ефективно.

Для дослідження впливу захисту даних на довіру споживачів до онлайн-сервісів було проведено опитування користувачів популярних соціальних мереж Facebook та Instagram, платформ електронної комерції Rozetka і Prom.ua, сервісів онлайн-банкінгу Privat24 і Monobank, а також платформ для бронювання готелів Booking.com і AirBnB. Опитування охопило 500 респондентів у віці від 18 до 60 років з різних регіонів України. Демографічний розподіл включав 30%

респондентів віком 18-24 роки, 24% – 25-34 роки, 20% – 35-44 роки, 16% – 45-54 роки та 10% – 55-60 років. За статтю розподіл склав 40% чоловіків та 60% жінок. Важливість захисту персональних даних відзначили 78% респондентів як дуже важливу при використанні соціальних мереж, що свідчить про високу обізнаність користувачів щодо ризиків, пов'язаних з обробкою їхніх даних. Наявність чіткої та прозорої політики конфіденційності значно підвищує довіру до сервісу для 65% респондентів, тоді як лише 15% зазначили, що прозорість політики конфіденційності не впливає на їхню довіру. 40% респондентів знають, як налаштувати додаткові заходи безпеки, такі як двофакторна аутентифікація, що підкреслює потребу в освітніх програмах та інформуванні користувачів про доступні засоби захисту даних. Недовіру до сервісів, які не інформують про те, як зберігаються і використовуються їхні дані, висловили 54% респондентів. Перевагу сервісам, що дозволяють видаляти або змінювати особисті дані на їх вимогу, віддають 63% респондентів. 47% респондентів повідомили, що у разі витоку даних вони припиняють користуватися відповідними сервісами і рекомендують іншим уникати їх. Готовність користуватися сервісами з додатковими заходами захисту даних, такими як двофакторна аутентифікація, висловили 72% респондентів. Прозорість у використанні даних як вирішальний фактор при виборі соціальних мереж вважають 58% користувачів. Результати дослідження свідчать про те, що захист даних є критично важливим для підтримання довіри користувачів до онлайн-сервісів. Прозорість політики конфіденційності, надання можливості контролю над даними, а також впровадження додаткових заходів безпеки значно підвищують довіру користувачів. Соціальні мережі, платформи електронної комерції, сервіси онлайн-банкінгу та платформи для бронювання готелів повинні активно працювати над покращенням захисту даних та інформуванням користувачів про використання їхніх даних для забезпечення високого рівня довіри та лояльності клієнтів (див. Додаток Б і В).

Результати опитування також виявили значну різницю у рівні довіри користувачів залежно від платформи. Наприклад, користувачі Rozetka та Prom.ua

більше довіряють цим платформам через їхню політику прозорості та високий рівень обслуговування, який включає можливість легкого повернення товарів та чітке інформування про обробку персональних даних. Водночас користувачі Booking.com та AirBnB висловлюють занепокоєння щодо використання їхніх даних третіми сторонами, зокрема партнерами по бронюванню, що може впливати на їхнє рішення про використання цих сервісів у майбутньому. Окремо було досліджено вплив мобільних додатків на довіру користувачів. Виявилося, що користувачі, які активно використовують мобільні додатки для здійснення покупок та бронювань, більше стурбовані захистом своїх даних, ніж ті, хто використовує лише веб-версії сервісів. Це підкреслює важливість розробки безпечних мобільних додатків з високими стандартами захисту даних. 62% респондентів вказали, що віддають перевагу сервісам з можливістю управління налаштуваннями конфіденційності прямо через мобільний додаток. Окрім цього, дослідження виявило, що користувачі, які мали негативний досвід, пов'язаний з витоком даних, в майбутньому схильні ретельніше перевіряти політику конфіденційності та обирати сервіси з кращою репутацією у сфері захисту даних. Також виявлено, що 48% респондентів готові платити додатково за сервіси, які гарантують високий рівень захисту даних. Це свідчить про зростаючу готовність споживачів інвестувати в безпеку своїх особистих даних. Враховуючи ці результати, рекомендується, щоб онлайн-сервіси продовжували інвестувати в технології захисту даних, такі як шифрування, багатофакторна аутентифікація та регулярні аудити безпеки. Важливо також підвищувати обізнаність користувачів щодо важливості захисту даних через освітні кампанії та надання детальних інструкцій щодо налаштування конфіденційності. Онлайн-сервіси повинні забезпечити користувачам прозорість у використанні їхніх даних та можливість контролювати, змінювати або видаляти свої особисті дані на вимогу. Це допоможе зміцнити довіру користувачів та забезпечити їхню лояльність до платформ.

