УДК 004.056:004.738.5(045) DOI: 10.31673/2412-4338.2020.010919

Ахрамович В. М., Чегренець В.М. *Державний університет телекомунікацій, Київ*

ТЕНДЕНЦІЇ РОЗВИТКУ ЗАХИСТУ ДАНИХ В СОЦІАЛЬНИХ МЕРЕЖАХ

Проведено аналіз захисту персональних та інших даних в соціальних мережах, вказано, що у адміністраторів та власників централізованих соціальних мереж є досьє на кожного із зареєстрованих користувачів, в якому є практично все – від паспортних даних до особистих переваг і поведінки в той чи інший час доби. Щоб протиставити проблемі зловживань з боку адміністраторів та власників соціальних мереж, необхідно виконати огляд рішень конфіденційності приватних даних користувачів. Вказані рішення характеризуються децентралізованим підходом через архітектуру клієнт-сервер, хмари або одноранговi мережі, такі рішення пропонують зберігати дані всіх користувачів в розподіленому вигляді.

У цій статті ми розглянули та порівняли параметри кількох децентралізованих соціальних мереж: клієнтсько-серверні мережі (Fediverse, Diaspora, Persona, Lockr, Vis-a-Vis, тощо); мережі на основі P2P (Peerson, Lifesocial.KOM, Prometheus, SETI @ Home, Distributed.net тощо). Основними перевагами мереж P2P є те, що: 1) вони не потребують спеціального адміністрування (нульовий адміністративний підхід); 2) вони мають самоорганізацію та пристосованість; 3) користувачі вміють вільно з'єднуватися та залишати мережу; 4) системи P2P автоматично обробляють ці події; 5) вони можуть комбінувати та використовувати великі обчислювальні ресурси для зберігання даних, тому що кожен вузол у системі P2P приносить деякі власні ресурси, наприклад, обчислювальну потужність чи пам'ять; 6) конфіденційність. Використовуючи локальну структуру P2P, користувачі можуть уникнути необхідності передавати будь-яку інформацію про себе комусь іншому. FreeNet – це прекрасний приклад того, як анонімність може бути вбудована в додаток P2P. Він надсилає повідомлення через інші вузли, щоб унеможливити відстеження оригінального автора. Це збільшує анонімність, використовуючи ймовірнісні алгоритми таким чином, що відстежувати шлях користувача під час аналізу мережевого трафіку непросто. Зазначено, що жодна з досліджуваних децентралізованих соціальних мереж не забезпечує комплексний захист персональних даних користувача та інших параметрів безпеки. Розглянуто та співставлено параметри декількох децентралізованих соціальних мереж, вказано, що жодна з досліджених децентралізованих соціальних мереж не забезпечує комплексного захисту персональних даних користувача та інших параметрів безпеки.

Ключові слова: *децентралізовані Інтернет соціальні-мережі, профіль користувача, персональні дані, групи даних, експерт, досьє, власники мереж, обчислювальні ресурси, хеш-таблиця, криптографія, ідентифікатор.*

Akhramovych V. M., Chegrenec V. M. *State University of Telecommunications, Kyiv*

DATA PROTECTION TENDENCIES ON SOCIAL NETWORKS

The analysis of personal and other data protection on social networks was conducted, also we pointed out that administrators and owners of centralized social networks have a dossier for all registered users, which has practically everything – from passport data to personal preferences and behavior at one or another time. To resist the problem of abuse by administrators and social network owners, you need to review all possible solutions for providing confidentiality of personal data. These solutions are characterized by a decentralized approach through client-server, cloud, or peer-to-peer architecture, offering to store the data of all users in a distributed form.

At this article we considered and compared the parameters of several decentralized social networks: client-server-based networks (Fediverse, Diaspora, Persona, Lockr, Vis-a-Vis, etc.); P2P-based networks

(Peerson, Lifesocial.KOM, Prometheus, SETI @ Home, Distributed.net etc.). The main advantages of P2P networks are: 1) they does not require special administration (zero administration approach); 2) they possess self-organization and adaptability; 3) peers are able to connect and leave the network freely; 4) P2P systems handle these events automatically; 5) they can combine and use huge computing resources to store data, because an each node in the P2P system brings some own resources, such as computing power or memory; 6) privacy. Using a locally-based P2P structure, users can avoid the need to pass any information about themselves to anyone else. FreeNet is a prime example of how anonymity can be built into a P2P application. It sends messages through other nodes to make it impossible to track the original author. This increases anonymity by using probabilistic algorithms in such a way that it is not easy to track a user's path while analyzing network traffic. We indicated that none of the investigated decentralized social networks provides comprehensive protection of the user's personal data and other security parameters.

