УДК 004.056

Т. В. Миронюк, *к.т.н.,*
доцент кафедри інформаційної безпеки та комп'ютерної інженерії,
e-mail: tanjamiron85@gmail.com,
Л. Т. Дуда, *магістрант,*
e-mail: lyubomir-duda@ukr.net.
Черкаський державний технологічний університет,
бульв. Шевченка 460, м. Черкаси, 18006, Україна

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ОНЛАЙН СПІЛКУВАННЯ

В даній статті розглядаються основні методи захисту он-лайн спілкування на прикладі програм та програмних комплексів для обміну повідомленнями. Розкривається проблема надмірного поширення персональних даних користувачами. Досліджуються основні технології захисту особистої інформації в мережі Інтернет. Особлива увага приділяється огляду спеціалізованих програмних продуктів для безпечного обміну повідомленнями інформацією, які присутні зараз на ринку. Сформульовано базові правила для користувачів, при дотриманні яких, спілкування та обмін контентом в мережі Інтернет стане більш захищеним, і не призведе до втрати особистої інформації і розголошення персональних даних. Описано створення експериментального онлайн-чату на основі узагальнених потреб та побажань користувачів з урахуванням недоліків подібних програм по безпечності, комфорту користування та надійності. Виділено найбільш важливі проблеми, які потрібно було вирішити при реалізації програмного продукту.

***Ключові слова**: онлайн спілкування, чати, соцмережі, методи захисту інформації, інтернет простір, інтернет.*

Постановка проблеми. Інтернет – важливий елемент сьогоднішнього людського життя. Навчання, спілкування з друзями, відпочинок завдяки необмеженим ресурсам глобальної мережі Інтернет стає цікавішим та змістовнішим. Інтернет вміщує великий навчальний, розважальний та інформаційний потенціал, який може становити певну небезпеку та нести деякий ризик. Особливо важливим є захист онлайн-спілкування та особистої інформації в онлайн-чатах.

Метою даної роботи є визначити та охарактеризувати найоптимальніші методи захисту для спілкування в он-лайн.

Виклад основного матеріалу. Як показує практика, в останні роки відбулося значне зростання кількості правопорушень в інформаційній галузі. Ірраціональне поширення суб'єктами персональних даних – причина більшості з них [1].

Окрім цього, одним з важливих аспектів порушення норм захисту особистих даних в інформаційних системах стало незаконне розповсюдження персональної інформації. Ця сторона суспільних відносин на сьогодні досліджена дуже мало. Захист персональних даних - надзвичайно важливе питання, науково-практичну актуальність якого важко переоцінити. То ж розглянемо детальніше це питання, зробимо спробу проаналізувати його та знайти методи і шляхи вирішення [2].

Виділимо найбільш популярні сервіси та протоколи захисту спілкування в онлайн чатах та соціальних мережах.

Для пересилання захищених повідомлень розроблений криптографічний протокол OTR. Для створення надійного шифрування протокол використовує комбінацію алгоритмів AES, симетричного ключа, алгоритму Діффі - Хеллмана і хеш-функції SHA-1.

Основна перевага OTR перед іншими засобами шифрування це його застосування на льоту, а не після підготовки повідомлення. Він був розроблений Микитою Борисовим і Яном Голдбергом. Для використання в сторонніх додатках розробники протоколу створили клієнтську бібліотеку. Тому, щоб захистити передачу даних по IM-каналах, можна скористатися спеціально призначеними для захисту додатками.

Ще один з подібних проектів – Cryptocat [3, 4]. Це додаток з відкритим вихідним кодом, написаний на JavaScript. Розширення можна встановлювати в Chrome, Firefox

і Safari. Крім цього, є клієнтська програма, але тільки для macOS. Cryptocat шифрує повідомлення на стороні клієнта і передає їх довіреному серверу. Для цього на стороні клієнта використовується симетричне шифрування повідомлень і файлів з використанням AES-256 і обраного ключа. Для кожного чату генерується новий ключ.