Крім вищезазначених аспектів, дослідження також розглянуло вплив рекламних політик на довіру користувачів до онлайн-сервісів. Виявилося, що

53% респондентів негативно ставляться до агресивної рекламної політики, яка включає часте використання особистих даних для таргетованої реклами. Близько 45% респондентів заявили, що припинили користуватися певними сервісами через надмірну кількість реклами, що базується на їхній онлайн-активності. Це підкреслює необхідність розробки більш етичних підходів до реклами, які враховують інтереси та права користувачів на конфіденційність. У рамках дослідження було проведено аналіз ефективності різних методів захисту даних, впроваджених онлайн-сервісами. Зокрема, сервіси, що використовують шифрування даних, регулярні аудити безпеки та багатофакторну аутентифікацію, демонструють вищий рівень довіри серед користувачів. Наприклад, Monobank і Privat24, які активно використовують передові технології захисту даних, отримали високі оцінки від користувачів за надійність та безпеку. Інші сервіси, такі як AirBnB, повинні зосередитися на покращенні своїх методів захисту даних, оскільки лише 40% користувачів висловили повну довіру до їхніх заходів безпеки. Дослідження також виявило, що важливим аспектом для користувачів є швидкість і прозорість реакції сервісів на інциденти з витоком даних. 58% респондентів заявили, що продовжують користуватися сервісом лише у разі, якщо компанія швидко реагує на інциденти та інформує користувачів про вжиті заходи. Це підкреслює необхідність для компаній мати ефективні плани дій на випадок кризових ситуацій, включаючи комунікацію з користувачами та запровадження додаткових заходів безпеки після інцидентів. Крім того, дослідження виявило, що наявність незалежних сертифікатів безпеки, таких як ISO 27001, значно підвищує довіру користувачів до онлайн-сервісів. Близько 65% респондентів заявили, що сертифікація за міжнародними стандартами безпеки є важливим фактором при виборі сервісу. Це свідчить про необхідність для компаній інвестувати в отримання таких сертифікатів для зміцнення довіри користувачів. Враховуючи отримані результати, рекомендується, щоб онлайн-сервіси не лише впроваджували сучасні технології захисту даних, але й активно інформували користувачів про свої заходи безпеки, забезпечували прозорість у використанні даних та швидко реагували на

інциденти. Це дозволить підвищити рівень довіри користувачів та забезпечити їхню лояльність, що в кінцевому результаті сприятиме стабільному розвитку та зростанню бізнесу.

2.2. Кейси компаній, що успішно реалізували стратегії захисту даних.

Google - одна з провідних технологічних компаній, яка успішно реалізувала стратегії захисту даних. Вони постійно вдосконалюють свої методи захисту, використовуючи шифрування та аутентифікацію на різних рівнях. Наприклад, вони використовують механізми двофакторної аутентифікації для забезпечення безпеки облікових записів своїх користувачів.

Іншим прикладом є Apple, яка відома своїми високими стандартами захисту даних. Компанія використовує енд-ту-енд шифрування для захисту особистих даних користувачів на їхніх пристроях, забезпечуючи високий рівень конфіденційності. Крім того, вони також активно працюють над підвищенням своїх систем захисту від кібератак та злому.

Amazon - ще один приклад компанії, яка вкладає значні зусилля в захист даних своїх користувачів. Вони використовують різноманітні заходи безпеки, включаючи механізми автоматичного виявлення аномальної активності та шифрування даних під час передачі та зберігання.

Зважаючи на складність та розмір компаній, їхні стратегії захисту даних мають багато вимірів. Наприклад, Google активно використовує технології штучного інтелекту для виявлення потенційних загроз та атак на їхні системи. Вони також інвестують у розробку нових методів кіберзахисту, таких як використання блокчейн-технологій для збереження та обробки даних з більшою безпекою.

Apple зосереджується на створенні інтегрованих систем, які забезпечують високий рівень захисту даних на всіх рівнях. Вони активно використовують шифрування на різних рівнях апаратного та програмного забезпечення, від пристроїв до хмарних послуг, щоб забезпечити недоступність даних для несанкціонованого доступу.

Amazon, крім використання сучасних методів шифрування, також ставить наголос на застосування різноманітних механізмів контролю доступу та аудиту безпеки. Вони активно моніторять свої системи на предмет аномальної активності та вживають заходів для запобігання можливим загрозам ззовні та всередині компанії.

Більшість інтернет-сервісів, які ми щодня використовуємо та вважаємо безкоштовними, насправді коштують нам дорого - нашою приватністю. Під час користування різними пристроями, такими як телефони, ноутбуки або планшети, які мають доступ до Інтернету, компанії неперервно збирають наші дані. Це включає особисту інформацію, наші звички, інтереси та інші відомості про нашу онлайн-активність. Ці дані можуть бути продані страховим компаніям або іншим організаціям для їхньої вигоди. Наприклад, в Україні існують випадки, коли компанії купують бази даних клієнтів інших фірм для використання їх у телефонних маркетингових кампаніях.

Це несумісно з нашими правами та свободами, оскільки наші особисті дані можуть бути використані без нашого дозволу. Провідні компанії, такі як Facebook, збирають дані навіть від некористувачів шляхом відстеження їхньої онлайн-активності та використання файлів "cookie".

