

УДК 004.056.5: 004.056.2

ЗАХИСТ НЕСТРУКТУРОВАНОЇ ІНФОРМАЦІЇ НА МОБІЛЬНОМУ ПРИСТРОЮ

DOI 10.36994 / 2788-5518-2023-01-05-21

Бровченко Є. М., Відкритий міжнародний університет розвитку людини «Україна», Інститут комп'ютерних технологій, Київ, Україна. <https://orcid.org/0000-0002-1416-0385>, yebrovchenko@hotmail.com

Самарай В. П., к.т.н., проф., Відкритий міжнародний університет розвитку людини «Україна», Інститут комп'ютерних технологій, Київ, Україна. <https://orcid.org/0000-0003-4419-1366>, samaraj@ukr.net

Даценко І. П., к.т.н., доц., Відкритий міжнародний університет розвитку людини «Україна», Інститут комп'ютерних технологій, Київ, Україна. <https://orcid.org/0000-0002-0047-413X>, docik_ivan@ukr.net

Павленко В. І., к.ф.-м.н., доц., Відкритий міжнародний університет розвитку людини «Україна», Інститут комп'ютерних технологій, Київ, Україна. <https://orcid.org/0000-0002-3958-0415>, pavlenko.v@i.ua

Серєда А.В., Відкритий міжнародний університет розвитку людини «Україна», Інститут комп'ютерних технологій, Київ, Україна. <https://orcid.org/0000-0002-4779-5475>, andrew.sereda@gmail.com

Анотація: У статті розглянуто проблеми використання мобільного пристрою в умовах активного використання та захист неструктурованої інформації. Основна увага приділена використанню мобільного пристрою як частини інформаційної системи та можливі заходи щодо захисту. Розвиток та динаміка використання сучасних інформаційних технологій у багатьох сферах життя вимагає від інженерів та розробників нових рішень, необхідно закласти міцний фундамент для подальшого розвитку та можливість ефективного удосконалення чи підтримки. Мобільний пристрій займає своє важливе місце у житті сучасної людини. Тому треба розглядати мобільний пристрій як не від'ємну складову сучасних інформаційних систем. Була проведена робота по вивченню проблеми в реальних умовах використання та взаємодії. Треба зазначити що питання безпеки є комплексним: починаючи від етапу створення та контроль на етапі експлуатації, також дуже важливим є інформаційна обізнаність та відповідальність кінцевого користувача. Кібербезпека виходить на принципово новий рівень. Існують певні готові інженерно-архітектурні рішення що допомагають інтегрувати мобільний пристрій в інформаційну систему, але ці рішення інколи не виконують поставлений завдань. Аналіз прикладної області та результати дослідження говорять про те що захист інформації в цілому є важливим та є попит на ефективні рішення. Не слід забувати також про економічну складову. Вироблено ряд рекомендацій щодо можливих заходів по безпеці.

Ключові слова: мобільний пристрій, захист інформації, неструктурована інформація, кібербезпека

PROTECTION OF UNSTRUCTURED INFORMATION ON A MOBILE DEVICE

Evgen Brovchenko, Open International University of Human Development "Ukraine", Kyiv, Ukraine. <https://orcid.org/0000-0002-1416-0385>, yebrovchenko@hotmail.com

Valery Samarai, Ph.D., Ass. Prof., Open International University of Human Development "Ukraine", Kyiv, Ukraine. <https://orcid.org/0000-0003-4419-1366>, samaraj@ukr.net

Ivan Datsenko, Ph.D., Open University of Human Development "Ukraine", Kyiv, Ukraine. <https://orcid.org/0000-0002-0047-413X>, docik_ivan@ukr.net

Volodymyr Pavlenko, Ph.D., Ass. Prof., Open University of Human Development "Ukraine", Kyiv, Ukraine. <https://orcid.org/0000-0002-3958-0415>, pavlenko.v@i.ua

Andrew Sereda, Open University of Human Development "Ukraine", Kyiv, Ukraine. <https://orcid.org/0000-0002-4779-5475>, andrew.sereda@gmail.com