Інші учасники розмови (до 10 чоловік в кімнаті) зможуть прочитати їх, тільки якщо самі вірно введуть той же самий ідентифікатор. Для надійної передачі ключів використовується алгоритм Діффі – Хеллмана, для генерації унікальних відбитків при аутентифікації – хеш-функція Whirlpool, а для перевірки цілісності повідомлень HMAC-WHIRLPOOL. Метод роботи з ключами перетворює Cryptocat в систему секретності, в якій навіть втрата закритого ключа не може скомпрометувати ключ сесії. Листування видаляється через півгодини відсутності активності, а сам сервіс працює з постійним SSL-шифруванням [2].

Ще один проект подібного роду Bitmessage [5], написаний Джонатаном Уорреном на Python. Bitmessage це децентралізована P2P-програма для обміну зашифрованими повідомленнями між двома або декількома користувачами. Вона використовує сильну криптографію, яка надійно захищає абонентів від прослуховування на рівні інтернет-провайдера або на сервері. Варто зауважити, що криптографічна система практично в точності копіює схему, яка використовується в P2P-системі Bitcoin, однак спрямована на обмін повідомленнями. Особливість Bitmessage полягає в тому, що факт спілкування двох користувачів практично неможливо довести: повідомлення передається не безпосередньо від користувача А до Б, а розсилкою всім учасникам мережі (подібний підхід реалізований в Tor). При цьому прочитати його може тільки той користувач, з яким встановлено з'єднання і який володіє коректним ключем для розшифровки [6].

Останнім проектом цього ряду, який буде розглянуто, буде Tor Chat [7]. Мережа Tor Chat є вільною децентралізованою високоанонімною криптозахищеною системою обміну миттєвими повідомленнями і файлами з відкритим кодом. Tor Chat в основі своїй використовує анонімну мережу Tor, але це повністю відокремлений проект. Анонімність передачі даних в більшості покладена на приховані сервіси Tor, Tor Chat, по суті, лише надбудова до них, що займається обробкою повідомлень. Криптозахист з'єднання двох користувачів також забезпечується прихованими сервісами Tor за допомогою асиметричного шифрування за стандартом RSA. Спочатку Tor Chat був написаний на Python, а клієнт для macOS, відповідно, на Objective C. На початку 2012 року був запущений проект jTorChat, що розробляється на Java. Поки в ньому не реалізована вся функціональність оригінального Tor Char, наприклад, відсутня передача файлів.

Також доцільно буде розглянути захищені сервіси для відео конференцій. Одним з таких проектів став Tox відкрита і вільна заміна Skype. Він використовує схожу на Skype модель організації взаємодії в мережі для поширення повідомлень, що використовує криптографічні методи для ідентифікації користувача і захисту транзитного трафіку від перехоплення. Підтримується обмін текстовими повідомленнями, голосовий зв'язок, відеодзвінки і передача файлів. Робота організована через простий і типовий для IM-клієнтів графічний інтерфейс.

Одне з ключових завдань проекту забезпечити приватність і таємницю листування, в тому числі захист від можливого аналізу трафіку хакерами. Для забезпечення адресації користувачів використовується розподілена хеш-таблиця (DHT), робота з якою організована в стилі BitTorrent. Канал зв'язку організовується за допомогою надбудови над протоколом UDP з реалізацією сеансового рівня (Lossless UDP).

Для ідентифікації кожного користувача використовується спеціальний публічний ключ, який також застосовується як відкритий ключ для шифрування. Окремо генерується закритий ключ для розшифровки повідомлень, зашифрованих з використанням ідентифікатора / відкритого ключа. Для організації комунікацій потрібно з'єднання до піру (англ. pear-to-pear), який може бути визначений вручну, або знайдений автоматично (доступна функція пошуку пірів в локальній мережі).

Код Tox написаний на мові C і поширюється під ліцензією GPLv3. Підтримуються платформи Linux, Windows і macOS. Для організації шифрування використовується бібліотека libsodium. Функціональність розробки поки знаходиться на рівні серії тестових прототипів, консольного клієнта, написаного з використанням бібліотеки ncurses, і графічного клієнта на базі Qt5.