Keywords: *decentralized Internet social networks, user profile, personal data, data groups, expert, dossier, network owners, computing resources, hash table, cryptography, identifier.*

Ахрамович В. Н., Чегренец В.М. *Государственный университет телекоммуникаций, Киев*

ТЕНДЕНЦИИ РАЗВИТИЯ ЗАЩИТЫ ДАННЫХ В СОЦИАЛЬНЫХ СЕТЯХ

Проведен анализ защиты персональных и других данных в социальных сетях, указано, что у администраторов и владельцев централизованных социальных сетей имеется досье на каждого из зарегистрированных пользователей, в котором есть практически все - от паспортных данных с личными предпочтениями и поведения в то или иное время суток. Чтобы противопоставить проблеме злоупотреблений со стороны администраторов и владельцев социальных сетей, необходимо выполнить обзор решений конфиденциальности личных данных пользователей. Указанные решения характеризуются децентрализованным подходом через архитектуру клиент-сервер, облако или одноранговые сети, такие решения предлагают хранить данные всех пользователей в распределенном виде.

В этой статье мы рассмотрели и сравнили параметры нескольких децентрализованных социальных сетей: клиентские-серверные сети (Fediverse, Diaspora, Persona, Lockr, Vis-a-Vis и т.д.); сети на основе P2P (Peerson, Lifesocial.KOM, Prometheus, SETI @ Home, Distributed.net и т.д.). Основными преимуществами сетей P2P является то, что: 1) они не требуют специального администрирования (нулевой административный подход); 2) они имеют самоорганизацию и приспособленность; 3) пользователи умеют свободно соединяться и оставлять сеть; 4) системы P2P автоматически обрабатывают эти события; 5) они могут комбинировать и использовать большие вычислительные ресурсы для хранения данных, потому что каждый узел в системе P2P приносит некоторые собственные ресурсы, например, вычислительную мощность или память; 6) конфиденциальность. Используя локальную структуру P2P, пользователи могут избежать необходимости передавать любую информацию о себе кому-то другому. FreeNet – это прекрасный пример того, как анонимность может быть встроена в приложение P2P. Он посылает сообщение через другие узлы, чтобы исключить отслеживания оригинального автора. Это увеличивает анонимность, используя вероятностные алгоритмы таким образом, что отслеживать путь пользователя при анализе сетевого трафика непросто. Отмечено, что ни одна из исследуемых децентрализованных социальных сетей не обеспечивает комплексную защиту персональных данных пользователя и других параметров безопасности. Рассмотрены и сопоставлены параметры нескольких децентрализованных социальных сетей, указано, что ни одна из исследованных децентрализованных социальных сетей не обеспечивает комплексной защиты персональных данных пользователя, и других параметров безопасности.

Ключевые слова: *децентрализованные Интернет социальные сети, профиль, персональные данные, группы данных, эксперт, досье, владельцы сетей, вычислительные ресурсы, хеш-таблица, криптография, идентификатор.*

1. Вступ. Реєструючись в соціальній мережі, ви заповнюєте профіль користувача: вказуєте адресу електронної пошти, номер телефону, ім'я, прізвище, вік, завантажуєте свої фото. Потім вам пропонують заповнити анкету, де ви можете перерахувати навчальні заклади, які ви закінчили, вказати сферу занять, інтересів, місце роботи, сімейний статус, місце народження та інше. Крім цих даних такі великі соціальні мережі, як Facebook, «ВКонтакте», Instagram, збирають про вас відомості у міру того, як ви користуєтеся їх сервісами. Розглянемо цей процес на прикладі найбільшої соціальної мережі в світі - Facebook. В цілому джерела інформації можна поділити на два типи: ті, які знаходяться в самому Facebook - так звані «внутрішні джерела», а також «цифрові відбитки», які збираються з вашого смартфона, комп'ютера або ноутбука. «Внутрішні джерела» теж можна розділити на дві умовні групи: на інформацію з вашої персональної сторінки і на ваші дії в мережі. Друга група даних збирається на основі вашої поведінки в мережі. Сервери Facebook записують кожну ваше дію: система уважно стежить за тим, які сторінки ви відвідуєте, як часто ви це робите, які фото і відео викладаєте, якого роду інформацію шукаєте, якого роду публікації цікавлять, в який час доби найбільш активні і т. д Крім того, збирається історія вашого пошуку, дані про те, з ким ви обмінюєтеся особистими повідомленнями і - навіть зміст цих повідомлень.

Експерти одностайні в тому, що Facebook займається стеженням за контентом особистих повідомлень, і тому є докази: так, наприклад, в інтерв'ю агентству Reuters топ-менеджер з безпеки Facebook Джо Салліван повідомив, що один педофіл був затриманий поліцією завдяки стеження за допомогою алгоритмів Facebook за повідомленнями користувачів. Також в політиці конфіденційності Facebook (так само як і у інших найбільших соціальних мереж, таких як «ВКонтакте», Instagram, LinkedIn, китайській QQ або Twitter) є пункт про те, що «всі дані, які використовуються у Facebook, належать Facebook», що не забороняє, а навіть дозволяє їм переглядати ваші особисті повідомлення.

