УДК 130.2:008

Наталія Шерепо

КРИПТОГРАФІЯ ЯК ГАРАНТ БЕЗПЕКИ ІНФОРМАЦІЇ В КУЛЬТУРІ СПІЛКУВАННЯ СОЦІАЛЬНИХ МЕРЕЖ

У статті проведено соціально-філософське дослідження сучасної теорії криптографії в контексті глобальної парадигми віртуальних соціальних мереж та її впливу на культуру спілкування в цих мережах. Доведено необхідність та визначено перспективи використання криптографії як гаранта безпеки інформації в Інтернеті, а також обґрунтовано, що феномен незахищеності інформації в соціальних мережах є не лише предметом дослідження на теоретичному рівні, а й глобальним політичним, ідеологічним та соціально-практичним явищем.

Ключові слова: *криптографія, культура спілкування, соціальна мережа, інформація, Інтернет.*

N. Sherepo. Cryptography as guarantor of security of information in culture of social network communication

In the present article there is made the sociological and philosophical investigation of contemporary theory of cryptography in the context of global paradigm of virtual social networks. The Author pays attention to the influence of cryptography to the culture of communication in such networks. It is analyzed the necessity of using the cryptography as guarantor of security of information in Internet. The Author states that non-security of information in social networks is global political, ideological and social phenomenon.

Key words: *cryptography, culture of communication, social network, information, Internet.*

Н. Шерепо. Криптография как гарант безопасности информации в культуре общения социальных сетей

В статье проведено социально-философское исследование современной теории криптографии в контексте глобальной парадигмы виртуальных социальных сетей и ее влияния на культуру общения в этих сетях. Доказана необходимость и обозначены перспективы использования криптографии как гаранта безопасности информации в Интернете, а также обосновано, что феномен незащищенности информации в социальных сетях является не только предметом исследования на теоретическом

уровне, но и глобальным политическим, идеологическим и социально-практическим явлением.

Ключевые слова: *криптография, культура общения, социальная сеть, иформация, Интернет.*

Життя сучасної людини змінюється надзвичайно стрімко, кожна нова технологія, будучи асимільована виміром здорового глузду, удосконалює цей світ. І в першу чергу, сьогодні це відбувається у сфері зв’язку та комунікації. Техніка настільки глибоко проникла в життя людини, настільки вплелась у тканину людської щоденності, що викоренити її із спільного світосприйняття і культурологічного контексту вже стає повністю і цілком неможливим. Такі драматичні трансформації потребують аналізу новітніх технологій крізь призму змін світобачення. Саме людина – основний компонент сучасних інформаційно-технологічних систем, адже новітні технології компонент – лише другорядний.

Сучасна епоха, що характеризується прискореним розсортуванням технічного прогресу, об’єднанням людства у всесвітньому масштабі, трансформується і переходить від традиційних тематик і проблем до інноваційних питань, які утворюються під впливом глобальних процесів. Комп’ютерні ігри, стільниковий зв’язок, всесвітня електронна мережа – це все, поступово проникаючи в життя звичайної людини, докорінно перетворює не тільки його, проте і саму людську індивідуальність.

Ефекти зростання анонімності ставлять під удар здавалось би незламну основу людського буття – тілесність. Весь простір існування особистості стає спроектованим, з’являється особливий когнітивно-комунікаційний стиль – атрибут нового інформаційного суспільства. Можна говорити про формування нової форми соціальності в контексті соціетальності [4, с. 7].

Соціальний простір епохи модерну та інформаційне поле існують сьогодні у світі здорового глузду, і суб’єкт вимушений перебувати у цих світах одночасно. Особистість існує в просторі потоків, у ситуації з величезною кількістю можливостей вибору, соціальні детермінанти послаблюються, суспільна система поступається неформальним об’єднанням і технологія сприяє цьому. Все більша кількість суспільних утворень являє собою соціальні мережі. Як особистість співіснує з іншими в глобальних соціальних мережах? Яка специфіка спілкування в соціальній мережі та яким чином можна убезпечити конфіденційність такого спілкування? Ось те коло питань, на які ми спробуємо дати відповіді у цій статті.