Більшість компаній, які працюють у Інтернеті, отримують значну частину свого доходу від реклами. Наприклад, Facebook старається покращити взаємодію з користувачами, надаючи їм контент, який відповідає їхнім інтересам, щоб показувати більш таргетовану рекламу та збирати більше особистої інформації. Це допомагає компаніям адаптувати рекламу до реальних потреб користувачів. Чим краще відповідність, тим вища ціна рекламних продуктів. Тому Facebook активно розвиває свої відділи, які відповідають за збільшення користувачів, аналіз даних, рекламу та юридичні аспекти.

Ми живемо в епоху, коли прибуток пов'язаний з персональними даними, тому всі користувачі наражені на ризики, пов'язані з неправомірним використанням своїх персональних даних третіми особами. Наприклад, якщо сайт знайомств не може захистити дані користувачів або починає торгувати ними

з недобросовісними рекламодавцями, це може призвести до спаму та інших неприємностей. В Україні такі ситуації стають все більш поширеними, що підтверджує дослідження провідних українських технологічних компаній щодо захисту персональних даних.

Згідно з проведеним дослідженням, восьмом з двадцяти обраних компаній отримали менш ніж 50% балів за захист персональних даних у своїй корпоративній політиці, що свідчить про низький рівень захисту цих даних. Серед них були такі компанії, як Eldorado.ua, DataGroup.ua, Lifecell.ua, Rozetka.com.ua, Makeup.com.ua, Silpo.ua, Lanet.ua і Triolan.com.

Наприклад, на веб-сайтах компаній Vodafone.ua, Silpo.ua, Triolan.com і Lanet.ua відсутня відмітка, що користувач дає згоду на оброблення його персональних даних, хоча це є вимогою законодавства. Десять компаній не повідомляють своїх користувачів про те, як довго вони будуть зберігати їхні дані. На сайтах Triolan.com, Makeup.com.ua, Silpo.ua та Lanet.ua користувачі не мають можливості видалити свої особисті дані. Із п'ятнадцяти досліджуваних компаній не описано процедуру видалення акаунту користувача після припинення договору або за умов некористування акаунтом. Додатково, десять компаній не розкривають місце зберігання даних користувачів, тобто розташування серверів залишається невідомим.

Це дослідження висвітлює проблему серед багатьох українських компаній, які не дотримуються правил захисту персональних даних користувачів, а також наголошує на нестачі адекватного правового регулювання цього питання в Україні. Виникає питання про компенсацію завданої шкоди через порушення правил користування персональними даними користувачів.

Чинне законодавство передбачає два можливі шляхи відшкодування завданої шкоди у таких випадках:

1. Відшкодування завданої шкоди через порушення умов договору.
2. Відшкодування шкоди за принципом дії виникає через делікт.

Більшість юристів рекомендує ознайомитися з усіма умовами платформи (умовами використання, політикою конфіденційності, правилами використання

файлів cookie і т. д.), оскільки ці документи визначають правила використання приватної інформації користувачів. Міжнародна судова практика і позиція міжнародних регуляторів визнають ці умови як публічну пропозицію та публічний договір. Наприклад, реєстрація облікового запису вважається прийняттям умов платформи. Таким чином, умови платформи є обов'язковими для виконання.

Проте реальність показує, що багато користувачів, зіткнувшись з довгими контрактами, не бажають читати політику конфіденційності, оскільки розуміють, що без погодження з нею вони не зможуть використовувати продукт. Користувачі готові передавати свою особисту інформацію інтернет-компаніям через невдоволення вивчати технічні деталі використання їх даних. Не всі користувачі розуміють, як саме компанії будуть використовувати їхні дані, але навіть ті, хто розуміє, можуть бути не в змозі відокремити розумні від нерозумних моделей використання, не кажучи вже про те, щоб контролювати, куди потрапляє їхня інформація.

У контексті обговорення умов використання платформи, виникає питання про відповідність загальним вимогам, встановленим законом, які необхідні для законності такого правочину. Ці вимоги передбачають, що зміст правочину не може протирічити інтересам держави і суспільства, його моральним засадам, а також, що воля учасника правочину має бути вільною та відповідати його внутрішній волі. Проте існують деякі проблеми, які ускладнюють відповідь на це питання.

По-перше, компанії мають велику владу змінювати умови своїх відносин зі споживачами без їхньої згоди. Більшість умов платформ дозволяють компаніям односторонньо змінювати ці умови без спеціальної згоди споживача. Ще більше, деякі компанії навіть не повідомляють споживачів про такі зміни, перекладаючи на них відповідальність за відстеження оновлень.

По-друге, компанії також мають можливість змінювати своє програмне забезпечення, послуги та пристрої. Наприклад, сучасна версія Facebook відрізняється від тієї, на яку підписувалися мільйони користувачів. Такі зміни

можуть включати оновлення, які стосуються безпеки та збору даних, проте часто не розкриваються користувачам.

По-третє, компанії зберігають право передавати інформацію про користувачів у разі злиття або продажу. Ці транзакції можуть становити загрозу конфіденційності даних, але часто здійснюються без відома або згоди користувачів.

Усі ці обставини свідчать про те, що умови використання платформ не завжди відповідають загальноприйнятим нормам та вимогам законодавства. Таким чином, можна сумніватися у здійсненні свободної волі користувача щодо передачі своїх персональних даних, навіть якщо він погодився з умовами безпосередньо чи навіть несвідомо.