Другий тип даних – це так звані «цифрові відбитки», які збираються безпосередньо з вашого смартфона або ноутбука, що включають у себе ваші контакти, встановлені додатки, а також всі дані про вашу операційну систему. Крім перерахованого вище багато додатків, такі як Instagram і ВКонтакте, збирають так звану годинну: інформацію про ваші поточні і минулі місця розташування і частоті відвідування вами різних точок на карті.

Таким чином, у власників соцмереж є досьє на кожного із зареєстрованих користувачів, в якому є практично все – від паспортних даних до особистих переваг і поведінки в той чи інший час доби.

У березні колишній співробітник Кембріджського Університету Крістофер Уайлі (Christopher Wylie) докладно розповів про те, що компанія Cambridge Analytica не тільки збирала, але і незаконно користувалася персональними даними мільйонів користувачів. Особливе місце в його оповіданні займає можлива співучасть Facebook, після довгих зволікань Цукерберг був змушений виступити з досить безбарвними вибаченнями, за якими пішли обіцянки докласти всіх зусиль для вирішення найбільшої PR-кризи, яка, можливо, буде мати юридичні наслідки.

2. Аналіз останніх досліджень і публікацій. Дослідники Eytan Adar and Bernardo A. Huberman в статті [1] розглядають роботу централізованої соціальної мережі та роблять висновок про залежність персональних даних від власників мережі.

Randolph Baden, Adam Bender, Daniel Starin, Neil Spring, and Bobby Bhattacharjee в роботі [2], Miguel Castro, Peter Druschel, Anne-Marie Kermarrec and Antony Rowstron в [4], Kalman Gra, Christian Groÿ, Dominik Stingl, Daniel Hartung, Aleksandra Kovacevic and Ralf Steinmetz в [9], Nicolas Kourtellis, Joshua Finnis, Paul Anderson, Jeremy Blackburn, Cristian

Borcea and Adriana Iamnitchi в [11], Thomas Paul, Sonja Buchegger and Thorsten Strufe в [13], аналізують децентралізовану соціальну мережу та роблять деякі початкові рекомендації зі збереження персональних даних.

Sonja Buchegger, Doris Schiöberg, Le Hung Vu, and Anwitaman Datta в роботі [3], M Rogers and S Bhatti в [16]. перевіряють соціальні мережі на P2P основі та показують початкові дані для використання таких мереж.

Tom Chothia and Konstantinos Chatzikokolakis в [5], Lalana Kagal, Chris Hanson, and Daniel Weitzner в [10] досліджують загальний доступ користувачів до соціальної мережі та проблему збереження даних в ній.

Peter Druschel and Antony Rowstron в [6] досліджують можливість зберігання даних за допомогою утиліт.

Borko Furht в [7] порівняльно досліджує можливість зберігання даних в централізованих та можливих децентралізованих соціальних мережах.

S Goldwasser, S Micali, and C Racko в роботі [8] обговорюють складність зберігання даних в соціальних мережах.

Thomas Locher, Patrick Moor, Stefan Schmid and Roger Wattenhofer в роботі [12] розгядають мережу BitTorrent та можливість збереження конфіденційності користувача. David Recordon and Drummond Reed в [14] досліджують ідентифікацію та аудентифікацію користувачів в мережі. Sean Rhea, Brighten Godfrey, Brad Karp, John Kubiatowicz, Sylvia Ratnasamy,

Scott Shenker, Ion Stoica, and Harlan Yu. в [15] аналізують можливість використання прикладних програм, технологій, архітектури та протоколи комп'ютерних комунікацій мереж.

Ching Man Au Yeung, Ilaria Liccardi, Kanghao Lu, Oshani Seneviratne, and Tim Berners-Lee в [17] прогнозують використання децентралізованих соціальних мереж.

В літературі про мережі P2P вже вирішувалась проблема анонімного зв’язку [5,16] та пропонувались рішення, які підходять для спільного використання, але виявляються недостатніми в контексті децентралізованих Інтернет-соціальних мереж (ДОСМ). Як приклад, добре відома методика маршрутизації Onion [15], де вузол відправника рекурсивно шифрує секретний вміст відкритим ключем вузлів, що складають шлях, до якого повинен слідувати вміст, коли він приймається в мережі Friend-to-Friend (F2F), коли співрозмовники співпрацюють завдяки їх дружбі, вимагає від відправника знати топологію графів у соціальній мережі, тобто інформацію, яку сама ДОСМ має на меті захищати. З іншого боку, коли мережа P2P не є F2F, потрібні відповідні стимулюючі механізми для співпраці між користувачами.

3. Постановка завдання.

Проаналізувавши наведені дані, параметри, функції соціальних мереж, відмічаємо загальну тенденцію розвитку соціальних мереж в сторону децентралізації в плані збереження персональних даних користувачів, робимо висновок, що необхідно дослідити різні типи децентралізованих соціальних мереж, їх характеристики, встановити недоліки та переваги збереження персональних даних в них.

4. Результати дослідження.