Annotation: Information technology (IT) and computer systems are becoming an integral part of modern man's life, irreplaceable assistants. The development of IT happens at lightning speed and has a great impact on our society, every day we could observe new technical and engineering inventions. Moreover, it can be both a certain integration into the work process - automation of the daily routine, and part of leisure - communication and entertainment, etc. The entire complex of technologies and systems improve and facilitate the performance of everyday tasks, open new opportunities and remove borders. 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. Today, a mobile device has a certain sacred meaning, it can contain a lot of different information or data. The nature and importance of this information may vary, but protection is a priority. And considering the developed dynamics and the uncertainty of some processes, engineers and developers face a difficult and important task to protect information systems and ensure reliable operation. To some extent, the mobile device can be considered the most problematic component. This device has a few advantages and features - this is exactly what makes it vulnerable to potential attackers and user actions can cause a few problems. This article is devoted to the problems of using mobile devices and protecting unstructured information. Protecting unstructured information on a mobile device is an important task from a cybersecurity perspective. Unstructured information can be in the form of text documents, emails, photos, videos, voice recordings, and other content stored on mobile devices. The main problems include loss or theft of a mobile device; operating system and software vulnerabilities; insufficient level of encryption and insufficient level of complexity of passwords; neglect of cyber hygiene. Existing engineering and architectural solutions do not always fulfill the task and may have problems with integration. Do not forget about the economic component. The analysis of the application area and the research results indicate that information protection in general is important and there is a demand for quick and effective solutions regarding the security of information systems in general and mobile devices. Only an integrated approach can provide an effective solution.

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 (AI) and machine learning: AI can help develop advanced defense mechanisms that automatically detect anomalous or suspicious activity and block potential threats; biometric authentication, improvements in biometric authentication technologies, such as facial recognition, fingerprints, can provide more reliable protection of unstructured information; application of blockchain technologies: blockchain can play an important role in ensuring information security, as it allows data to be stored distributed and protected from changes; development of quantum-resistant encryption algorithms: with the development of quantum computers, there is a need for new encryption algorithms that can withstand the power of quantum hacking; privacy by design (Privacy by Design): designing mobile devices and applications with user privacy in mind will help protect unstructured information on mobile devices; user education and awareness: increasing users' awareness of cyber security and teaching them effective methods of protecting information on mobile devices will help reduce the risk of security incidents; 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. Ensuring data security and privacy in the digital world remains a priority as the number of mobile devices and their use continues to grow.

The modern user of mobile devices has certain requirements related to ergonomics and the level of information awareness. The development of the industry requires fast, reliable, and effective solutions that fall not only in the economic plane, but also in the plane of cyber security. The use of mobile devices can adapt to the fast-paced modern security needs of an organization and can be easily configured to meet specific requirements. A mobile device is convenient and affordable for many users, it is usually close to the user and can be used as an additional security element.

Key words: *mobile device, information protection, unstructured information, cyber security*

Вступ

Інформаційні технології (ІТ) та обчислювальні системи стали невід'ємною частиною життя сучасної людини, незамінними помічниками. Розвиток ІТ відбувається так швидко, що майже кожен день ми маємо можливість спостерігати нові технічні та інженерні винаходи. 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 спрощують виконання повсякденних задач, відкривають нові можливості та прибирають кордони. Важко уявити собі сучасну людину без мобільного телефону чи планшета, що має майже безперервний та безлімітний доступ 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 розвитку та невизначеність деяких процесів, перед інженерами та розробниками стоїть важке та важливе завдання по захисту інформаційних систем та забезпеченню надійної роботи. До певної міри 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. Данна стаття 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. Існуючі 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.

Виконання досліджень

Як відомо обчислювальна система - це сукупність апаратних і програмних компонентів, які взаємодіють для вирішення обчислювальних завдань. Обчислювальні системи можуть включати різноманітні пристрої, такі як комп'ютери, мобільні телефони, планшети, сервери, ноутбуки, суперкомп'ютери. Слід розуміти що перелік цих складових може змінюватись, причому деякі пристрої можуть зникати, а про деякі ми сьогодні навіть і не здогадуємось. Система складається з апаратного та програмного забезпечення. Апаратна частина - це фізичні компоненти комп'ютерної системи, які виконують обчислювальні операції, операції по збереженню та керуванню. Програмне забезпечення - це набір програм, що контролюють та керують роботою апаратної частини комп'ютера. Воно може включати в себе операційні системи, драйвери пристроїв, програми-редактори, веб-браузери, мультимедійні прошивки та інші програми. Обчислювальні системи можуть бути використані для різноманітних завдань, таких як обробка даних, створення документів, візуалізація інформації, аналіз даних, ігри та інше. Вони можуть бути використані в різних галузях, таких як наука, бізнес, медицина, техніка, транспорт, тощо. Рівень інтеграції обчислювальних систем у повсякденне життя з часом буде лише збільшуватись та набувати нових рис.