У 2013 році більше чверті українських інтернет-користувачів здійснили покупки на eBay, Amazon та інших онлайн-торгових майданчиках. Прогнозується, що популярність цих платформ буде зростати, що поставить у складну ситуацію вітчизняних інтернет-магазинів. Аналітики стверджують, що у результаті в Україні залишиться лише декілька ресурсів, які зможуть впровадити передові технології та здобути довіру клієнтів. Тому українським інтернет-магазинам рекомендується підвищувати рівень довіри та обслуговування споживачів.

Зростає довіра не лише до закордонних, а й до українських інтернет-магазинів. У закордонних магазинах довіру споживачів впливають низькі ціни на товари, висока якість продукції, безкоштовна доставка, а у вітчизняних – переважно цінова політика на побутову техніку та електроніку. Тільки великі інтернет-магазини дотримуються стандартів якості обслуговування. Також для споживача важливі знаки довіри, такі як сертифікація третіми особами. Наприклад, веб-сайти VeriSign і Entrust проводять сертифікацію щодо перевірки автентичності та управління цифровими сертифікатами в Інтернеті.

Для зміцнення довіри між споживачами та інтернет-магазинами можна залучити довірених третіх осіб, так званих "брокерів довіри в Інтернеті",

наприклад, ePublicEye.com, який збирає дані споживачів та відгуки про постачальників різних товарів та послуг в Інтернеті.

Зарубіжні інтернет-магазини мають різні організації, які готові підтвердити їхню надійність та безпеку. У США та Канаді є BBBOnLine, у Великобританії – ShopSafe та Office of Fair Trading, в Європі – Eurochambres та Fedma, в Кореї – KIEC, а в Сінгапурі – CommerceNet, Singapore. Існує також Global Trustmark Alliance, яка об'єднує ці організації з метою переконати покупців у безпеці та надійності інтернет-магазину. В Україні наразі існує лише Асоціація учасників електронного бізнесу в Україні, яка планує здійснювати сертифікацію інтернет-магазинів у майбутньому.

Індивідуальна схильність споживача довіряти, особливо у випадках, коли він не має попереднього досвіду покупок в інтернет-магазинах, може впливати на його рівень довіри. Згідно з дослідженням Hofstede, 1980, ця схильність визначається культурним середовищем, типом особистості та рівнем досвіду.

Схильність довіряти є особистісною характеристикою, яка впливає на те, як покупець оцінює надійність продавця. Чим вищий цей рівень, тим більший вплив мають атрибути довіри на загальне формування довіри.

Досліджено концептуальну модель довіри споживачів до інтернет-магазинів, зокрема в просторі онлайн середовища. Важливо розглянути питання будування та підтримки довіри самими відвідувачами сайту магазину. Наприклад, 42% покупців формують своє уявлення про сайт на основі його дизайну, тоді як 52% користувачів ніколи не повернуться на сайт, який їм не сподобався з естетичної точки зору [26].

Довіру споживачів до сайту можна розглядати через призму його наповнення: графічний дизайн, структура, контент та дизайн, які гармонізуються з очікуваннями цільової аудиторії.

Навіть якщо веб-сторінка має оптимізований інтерфейс, спрямований на підвищення довіри споживачів через дизайн, важливо також інформувати клієнтів про можливі ризики та їхні права на захист. Дослідження показали, що лише 12% респондентів, які надають свої особисті дані, розраховують на

отримання якоїсь вигоди або спеціальних пропозицій відповідно до цього. Ще 26% не вбачають власних особистих даних як цінності і не висловлюють стурбованості щодо їхнього використання. Близько 41% знають, що соціальні мережі можуть використовувати їхні дані для рекламних цілей, тоді як 34% розуміють, як захищати свою конфіденційність у веб-браузері. У сучасних умовах лише дуже мало відвідувачів веб-сайтів повідомляють про проблеми з інтернет-магазинами та порушення конфіденційності. Оскільки рівень довіри кожного покупця є динамічним та залежить від його дій і реакцій, інтернет-магазинам рекомендується створювати довірчі відносини зі своїми клієнтами.

Виникає ідея впровадження поняття "страхування від інтернет-загроз". Деякі учасники ринку інтернет-торгівлі можуть діяти як гаранти під час здійснення угод. Страхування може бути корисним у двох аспектах довіри: перш за все, для покупця, який бажає переконатися, що товар буде доставлений вчасно та в незмінному стані; і, звичайно ж, для продавця, який бажає переконатися, що покупець виплатить за отриманий товар.