Децентралізовані Інтернет соціальні-мережі (ОСМ). Щоб протиставити проблемі зловживань з боку адміністраторів та власників соціальних мереж (СМ), необхідно виконати огляд рішень конфіденційності приватних даних користувачів.

Вказані рішення характеризуються децентралізованим підходом через архітектуру клієнт-сервер, хмара або однорангові мережі, такі рішення пропонують зберігати дані всіх користувачів в розподіленому вигляді. В останні роки було запропоновано кілька рішень [13] з метою запобігання присутності будь-якої всезнаючої сутності. Ці рішення, відомі як децентралізовані Інтернет-соціальні мережі (ДОСМ) [7], спрямовані на розповсюдження створеного користувачем вмісту: у всіх них дані користувачів доступні з декількох локацій. Обмеження доступу до таких конфіденційних даних часто забезпечується прийняттям методів шифрування або списків контролю доступу. Поточні ДОСМ можна розділити на дві основні групи:

–децентралізовані ОСМ на базі клієнт-сервер;

–СМ на базі P2P.

Перебуваючи в ДОСМ на базі клієнт-сервера, кожен користувач контролює одну або декілька (принаймні логічно) централізованих обчислювальних служб і служб зберігання даних, що працюють в реальній або віртуальній інфраструктурі.

На основі P2P ДОСМ кожен вузол користувача приєднується до відомої або виділеної мережі P2P, де обчислювальні ресурси та сховища діляться між користувачами.

Децентралізовані СМ на основі клієнта-сервера. Розподілені спеціалізовані серверні підходи вимагають придбання або розгортання веб-простору, де розміщені особисті чутливі дані користувачів, доступ до яких обмежений лише авторизованими користувачами. На користь гарантії повної доступності даних вони часто вимагають від користувача ОСМ оплати послуги зберігання, або обслуговування технічної інфраструктури. Коли послуга зберігання даних надається безкоштовно, у цих рішеннях часто відсутні механізми стимулювання, що гарантують надійність послуги [17]. Пропонується обмежений вибір, який дозволяє користувачам обирати один або кілька надійних серверів для розміщення декількох ресурсів, кожен з яких ідентифікований URI, URI - уніфікований (однаковий) ідентифікатор ресурсу, наприклад, журнал їх діяльності, фотоальбом та, що найголовніше, їх Friend-Of- (знайомі, друзі і т.д). Інформація A-Friend (FOAF), (англ. Friend of a Friend) - проект по створенню моделі машинно-читаних домашніх сторінок і соціальних мереж, заснований Ліббі Міллером і Деном Бріклі. Серцем проекту є специфікація, яка визначає деякі вирази, які використовуються в висловлюваннях (англ. Statements) про будь-кого, наприклад: ім'я, стать та інші характеристики. Щоб послатися на ці дані використовується ідентифікатор, що включає унікальні властивості одного (наприклад, SHA1 сума від E-Mail адреси, Jabber ID, або URI домашньої сторінки, веблогу), яку можна редагувати за допомогою відкритих протоколів, таких як WebDAV2 (WebDAV (Web Distributed Authoring and Versioning) або просто DAV - набір розширень і доповнень до протоколу HTTP, що підтримують спільну роботу користувачів над редагуванням файлів і управління файлами на віддалених веб-серверах). У вказаних рамках користувачі отримують ідентифікацію у вигляді URI (Web ID), що вказує на посилання у FOAF користувача, яке зберігається на надійному сервері, що, в свою чергу, вказує на веб-ідентифікатор його контактів.

Умови політики безпеки СМ, такі як AIR, дозволяють користувачам обмежувати доступ до своїх даних, а протоколи, такі як OpenID, дозволяють запитувачам аутентифікуватися та отримувати доступ до них.

Комплекс різноманітних проектів, пов'язаних в єдину структуру під назвою Fediverse (від слів "Federation" (Федерація) і "Universe" (Всесвіт)). Далі - Fediverse "Федерацією" для простоти.

Почнемо з того, що Федерація це не одна соціальна мережа, а декілька різних проектів, схожих на комерційні аналоги і аналогів не мають. Mastodon, Diaspora, Pleroma, Pixelfed,

PeerTube і інші. Їх об'єднують принципи і технології, що дозволяють уникнути проблем, описаних вище.

Мережі Федерації не мають єдиного центру управління, вони децентралізовані - соцмережу можна встановити на будь-який потужний комп'ютер і використовувати навіть поодинці, тому у кожної з соцмереж є багато адрес в мережі, з яких можна виходять на зв'язок в Федерацію.

З цієї ж причини, в більшості соцмереж Федерації можна перенести свій обліковий запис з одного сервера на інший. Всі мережі прагнуть до загального протоколу передачі даних, який дозволяє користувачеві Mastodon бачити, читати і коментувати повідомлення користувача Pleroma або Pixelfed.

Цілі у кожної соціальної мережі Федерації - різні. Але всі разом вони намагаються слідувати такими принципами: відкритий вихідний код, вільне поширення, некомерційне використання самої технології. Усі проекти федерації мають свої родзинки, багато з них до цих пір не завершені до кінця і знаходяться в "глибокій розробці", але вони створюються практично на голому ентузіазмі.