Крім того, в операційній системі GNU[8] створюється альтернатива під назвою GNU Free Call. Цей проект націлений на розробку і впровадження по всьому світу безпечних і самоорганізованих комунікаційних сервісів. В якості базового протоколу в GNU Free Call буде використовуватися SIP, підтримка якого забезпечена за допомогою VoIP-сервера GNU SIP Witch. Комунікаційна мережа побудована з використанням P2P-технологій і має топологію mesh-мережі, в якій кожна клієнтська точка мережі пов'язана через сусідні клієнтські точки. Кінцевою метою проекту є формування VoIP-мережі, що нагадує Skype за можливостями і зручностю використання.

З технічного боку для реалізації проекту в GNU SIP Witch, крім функції маршрутизації SIP-дзвінків, буде забезпечена підтримка роботи в ролі захищеного VoIP-проксі, додана можливість зберігання кеша хостів і виконання функцій обміну маршрутами з сусідніми вузлами mesh-мережі. Підтримка VoIP-проксі дозволить спростити побудову призначених для користувача інтерфейсів і створення додатків для мобільних пристроїв, оскільки забезпечить підтримку прийому і здійснення дзвінків з будь-яких SIP-сумісних програмних телефонів.

Клієнтське ПЗ для роботи в мережі GNU Free Call буде підтримувати широкий спектр різноманітних програмних платформ. Мережа буде мати повністю децентралізовану структуру, не прив'язану до окремих керуючим серверів.

Взагалі, поняття соціальні мережі слабо в'яжуться з концепцією анонімності та конфіденційності листування. Ці сервіси стали джерелом інформації про осіб різного віку: люди пишуть в соцмережі все про себе, своїх близьких і друзів, викладають життєві фото і відео. Можна обмежити доступ до цих відомостей, але це не перешкода для спецслужб. Відомі випадки, коли за запитом влади їм передавалися цікаві для них дані про користувачів. Безумовно, соцмережі це не найкращий спосіб для спілкування. Але іноді хочеться поділитися чимось з рідними або розповісти про досягнення близьким друзям. Тому, навіть, соцмережі відіграють позитивну роль.

Щоб захистити свої приватні дані від шахраїв, хакерів або спецслужб, можна скористатися вільними захищеними аналогами. У них, звичайно, набагато менше користувачів, але тим краще. І чим більше користувачів будуть розуміти значущість приватності інформації, а до цього все йде, тим більше їх число буде переходити в захищені соцмережі.

Одна з таких мереж Friendica. Проект було розпочато в 2011 році Майком Макгрівіном. Friendica вільна соціальна мережа з відкритим вихідним кодом, що дислокується на GitHub. Вона надає широкий вибір конекторів для різноманітних соціальних мереж: як традиційних (Facebook, Twitter), так і нових (Diaspora, Identi.ca). Крім того, за допомогою Friendica можна обмінюватися листами і читати RSS-стрічки. Якщо в Friendica зробити фото закритим, то воно насправді буде в публічному чаті і ніхто (крім, природно, власника і обраних ним осіб) не зможе отримати до нього доступ.

В даний час йде розробка наступної версії соцмережі під назвою Red (що з іспанського означає «мережу»). За словами авторів, під час розробки Friendica були усвідомлені деталі і обкатані механізми розробки соцмереж, тому наступний проект стане ще кращим і буде позбавлений від фундаментальних недоліків першої версії.

Ще одна захищена соціальна мережа, на яку можна звернути увагу, – це Diaspora [9]. Дана мережа базується на трьох базових принципах. На відміну від традиційних соцмереж, де дані зберігаються в одному датацентрі, в Diaspora, як і в багатьох захищених в Інтернеті продуктах, дані зберігаються децентралізовано. У цьому випадку дані зберігаються не на центральному сервері, а на подах (pod) - комп'ютерах тих користувачів, хто надав їх для цієї мети. Другий принцип, звичайно ж, свобода. Третій принцип - секретність. Ніхто, крім вас, не має доступу до твоїх даних, а хто може їх переглядати, визначаєте ви самі, встановлюючи дозволи. Дані принципи діють глобально, тобто ніхто їх не порушить.

