DOI: https://doi.org/10.36910/6775-2524-0560-2025-59-14
УДК 004.056.5
Деркач Марина Володимирівна[1,2], к.т.н., доцент
https://orcid.org/0000-0001-8977-2776
Кондратенко Роман Андрійович[2], студент
https://orcid.org/0009-0005-7294-0645
Барбарук Віктор Миколайович[2,3], к.т.н., доцент
https://orcid.org/0000-0001-9558-0965
[1]Тернопільський національний технічний університет імені Івана Пулюя, м. Тернопіль, Україна,
[2]Східноукраїнський національний університет імені Володимира Даля, м. Київ, Україна,
[3]Київський політехнічний інститут імені Ігоря Сікорського, м. Київ, Україна

ІНФОРМАЦІЙНА СИСТЕМА ФОРМУВАННЯ СОЦІАЛЬНОГО ПРОФІЛЮ ОСОБИСТОСТІ ЗАВДЯКИ OSINT-ТЕХНОЛОГІЇ

Деркач М. В., Кондратенко Р. А., Барбарук В. М. Інформаційна система формування соціального профілю особистості завдяки OSINT-технології. Зростання обсягу даних, доступних в онлайн-джерелах, створює нові можливості в різних сферах діяльності та сприяє виявленню закономірностей, трендів та знань, що є підставою для розробки. У статті представлена розроблена інформаційна система формування соціального профілю особистості завдяки OSINT-технології, яка забезпечує комплексний підхід до збору, обробки, захисту даних з популярного месенджера Telegram. Використання бібліотеки WTelegramClient дозволило забезпечити надійний та зручний спосіб взаємодії з Telegram API для ефективного збору різних типів даних, включаючи текстові повідомлення, медіа файли та вебпосилання. Для забезпечення конфіденційності та безпеки даних впроваджено кілька рівнів захисту. Використано криптографічний протокол SSL для шифрування даних, що забезпечує захищений канал зв'язку між клієнтом і сервером. Власний протокол месенджера MTProto гарантує безпечну передачу даних у межах Telegram. Для зберігання даних використано базу даних MSSQL, яка також підтримує захищене з'єднання, автентифікацію/авторизацію, шифрування даних. Інтерфейс, створений на основі Angular та spartan.ng, інтуїтивно зрозумілий, дозволяє легко візуалізувати та аналізувати зібрані дані, надає доступ до всіх функціональних можливостей розробленої системи. Загалом, інформаційна система формування соціального профілю особистості забезпечує зручну та ефективну роботу з великими обсягами інформації, надаючи користувачам можливість працювати з конфіденційною інформацією у безпечному середовищі.
Ключові слова: інформаційна система, OSINT-технології, кібербезпека, конфіденційність, шифрування.

Derkach M., Kondratenko R., Barbaruk V. Information system for forming a social profile of an individual using OSINT technologies. The growth of the volume of data available in online sources creates new opportunities in various fields of activity and contributes to the identification of patterns, trends and knowledge, which is the basis for development. The article presents the developed information system for forming a social profile of an individual thanks to OSINT technology, which provides a comprehensive approach to collecting, processing and protecting data from the popular Telegram messenger. The use of the WTelegramClient library made it possible to provide a reliable and convenient way of interacting with the Telegram API for the effective collection of various types of data, including text messages, media files and web links. To ensure confidentiality and security of data, several levels of protection have been implemented. The SSL cryptographic protocol is used for data encryption, which provides a secure communication channel between the client and the server. The messenger's own MTProto protocol guarantees secure data transmission within Telegram. The MSSQL database is used to store data, which also supports a secure connection, authentication/authorization, and data encryption. The interface, created based on Angular and spartan.ng, is intuitive, allows easy visualization and analysis of collected data, provides access to all the functionalities of the developed system. In general, the information system for forming a social profile of a person provides convenient and effective work with large amounts of information, giving users the opportunity to work with confidential information in a secure environment.
Keywords: information system, OSINT technologies, cybersecurity, privacy, encryption.