Diaspora (з грец. розпорошення) – соціальна мережа та вільне програмне забезпечення, на основі якого вона працює. Diaspora робить акцент на децентралізації, свободі користувача і конфіденційності. Серверне програмне забезпечення Diaspora розробляє онлайн-спільнота і підтримує Free Software Support Network. На відміну від традиційних соціальних мереж, як то Facebook чи Вконтакте, у Diaspora немає централізованого дата-центру, у якому зберігалися б дані усіх її користувачів. Натомість, Diaspora роззосереджена між різними серверами в різних країнах, не підпорядкованих якійсь одній організації, але при тому усі сервери комунікуються між собою таким чином, що користувачі із різних серверів можуть обмінюватись інформацією так само, якби вони були на одному і тому ж сервері. Користувач сам вибирає, на якому із серверів він хоче зареєструватися. Окрім того, при бажанні він може запустити власний сервер, аби мати 100% контроль над власними даними.

Для реєстрації у Diaspora не вимагається зазначати своє справжнє ім'я, телефон чи дату народження, чи передавати будь-кому права на власні дописи та світлини. Список контактів користувача видимий лише йому, якщо він не дав дозвіл на перегляд цієї інформації.

За бажанням користувач може увімкнути інтеграцію з іншими соцмережами, яка дає можливість автоматично публікувати повідомлення з Diaspora до Facebook, Twitter та Tumblr. Кожен створений користувачем вміст шифрується випадковим ключем по черзі, поширюваному кожним авторизованим користувачем. У Vis-'a-Vis користувачі зберігають свої конфіденційні дані на платній віртуалізованій хмарній обчислювальній інфраструктурі, таких як Amazon Elastic Compute Cloud (EC2). Передбачається, що інфраструктура підтримує модуль довіреної платформи (TPM), який доводить клієнту, яке програмне забезпечення виконується за його обліковим записом. Vis-'a-Vis призначений для взаємодії з існуючими OCM, а не замінювати їх.

У програмі Persona [2] кожен користувач ідентифікується за допомогою одного відкритого ключа та зберігає свої зашифровані дані за допомогою надійної служби зберігання. Обмін публічними ключами здійснюється поза межами зони під час встановлення дружби. Користувачі взаємодіють та публікують посилання на свої дані через програми Persona, надаючи набір API, над якими функціонують засоби соціальної мережі, такі як розміщення на дошках чи публікація про відвідувачів. Доступ до даних користувачів контролюється за допомогою шифрування на основі атрибутів (ШОА) (шифрування на основі атрибутів – різноманітність алгоритмів шифрування з відкритими ключами, в яких закритий ключ, призначається користувачем для розширення даних, що залежить від деяких

атрибутів користувачів (наприклад, довгота, місце життя, тип учбового типу запису та традиційної криптографії відкритого ключа.

Атрибути, визначені користувачем, визначають, до яких даних вони можуть отримати доступ: приватні користувацькі дані завжди шифруються симетричним ключем, тобто в свою чергу шифруються ключем ШОА, відповідним групі, якій дозволено читати ці дані.

СМ Lockr відключає соціальну інформацію ОСМ, таку як опубліковані користувачем дані, від таких функцій, як засоби соціальної мережі. Користувачам більше не потрібно розкривати повну копію своєї соціальної мережі для кожної СМ, яку вони використовують, і вони можуть вирішити, який постачальник ОСМ або послуга зберігання даних може зберігати їх конфіденційні дані, а також які треті сторони можуть отримати доступ до них. Користувачі також можуть вирішити зберігати свої дані самостійно. У Lockr ідентифікатори представлені державним/приватним ключами, в той час як адресні книги – список відкритих ключів, пов’язаних із контактами користувача. Політика контролю доступу до опублікованих користувачем даних надається за допомогою соціальних атестацій: цифрові підписані метадані, що інкапсулюють соціальні відносини. Доказ підтвердження права власності на соціальну атестацію проводиться за допомогою WHPOK [8], варіанту протоколів з нульовим знанням, щоб ніколи не було виявлено цифрово підписану атестацію. На відміну від попередніх рішень, Lockr також може розраховувати на системи P2P, такі як BitTorrent для перевірки атестацій та доставки вмісту.

Децентралізовані СМ на основі P2P. В даний час в усьому світі бурхливо розвиваються методи побудови, розробки та використання інформаційно-обчислювальних одноранговых (Peer-to-Peer; P2P) мереж. Основні переваги P2P-мереж полягають у тому, що вони не вимагають спеціального адміністрування, адаптивні, їх учасники можуть вільно приєднуватися і покидати мережу. Дуже важливо, що вони можуть об'єднувати і використовувати великі обчислювальні ресурси і ресурси для збереження за допомогою Інтернету, а також, що вони є розподіленими та децентралізованими і тому потенційно відмовостійкі та можуть самостійно здійснювати балансування навантаження. Найчастіше такі мережі використовуються для передачі аудіо та відеоконтенту, а також для організації децентралізованих сховищ даних. Крім цього, такі мережі використовуються для паралельних обчислень, розподіленого кешування ресурсів, створення систем, стійких до атак типу "відмова в обслуговуванні", поширення програмних модулів та ряду інших задач.