На основні дослідження методів захисту спілкування, розглянутих вище, можливо сформувати алгоритм роботи для учасників онлайн-чатів.

1. На веб-сайті чату чи соціальної мережі потрібно читати положення політики приватності (іноді її називають "політикою конфіденційності") і читати пункти, що відносяться до безпеки ваших даних. Скажімо, чи залишає власник мережі за собою право використовувати цю інформацію в маркетингових дослідженнях.

2. З'ясовуємо, які програмні способи пропонує власник мережі для захисту даних. Наприклад, при заповненні профілю користувача, чи можна поставити потрібну помітку, щоб ця інформація не показувалася іншим користувачам.

3. Якщо планується проведення якоїсь онлайнової акції, можливо, слід завести для цього інший аккаунт, а не той, який був використаний в попередній акції або хоча б інший псевдонім (нік).

4. При обранні онлайн чату потрібно бути обережним, якщо є потреба користуватися своїм акаунтом з чужого комп'ютера. Не забувати очищати історію і кеш браузера і видаляти збережений ним пароль.

5. По можливості використовувати захищений (SSL) доступ (https: // ...). Таким чином можна шифрувати сеанси зв'язку між вашим браузером і мережею.

Онлайн чат може містити інструменти для інтеграції з іншими подібними мережами або сервісами. Наприклад, при публікації чого-небудь в Twitter, ця новина автоматично з'являється на сторінці користувача в Facebook. Потрібно бути обережним з інтеграцією. На будь-якому ресурсі можна діяти анонімно і відчувати себе захищеним, але лише до певного часу. Автоматична інтеграція може розкрити особистість користувача [10].

6. Не потрібно використовувати чат або інший подібний сервіс в якості основного сховища інформації. Це не особистий сайт певного користувача, а резервне копіювання, зазвичай, не входить в набір стандартних інструментів. Якщо рішенням власника (а може, і під тиском уряду) сторінка користувача виявиться заблокованою або видаленою, відновити її буде неможливо. Потрібно пам'ятати, що власнику мережі простіше позбутися від "незручного" користувача, ніж вступати в конфлікт з урядом, ризикуючи втратити набагато більше [11].

У багатьох соціальних мережах можна поспілкуватися з друзями в реальному часі. Мабуть, немає менш безпечного способу обмінюватися інформацією в інтернеті, ніж цей. Якщо все-таки без чату не обійтися, потрібно переконатися, що всі учасники розмови увійшли на сайт з використанням захищеного протоколу (https: // ...), а краще скористатися якою-небудь незалежною програмою для обміну миттєвими повідомленнями.

На основі проведеного дослідження було спроектовано та розроблено експериментальний чат з урахуванням всіх недоліків подібних програм та побажань користувачів. Для розробки було обрано мову програмування PHP. Графічний інтерфейс оформлено за допомогою мови розмітки HTML та мови стилів CSS. Також в інтерфейсі присутні функції, що реалізовані на JS та JQuery. Це додає програмі динамічності та швидкості. Чат має стандартну для подібних програм архітектуру «клієнт - сервер» та посилений декількома сторонніми сервісами авторизації використовуючи API цих сервісів.

Одним з таких сервісів є SMS авторизація. Цей сервіс є доволі поширеним, але мало хто використовує його в своїх продуктах так як більшість таких сервісів є платними. В розробленому чаті SMS авторизація представлена зв’язком профілю користувача з номером його телефону. При кожній авторизації, крім введення логіну та пароля, користувач буде отримувати код підтвердження на свій мобільний телефон. Це називається двох факторною авторизацією.

База даних користувачів зашифрована два рази підряд використовуючи алгоритм шифрування MD5 з додаванням додаткового слова (solt). Якщо припустити, що база даних буде викрадена, то на розшифрування даних піде дуже багато часу, або дані розшифрувати буде взагалі неможливо.