Взагалі, термін соціальна мережа трактується як соціальна структура, що утворена індивідами або організаціями. Вона відображає розмаїття зв'язків між ними через соціальні взаємостосунки, починаючи з випадкових знайомств і закінчуючи тісними родинними вузами [4, с. 10].

Теорія соціальних мереж розглядає соціальні взаємовідносини в термінах вузлів та зв'язків. Вузли є відособленими акторами в мережах, а зв'язки відповідають стосункам між акторами.

Соціальні мережі використовувались і для дослідження взаємодій компанії, характеризуючи багато неформальних зв'язків, які поєднують між собою представників керівництв, а також асоціації та зв'язки між окремими робітниками в різних компаніях. Ці мережі дають можливості компаніям збирати інформацію, утримувати конкуренцію, навіть таємно змовлятись про встановлення цін або політик.

Одночасно соціальні мережі не поступаються пошуковим системам і в доступності: соціальні мережі стали міцною частиною повсякденності. Багато користувачів підтримують контакт між собою вже не стільки через SMS і телефонні дзвінки, скільки переписуючись у Мережі – мобільний телефон тепер використовується і для цього. Соціальні мережі не тільки змінили культуру спілкування та комунікативну поведінку користувачів (адже тепер відходять на другий план чати і електронна пошта). Вони також змінюють принципи переміщення веб-серферів по Мережі. Якщо раніше майже всі використовували для орієнтації в мережевому просторі пошукові системи, то сьогодні уже 20% користувачів Інтернету шукають і знаходять потрібну їм інформацію через соціальну мережу [10, с. 6]. І ця тенденція зміцнюється. Якщо раніше ви починали свій день в Інтернеті зі сторінки пошукової сторінки, то сьогодні перший візит – у соціальну мережу. Спеціалісти підкреслюють, що в соціальних мережах підприємства можуть знайти своїх клієнтів і встановить з ними довготривалі контакти [10, с. 7]. Для того, щоб допомогти приватним компаніям створити свої представництва в соціальних мережах, навіть з'явились спеціальні агентства. Своєю метою вони вважають перетворити пасивних користувачів в активних прихильників марки, що рекламується.

Все це наводить на думку про те, що спілкування між усіма ланками соціальної мережі повинно бути коректним з боку політичного, емоційного та інших важливих аспектів ефективної взаємодії, що, своєю чергою, і становитиме принципово нову культуру спілкування в Інтернеті – культуру спілкування віртуальних соціальних мереж.

Зазначимо, що спілкування як таке є мірилом моральної культури

людини. Будь-який людський контакт виникає за умов певного культурного середовища, чи то об’єктивно існуючої реалії, чи то віртуального контексту, учасники спілкування займають ті чи інші соціальні позиції [5, с. 13].

Власне, будь-який прояв людської культури, як і культура загалом, може бути розглянутий як культура спілкування, оскільки за самою своєю сутністю культура є інтерсуб’єктивною. Водночас про культуру спілкування нерідко говорять і в особливому значенні. В такому випадку під культурою спілкування розуміють передусім наявні в суспільстві і в людському житті форми спілкування як такого, форми його структурування й ціннісної організації, а також їхню реалізацію безпосередньо в стосунках між людьми.

Для сучасної інтелектуально розвиненої людини, яка володіє всіма нормами усного й писемного мовлення, Інтернет – безмежна можливість збагачення культурного мовленнєвого рівня, презентації власних винаходів.

Серед основних рис спілкування в Інтернеті прийнято виділяти такі:

1. Анонімність, яка може призвести до безкарності, розкутості, і безвідповідальності поведінки учасників спілкування.

2. Відсутність невербальної інформації.

3. Добровільність контактів. Користувач добровільно зав’язує контакти чи може перервати їх у будь-який момент.

4. Стійке прагнення до емоційного наповнення тексту, що виражається у створенні спеціальних знаків для позначення емоцій.

5. Прагнення до нетипової, ненормативної поведінки. Найчастіше користувач презентує себе по-іншому, ніж у реальному житті, програє не реалізовані в діяльності поза мережею ролі, сценарії, і, не знаючи співрозмовника, створює його образ, відмінний від реального.

6. Більша, ніж у реальному світі, залежність від співрозмовника у спілкуванні. Наслідком є порушення безпосереднього живого спілкування.