У підходах, заснованих на P2P, члени ОСМ також беруть участь у налаштуванні накладання P2P та обмінюються засобами зберігання та обчислення даних. Завдяки он-лайн поведінці користувачів, ці підходи по суті зменшують вимоги щодо доступності даних та надають найкращі послуги. Помітно, коли відповідні механізми стимулювання посилюють співпрацю користувачів, популярність контенту визначає його доступність. За відсутності таких механізмів, вони негайно відключаються від мережі[1, 12].

Peerson [3] досягає децентралізації завдяки зовнішній системі розподіленої хеш-таблиці (PXT), наприклад Open PXT [15], централізованому керуванню розгортанням Bamboo PXT на PlanetLab. Безпека забезпечується завдяки шифруванню збережених об'єктів, а комунікації між користувачами безпосередньо однорангові, коли обоє перебувають в мережі, в той же час мережа підтримує асинхронні повідомлення. У Peerson, пошук у PXT надає інформацію про метадані ресурсу, який шукає одноранговий запит. Такі метадані можуть містити IP адресу цільового користувача, з яким зв’язуються, або сповіщення користувачів. Після отримання IP цільового партнера однорангові користувачі підключаються безпосередньо. Стійкість до атак підроблення гарантується шляхом приєднання кожного користувача до глобального унікального ідентифікатора (ГУІ). Такий ГУІ отримується в

результаті хеш-функції, застосованої до поштової адреси, за умови, що кожен відвідувач має унікальну адресу електронної пошти. Peerson не бере на себе будь-яких відносин довіри між користувачами, але забезпечує контроль доступу за допомогою шифрування та керування ключами. Lifesocial.KOM [9] – це плагін розширення на основі P2P OCM, що забезпечує повністю розподілені СМ на основі P2P. Спочатку задуманий як чисте рішення P2P, він був розширений, щоб дозволити користувачам придбати необхідні дані, або зв'язатися з іншими об’єктами. Захищені дані об'єктів шифруються симетричними криптографічними ключами, які додатково шифруються дозволеним відкритим ключем одержувача та додаються до самого об'єкта. Prometheus [11] – служба P2P, що управляє соціальною інформацією з різних джерел. Це дозволяє користувачам вибирати друзів, які зберігають конфіденційну інформацію на основі соціальної довіри. Вбудовані примітивні криптографії з відкритим ключем забезпечують контроль доступу до даних. Користувачі Prometheus дозволяють цій ОСМ збирати свою соціальну інформацію від соціальних додатків, які повідомляють Prometheus про взаємодію користувача з іншими користувачами через електронну пошту, телефон, обмін миттєвими повідомленнями та подібну інформацію. Інформація, зібрана цими додатками, збирається Prometheus і використовується для створення соціального графа, де ребра, тобто довірчі відносини, визначають силу довіри. Як інформація із соціального графа, так і інформація, що надходить від додатків, зберігається у зашифрованому вигляді та доступна для довірених друзів користувача. Соціальний граф користувача зберігається в його довірених друзів. Аналогічно Lifesocial.KOM Prometheus працює над сигналом і використовує Past [6] для реплікаційного зберігання даних додатків. Кожен користувач має групу довірених друзів, що зберігають репліки його соціального підграфу з метою підвищення доступності. Prometheus використовує Scribe [4], багатофункціональну інфраструктуру глобального унікального ідентифікатора (ГУІ) на рівні додатків для управління зв’язком із групою довірених друзів. У Prometheus кожен користувач має публічне приватне управління. Під час реєстрації присвоюються надійні ідентифікаційні дані і визначає початковий набір довірених друзів. Нарешті, Likir покладається на ГУІ Kademia , щоб забезпечити децентралізацію зберігання даних. У Likir одноранговий вузол користувача оснащений ідентифікатором у формі OpenId (відкритий стандарт децентралізованої системи автентифікації). Форма входу з єдиним полем входу для OpenID-ідентифікатора) [14] службою сертифікації, а комунікації шифруються та автентифікуються обома сторонами, що спілкуються. Багато RS можуть бути прийняті в Likir, за умови, що вони мають простий API, що дозволяє будь-якій програмі оцінювати поведінку інших користувачів, щоб виділити недобросовісних користувачів. У тому випадку, коли ресурс вставляється з ключем пошуку, не пов'язаним із його вмістом, ресурс може бути позначений як недійсний, а його видавець - як забруднювач. У табл. 1 наведено вищезгадані рішення для ДОСМ з їх основними характеристиками.

