ЗАХИСТ НЕСТРУКТУРОВАНОЇ ІНФОРМАЦІЇ НА МОБІЛЬНОМУ ПРИСТРОЇ

Євген Бровченко
Відкритий міжнародний університет розвитку людини «Україна», Київ

PROTECTION OF UNSTRUCTURED INFORMATION ON MOBILE

Abstract. It is difficult to imagine a modern person without a mobile phone or tablet, which has almost continuous and unlimited access to the Internet or the worldwide global network. The nature and importance of this information may vary, but protection is a priority. The future of protecting unstructured information on mobile devices will be based on a combination of technological innovations and increased user awareness of cybersecurity issues. Some areas of development include the use of artificial intelligence and machine learning; biometric authentication, improvements in biometric authentication technologies, such as facial recognition, fingerprints, can provide more reliable protection of unstructured information; application of blockchain technologies; development of quantum-resistant encryption algorithms; privacy by design; user education and awareness; development of the legislation and regulatory framework, improvement of the legislation and regulatory framework in the field of cyber security will contribute to the creation of a reliable environment for the protection of unstructured information. Securing unstructured information on mobile devices will rely on a combination of technological advances, user education, and collaboration between various parties such as developers, service providers, and lawmakers.

Інформаційні технології (ІТ) та обчислювальні системи з кожним днем все більше стають невід'ємною частиною життя сучасної людини, незамінними помічниками. Розвиток ІТ відбувається зі швидкістю блискавки та має великий вплив на наше суспільство, кожний день ми маємо можливість спостерігати нові технічні та інженерні виноходи. Причому це може бути як певна інтеграція у робочий процес – автоматизація повсякденної рутини, так і частина дозвілля – спілкування та розваги, тощо. Весь комплекс технологій та систем поліпшують та спрошують виконання повсякденних задач, відкривають нові можливості та прибирають кордони. Важко уявити собі сучасну людину без мобільно телефону чи планшету, що має майже безперервний та безлімітний доступом до Інтернету чи всесвітньо глобальної мережі. Сьогодні мобільний пристрій має певний сакральний сенс, він може містити багато різноманітної інформації чи даних. Природа та важливість цієї інформації може бути різною, але захист має пріоритетне значення. А

враховуючи динаміку розвиту та невизначеність деяких процесів, перед інженерами та розробниками стоїть важке та важливе завдавання по захисту інформаційних систем та забезпеченню надійної роботи. До певної мірі мобільний пристрій можна вважати найбільш проблематичною складовою. Цей пристрій має ряд переваг та особливостей – власне це й роблять його уразливим перед потенційними зловмисниками та й дії користувача можуть спричинити ряд проблем. Доповідь присвячена проблематиці використання мобільних пристроїв та захисту неструктурованої інформації. Захист неструктурованої інформації на мобільному пристрої є важливим завданням з точки зору кібербезпеки. Неструктурована інформація може бути у вигляді текстових документів, електронних листів, фотографій, відео, записів голосу та іншого контенту, який зберігається на мобільних пристроях. До основних проблем можна віднести: втрата або крадіжка мобільного пристрою; вразливості операційної системи та програмного забезпечення; недостатній рівень шифрування та недостатній рівень складності паролів; нехтування кібергігієною. Існуючи інженерно-архітектурні рішення не завжди виконують поставлену задачу та можуть мати проблеми з інтеграцією. Не слід забувати й про економічну складову. Аналіз прикладної області та результати дослідження говорять про те що захист інформації в цілому є важливим та є попит на швидкі та ефективні рішення щодо безпеки інформаційних систем в цілому та мобільного пристрою зокрема. Лише комплексний підхід може забезпечити ефективне рішення.

Неструктурована інформація - це дані, які не мають чіткої структури або не відповідають певному формату, що ускладнює їх обробку та аналіз. Вона може включати текстові документи, електронні листи, аудіо- та відеофайли, зображення, веб-сторінки, соціальні мережі та інші форми даних. У порівнянні зі структурованою інформацією, яка зазвичай зберігається у реляційних базах даних або таблицях, неструктуровані дані не підпорядковуються певному схемі або моделі. Однак важливим аспектом є захист неструктурованої інформації, оскільки ці дані можуть містити конфіденційну або чутливу інформацію, яка повинна залишатися в безпеці. Зокрема, на мобільних пристроях неструктурована інформація може бути особливо вразливою до крадіжки та злому через відносно низький рівень безпеки цих пристроїв порівняно зі стаціонарними комп'ютерами. Тому розробка та впровадження ефективних методів захисту є дуже важливою.

До основних загроз можна віднести: втрата пристрою, злом акаунтів, шкідливе програмне забезпечення, небезпечні мережі Wi-Fi, фізичний доступ, віддалений доступ, сумнівні хмарні сервіси.