У наш час обробка інформації досягла небаченого рівня, і це тільки початок зростання збору особистих даних окремими організаціями та компаніями для різних цілей. Використання цих даних часто відбувається без прозорості для осіб, чий приватний життєвий простір безпосередньо стосується цих даних. Експерти вважають, що існуючі правові механізми та згоди для відповідальної та безпечної обробки даних є недостатньо ефективними. У 2019 році Комісія уряду Німеччини з етики даних прийшла до висновку, що більшість онлайн-сервісів, заснованих на даних, фактично займаються торгівлею як самими даними, так і аналітичними результатами для здобуття прибутку. Однак неможливо уявити розвиток торгівлі в цифрову епоху без сучасних інтернет-платформ, і споживачі послуг постійно виражають стурбованість стосовно безпеки зберігання інформації та захисту своїх особистих даних. Якщо раніше опитування було єдиним способом отримання об’єктивної інформації про особисті мотиви поведінки споживачів, то сьогодні клієнти генерують все більше даних завдяки проведенню значної кількості часу в Інтернеті. Аналіз цих

даних дає готеліерам змогу краще зрозуміти потреби своїх клієнтів та надати індивідуальні послуги, що підвищує ймовірність позитивного вибору їх закладу гостинності.

Персональні дані є поширеними у цифровому середовищі і можуть бути дуже цінними, ведучи до ненавмисного вторгнення у приватне життя власника даних. Однак хоча окремі особи можуть бути занепокоєні щодо розголошення своєї особистої інформації, вони зазвичай не виявляють поведінкової обережності. Цінність, культура і самооцінка особистих даних залежить від індивідуальних та міжкультурних відмінностей, таких як колективістська або індивідуалістична культури. Наприкінці березня 2018 року стало відомо, що компанія Cambridge Analytica використала недозволено зібрані дані з профілів понад 87 мільйонів користувачів Facebook для створення психографічної адаптованої реклами, яка, як стверджується, впливала на уподобання під час президентських виборів у США 2016 року. Проте після цього інциденту багато осіб не видалили свої облікові записи, не змінили налаштування конфіденційності та навіть не виявили стурбованості, вважаючи, що вони не вразливі до такого виду реклами та не розуміючи, як автоматизовані підходи та алгоритми працюють із їхніми особистими даними. Аналіз набору даних про лайки користувачів Facebook показує, що ці цифрові записи можуть служити для автоматичного та точного прогнозування різноманітних особистих атрибутів, таких як сексуальна орієнтація, етнічна приналежність, релігійні та політичні погляди, особистість, рівень інтелекту, щастя, звички вживання речовин, розлучення з батьками, вік і стать [27].

Для дослідження чинників, що впливають на довіру до онлайн-сервісів та бажання молоді зберегти приватність шляхом відмови від розкриття особистих даних у Інтернеті або бажання ними ділитись, було проведено опитування 129 студентів (віком від 18 до 23 років; 30,2% чоловіків, 69,8% жінок). Незважаючи на стрімкий розвиток Інтернет-сервісів, більшість респондентів у своєму виборі чи довіряти все ще керуються рекомендаціями друзів та знайомих (див. рис. 1).

Цікавим є той факт, що лише 4,7% опитаних користуються інформацією, розміщеною на офіційному веб-сайті, приймаючи рішення. Низький показник може пояснюватися складністю пошуку, оскільки лише 27,9% всіх опитаних зверталися до сайту. Таким чином, лише 11,6% респондентів не мали жодних проблем із знаходженням необхідної інформації (див. рис. 2) [18].

Використання мобільних додатків дозволяє клієнтам швидко та зручно знаходити відповіді на стандартні запитання щодо роботи онлайн-сервісів, але вимагає введення персональних даних під час реєстрації. Більшість опитаних не вважають проблемою подальшу конфіденційність своїх особистих даних, або вважають, що це не настільки важливо порівняно з можливими перевагами використання сайту або мобільних додатків (див. рис. 3).

Програми лояльності, які використовуються в онлайн-сервісах, часто мають за мету створення баз даних з особистої інформації клієнтів. Практично всі респонденти (97,8%) висловлюють занепокоєння щодо подальшого використання їхніх особистих даних і тому не виявляють інтересу до участі в програмах лояльності. Крім того, 39,5% опитаних вважають, що можлива нав’язлива реклама та акційні пропозиції є основною причиною їхнього занепокоєння при реєстрації (див. рис.4). Крім того, не існує чіткого розуміння того, кому належатимуть дані після їх передачі компанії, оскільки клієнти бажають залишити за собою право власності на свої особисті дані [18].

Під час внесення особистих даних 93% опитаних вказують свій діючий номер телефону, але лише 58,1% – постійну електронну адресу. Для реєстрації на веб-сайтах майже 35% респондентів створюють окремі електронні адреси, щоб уникнути надмірної реклами. Іншою причиною таких дій є недоуміння клієнтів про те, які переваги вони можуть отримати від надання електронної адреси та тривалість зберігання цих даних [18].

Збільшення обсягу персональних даних в Інтернеті позбавляє людей контролю над їхньою особистою інформацією, яка може використовуватися для аналізу без додаткової згоди. Споживачі, які піклуються про приватність і намагаються обмежувати доступ до своїх особистих даних, стикаються зі

значними труднощами і мають обмежений вибір інструментів. Фактично, відмова від надання особистих даних створює економічні та психологічні перешкоди, оскільки вона передбачає оплату готівкою, що ускладнюється порівняно з електронними платежами, або відмову взагалі від покупки товару чи послуги. Для покращення спілкування з клієнтами онлайн-сервіси повинні звернути увагу на етичні аспекти зберігання та використання персональних даних клієнтів, а також надавати третім особам для аналізу лише анонімні дані, щоб підвищити рівень довіри.