Постановка проблеми. У сучасному цифровому суспільстві величезна кількість даних про особистість доступна з відкритих джерел – соціальних мереж, вебсайтів, форумів, блогів, баз даних, медіа, публічних реєстрів тощо [1]. Це створює для організацій, служб безпеки, HR-відділів, аналітиків, як нові можливості — аналіз репутації, підвищення кібербезпеки, так і ризики — маніпуляції, порушення приватності. Тому у світі, де інформація стає ключем до успіху, зростає потреба в ефективних інструментах для збору та аналізу даних про особистість. Технології OSINT (Open Source Intelligence – розвідка з відкритих джерел) дозволяють ефективно збирати, обробляти та аналізувати дані. Наразі існують такі популярні системи формування соціального профілю особистості на основі OSINT-технологій, як Fama, Hootsuite Insights, Mention, Talkwalker, Socialbakers та Falre.io. Водночас, більшість існуючих інформаційних систем не забезпечують достатньо точного, комплексного й структурованого аналізу особистих даних із відкритих джерел. В умовах кіберзагроз, дезінформації та соціальної інженерії важливо створювати інформаційні системи, які допомагають формувати цілісний, структурований соціальний профіль особистості на

© Деркач М. В., Кондратенко Р. А., Барбарук В. М.

основі достовірних відкритих джерел, забезпечуючи при цьому релевантність та етичність обробки інформації.

Аналіз останніх досліджень і публікацій. Так у дослідженні [2] представлено систему на основі OSSINT, яка дозволяє виявляти приховану інформацію в профілях користувачів соціальних мереж, зокрема Facebook. Система аналізує мережу друзів користувача та може передбачати нові зв'язки, що дозволяє інферувати особисті дані, які користувач вважав приватними. Автори статті [3] пропонують класифікацію даних та інструментів OSINT, пов'язаних з ідентичністю, що допомагає систематично шукати та аналізувати дані для виявлення можливих векторів атак та прийняття контрзаходів. Дослідження [4] пропонує метод виявлення підозрілої поведінки користувачів Facebook за допомогою машинного навчання та OSINT, що може бути корисним для безпекових організацій у прогнозуванні внутрішніх загроз. У статті [5] представлено гнучкий фреймворк для масштабування OSINT-розслідувань за допомогою краудсорсингу, що дозволяє ефективно залучати новачків до підтримки професійних розслідувань.

Аналіз публікацій підтверджує, що розробка подібних систем є актуальною задачею, і як для кібербезпеки, так і для кадрового аналізу, антикорупційної діяльності, цифрової безпеки та досліджень у соціальній сфері.

Метою статті є розроблення інформаційної системи формування соціального профілю особистості для збору, аналізу та візуалізації даних з онлайн-джерел, таких як чати, канали, групи та форуми завдяки OSINT-технології.

Вирішення проблеми. Одним з основних джерел інформації став такий популярний месенджер, як Telegram, що надає можливість створення як публічних, так і приватних каналів та груп. Згідно з дослідженням платформи Statista, станом на лютий 2025 року кількість активних користувачів Telegram перевищує 950 мільйонів на місяць, з яких значна частина використовує месенджер для обміну конфіденційною інформацією та участі в спеціалізованих групах. Це робить Telegram цінним джерелом для дослідження сучасних кіберзагроз та методів захисту від них.

Збір даних є критичним етапом у будь-якому дослідженні, оскільки саме від якості зібраної інформації залежить точність і надійність результатів. Існує кілька ключових технологій OSINT розвідки, таких як використання скраперів веб-сторінок, API соціальних мереж та інструментів аналізу тексту.

Отже, розроблена інформаційна система автоматизує процес збору даних завдяки бібліотеці WTelegramClient, забезпечуючи їх регулярне оновлення та збереження, використовуючи запити до Telegram API для отримання повідомлень, інформації про учасників груп і каналів, а також іншої корисної інформації: відправник, чат, медіа файли, текст, вебпосилання та метадані [6]. Це дозволяє швидко збирати великі обсяги даних для подальшого аналізу, фільтрації та відправки даних до сховища. Telegram API використовує свій власний криптографічний протокол MTProto [7], який забезпечує потокове шифрування перед взаємодією клієнтів з сервером завдяки REST API.