Також важливою частиною таких чатів є обмін файлами з різноманітними розширеннями. Це є доволі проблемною частиною тому, що файли можуть містити прихований код який може бути використаний щоб нанести шкоду системі. Таким способом можна викрасти особисті дані користувачів або навіть базу даних. Ця проблема вирішена використанням стандартних функцій мови PHP для розпізнавання та очистки файлів та повідомлень від вставок програмного коду. Статистичні дані показують, що дані функції працюють доволі непогано і їх можна використовувати для розробки. Додатково потрібно зазначити, що сьогодні у більшості хостинг-провайдерів є функції які додатково захищають системи від вставок шкідливого коду.

В результаті було розроблено експериментальний онлайн-чат, в якому враховано більшість потреб користувачів по комфорту, безпеці та надійності. Система, звичайно, не є ідеальною але повністю підходить для вико-

ристання в корпоративних цілях для невеликих компаній, що не хочуть використовувати глобальні сервіси. При наявності ресурсів, даний програмний продукт можна поширювати та використовувати для більшої кількості користувачів.

Висновки. Було розглянуто декілька програм та програмних комплексів для обміну повідомленнями та спілкування в мережі.

Розглянуто методи захисту при он-лайн спілкуванні та сформульовано найоптимальніший алгоритм роботи для учасників онлайн-чатів.

В результаті дослідження було розроблено експериментальний онлайн-чат, в якому враховано та вдосконалено недоліки існуючих програмних продуктів.

Список літератури

1. Мироненко А. В. Темпоральні виміри Інтернет-реальності. *Психологічні та педагогічні проблеми Інтернет-реальності : наук.-практ. сем., 14 лютого 2012 р.*: тези доп. Київ, 2012. URL: http://ispp.org.ua/podiy_37.htm – Назва з екрану.
2. Удалова О. А., Швед О. В., Євсюкова М. В. та ін. Безпечне користування сучасними інформаційно-комунікативними технологіями: методичні рекомендації. К.: Україна, 2010. 72 с. URL: http://static.klasnaocinka.com.ua/uploads/editor/4916/401901/sitepage_71/files/bezpechne_koristuvannya_ikt.pdf – Назва з екрану.
3. Greenberg A. Crypto.cat Aims To Offer Super-Simple Encrypted Messaging. *Forbes*. URL: https://www.forbes.com/sites/andygreenberg/2011/05/27/crypto-cat-aims-to-offer-super-simple-encrypted-messaging – Назва з екрану.
4. Kirk J. Cryptocat Aims for Easy-to-use Encrypted IM Chat. *IDG News Service*. URL: https://www.pcworld.com/article/251837/cryptocat_aims_for_easytouse_encrypted_im_chat.html – Назва з екрану.
5. Cawrey D. Bitmessage is the Bitcoin of online communication. *Coindesk*. URL: https://www.coindesk.com/bitmessage-is-the-bitcoin-of-online-communication/ – Назва з екрану.
6. Павленко Д. Як захистити персональні дані. URL: http://www.epravda.com.ua/columns/2011/09/30/300156/ – Назва з екрану.
7. Interview with Bernd Kreuss of TorChat. *Free Software Foundation*. URL: https://www.fsf.org/blogs/licensing/interview-with-bernd-kreuss-of-torchat – Назва з екрану.
8. Ru.wikipedia.org. GNU. URL: https://ru.wikipedia.org/wiki/GNU.
9. Vernon A. Striking back at Facebook, the open-source way. *Network World*. URL: https://www.networkworld.com/article/2230713/microsoft-subnet/striking-back-at-facebook--the-open-source-way.html – Назва з екрану.
10. Обуховська Т. І., Шуляк В. П. Персональні дані: теорія та реальність. *Електронне урядування*. 2011. № 2. С. 76–88.
11. Обуховська Т. І. Нормативно-правове забезпечення обробки та циркуляції персональних даних. *Вісн. НАДУ*. 2011. № 4. С. 119–126.