Методи захисту: шифрування даних, автентифікація користувачів, резервне копіювання і відновлення даних, оновлення програмного забезпечення, встановлення антивірусного ПЗ, блокування небезпечних додатків, використання захищених мереж, управління доступом до додатків, застосування політик безпеки, віддалення управлянні даними. Також є важливим використовувати програмні рішення для захисту неструктурованої інформації: антивіруси, файрволи, програми для шифрування та управління паролями. До можливих прикладів можна віднести наступне: шифрування даних: програми для шифрування даних, такі як VeraCrypt, AxCrypt, або BitLocker, дозволяють шифрувати файли та теки на пристрої, забезпечуючи захист інформації від несанкціонованого доступу; віртуальні приватні мережі (VPN): використання VPN-служб, таких як ExpressVPN, NordVPN або CyberGhost, дозволяє забезпечити анонімність онлайн-активності, шифрувати передачу даних та обмежити доступ до чутливої інформації; захист від вірусів та шкідливого ПЗ: антивірусні програми, такі як Norton або McAfee, забезпечують захист від вірусів, троянських коней, шпигунського та шкідливого програмного забезпечення; менеджери паролів: менеджери паролів, такі як LastPass, Dashlane або 1Password, допомагають зберігати та генерувати складні паролі, забезпечуючи захист різних аккаунтів користувача; резервне копіювання даних: рішення для резервного копіювання даних, такі як Acronis, Veeam або Carbonite, дозволяють створювати резервні копії важливої інформації, забезпечуючи відновлення даних в разі втрати або пошкодження; управління доступом та співпраця: рішення для управління доступом та співпраці, такі як Microsoft Azure Information Protection, Box або Google Workspace, дозволяють контролювати доступ до чутливої інформації, налаштовувати дозволи та співпрацювати над документами в безпечному середовищі . Ці програмні рішення допомагають забезпечити захист неструктурованої інформації на мобільних пристроях та комп'ютерах, а також допомагають користувачам контролювати доступ до своїх даних. Вибір відповідного рішення для захисту інформації залежить від конкретних потреб користувача та його середовища роботи.

Не слід забувати про роль користувача: розуміння важливості захисту даних, використання сильних паролів, регулярне оновлення ПЗ а головне освіта з питань безпеки.

Майбутнє захисту неструктурованої інформації на мобільних пристроях буде засноване на поєднанні технологічних нововведень та підвищенні обізнаності користувачів з питань кібербезпеки. Деякі напрямки розвитку включають: Застосування штучного інтелекту (AI) та машинного навчання: AI може допомогти в розробці розширених

механізмів захисту, що автоматично виявляють аномальні або підозрілі дії та блокують потенційні загрози. Біометрична автентифікація: покращення технологій біометричної автентифікації, таких як розпізнавання обличчя, відбитків пальців, можуть забезпечити більш надійний захист неструктурованої інформації. Застосування блокчейн-технологій: блокчейн може відігравати важливу роль у забезпеченні безпеки інформації, оскільки він дозволяє зберігати дані розподіллено та захищено від змін. Розвиток квантово-стійких алгоритмів шифрування: з розвитком квантових комп'ютерів створюється потреба в нових алгоритмах шифрування, які можуть витримати потужність квантового злому. Приватність за замовчуванням (Privacy by Design): проектування мобільних пристроїв та застосунків з врахуванням приватності користувачів сприятиме захисту неструктурованої інформації на мобільних пристроях. Освіта та обізнаність: підвищення обізнаності користувачів щодо кібербезпеки та навчання їх ефективним методам захисту інформації на мобільних пристроях допоможе зменшити ризик виникнення інцидентів, пов'язаних з безпекою. Розвиток законодавства та нормативної бази: вдосконалення законодавства та нормативної бази у галузі кібербезпеки сприятиме створенню надійного середовища для захисту неструктурованої інформації. Захист неструктурованої інформації на мобільних пристроях базується на комбінації технологічного прогресу, навчання користувачів та співпраці між різними сторонами, такими як розробники, постачальники послуг та законодавці. Забезпечення безпеки та приватності даних в цифровому світі залишається пріоритетом, оскільки кількість мобільних пристроїв та їх використання продовжують зростати. Сучасній користувач мобільних пристроїв має певні вимоги що спарюються на ергономіку та рівень інформаційної обізнаності. Розвиток галузі в цілому вимагає швидких, надійних та ефективних рішень що потрапляють не лише в економічну площину а й площину кібербезпеки. Використання мобільних пристроїв може адаптуватися до швидких сучасних потреб безпеки організації та може бути легко налаштований відповідно до конкретних вимог. Мобільний пристрій є зручним і доступним для багатьох користувачів, він зазвичай знаходиться поруч з користувачем і може використовуватися як додатковий елемент безпеки.

Література

1.Бровченко, Є. М., Самарай, В. П., Даценко, І. П., Павленко, В. І. (2023). Мобільний пристрій як частина адаптивної кейс-менеджмент системи. Інфокомунікаційні та комп’ютерні технології, 2(04), 157-163.

https://doi.org/10.36994/2788-5518-2022-02-04-18 (дата звернення: 25.05.2023)

2.Gámez, N., García-Sánchez, P., & Pérez, J. (2020). User authentication using mobile devices: A review. Information Fusion, 55, 153-170.

3.Kang, Y., Zhang, N., Zhu, X., & Huang, Y. (2021). A novel authentication mechanism based on dynamic cognitive keystroke on mobile devices. IEEE Access, 9, 32098-32107.

4.Yavuz, A. G., Akgu ̈n, M. A mobile-based multi-factor authentication system using biometric and location information. International Journal of Computer Science and Network Security, 17(5), 181-187, (2017).