Наприклад, для отримання вмісту чату потрібно викликати функцію з необхідними параметрами та отримати результат. У MTProto TL-схема (мова типів, що використовуються API, для представлення оголошених типів і функцій) буде серіалізована у двійковий формат, перш ніж вона буде вбудована як корисне навантаження повідомлень:

Лістинг 1. TL-схема прикладу

```
auth.sentCode#efed51d9 phone_registered:Bool phone_code_hash:string
send_call_timeout:int is_password:Bool =
auth.SentCode;auth.sentAppCode#e325edcf phone_registered:Bool
phone_code_hash:string send_call_timeout:int is_password:Bool =
auth.SentCode;---functions---auth.sendCode#768d5f4d phone_number:string
sms_type:int api_id:int api_hash:string lang_code:string = auth.SentCode;
```

Таким чином, використання Telegram API є оптимальним рішенням для збору даних з Telegram, забезпечуючи ефективність, точність і безпеку процесу. Саме забезпечення конфіденційності та безпеки даних є одним з найважливіших аспектів, особливо тому, що мова йде про обробку та зберігання особистої інформації користувачів. У розробленій інформаційній системі застосовуються декілька рівнів захисту, оскільки разом з MTProto використовується криптографічний протокол SSL (Secure Sockets Layer), що забезпечує захищений канал зв'язку між

© Деркач М. В., Кондратенко Р. А., Барбарук В. М.

клієнтом і сервером. Він використовується для шифрування даних, що передаються через Інтернет, запобігаючи їх перехопленню та несанкціонованому доступу.

Архітектура розробки, зображена на рисунку 1, також передбачає сховище даних та інтерфейс користувача, що забезпечує користувачам доступ до візуалізації даних, пошуку, фільтрації, групуванню, тощо. Ця архітектура є гнучкою та може бути розширена за рахунок додавання нових компонентів та функціональних можливостей.

В якості сховища даних використано базу даних Microsoft SQL Server (MSSQL), для комунікації та генерації міграцій для бази даних застосовано фреймворк об'єктно-реляційного відображення (ORM) з відкритим вихідним кодом Entity Framework Core. Основні заходи захисту, що застосовуються до бази даних MSSQL, включають:

1. Доступ до бази даних здійснюється через захищене з'єднання, яке шифрує всі дані, що передаються між системою і базою даних.
2. Доступ до бази даних захищений паролем, який забезпечує, що тільки авторизовані користувачі можуть отримати доступ до конфіденційної інформації. Крім того, використовуються механізми контролю доступу, які обмежують права користувачів і дозволяють доступ лише до тих даних, що їм необхідні для виконання своїх завдань.
3. MSSQL підтримує шифрування даних як на рівні бази даних, так і на рівні окремих таблиць й стовпців. Це дозволяє забезпечити додатковий рівень захисту для конфіденційної інформації, навіть якщо зловмисники отримають доступ до фізичних файлів бази даних.

Завдяки використанню SSL для захисту передачі даних, MTProto для захищеної комунікації у Telegram, а також надійних заходів безпеки в базі даних MSSQL, інформаційна система забезпечує високий рівень захисту конфіденційності та безпеки даних користувачів. Ці заходи гарантують, що всі дані залишаються захищеними від несанкціонованого доступу та зловживань, забезпечуючи надійність та довіру до розробки.

