Отже, очевидно, що від акцентованої уваги безперечно актуальних та гострих проблем освіти у сучасному кіберпросторі, треба еволюціонувати у бік системного вивчення та осучаснення номадології у реалії освітнього сьогодення, як нової мобілістичної форми мислення особистості XXI століття.

Список використаних джерел:

1. Горбунова Людмила. Номадизм як спосіб мислення та освітня стратегія. *Філософія освіти*. 1–2 (9). 2010. С. 103–114.
2. Завгородня Ю. Політичне протистояння в кіберпросторі: глобалізацій ний аспект. *Вісник Львівського університету. Серія філос.-політолог. студії.* 2022. Випуск 40, с. 148–153. DOI https://doi.org/10/30970/PPS.2022.40.19
3. Закон України «Про основні засади забезпечення кібербезпеки України». 05 жовтня 2017 року № 2163-VII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
4. Рішення Ради національної безпеки і оборони України «Про План реалізації Стратегії кібербезпеки» від 30 грудня 2021 року. Указ Президента України від 1 лютого 2022 року № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text
5. Рішення Ради національної безпеки і оборони України «Про Стратегію національної безпеки України» від 14 вересня 2020 року. Указ Президента України від 14 вересня 2020 року № 37/2022. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text
6. Пучков О. О., Уваркіна О. В. Емерджентні властивості сучасної освіти. *Актуальні питання лінгвістики, професійної лінгводидактики, психології і педагогіки вищої школи*: збірник статей VI Міжнародної науково-практичної конференції (м. Полтава, 25-26 листопада 2021 р.). Полтава : Вид-во «Астрая», 2021. С. 257–261.

Ключові слова: ризомний простір, номади, кібербезпека, діджиталізація, кіберобізнаність.

Key words: rhizome space, nomads, cybersecurity, digitalization, cyberknowledge.

АХМАМЕТЬЄВА ГАННА ВАЛЕРІЇВНА

Національний університет «Одеська юридична академія», доцент кафедри кібербезпеки, кандидат технічних наук

ПЕРЕВАГИ І НЕДОЛІКИ ВИКОРИСТАННЯ СТЕГАНОГРАФІЇ В МЕСЕНДЖЕРАХ

Сучасні технології та Інтернет-комунікації сприяють миттєвому обміну інформацією між користувачами різних країн світу. Засобами веб-сайтів, електронної пошти, месенджерів, файлообмінників, хмар-

них сховищ можна передавати будь-які дані, будь то текстові документи та повідомлення, аудіозаписи, фото, відео та багато інших. Однак далеко не всі інструменти Інтернет-комунікації є безпечними. Якщо необхідно передати загальнодоступну або несекретну інформацію, то існуючі системи моніторингу не створюють особливих проблем, хоч можуть відстежувати активність та інтереси користувача. Але якщо необхідно передати конфіденційну інформацію і при цьому відсутні захищені канали зв'язку (або неможливо в даний конкретний момент скористатися захищеними засобами зв'язку), то моніторинг трафіку і ресурсів створює велику загрозу збереженню в таємниці персональної або комерційної інформації.

Якщо розглядати найпоширеніші на сьогодні засоби зв'язку – месенджери, то багато з них використовують наскрізне шифрування, яке може захистити конфіденційну інформацію від сторонніх осіб. Однак не все так однозначно. Не менш важливим фактором в забезпеченні безпеки інформації в месенджерах є наявність шифрування бекапів в хмарі, відкритого коду, відсутність збору даних і метаданих та їх передача третім особам. Найчастіше конфіденційна інформація може передаватися як окремий файл, який так чи інакше осідає в хмарному сховищі, резервних копіях, тощо. Часто резервні копії та дані в хмарному сховищі зберігаються без шифрування. У випадку, коли месенджер має повністю відкритий код, просунуті користувачі та аудитори можуть перевірити відповідність коду заявленому функціоналу, наявності шифрування резервних копій та відсутність збору даних, інакше це неможливо, і безпека інформації може залишатися під загрозою.

Особливу небезпеку становлять корпоративні і групові чати, які забезпечують спілкування і обмін інформацією групи осіб. Не всі групові чати в месенджерах мають наскрізне шифрування, що в умовах дистанційних форм праці для певної категорії організацій і підприємств є суттєвим недоліком.

В таблиці 1 [1] наводиться коротка характеристика найпопулярніших месенджерів в Україні за даними [2].

Слід зазначити, що всі з розглянутих месенджерів підтримують наскрізне шифрування для дзвінків/відеодзвінків, не мають повністю відкритого вихідного коду (як клієнтської, так і серверної сторони), шифрування метаданих (відправника, отримувача, час відправки/читання, тощо).

Тобто всі з популярних в Україні месенджерів мають недоліки, пов'язані з недостатнім забезпеченням безпеки конфіденційної інформації.