7. Відсутність єдності простору і часу, тобто Інтернет дає можливість бути одночасно у різних місцях, а також спілкуватися з людьми з інших годинних поясів.

8. Характер спілкування – майже завжди письмовий [5, с. 38].

А такі специфічні ознаки віртуального спілкування створило і нові соціальні, етичні і політичні проблеми серед широкого розповсюдження мереж. Популярною рисою багатьох мереж є конференції або електронні дошки оголошень, де люди можуть обмінюватись по-

відомленнями з різноманітних тем. До тих пір, поки предмет, що обговорюється, не виходив за межі техніки або вподобань.

Проблеми почалися з виникненням конференцій, присвячених темам, по-справжньому хвилюючих людей, таким як політика чи релігія. Погляди, яких дотримуються одні люди, можуть виявитися образливими для інших. Адже вони і справді часто далекі від норм політкоректності. Крім того, мережеві технології, як відомо, не обмежені тільки лише передачею тексту. Без особливих проблем по Мережі ходять фотографії високої якості і навіть відеофрагменти. Деякі люди є прихильниками позиції «живи і дай жити іншим», однак інші вважають, що розміщення в мережі деяких матеріалів просто неприпустимо. Законодавство різних країн мають різні погляди на цю проблему.

Люди подають до суду на мережевих операторів, вважаючи їх відповідальними за зміст сайтів, подібно тому, як газети і журнали несуть відповідальність за зміст своїх сторінок. У відповідь оператори мереж стверджують, що мережа подібна телефонній компанії або поштовому відділенню, і вони не можуть відповідати за те, що говорять їх клієнти, а тим паче управляти змістом цих розмов. Крім того, якщо б оператори були зобов'язані повідомлення піддавати впливу цензурі, їм довелось би видаляти всі повідомлення, які залишають навіть найменшу можливість судового позову, і, таким чином, порушують права користувачів на свободу слова. Можна зі впевненістю сказати, що подібні дебати будуть тягнутись ще досить довго.

Ще однією сферою конфліктів виявилися права найманих робітників, що вступили в протиріччя з правами роботодавців. Деякі роботодавці вважають, що мають право піддавати впливу цензурі повідомлення своїх робітників, включаючи повідомлення, послані з домашніх терміналів після роботи. Не всі із цим погоджуються.

Якщо навіть роботодавець має право звертатися подібним чином з кореспонденцією своїх робітників, то як же бути з державними університетами і їх студентами? А як же школи та учні?

Дуже серйозною проблемою є також взаємини держави і громадян. Відомо, що ФБР встановило на серверах багатьох постачальників послуг Інтернету системи спостережень за всіма вхідними і вихідними повідомленнями. В принципі, подібними діями займається не тільки ФБР, проте і звичайні веб-дизайнери. Взяти хоча б cookie-файлы, які містять інформацію про те, що користувач робив в Мережі, і дозволяють нечистим на руку компаніям дізнаватись конфіденційну інформацію і передавати через Інтернет номери кредитних карток та інші важливі ідентифікатори [6, с. 818].

У перші десятиліття свого існування комп’ютерної мережі використовувались, в першу чергу, університетськими дослідникам для обміну електронної поштою і співробітниками корпорацій для спільного використання принтерів [6, с. 924]. У таких умовах питання безпеки не привертали великої уваги. Однак тепер, коли мільйони звичайних громадян користуються мережами для управління своїми банківськими рахунками, заповнення податкових декларацій, купують товари в інтернет-магазинах, проблема мережевої безпеки та захисту інформації у спілкуванні стає все більш актуальною.

Вона включає в себе велике коло питань, пов’язаних із різноманітними людськими гріхами. В найпростішому вигляді служби безпеки гарантують, що надмірно цікаві особистості не зможуть читати, або, що ще гірше, змінювати повідомлення, які адресовані іншим. Служби безпеки попереджають спроби отримання доступу до віддалених служб тим користувачам, які не мають на це право. Крім того, система безпеки дозволяє визначити, чи написане повідомлення «Сплатіть рахунки до п’ятниці» тим відправникам, чиє ім’я в ньому вказано, або ж це фальсифікація. Крім того, системи безпеки вирішують проблеми, пов’язані з перехватом і повторним відтворення повідомлень і з людьми, які намагаються заперечувати, що вони відправляли ці повідомлення.