2.3. Проблеми впровадження онлайн-сервісів для споживачів під час російсько-української війни

Проблеми впровадження онлайн-сервісів для споживачів під час російсько-української війни пов'язані з різними факторами. По-перше, конфлікт між Росією та Україною спричинив значну нестабільність у регіоні, що призвело до складнощів у забезпеченні надійності і безпеки онлайн-сервісів. Бойові дії, блокади та інші обмеження можуть призвести до перебоїв у доступі до Інтернету та інфраструктурних проблем для провайдерів цифрових послуг.

По-друге, політичні та економічні санкції, які були введені проти Росії, можуть мати вплив на доступність певних онлайн-сервісів для користувачів у цьому регіоні. Це може бути пов'язано з обмеженням доступу до платформ або послуг, які мають російське походження, а також з фінансовими обмеженнями, які впливають на роботу платіжних систем та електронних грошей.

По-третє, сама соціально-психологічна ситуація в регіоні може впливати на сприйняття та використання онлайн-сервісів. Воєнний конфлікт може призвести до зростання страху серед населення щодо конфіденційності даних та безпеки в Інтернеті. Крім того, ескалація напруги може спричинити психологічний стрес та відволікання від онлайн-активностей.

У цілому, впровадження онлайн-сервісів для споживачів під час російсько-української війни стикається з різними викликами, пов'язаними з безпекою, доступністю та соціально-психологічними аспектами.

Звичайно, ось кілька прикладів проблем, які можуть виникнути впродовж російсько-української війни:

1. Перебої у доступі до Інтернету. Воєнні дії можуть призвести до пошкодження інфраструктури зв'язку, такої як кабелі та телекомунікаційні вежі, що може призвести до перебоїв у доступі до Інтернету для користувачів.
2. Обмеження доступу до певних платформ і сервісів. Державні органи можуть ввести обмеження на доступ до певних інтернет-ресурсів або платформ, які вони вважають неприйнятними чи небезпечними у зв'язку з військовою ситуацією.
3. Безпека даних. Зростаюча кількість кібератак та хакерських атак може підірвати довіру користувачів до онлайн-сервісів, особливо в умовах війни, коли інформаційна безпека стає особливо важливою.
4. Економічні обмеження. Фінансові санкції та обмеження можуть вплинути на доступність платних онлайн-сервісів, таких як стрімінгові платформи або онлайн-магазини, для користувачів у зоні конфлікту.
5. Психологічні наслідки. Підвищений рівень стресу та тривоги серед населення у зоні конфлікту може призвести до зменшення зацікавленості у використанні онлайн-сервісів, а також зростання побоювань щодо конфіденційності та безпеки даних в Інтернеті.

Зростаюча загроза кібератак та хакерських атак може миттєво підірвати довіру користувачів до інтернет-платформ та сервісів. Військовий конфлікт, особливо між країнами, може спровокувати ще більше агресивних дій у кіберпросторі, оскільки інформаційні системи стають одним із основних об'єктів для атаки. Втрати даних, порушення конфіденційності та доступ до особистої інформації можуть значно підірвати віру користувачів у безпеку інтернет-платформ. Це може призвести до відмови від користування онлайн-сервісами та переходу до менш небезпечних, але менш зручних альтернатив. Тому захист даних стає надзвичайно важливою задачею для будь-якої компанії або сервісу, особливо в умовах військового конфлікту.

В Україні виявлено два методи блокування інтернет-ресурсів, як пояснює Максим Дворовий, головний юрист громадської організації "Лабораторія цифрової безпеки". Перший тип блокування здійснюється за допомогою закону "Про санкції", що прийняли ще у 2014 році, та відповідними указами президента. Наприклад, у 2017 році такі закони дозволили заблокувати сервіси чотирьох російських компаній: "ВКонтакте", "Одноклассники", "Яндекс" та "Mail.ru".

Згідно з аналітичним звітом "Лабораторії цифрової безпеки", з того часу застосовано таку санкцію щодо понад 600 інтернет-ресурсів різноманітного спрямування, від сайтів органів окупаційної влади у Криму до російських онлайн-магазинів літератури, а також донецьких та луганських квазімедіа та сторінок платіжних систем у соціальних мережах Facebook та Twitter.

Другий метод блокування, новіший, запрацював після введення воєнного стану на території України у 2022 році. Це блокування, здійснюване у межах виконання розпоряджень Національного центру оперативно-технічного управління електронними комунікаційними мережами України (НЦУ), який діє під керівництвом Держспецзв'язку. Його повноваження визначається постановою Кабінету міністрів України № 812 "Деякі питання оперативно-технічного управління телекомунікаційними мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану".