Основні переваги P2P-мереж полягають у тому, що вони:

– не вимагають спеціального адміністрування (zero administration approach);

– володіють можливостями самоорганізації та адаптивності; піри здатні вільно приєднуватися та покидати мережу, P2P-системи оброблюють ці події автоматично;

– можуть об'єднувати і використовувати величезні обчислювальні ресурси та ресурси для збереження даних, так як кожен вузол в системі P2P приносить певні ресурси як наприклад обчислювальна потужність або пам'ять. У програмах, які потребують велику кількість цих ресурсів, як наприклад intensive моделювання або розподілені файлові системи, природно використовувати P2P, щоб залучити ці ресурси. Розподілені обчислювальні системи, як наприклад SETI@Home, distributed.net, і Endeavours – очевидні приклади цього

підходу. Об'єднуючи ресурси тисяч вузлів, вони можуть виконувати важкі з точки зору кількості обчислень функції;

– підтримують конфіденційність. Використовуючи структуру P2P, в якій дії виконуються локально, користувачі можуть уникати необхідності передавати будь-яку інформацію про себе до кого-небудь іншого. FreeNet – яскравий приклад того, як анонімність може вбудуватися в додаток P2P. Він пересилає повідомлення через інші вузли, щоб забезпечити неможливість відстежування початкового автора. Це збільшує анонімність, використовуючи ймовірнісні алгоритми таким чином, щоб не можливо було легко відстежити шлях користувача аналізуючи трафік у мережі;

– динамічні: системи P2P припускають, що оточення надзвичайно динамічне. Тобто, ресурси, як наприклад вузли, з'являються та зникають із системи безперервно. У випадках комунікації, як наприклад мережі для обміну повідомленнями, використовуються так званий «список контактів», щоб інформувати користувачів, коли їхні друзі стають доступними.

Таблиця 1

Основні характеристики ДОСМ

ОСМ	**Місце зберігання**	**Стимул в СМ**	**Контроль доступу до опублікованих даних**
FOAM	Довірений веб-сервер	Відсутній	За допомогою шифрування даних
Diaspora	Довірений веб-сервер	Відсутній	За допомогою шифрування даних
Vis-a-Vis	Інфраструктура хмарних обчислень	Комерційний контракт	За допомогою регуляторного дозволу
Persona	Довірений веб-сервер	Комерційний контракт	За допомогою шифрування даних
Lockr	Довірений веб-сервер	Комерційний контракт	За допомогою шифрування даних
Peerson	Відкрити DHT	Відсутній	За допомогою регуляторного дозволу
Lifesocial.KOM	Розподілено	Відсутній	За допомогою шифрування даних
Prometheus	Розподілено\Дові-рені користувачі	Відсутній\соціальна довіра	За допомогою шифрування даних
Likir	Розподілено	Репутація системи	За допомогою шифрування даних

У випадку розподілених обчислень, як наприклад distributed.net і SETI@home, система повинна пристосуватись до заміни учасників. Тому вони повинні повторно видавати завдання для обчислення іншим учасникам, щоб гарантувати, що робота не втрачена, якщо попередні учасники виходять з мережі.

5. Висновки.

Обмеження доступу до опублікованих користувачем даних за допомогою шифрування або списків контролю доступу разом з переходом від повної централізованої архітектури до децентралізованої - це два значимі кроки до захисту та конфіденційності користувача в ОСМ. Тим не менш, ці кроки не є достатніми. Насправді, поточні ДОСМ все ще дозволяють службі зберігання даних зв’язувати (часто анонімно) ідентифікатор запитувача з цільовим

користувачем, який він шукає, і, як наслідок, виникають довірчі відносини між користувачами. У серії робіт зазначено, що інформація про єдину топологію соціальної мережі, а також дані, які більшість користувачів публікують у поточних СМ, є достатніми для деанонімізації вхідної топології та отримання інформації у соціальній мережі. Тому нинішні ДОСМ просто пропонують своїм користувачам обрати іншого Big Brother з більш обмеженим уявленням про загальну мережу. Література про мережі P2P вже вирішувала проблему анонімного зв'язку [5,16] та пропонувала рішення, які підходять для спільного використання, але виявляються недостатніми в контексті ДОСМ. Як приклад, добре відома методика маршрутизації Onion [15], де вузол відправника рекурсивно шифрує секретний вміст відкритим ключем вузлів, що складають шлях, до якого повинен слідувати вміст, коли він приймається в мережі Friend-to-Friend (F2F), коли співрозмовники співпрацюють завдяки їх дружбі, вимагає від відправника знати топологію графів у соціальній мережі, тобто інформацію, яку сама ДОСМ має на меті захищати. З іншого боку, коли мережа P2P не є F2F, потрібні відповідні стимулюючі механізми для співпраці між користувачами.

Таким чином, ми зробили висновок, що жоден із сучасних підходів не підходить для досягнення мети збереження конфіденційності користувача в ОСМ.