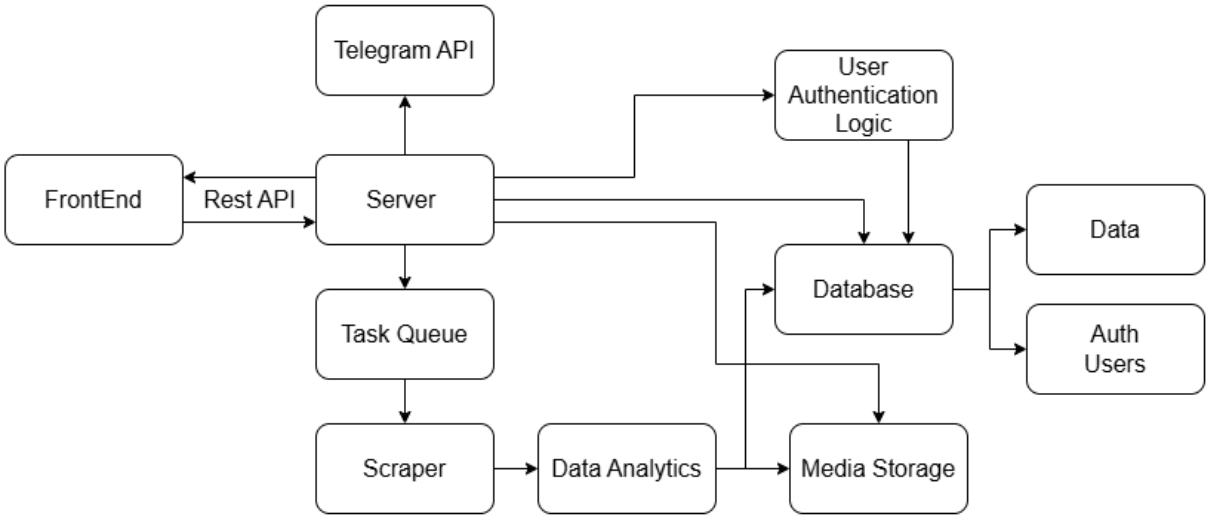


Рис. 1 – Архітектура інформаційної системи

Ще одним критично важливим етапом є розробка інтерфейсу користувача, який є простим у використанні як для досвідчених користувачів, так і для початківців, надаючи можливість візуалізувати зібрані та проаналізовані дані.

Для цього використано фреймворк Angular у поєднанні з бібліотекою компонентів spartan.ng для створення сучасного, інтерактивного та продуктивного інтерфейсу користувача. Angular забезпечує модульність, повторне використання коду та інтеграцію з багатьма іншими бібліотеками та інструментами, а також використовуючи Angular, створено рефлективний інтерфейс, який автоматично оновлюються у відповідь на зміни даних. Це означає, що користувачі зможуть бачити актуальні дані в режимі реального часу, без необхідності перезавантажувати сторінку. Бібліотека spartan.ng надає широкий набір готових компонентів, таких як таблиці, форми, кнопки та навігаційні панелі, що дозволило швидко створити інтуїтивно зрозумілі елементи інтерфейсу, які відповідають сучасним стандартам дизайну та забезпечують високий рівень користувацького досвіду.