Загалом, НЦУ відповідає за контроль та відновлення функціонування телекомунікаційних мереж у разі їх пошкодження, а також видавання розпоряджень щодо оперативно-технічного управління цими мережами, які обов'язково виконують провайдери.

Держспецзв'язок заявляє, що для блокування необхідні рішення Ради національної безпеки та оборони України, які визначають перелік ресурсів. Ці рішення набувають законної сили після указів президента.

Після широкомасштабного вторгнення список російських ресурсів, які підлягали блокуванню, був значно розширений та уточнений, повідомило ДОУ у відомстві. Це включає автономні системи, які використовує Росія для кібератак на українські інформаційні ресурси та поширення неправдивої

пропагандистської інформації щодо перебігу вирішеної війни та для дискредитації органів влади.

Питання щодо застосування, скасування та внесення змін до санкцій розглядає Рада національної безпеки та оборони України, а потім передає їх на розгляд Верховній Раді, президентові, Кабміну, Нацбанку та СБУ.

Наприклад, 27 лютого 2022 року НЦУ видало розпорядження про блокування автономних систем (AS) (повний перелік доступний на їхньому сайті). Це призвело до заблокування понад 48 мільйонів IP-адрес у російському сегменті Інтернету, що суттєво обмежило доступ до російських веб-сайтів. Однак, зауважують у "Лабораторії цифрової безпеки", наскільки успішно провайдери виконали це розпорядження, невідомо, оскільки звіти про це не є публічними.

"Сутність розпоряджень НЦУ не деталізується в нормативних актах. Відповідно, НЦУ може зобов'язувати постачальників електронних комунікаційних послуг обмежувати доступ до окремих Інтернет-ресурсів", - пояснюють експерти "Лабораторії цифрової безпеки".

Умови російсько-української війни створили значні перешкоди для впровадження онлайн-сервісів для споживачів. Кібербезпека стала однією з ключових проблем, оскільки зросла загроза кібератак та хакерських атак. Безпека даних стала надзвичайно важливою, оскільки існує ризик несанкціонованого доступу до особистої інформації користувачів через кібератаки. Обмеження доступу до певних платформ і сервісів також ускладнює використання онлайн-сервісів для споживачів. Враховуючи ці фактори, важливо розробляти та впроваджувати ефективні заходи з кібербезпеки та захисту даних для забезпечення безпечного користування онлайн-сервісами під час конфлікту.

2.4. Рекомендації для бізнесів щодо покращення захисту даних

Забезпечення безпеки даних для бізнесу стає все більш важливим у сучасному цифровому світі. Ось кілька рекомендацій для покращення захисту даних:

1. Встановлення міцної кібербезпекової політики, яка включає в себе правила щодо паролів, доступу до даних і захисту від вірусів та шкідливих програм.

2. Регулярне навчання персоналу з питань кібербезпеки, щоб працівники були усвідомлені щодо потенційних загроз і знали, як діяти в разі кібератаки.

3. Використання надійного програмного забезпечення для захисту мережі і системи від несанкціонованого доступу та вірусів.

4. Регулярне оновлення програмного забезпечення та виявлення і виправлення вразливостей для запобігання експлуатації потенційних слабкостей.

5. Застосування шифрування для захисту конфіденційної інформації під час передачі через мережу і зберігання на пристроях.

6. Регулярні аудити безпеки для перевірки ефективності заходів захисту даних і виявлення можливих проблем.

7. Резервне копіювання даних і забезпечення їх доступності в разі катастроф або кібератак.

8. Встановлення строгих правил доступу до даних і обмеження прав доступу залежно від потреб користувачів.

9. Співпраця з професійними консультантами з кібербезпеки для розробки і впровадження комплексних стратегій захисту даних.

10. Постійне моніторинг та відслідковування активності в мережі для виявлення підозрілих дій і негайної реакції на потенційні загрози.

Ось кілька рекомендацій щодо впливу на довіру споживачів до онлайн-сервісів:

1. Прозорість. Забезпечте чіткість та прозорість у використанні даних. Інформуйте користувачів про те, які саме дані збираються, як вони будуть використовуватися і кому можуть бути передані.

2. Безпека. Зробіть безпеку даних пріоритетом. Захистіть особисту інформацію користувачів за допомогою надійних технологій шифрування та інших методів захисту.

3. Дотримання правил. Впевніться, що ваші сервіси дотримуються всіх законів та нормативних вимог, що стосуються захисту даних.

4. Контроль над даними. Надайте користувачам можливість контролювати свої дані, включаючи можливість видаляти, редагувати або обмежувати доступ до них.

5. Підтримка клієнтів. Забезпечте ефективну підтримку клієнтів у разі запитів або проблем, пов'язаних з безпекою даних.

6. Відкритість до зворотного зв’язку. Створіть механізми для збору відгуків користувачів і відкритість до їхніх пропозицій та скарг щодо політики захисту даних.

7. Освіта користувачів. Забезпечте користувачів необхідною інформацією та ресурсами щодо кібербезпеки та захисту їхніх особистих даних.