Отже що таке мобільний пристрій? Мобільний пристрій - це портативний електронний пристрій, який має можливість підключення до мережі зв'язку та доступу до різноманітних сервісів та додатків. У сучасному світі мобільні пристрої стали невід'ємною частиною життя людей, і це змінило спосіб, яким ми спілкуємося, взаємодіємо, працюємо та розважаємося. Однією з основних функцій мобільного пристрою є забезпечення зв'язку, що дозволяє користувачам здійснювати дзвінки та відеодзвінки, надсилати та отримувати повідомлення, електронну пошту та інші форми комунікації. Мобільні пристрої також забезпечують доступ до Інтернету, що дає користувачам можливість шукати інформацію, переглядати відео, грати в ігри, слухати музику та виконувати інші дії. Мобільні пристрої також стали необхідним інструментом для роботи та навчання, дозволяючи користувачам працювати з електронною поштою, текстовими документами, електронними таблицями та іншими програмами. Вони можуть бути використані для спостереження за здоров'ям та фітнесом, ведення щоденника, планування та організації розкладу та інших аспектів життя. Однією з основних переваг мобільних пристроїв є їх портативність та доступність, що дозволяє людям бути зв'язаними та отримувати інформацію в будь-якому місці та в будь-який час. У цілому, мобільні пристрої стали невід'ємною частиною життя сучасної людини, і вони продовжують еволюціонувати та вдосконалюватися. Завдяки їхній функціональності та зручності використання, мобільні пристрої дозволяють людям бути більш продуктивними та організованими в їхньому житті та роботі.

Можна відділити такі основні типи мобільних пристроїв:

- Смартфоне - найпоширенішим типом мобільних пристроїв. Вони поєднують в собі функціональність мобільного телефону і комп'ютера, забезпечуючи широкий спектр можливостей, таких як здійснення дзвінків, відправлення повідомлень, серфінг в Інтернеті, встановлення додатків тощо.

- Планшет - це портативні пристрої з екраном сенсорного керування, більшими, ніж у смартфонів, зазвичай від 7 до 12 дюймів. Вони надають можливість виконувати багато завдань, подібних до комп'ютера, таких як перегляд веб-сторінок, перегляд відео, читання електронних книг, встановлення додатків і т. д.

▪ Ноутбук – персональний комп'ютер зі складним корпусом, що містить клавіатуру та дисплей. Вони надають широкі можливості, які забезпечують роботу з текстом, виконання завдань, перегляд мультимедійного контенту, доступ до Інтернету.

▪ Ультрабук - це тонкий, легкий і потужний ноутбук з довгим часом автономної роботи. Вони надають високу продуктивність і можливості, подібні до ноутбуків, але з меншими розмірами та вагою.

▪ Пристрій що носить (wearables) – різноманітні гаджети, які можуть бути одягнуті на тіло, наприклад, смарт-годинники, фітнес-браслет.

Існують основні операційні системи: Android, iOS, Windows/Mobile, BlackBerry, KaiOS. Різноманіття мобільних пристроїв з одного боку дає можливість обрати саме те що треба користувачу, з іншого боку ускладнює роботу проєктувальників та розробників.

Особливу увагу слід приділити Android Enterprise. Отже Android Enterprise (раніше відомий як Android for Work) - це програма та набір функцій, розроблених компанією Google для підприємств, які використовують мобільні пристрої на базі операційної системи Android. Android Enterprise надає розширені можливості керування і захисту даних, що дозволяє організаціям легко і безпечно інтегрувати та керувати пристроями Android в корпоративному середовищі.

Деякі ключові функції та можливості Android Enterprise включають:

1. Робочі профілі: дозволяє розділити особисті дані і програми від корпоративних на пристрої з Android. Це дозволяє зберігати особисті дані окремо від корпоративних даних і додатків.

2. Управління пристроями: забезпечує централізоване управління пристроями, що дозволяє адміністраторам віддалено керувати налаштуваннями, політиками безпеки, встановлювати додатки та проводити оновлення.

3. Політики безпеки: дозволяє встановлювати політики безпеки на пристроях, такі як вимоги до паролів, шифрування даних, обмеження функцій пристрою та інші заходи безпеки.