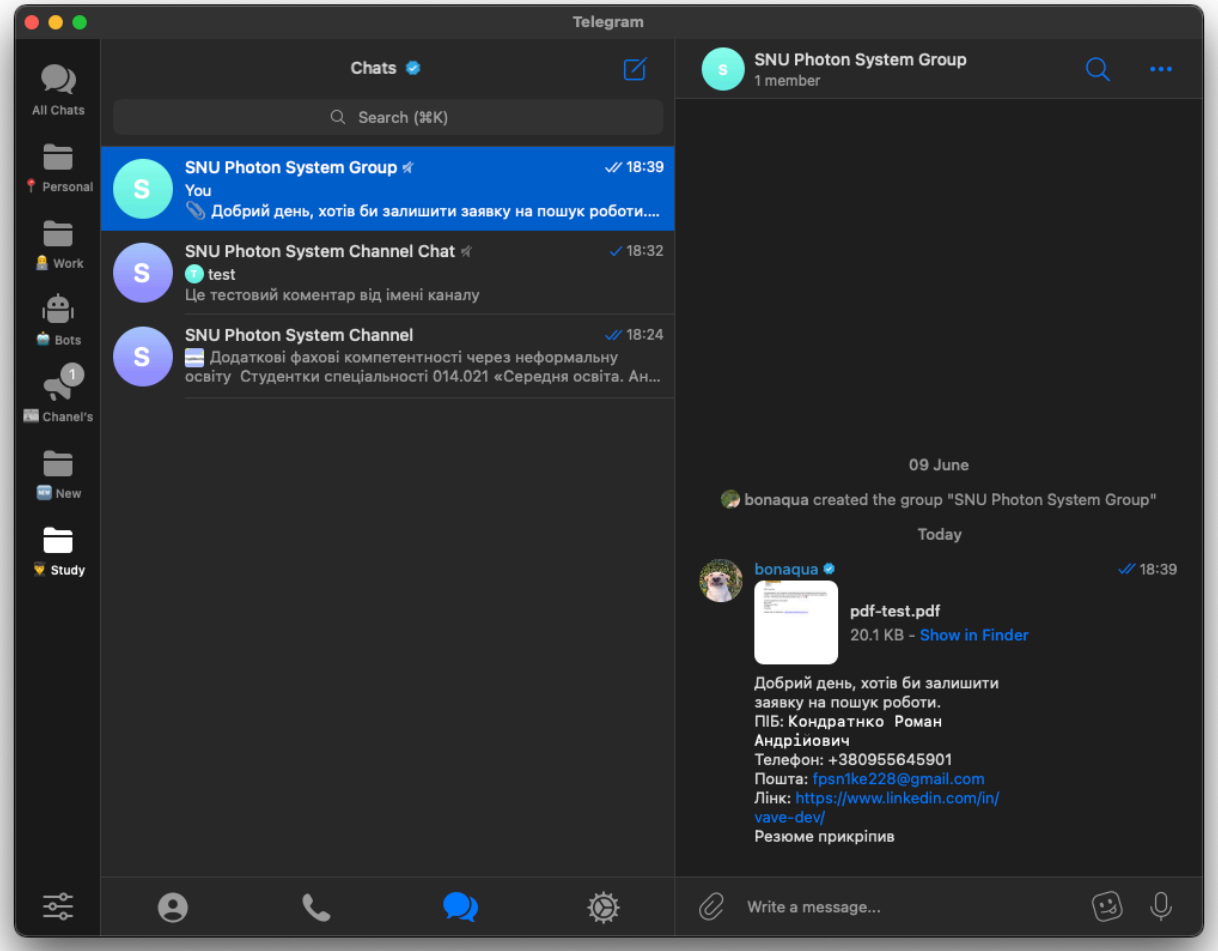
© Деркач М. В., Кондратенко Р. А., Барбарук В. М.

Результати тестування. Для проведення тестування підготовлено акаунт, що використано для збору важливих або чутливих даних, медіа та іншої інформації користувачів з груп, каналів, чатів. Також підготовлено групу, канал та чат в Telegram, зроблено пост в каналі з новиною, залишено коментарі під постом, й відправлено файл разом з повідомленням, що містить чутливі дані (рис. 2).

Тепер можна перейти до алгоритму збору і аналізу даних, що буде працювати у фоновому режимі після запуску системи. Завдяки бібліотеці WTelegramClient можна підписатися на оновлення з підготовленого акаунту і отримувати усі нові повідомлення, потрібні дані та зберігати їх до бази даних. Після чого вони одразу доступні в інтерфейсі користувача.