8. Чесність та довіра. Дотримуйтесь обіцянок, які ви даєте користувачам, і будуйте довіру шляхом чесного та етичного ведення бізнесу.

9. Аудит безпеки. Проводьте регулярні аудити безпеки для виявлення потенційних порушень або вразливостей у системі.

Узагальнюючи, необхідно постійно вдосконалювати політику захисту даних і впроваджувати нові технології та методи захисту.

ВИСНОВКИ ДО РОЗДІЛ 2

Дослідження показало, що стан захисту даних в онлайн-сервісах є важливою проблемою, яка потребує постійної уваги та вдосконалення. Аналіз сучасного стану виявив, що багато онлайн-сервісів не забезпечують належного рівня безпеки даних, що призводить до численних інцидентів витоку інформації та порушень конфіденційності.

Однією з основних проблем є недостатня прозорість у використанні та обробці персональних даних користувачів. Багато сервісів не інформують своїх клієнтів про те, як їхні дані збираються, зберігаються і використовуються, що викликає недовіру та занепокоєння серед споживачів. Крім того, відсутність ефективних механізмів контролю за доступом до даних і їхнім зберіганням створює ризики несанкціонованого доступу та використання інформації.

Дослідження показало, що більшість користувачів вважають захист своїх персональних даних дуже важливим фактором при виборі онлайн-сервісів. Однак, багато з них стикаються з труднощами у забезпеченні конфіденційності своїх даних через недостатню освіченість у питаннях кібербезпеки та складність існуючих механізмів захисту.

Перспективи покращення захисту даних в онлайн-сервісах пов'язані з впровадженням нових технологій та вдосконаленням існуючих методів захисту. Зокрема, важливим є застосування сучасних інструментів шифрування, двофакторної аутентифікації та систем виявлення аномалій у мережевій активності. Крім того, необхідно підвищувати рівень освіченості користувачів щодо питань кібербезпеки та забезпечувати їм можливість контролювати свої дані.

Таким чином, для забезпечення надійного захисту даних в онлайн-сервісах необхідно впроваджувати сучасні технології захисту, підвищувати прозорість процесів обробки даних та активно працювати над покращенням освіченості користувачів щодо питань кібербезпеки. Це дозволить не лише забезпечити

безпеку особистої інформації, але й підвищити довіру споживачів до онлайн-сервісів.

ВИСНОВКИ

Висновки роботи підтверджують важливість захисту даних у сучасному інтернет-середовищі. Проведено огляд сучасних методів та інструментів захисту даних, таких як шифрування, двофакторна аутентифікація, використання мережевих брандмауерів та антивірусного програмного забезпечення, що дозволило встановити їхню ефективність у запобіганні кіберзагрозам. Вивчено правові аспекти захисту даних в контексті онлайн-сервісів, зокрема звернуто увагу на GDPR та інші регуляторні акти, які встановлюють вимоги до обробки особистих даних. Ці нормативні документи є фундаментальними для забезпечення прав користувачів і накладають на компанії обов’язок щодо прозорості та відповідальності у використанні персональної інформації. Досліджено вплив заходів із захисту даних на довіру споживачів, виявлено, що ефективна політика захисту даних значно підвищує довіру споживачів до онлайн-сервісів. Зокрема, користувачі схильні більше довіряти сервісам, які відкрито інформують про свої заходи безпеки та надають можливість контролювати свої дані. Проаналізовано статистичні дані щодо інцидентів витоку даних та їх впливу на репутацію онлайн-сервісів, що дозволило виявити, що навіть один випадок порушення безпеки може суттєво підірвати довіру споживачів і призвести до втрати клієнтів. Це підкреслює необхідність для компаній мати чіткі процедури реагування на інциденти та комунікації з користувачами. Проведено опитування користувачів онлайн-сервісів для виявлення їхньої думки про важливість захисту даних. Результати свідчать про те, що більшість користувачів вважають захист особистих даних однією з ключових пріоритетних вимог при використанні онлайн-сервісів. Це свідчить про високий рівень обізнаності та вимогливості сучасних користувачів щодо конфіденційності та безпеки своїх даних. На основі проведеного аналізу та

досліджень розроблено рекомендації для покращення заходів із захисту даних, включаючи посилення технічних заходів безпеки, підвищення освіченості персоналу, вдосконалення політик конфіденційності та активну комунікацію з користувачами щодо заходів захисту даних. Ці рекомендації спрямовані на підвищення рівня захисту даних та формування більшої довіри користувачів. Загальний висновок дослідження полягає в тому, що ефективний захист даних є критично важливим для забезпечення довіри споживачів до онлайн-сервісів та успішної діяльності підприємств в цифровому середовищі. Безпека даних не лише сприяє збереженню довіри споживачів, але й є ключовим чинником успіху для бізнесу в цифровому світі, підвищує репутацію компанії, зменшує ризики витрат на компенсацію шкоди внаслідок порушень безпеки, а також сприяє покращенню взаєморозуміння з клієнтами та зміцненню їхньої довіри. Таким чином, захист даних є стратегічно важливою складовою для будь-якої організації, що працює в онлайн-середовищі.