Більшість проблем безпеки виникає через зловмисників, які намагаються вилучити яку-небудь користь для себе або нанести шкоду іншим [6, с. 815].

Стає зрозумілим, що завдання забезпечення безпеки соціальних мереж включає в себе значно більше, ніж просте вилучення програмних помилок. Часто стоїть мета протистояти розумному, переконаному та іноді гарно фінансованому супротивнику. Також стає очевидним, що міри, які здатні зупинити випадкового порушника, мало вплинуть на серйозного злочинця. Статистика, збираємо міліцією, говорить про те, що більшість атак вчиняються не ззовні, а зсередини – заздрісними або невдоволеними чимось людьми. З чого випливає, що системи безпеки повинні враховувати і цей факт [6, с. 815].

Комп’ютерні мережі надають можливість для посилання анонімних повідомлень. У деяких ситуаціях така необхідність існує. Наприклад, таким чином студенти, солдати чи звичайні громадяни можуть поскаржитись на незаконні дії професорів, офіцерів, керівництва і політиків, не остерігаючись репресій.

Наступними видом антисуспільних злочинів, що породили комп’ютерні мережі, є електронна макулатура (спам), що, на жаль, стала частиною нашого життя.

Крадіжки конфіденційної інформації, на жаль, також стали досить

розповсюдженим явищем. Нові крадії нічого не взловлюють фізично. Вони крадуть лише декілька здавалось би нічого за значущих символів. Ці символи виявляються, наприклад, номерами кредитних карток. Нарешті, можливість передачі через Інтернет досить якісної аудіо- і відеоінформації дозволило зацікавленим особам порушувати всі закони про авторські права. А вичислити порушників, як виявилось, досить складно.

Отже, подібно друкарському станку 500 років потому, комп'ютерні мережі надають нові способи розповсюдження громадянами їх поглядів серед найрізноманітнішої аудиторії. Нова свобода розповсюдження інформації несе за собою і нові невирішені політичні, соціальні і моральні проблеми.

Багато із цих проблем можуть бути вирішеними, якщо комп'ютерна індустрія серйозно займеться питаннями захисту інформації.

Інтернет і технології захисту інформації – це ті області, в яких дуже тісно переплелись соціальні питання, державна політика і технології. Ми коротко розглянемо три проблеми: конфіденційність, свободу слова й авторські права.

За останнє десятиліття уряд держави отримав можливість дуже легко шпигувати за громадянами, а громадяни – з не меншою легкістю попереджати шпигунство [6, с. 924]. У XVIII столітті для отримання доступу до особистих документів громадянина потребувалось вислати до нього додому міліціонера. В наш час телефонні компанії і постачальники послуг Інтернет забезпечують всіх, хто може пред'явити відповідний орден, прослуховуючими засобами. З їх допомогою задача міліціонера дуже полегшується [6, с. 924].

Та все ж таки, використання такого специфічного алгоритму, як криптографія, значною мірою змінює справу. Будь-який бажаючий може згенерувати добре захищеного і надійного ключа, і в результаті він отримає впевненість в тому, що більше ніхто не зможе прочитати його електронну пошту, незалежно від наявності у нього ордера на обшук. Уряд це прекрасно розуміє, і йому, звісно, це не подобається. В реальності конфіденційність означає, що уповноваженим органам дуже тяжко стежити за злочинцями різних сфер, а також за журналістами і політичними опонентами [6, с. 924]. Не дивно, що більшість урядів забороняють використання і експорт криптографії.

Слово криптографія походить від грецького слова, яке означає «прихований лист» [6, с. 818]. Історія її довга і яскрава та починається вона декілька тисяч років тому. Історично використовували і розвивали мистецтво криптографії представники чотирьох професій: військ-

кові, дипломатичний корпус, люди, які вели щоденники, і коханці. Із них найбільш важливу роль у розвитку цієї сфери відіграли військові.

До виникнення комп’ютерів одним із основних стримуючих чинників у криптографії була нездатність шифрувальника виконати необхідне перетворення – нерідко на полі бою за допомогою нескладного обладнання. Крім того, досить складною задачею було швидке переключення з одного криптографічного методу на інший. Та все ж таки, небезпека того, що шифрувальник може бути захоплений супротивником, спонукала розвити здатність до постійної зміни криптографічних методів.