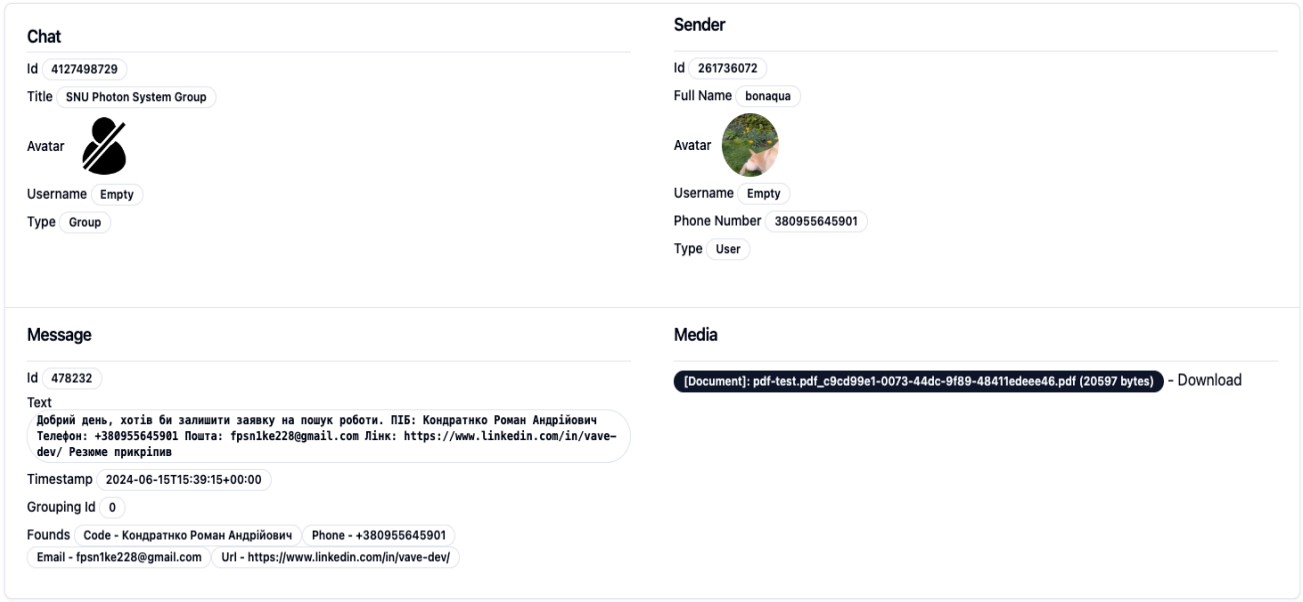
Також передбачено аналіз оновлень, що включає:

– валідацію, тобто перевірку типу оновлення, ідентифікатор списку прослуховування;
– наявність ідентифікатора відправника, чата в базі даних;
– тип вмісту повідомлення - медіа файли, документи та статус – особисте або групове повідомлення;
– наявність чутливої інформації у тексті повідомлення.



а)

© Деркач М. В., Кондратенко Р. А., Барбарук В. М.



б)

Рис. 2 – Демонстрація з чутливими даними: а) Повідомлення з акаунту Telegram, б) Інтерфейс користувача розробленої інформаційної системи

На рисунку 2 для прикладу показано тестування розробленої інформаційної системи підчас роботи з чутливими даними, а саме як тільки в групі з'явилось повідомлення, що містить файл-резюме та контактні дані відправника, система отримала це повідомлення, занесла його вміст і безпосередньо файл в базу даних, і тепер вміст повідомлення залишиться в базі даних системи, навіть, якщо повідомлення буде видалено з групи. На рисунку 2а видно, що повідомлення з чату, але відправник – група, і у секції Founds з'явились чутливі дані.

В цілому інформаційна система формування соціального профілю особистості здатна автоматично виявляти дані з онлайн-джерел, таких як чати, канали, групи та форуми месенджера Telegram завдяки OSINT-технології; класифікувати формати даних, такі як текст, зображення, відео та аудіо; фільтрувати дані за ключовими словами, темами, авторами або іншими критеріями.

Висновки. Розроблена інформаційна система формування соціального профілю особистості завдяки OSINT-технології є надійним інструментом для збору та аналізу даних з Telegram, забезпечуючи комплексний підхід і високий рівень безпеки та зручності використання. Здатна ефективно підтримувати дослідження та аналіз, надаючи користувачам можливість працювати з конфіденційною інформацією у безпечному середовищі. Забезпечення конфіденційності та безпеки даних стало пріоритетом у розробці. Для цього впроваджено кілька рівнів захисту, включаючи використання SSL для шифрування переданих даних, протокол MTProto для забезпечення безпеки комунікації у Telegram та захист бази даних MSSQL паролями та іншими механізмами контролю доступу. Ці заходи гарантують, що всі дані залишаються захищеними від несанкціонованого доступу та зловживань. Завдяки використанню Angular та spartan.ng, розроблено ефективний та зручний інтерфейс користувача, який дозволив легкий доступ до даних та їх візуалізацію, полегшуючи користувачам роботу з великими обсягами інформації, що забезпечить високий рівень задоволення користувачів, які зможуть швидко знаходити та обробляти необхідну інформацію.