4. Магазин додатків для підприємств: надає можливість створювати власний магазин додатків для підприємств, де адміністратори можуть контролювати доступні додатки та встановлювати їх на пристрої.

5. Інтеграція з обліковими записами Google Workspace: компанії, які використовують Google Workspace (раніше G Suite), можуть легко інтегрувати свої корпоративні облікові записи з Android Enterprise і керувати доступом до облікових записів та сервісів.

6. Захист даних: можна використовувати різні методи захисту даних, такі як шифрування пристроїв, вимоги до паролів, обмеження прав доступу та інші політики безпеки, щоб забезпечити конфіденційність і цілісність даних.

7. Інтеграція з іншими системами: може інтегруватися з різними корпоративними системами, такими як системи керування ідентифікацією (IAM), системи електронної пошти та календаря, хмарні сервіси для зберігання даних та багато іншого.

8. Завдання та автоматизація: створювання різних завдань та автоматизування процесів на пристроях, що дозволяє підвищити продуктивність та ефективність користувачів.

Неструктурована інформація - це інформація, яка не зберігається у структурованому форматі бази даних або в іншому структурованому форматі. Наприклад, це можуть бути тексти, документи, електронні листи, фотографії, відео та інші файли, які зберігаються на різних пристроях, таких як комп'ютери, мобільні телефони, планшети та інші пристрої з можливістю зберігання даних. Неструктурована інформація зазвичай не має чіткої структури, тому вона може бути складнішою для організації та обробки, порівняно з інформацією, яка зберігається у структурованих форматах. Проте, неструктурована інформація містить в собі багато важливих даних, таких як особисті інформаційні дані, комерційні та бізнес-документи, що можуть мати значення для користувачів та організацій, тому захист неструктурованої інформації є дуже важливою та пріоритетною задачею.

Характеристики неструктурованої інформації:

▪ Текстовий контент: мобільний пристрій містить значну кількість текстової інформації, яка може бути неструктурованою. Це можуть бути нотатки, записи, електронні книги, блоги, коментарі, соціальні медіа, статті та інше. Цей текст може бути у різних форматах, включаючи неперервний потік тексту, списки, маркери, таблиці або навіть скановані документи.

▪ Мультимедійний контент: мобільний пристрій дозволяють зберігати і отримувати доступ до різноманітного мультимедійного контенту, який також може бути неструктурованим. Це

включає фотографії, відео, аудіозаписи, графіку, анімацію та інші типи медіа. Цей контент може бути в неструктурованій формі без додаткової метаданих або організації.

- Соціальні медіа та комунікація: мобільний пристрій широко використовуються для соціальних мереж, месенджерів та інших комунікаційних платформ. Інформація, що обмінюється через ці канали, може бути неструктурованою, включаючи повідомлення, коментарі, пости, фотографії, відео та інші медіа.

- Веб-сторінки та блоги: мобільний пристрій дозволяють переглядати веб-сторінки та блоги. Ця інформація також може бути неструктурованою, залежно від оформлення сторінки, наявності текстових блоків, заголовків, списків, посилань тощо.

- Документи і файлова система: мобільний пристрій можуть містити різні документи у форматах, таких як PDF.

Неструктурована інформація на мобільних пристроях є широко поширеним явищем і включає текстовий контент, мультимедійний контент, соціальні медіа, веб-сторінки та блоги, а також документи і файлову систему. Ця інформація може бути в різних форматах і організаціях, що може створювати виклики в управлінні, пошуку та використанні її. Управління неструктурованою інформацією на мобільних пристроях є важливим завданням. Користувачі повинні мати ефективні інструменти для організації, пошуку і доступу до цієї інформації. Технології обробки мови, комп'ютерного зору, машинного навчання та інші інновації в галузі штучного інтелекту можуть впроваджуватися для автоматизації розпізнавання та організації неструктурованої інформації. Досягнення в області розпізнавання тексту, обробки мови та аналізу великих обсягів даних роблять неструктуровану інформацію більш доступною та корисною для користувачів мобільних пристроїв. Продовжується розвиток інструментів та технологій, що допомагають в організації і використанні цієї інформації на мобільних пристроях. Загалом, неструктурована інформація на мобільних пристроях є важливим аспектом сучасного інформаційного оточення. Розвиток і використання інструментів для управління цією інформацією відкриває нові можливості для користувачів, забезпечуючи зручний доступ до ресурсів.