Отже, криптографія являє собою інструмент, що використовується для забезпечення конфіденційності інформації, перевірки її цілісності й автентичності. Всі сучасні криптографічні системи основані на принципі Керкгофа, що говорить про те, що алгоритми повинні бути доступні всім бажаючим, а ключі – тримаються в таємниці [6, с. 934]. Більшість алгоритмів при шифруванні тексту виконують складні перетворення, що включають в собі заміни і перестановки. Та все ж таки, якщо вийде реалізувати на практиці принципи квантової криптографії, то за допомогою одноразових блокнотів можна буде створити дійсно надійні криптосистеми.

Всі криптографічні алгоритми можна розділити на два типи: з симетричними ключами та з відкритими ключами. Алгоритми зі симетричними ключами при шифруванні викривляють значення в послідовності ітерацій, параметризованим ключем [6, с. 934].

Повідомлення, які підлягають шифруванню, називаються відкритим текстом, перетворюються за допомогою функції, другим вхідним параметром якої є ключ. Результат процесу шифрування, що називається зашифрованим текстом [4, с. 819].

У першому приближенні проблеми безпеки мереж можуть бути розділені на чотири суміжні області: секретність, аутентифікація, забезпечення чіткого виконання зобов’язань і забезпечення цілісності. Секретність (конфіденційність) означає попередження попадання інформації в руки неавторизованих користувачів. Аутентифікація дозволяє визначити, з ким ви розмовляєте, перед тим, як надати співрозмовнику доступ до секретної інформації або вступити з ним в ділові взаємини. Проблема забезпечення чіткого виконання зобов’язань має справу з підписами.

Всі ці аспекти (секретність, уатентифікація, забезпечення чіткого виконання зобов’язань і забезпечення цілісності) зустрічаються і в традиційних системах, проте з деякими суттєвими відмінностями.

Секретність і цілісність досягаються за допомогою замовних листів.

Однак, коли конфіденційність краще всього забезпечується якраз відсутністю аутентифікації, тобто встановленням анонімних з'єднань. Анонімність популярна як при передачі повідомлень між двома користувачами, так і в мережевих телеконференціях.

Розглянемо деякі приклади. По-перше, політичні дисиденти, які живуть при авторитарному режимі, для того, щоб запобігти репресії, можуть захотіти спілкуватись анонімно. По-друге, різноманітні порушення в багатьох комерційних, освітянських, урядових та інших організаціях часто виявляються не без допомоги тих людей, які бажають залишатись невідомими. По-третє, прихильники нетрадиційних соціальних політичних або релігійних переконань бачать одну із небагатьох можливостей спілкування в телеконференціях, де вони можуть приховувати свої справжні імена. По-четверте, більшість надає перевагу обговорювати алкоголізм, душевні хвороби, сексуальні проблеми тощо.

Сфера застосування принципів анонімності не обмежується однією електронною поштою. Існують також послуги, які дозволяють анонімно дивитися інтернет-матеріали.

Конфіденційність пов'язана з проблемою приховування від посторонніх очей інформацію, яка не підлягає розголосу. Іншим ключовим соціальним аспектом є, безперечно, свобода слова і її протилежність – цензура. В цьому випадку органи влади намагаються обмежити спектр інформації, яку громадяни можуть читати і опубліковувати. Всесвітнє павутиння з її мільйонами сторінок – це справжній рай для цензури.

Більшість ніяк не можуть зрозуміти, що Всесвітнє павутиння – справді всесвітнє. Воно охоплює всю земну кулю. В різних країнах існують різні думки про те, що повинно, а що не повинно бути в Мережі.

У країнах, де цензура застосовується особливо широко, завжди існують дисиденти, що використовують свої методи обходу цієї цензури. криптографія, звичайно, дозволяє посилати секретні повідомлення так, щоб ніхто не зміг дізнатися їх сенс. Таким чином, політики, які зазвичай не дуже добре володіють математикою, розуміють та застосовують принцип транзитивності. Виручити можуть анонімні розсилки, проте і їх місцевий уряд може заборонити, і тоді для відправки повідомлень за кордон знадобиться експортна ліцензія. Таким чином, анонімні розсилки – це також не панацея. Однак Всесвітнє павутиння завжди знайде вихід із такого становища.