Одним з рішень проблем безпеки може стати використання стеганографічних засобів, які дозволяють приховано вбудувати конфіденційні дані в загальнодоступний несекретний інформаційний контент. Оскільки сучасні месенджери мають можливість передавати документи, мультимедійні дані (зображення, відео, аудіо-повідомлення), то не виникає суттєвих заперечень щодо організації такого прихованого каналу зв'язку. Для підготовки несекретного інформаційного контенту

з конфіденційними даними достатньо мати стеганографічну програму або програмно реалізований стеганографічний алгоритм на персональному комп'ютері або мобільному пристрої, та заздалегідь оговорити із зацікавленими користувачами параметри стеганографічної системи (пропускну спроможність прихованого каналу зв'язку, стеганографічний ключ, певні параметри конкретного стеганографічного алгоритму, тощо). Існує величезна кількість стеганографічних методів, стійких до різних атак, зокрема, стисненню, зашумленню тощо.

Таблиця 1 – Порівняльний аналіз популярних месенджерів в Україні

Характеристика	**Viber**	**WhatsApp**	**Facebook Messenger**	**Telegram**
Підтримка наскрізного шифрування за умовчанням	Так	Так	Ні (потрібно самостійно почати захищений чат)	Ні (потрібно самостійно почати захищений чат)
Збір особистих даних користувача з боку адміністрації	Контакти, контактна інформація, ідентифікатори			
	Контент користувача, місцерозташування, покупки			–
	–	Фінанси	Здоров'я та фітнес, фінанси, історія пошуку, історія переглядів	
Хешування персональної інформації (номер, список контактів)	Ні	Ні	Ні	Так
Шифрування бекапу переписки в хмарі	Ні	Ні	Ні	Так

Таким чином, через недостатньо захищені месенджери ми отримуємо можливість таємно від адміністрації та служб моніторингу передавати конфіденційні дані. В цьому випадку на хмару потрапить несекретний інформаційний контент, який не приверне до себе особливої уваги. Використання стеганоаналітичних алгоритмів майже не практикується – існує лише обмежена кількість програмних реалізацій стеганоаналітичних методів, зокрема McAfee Steganography Analysis Tool [3]. Слід зазначити, що стеганоаналіз є чутливим до обраного стеганографічного методу, тобто існуючі засоби стеганографії за певних умов взагалі не можуть виявити наявність прихованого повідомлення (конфіденційних даних). Навіть якщо наявність приховано вбудованої інформації буде доведено, вилучити конфіденційні дані при використанні стеганографічного ключу та інших параметрів неможливо, їх можна лише зруйнувати. Сучасний стан розробок в області стеганоана-

лізу не дозволяє вилучати повідомлення, тільки виявляти факт його наявності.

Серед недоліків можна визначити наступні:

1) недостатня освітленість стеганографії в інформаційному просторі (це можна розглядати і як перевагу в тому сенсі, що приділяється недостатня увага стеганоаналізу через специфічність напряму);

2) обмежена кількість програмно реалізованих стеганографічних методів (якщо для персональних комп'ютерів ще існують реалізації, то мобільні додатки майже відсутні);

3) для надійного захисту конфіденційних даних слід ретельно підбирати стеганографічний метод, вивчати його характеристики та аналізувати наукові дослідження.

Як бачимо, ці недоліки пов'язані в основному з недостатньою освітленістю напрямів стеганографії та стеганоаналізу в інформаційному просторі, які з часом можна вирішити, розробивши прикладні стеганографічні додатки або месенджер з функціоналом організації прихованої комунікації засобами стеганографії.

В роботі проаналізовані основні недоліки безпеки конфіденційних даних за умови їх передачі в месенджерах, визначені основні переваги і недоліки використання стеганографічних систем в месенджерах.

Список використаних джерел:

1. Денис Ли. Сравнительный анализ безопасности и приватности мессенджеров. [Електронний ресурс]: публікація від 31 березня 2021 року. Режим доступу: https://www.anti-malware.ru/compare/Messengers-security-and-privacy
2. Опитування: Viber, Facebook Messenger і Telegram – найпопулярніші месенджери серед українців [Електронний ресурс]: публікація від 19 Листопада 2021 року. Режим доступу: https://ms.detector.media/sotsmerezhi/post/28531/2021-11-19-opytuvannya-viber-facebook-messenger-i-telegram-naypopulyarnishi-mesendzhery-sered-ukraintsiv/
3. McAfee Steganography Analysis Tool [Електронний ресурс. Режим доступу: https://www.mcafee.com/enterprise/en-us/downloads/free-tools/steganography.html

Ключові слова: Месенджер, захист інформації, безпека даних, стеганографія.
Key words: Messenger, information protection, data security, steganography.