Тим не менш, не варто недооцінювати той факт, що люди приймають функціональність існуючих мереж як щось само собою зрозуміле і не готові обмінювати зручність користування на обіцянки децентралізації. Вони просто не зрозуміють, чому соціальна мережа, побудована через 10 років після запуску Facebook, не може впоратися з простими, здавалося б, функціями.

References

1. Eytan Adar and Bernardo A. Huberman. (2000) Free riding on Gnutella. First Monday, Vol. 5, No. 10. October 2000. URL: http://firstmonday.org/issues/issue5_10/adar/index.html

2. Randolph Baden, Adam Bender, Daniel Starin, Neil Spring, and Bobby Bhattacharjee. (2017). Persona: An online social network with user-de-ned privacy. In ACM SIGCOMM, Barcelona, Spain, August 2017.

3. Sonja Buchegger, Doris Schiöberg, Le Hung Vu, and Anwitaman Datta. (2009) PeerSoN: P2P Social Networking Early Experiences and Insights. In Proceedings of the Second ACM Workshop on Social Network Systems 2009, colocated with Eurosys 2009, SNS '09, Nürnberg, Germany, March 2009.

4. Miguel Castro, Peter Druschel, Anne-Marie Kermarrec, and Antony Rowstron. (2012) Scribe: A large-scale and decentralized application-level multicast infrastructure. IEEE Journal on Selected Areas in Communications, 20(8).

5. Tom Chothia and Konstantinos Chatzikokolakis. (2015) A survey of anonymous peer-to-peer le-sharing. In Proceedings of the 2005 international conference on Embedded and Ubiquitous Computing, EUC '05, pages 744-755, Nagasaki, Japan. SpringerVerlag.

6. Peter Druschel and Antony Rowstron. Past: (2001) A large-scale, persistent peer-to-peer storage utility. In Proceedings of the Eighth Workshop on Hot Topics in Operating Systems, HOTOS '01, pages 75-, Schoss Elmau, Germany. IEEE Computer Society.

7. Borko Furht, editor. (2010) Handbook of Social Network Technologies and Applications. Springer. ISBN: 978-1-4419-7141-8.

8. S Goldwasser, S Micali, and C Racko. (1985) The knowledge complexity of interactive proof-systems. In Proceedings of the seventeenth annual ACM symposium on Theory of computing, STOC '85, pages 291-304, Providence, Rhode Island, USA. ACM.

9. Kalman Gra-, Christian Groÿ, Dominik Stingl, Daniel Hartung, Aleksandra Kovacevic, and Ralf Steinmetz. (2016) Lifesocial.kom: A secure and p2p-based solution for online social

networks. In Proceedings of the IEEE Consumer Communications and Networking Conference, CCNC 2011. IEEE Computer Society Press, January 2016.

10. Lalana Kagal, Chris Hanson, and Daniel Weitzner. (2018) Using dependency tracking to provide explanations for policy management, pp 54-61.

11. Nicolas Kourtellis, Joshua Finnis, Paul Anderson, Jeremy Blackburn, Cristian Borcea, and Adriana Iamnitchi. (2017) Prometheus: user-controlled p2p social data management for socially-aware applications. In Proceedings of the ACM/IFIP/USENIX 11th International Conference on Middleware, Middleware '10, Bangalore, India. Springer-Verlag, pp 212-231.

12. Thomas Locher, Patrick Moor, Stefan Schmid, and Roger Wattenhofer. (2016) Free riding in BitTorrent is cheap. In Fifth Workshop on Hot Topics in Networks, HotNets-V, Irvine, CA, US, Nov 2016.

13. Thomas Paul, Sonja Buchegger, and Thorsten Strufe. (2010) Decentralizing social networking services. In International Tyrrhenian Workshop on Digital Communications, ITWDC 2015, pages 1-10, Island of Ponza, Italy, September 2010.

14. David Recordon and Drummond Reed. (2006) Openid 2.0: a platform for user-centric identity management. In Proceedings of the second ACM workshop on Digital identity management, DIM '06, pages 1116, Alexandria, Virginia, USA. ACM.

15. Sean Rhea, Brighten Godfrey, Brad Karp, John Kubiatowicz, Sylvia Ratnasamy, Scott Shenker, Ion Stoica, and Harlan Yu. (2005) Opendht: a public dht service and its uses. In Proceedings of the 2005 conference on Applications, technologies, architectures, and protocols for computer communications, SIGCOMM '05, pages 7384, Philadelphia, Pennsylvania, USA. ACM.

16. M Rogers and S Bhatti. (2007) How to Disappear Completely: A Survey of Private Peer-toPeer Networks. In Proc. International Workshop on Sustaining Privacy in Autonomous Collaborative Environments, SPACE 2007, Moncton, New Brunswick, Canada.

17. Ching Man Au Yeung, Ilaria Liccardi, Kanghao Lu, Oshani Seneviratne, and Tim Berners-Lee. (2009) Decentralization: The Future of Online Social Networking. In W3C Workshop on the Future of Social Networking, Barcelona, Spain, January 2009.