Для захисту мобільно пристрою в цілому та інформації що зберігається на ньому зокрема досить ефективною є використання біометричної ідентифікації. Біометрія - це використання фізичних або поведінкових характеристик людини для ідентифікації, аутентифікації та авторизації. На сучасних мобільних пристроях все більше використовуються біометричні методи для захисту неструктурованої інформації, що зберігається на них. Використання біометрії дозволяє підвищити безпеку і зручність доступу до цієї інформації.

Технології біометричної ідентифікації на мобільних пристроях:

- Сканування відбитків пальців: сканер вбудований в сенсорний екран або на задній панелі пристрою. Відбиток пальця порівнюється з збереженими біометричними даними, що дозволяє впізнати користувача.

- Розпізнавання обличчя: камера пристрою використовується для захоплення обличчя користувача, яке порівнюється з попередньо збереженими біометричними даними.

- Розпізнавання відбитків очей: сітківка може бути використані для ідентифікації користувача. Спеціальні камери або сенсори захоплюють деталі очей і порівнюють їх з шаблонами біометричних даних.

- Розпізнавання голосу: вбудований мікрофон записує голос користувача, який порівнюється з попередньо збереженими голосовими шаблонами.

Переваги використання біометрії на мобільних пристроях:

- Вищий рівень безпеки. Біометричні дані є унікальними для кожної особи і майже неможливо підробити або підміняти. Це дозволяє забезпечити високий рівень ідентифікації та аутентифікації користувача.

- Зручність використання. Використання біометрії на мобільних пристроях забезпечує зручний та швидкий доступ до інформації.

- Ізольованість зберігання. Біометричні дані зазвичай зберігаються в зашифрованому вигляді на самому пристрої. Це зменшує ризик їх витоку або несанкціонованого доступу до них.

- Можливості багатофакторної аутентифікації. Біометричні методи можуть бути поєднані з іншими методами аутентифікації, такими як пін-коди або паролі, для створення більш надійного і багатоетапного процесу ідентифікації.

- **Необхідність фізичного присутності.** Використання біометрії вимагає фізичної присутності особи для ідентифікації. Це ускладнює можливість несанкціонованого доступу до пристрою або даних.

Наступним кроком можна вважати захист інформації на рівні операційної системи чи мобільно додатку. MAM (Mobile Application Management) є скороченням від англійського терміну "Mobile Application Management". Він відноситься до підходу до управління мобільними додатками в організації. MAM використовується для керування та контролю мобільними додатками, які встановлюються на пристрої користувача. Це може бути застосунок для внутрішнього використання в організації або публічний додаток, який користувачі завантажують з магазинів додатків. Основна мета MAM полягає в управлінні додатками на рівні самого додатку, незалежно від пристрою. Вона надає можливості забезпечити безпеку, контроль та конфігурацію додатків, а також здійснювати моніторинг, оновлення та віддалене управління додатками на мобільних пристроях. Деякі можливості MAM можуть включати: можливість встановлення та виконання політик, що стосуються використання додатків, таких як обмеження функцій або доступу до даних; здатність забезпечувати безпеку додатків шляхом використання шифрування, контролю доступу та ідентифікації користувачів; можливість розповсюдження додатків на пристрої користувачів через магазини додатків або корпоративні канали, а також віддалене оновлення додатків; здатність збирати дані про використання додатків, продуктивність та поведінку користувачів для аналізу та прийняття відповідних рішень. MDM (Mobile Device Management) є скороченням від англійського терміну "Mobile Device Management". Це підходу до управління мобільними пристроями в організації. MDM використовується для централізованого керування, контролю та захисту мобільних пристроїв, таких як смартфони та планшети, що використовуються в організації. Він надає можливості забезпечення безпеки, налаштування, моніторингу та віддаленого управління мобільними пристроями з одного централізованого інтерфейсу. Основна мета MDM полягає в забезпеченні безпеки, конфігурації та керування мобільними пристроями в організації. Деякі можливості MDM включають: можливість реєстрації мобільних пристроїв в системі MDM та їх прив'язка до конкретних користувачів або груп; здатність встановлення та забезпечення політики безпеки на мобільних пристроях, включаючи налаштування паролів, шифрування даних, віддалене видалення даних тощо; можливість віддалено налаштовувати пристрої та встановлювати додатки, контролювати доступ до магазинів додатків та обмежувати встановлення небезпечних або небажаних додатків; здатність збирати дані про стан та використання мобільних пристроїв, включаючи інформацію про батарею, сигнал мережі, використання пам'яті.