References

1. Myronenko, A. (2012) Temporalni vymiry Internet-realnosti. In: Psyxologichni ta pedagogichni problemy Internet-realnosti. [online] Kiev. URL: http://ispp.org.ua/podiy_37.htm [Accessed 2 Nov. 2017].
2. Udalova O. and Shved O. and Yevsyukova M. (2010) Bezpechne korystuvannya suchasnymy informacijno-komunikatyvnymy texnologiyamy: metodychni rekomendaciyi [online] Kiev. URL: http://static.klasnaocinka.com.ua/uploads/editor/4916/401901/sitepage_71/files/bezpechne_koristuvannya_ikt.pdf [Accessed 2 Nov. 2017].
3. Greenberg, A. (2011) Crypto.cat Aims To Offer Super-Simple Encrypted Messaging. [online] Forbes.com. URL: https://www.forbes.com/sites/andygreenberg/2011/05/27/crypto-cat-aims-to-offer-super-simple-encrypted-messaging [Accessed 2 Nov. 2017].
4. Kirk, J. (2012) Cryptocat Aims for Easy-to-use Encrypted IM Chat. [online] PCWorld. URL: https://www.pcworld.com/article/251837/cryptcat_aims_for_easytouse_encrypted_im_chat.html [Accessed 2 Nov. 2017].
5. Cawrey, D. (2013). Bitmessage is the Bitcoin of online communication - CoinDesk.

[online] CoinDesk. URL: https://www.coindesk.com/bitmessage-is-the-bitcoin-of-online-communication/ [Accessed 3 Nov. 2017].
6. Pavlenko, D. (2011). Yak zaxystyty personalni dani. [online] epravda.com. URL: http://www.epravda.com.ua/columns/2011/09/30/300156 [Accessed 3 Nov. 2017].
7. Fsf.org. (2017). Interview with Bernd Kreuss of TorChat — Free Software Foundation — working together for free software. [online] URL: https://www.fsf.org/blogs/licensing/interview-with-bernd-kreuss-of-torchat [Accessed 3 Nov. 2017].
8. Ru.wikipedia.org. (2017). GNU. [online] URL: https://ru.wikipedia.org/wiki/GNU [Accessed 4 Nov. 2017].
9. Vernon, A. (2017). Striking back at Facebook, the open-source way. [online] Network World. URL: https://www.networkworld.com/article/2230713/microsoft-subnet/striking-back-at-facebook--the-open-source-way.html [Accessed 5 Nov. 2017].
10. Obuxovska, T. and Shulyak, V. (2011). Personalni dani: teoriya ta realnist. *Elektronne uryaduvannya*, (2), pp.76-88.
11. Obuxovska, T. (2011). Normatyvno-pravove zabezpechennya obrobky ta cyrkulyaciyi personalnyx danyx. *Visnyk NADU*, (4), pp.119-126.

T. V. Myronyuk, *Ph.D.,*
associate professor of information security and computer engineering chair,
e-mail: tanjamiron85@gmail.com,
L. T. Duda, *master,*
e-mail: lyubomir-duda@ukr.net,
Cherkasy State Technological University,
Shevchenko blvd., 460, Cherkasy, 18006, Ukraine

RESEARCH OF ONLINE COMMUNICATION PROTECTION METHODS

This article discusses the basic methods of protecting online communication on the example of applications and software systems for messaging. The problem of excessive dissemination of personal data by users is revealed. The main technologies of protection of personal information on the Internet are investigated. Particular attention is paid to the review of specialized software for the secure exchange of messages on the information currently available on the market. Basic rules are formulated for users whose adherence to, communication and content sharing on the Internet will become more secure and will not result in loss of personal information and disclosure of personal data. Describes the creation of an experimental online chat based on the general needs and wishes of users, taking into account the drawbacks of similar programs for safety, comfort and reliability. Highlights the most important issues that need to be addressed when implementing a software product.

Keywords*: online communication, chats, social networks, methods of information security, internet space, internet*.

Рецензенти: Т. О. Прокопенко, д.т.н., доцент,
О. В. Кириченко, д.т.н., с.н.с.