Список бібліографічного опису

1. М.В. Деркач, В.Ю. Остополець, В.С. Дерев'янченко. Розробка мобільного додатку для визначення автентичності медіа файлу. Вісник Східноукраїнського національного університету імені Володимира Даля. Київ: СНУ ім.В.Даля, 2023. № 3(279). С.5-10.
2. Cascavilla, G., Beato, F., Burattin, A., Conti, M., & Mancini, L. V. (2016). OSSINT-Open Source Social Network Intelligence An efficient and effective way to uncover" private" information in OSN profiles. *arXiv preprint arXiv:1611.06737*.
3. Walkow, M., & Pöhn, D. (2024). Systematically Searching for Identity-Related Information in the Internet with OSINT Tools. *arXiv preprint arXiv:2407.16251*.
4. Panagiotou, A., Ghita, B., Shiaeles, S., & Bendiab, K. (2019). A machine-learning approach to Detect users' suspicious behaviour through the Facebook wall. *arXiv preprint arXiv:1910.14417*.

© Деркач М. В., Кондратенко Р. А., Барбарук В. М.

5.Mukhopadhyay, A., Venkatagiri, S., & Luther, K. (2024). OSINT Research Studios: A Flexible Crowdsourcing Framework to Scale Up Open Source Intelligence Investigations. *Proceedings of the ACM on Human-Computer Interaction*, *8*(CSCW1), 1-38.
6.T. Sušánka, J. Kokeš. Security Analysis of the Telegram IM. In Proceedings of the 1st Reversing and Offensive-oriented Trends Symposium (ROOTS). Association for Computing Machinery, New York, NY, USA. 2017. pp. 1–8.
7.М.В. Деркач, О.Є. Мишко. Використання алгоритму шифрування AES-256-CBC для зберігання даних автентифікації автономного помічника. Наукові вісті Далівського університету. Електронне видання. №24. 2023.

References

1.Derkach M., Ostopolets V., Derevyanchenko V. Development of mobile application for determining authenticity of media file. Вісник VISNIK OF THE VOLODYMYR DAHL EAST UKRAINIAN NATIONAL UNIVERSITY. Kyiv: EUNU, 2023. № 3(279). P.5-10.
2.Cascavilla, G., Beato, F., Burattin, A., Conti, M., & Mancini, L. V. (2016). OSSINT-Open Source Social Network Intelligence An efficient and effective way to uncover" private" information in OSN profiles. *arXiv preprint arXiv:1611.06737*.
3.Walkow, M., & Pöhn, D. (2024). Systematically Searching for Identity-Related Information in the Internet with OSINT Tools. *arXiv preprint arXiv:2407.16251*.
4.Panagiotou, A., Ghita, B., Shiaeles, S., & Bendiab, K. (2019). A machine-learning approach to Detect users' suspicious behaviour through the Facebook wall. *arXiv preprint arXiv:1910.14417*.
5.Mukhopadhyay, A., Venkatagiri, S., & Luther, K. (2024). OSINT Research Studios: A Flexible Crowdsourcing Framework to Scale Up Open Source Intelligence Investigations. Proceedings of the ACM on Human-Computer Interaction, 8(CSCW1), 1-38.
6.T. Sušánka, J. Kokeš. Security Analysis of the Telegram IM. In Proceedings of the 1st Reversing and Offensive-oriented Trends Symposium (ROOTS). Association for Computing Machinery, New York, NY, USA. 2017. pp. 1–8.
7.Derkach M., Mishko O. Using AES-256-CBC encryption algorithm to store autonomous assistant authentication data. Scientific news of Dahl university. Electronic edition. №24. 2023.

© Деркач М. В., Кондратенко Р. А., Барбарук В. М.