Не слід забувати й про користувача інформаційних систем. Користувач подекуди може бути найслабкішим та вразливішим елементом. Обізнаність користувача щодо безпеки при користуванні мобільним пристроєм є важливим аспектом для забезпечення захисту особистих даних і запобігання кіберзлочинності. Всі ці моменти слід забезпечувати, контролювати та поліпшувати. Можна виділити основні аспекти: захист паролів: користувачі повинні встановлювати міцні паролі або використовувати біометричні методи аутентифікації для захисту своїх пристроїв; важливо використовувати унікальні та складні паролі і не ділитися ними з іншими особами; оновлення програмного забезпечення регулярно, оновлення операційної системи та програмного забезпечення на пристрої є важливим, оскільки виробники випускають оновлення та виправлення для заповнення потенційних слабких місць; встановлення довірених додатків, користувачі повинні завантажувати додатки тільки з офіційних магазинів додатків, таких як Google Play або App Store, і перевіряти рейтинги та відгуки інших користувачів перед встановленням; уважність при відкритті посилань та відправці особистої інформації, користувачі повинні бути обережними при натисканні на посилання в недовіреному повідомленні або електронній пошті та уникати надсилання особистих чутливих даних через ненадійні канали комунікації; використання антивірусного програмного забезпечення, встановлення добре відомого антивірусного програмного забезпечення на мобільний пристрій може допомогти виявити і запобігти інфікуванню шкідливим програмним забезпеченням.

Висновок

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 розподілено 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 користувачів: 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 спиратиметься 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.

Сучасний користувач мобільних пристроїв має певні вимоги що стосуються 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), С. 157–163. <https://doi.org/10.36994/2788-5518-2022-02-04-18>.
2. Choi, J. S., & Kim, H. S. (2019). An Efficient Encryption Method for Securing Unstructured Data on Mobile Devices. IEEE Access, 7, 124616-124626.
3. Krcmar, Helmut, ed. Mobile Computing: Concepts, Methodologies, Tools, and Applications. IGI Global, 2018.
4. Liu, Z., Huang, L., Gao, Y., Wang, Z., & Yang, X. (2017). Research on cloud computing security and privacy protection model. Cluster Computing, 20(3), 1893-1901.
5. Madden J., Madden B. Enterprise Mobility Management: Everything you need to know about MDM, MAM, and BYOD. – Jack Madden, 2013. 176 p.
6. Sarker, S., & Chatterjee, S. (2018). Big data analytics: A literature review paper. Journal of Business Research, 93, 240-253.
7. Yang, Y., Luo, X., & Wu, J. (2019). Protecting Sensitive Data in Mobile Devices with Security-Enhanced Linux and Encryption Technologies. Mobile Networks and Applications, 24(5), 1648-1660.
8. The official Android Enterprise website: <https://www.android.com/enterprise/>

References

1. Evgen Brovchenko, Valery Samarai, Ivan Datsenko, Volodymyr Pavlenko. (2023). MOBILE DEVICE AS PART OF AN ADAPTIVE CASE MANAGEMENT SYSTEM. INFOCOMMUNICATION AND COMPUTER TECHNOLOGIES, 2(04), P. 157–163. <https://doi.org/10.36994/2788-5518-2022-02-04-18>. [in Ukrainian]
2. Choi, J. S., & Kim, H. S. (2019). An Efficient Encryption Method for Securing Unstructured Data on Mobile Devices. IEEE Access, 7, 124616-124626.
3. Krcmar, Helmut, ed. Mobile Computing: Concepts, Methodologies, Tools, and Applications. IGI Global, 2018.
4. Liu, Z., Huang, L., Gao, Y., Wang, Z., & Yang, X. (2017). Research on cloud computing security and privacy protection model. Cluster Computing, 20(3), 1893-1901.
5. Madden J., Madden B. Enterprise Mobility Management: Everything you need to know about MDM, MAM, and BYOD. – Jack Madden, 2013. 176 p.
6. Sarker, S., & Chatterjee, S. (2018). Big data analytics: A literature review paper. Journal of Business Research, 93, 240-253.
7. Yang, Y., Luo, X., & Wu, J. (2019). Protecting Sensitive Data in Mobile Devices with Security-Enhanced Linux and Encryption Technologies. Mobile Networks and Applications, 24(5), 1648-1660.
8. The official Android Enterprise website: <https://www.android.com/enterprise/>