Конфіденційність і цензура – це ті сфери, в яких стикаються технологічні аспекти й суспільні інтереси. Третьою такою областю є захист авторських прав. Авторське право гарантує свободу розпорядження інтелектуальною власністю її творців, якими можуть бути, наприклад, художники, письменники, композитори, музиканти, фотографи, кінорежисери, хореографи і т. ін. Авторське право видається на певний термін, який зазвичай рівняється терміну життя автора плюс 50 років. Після закінчення цього терміну інтелектуальна власність стає надбанням суспільства [6, с. 931].

Кіберпростір нічім не відрізняється від соціума: і там, і там постійно стикаються інтереси різних груп, що призводить до боротьби і судових позивів, результатом яких все ж таки рано чи пізно становиться знаходження певного компромісу.

Підбиваючи підсумки зіставлення сутності теорії криптографії та культури спілкування в соціальній мережі дозволяє нам сформулювати низку таких висновків:

По-перше, культура спілкування в соціальній мережі охоплює більш глибинні шари соціальних перетворень на сучасному етапі загальноцивілізаційного розвитку, ніж загальноприйнята культура спілкування в об’єктивно наявній реальності.

По-друге, розглянувши вітчизняні і закордонні джерела інформації, нами було виявлено, що далеко не кожна концепція культури спілкування постмодерну охоплює сферу інформації та її ролі в соціальних процесах у тому значенні, як це роблять теоретики інформаційного суспільства.

Наступним висновком стало розуміння того, що особливістю комунікативних теорій суспільного розвитку є те, що вони не розглядають інформацію та комунікаційні технології як сутнісну рису лише сучасного суспільства. У них обґрунтовується теза, що комунікація в будь-якому суспільстві і в будь-який історичний період його існування є наріжним каменем функціонування суспільства.

Отже, культура спілкування в соціальній мережі має свою специфіку, та все ж таки не має суттєвих відмінностей від загальноприйнятої культури спілкування загалом. Відповідно до цього положення дві сфери мають дотичні проблематики свого існування. Та все ж віртуальне спілкування в соціальних мережах має переважно письмовий характер, що акцентує увагу на створенні додатковому захисті інформації в соціальних мережах, що існують.

Література:

1. Берхин Н. Б., Крутоус В. П. Является ли познание целью искусства? Два взгляда на одну проблему. – М.: Знание, 1989. – 64 с.

2. Гольдштейн Б. С., Соколов Н. А., Яновський Г. Г. Сети связи: Учебник для ВУЗов. – СПб.: БХВ-Петербург, 2010. – 400 с.

3. Ведмедєва Л. Ідеї Олександра Потебні про людинотворчу природу мистецтва і культурний контекст сучасності // Людинознавчі студії: Зб. наук. праць Дрогобицького державного педагогічного університету імені Т. Г. Франка / Ред. кол. Т. Біленко (гол. ред.), М. Кашуба, В. Мовчан, В. Кремінь та ін. – Дрогобич: Вимір, 2001. – Випуск 3. – С. 63-72.

4. Вісник Національного авіаційного університету. Філософія. Культурологія: Зб. наук. праць. – № 2 (4). – К.: НАУ, 2006. – 224 с.

5. Гічан І. С., Назаренко Д. В. Психотехнологія ділового спілкування. – К.: НАУ, 2003. – 78 с.

6. Компьютерные сети. 4-е изд. / Э. Таненбаум. – СПб.: Питер, 2006. – 992 с.

7. Комп'ютерні мережі. Підручник / За ред. Ю. С. Ковтанюка. – К.: Видавництво «Юніор», 2005. – 400 с.

8. Лиотар Ж.-Ф. Ситуация постмодерна // Философская и социологическая мысль. – 1995. – № 5-6. – С. 15-38.

9. Маліков В. В. Культура ділового спілкування менеджера. – Х.: ХНАДУ, 2001. – 146 с.

10. Пелипенко А. А. Постмодернизм в контексте переходных процессов // Человек. – 2001. – № 4. – С. 5-17.

11. Тоффлер Э. Третья волна. – М.: Изд-во АСТ, 1999. – 782 с.