УДК 004.63
Лупенко А. М., д.т.н., Гарасівка А. В.
Тернопільський національний технічний університет імені Івана Пулюя, Україна

РОЛЬ ТА ПЕРЕВАГИ РЕЗЕРВНОГО КОПІЮВАННЯ ДАНИХ МОБІЛЬНИХ ПРИСТРОЇВ У СУЧАСНОМУ ЦИФРОВОМУ СВІТІ

Lupenko A. M., D.E.Sc., Harasivka A. V.

ROLE AND BENEFITS OF MOBILE DATA BACKUP IN TODAY'S DIGITAL WORLD

У епоху безперервних технологічних інновацій та зростаючої залежності від мобільних пристроїв, резервне копіювання та шифрування даних стає критично важливою складовою для забезпечення безпеки та стабільності інформації. Окрім створення резервних копій важливою складовою безпеки є і шифрування. Шифрування даних на мобільних пристроях є ефективним заходом безпеки, що допомагає захистити особисті, корпоративні та конфіденційні дані від різних загроз інформаційної безпеки. А від можливої втрати чи пошкодження пристрою чи його елементів завадить вчасне та ефективне резервне копіювання даних.

Користувачі Android можуть використовувати Google Drive для автоматичного резервного копіювання своїх даних, таких як фотографії, відео, контакти та додатки. Користувачі пристроїв Samsung можуть використовувати службу Samsung Cloud для резервного копіювання даних, включаючи налаштування пристрою, додатки та дані контактів. Це забезпечує синхронізацію між пристроями Samsung.

Користувачі iOS можуть використовувати iCloud для автоматичного резервного копіювання фотографій, відео, повідомлень, додатків та інших даних. iCloud дозволяє зручно відновлювати дані на нових пристроях чи в разі втрати чи поломки. iTunes дозволяє власникам ПК з ОС macOS створювати резервні копії своїх iOS-пристроїв на комп'ютері. Це може бути корисним для тих, хто віддає перевагу зберіганню резервних копій на локальних пристроях.

Резервне копіювання мобільних пристроїв має численні переваги, які важливі для забезпечення безпеки та надійності даних. Ось деякі з ключових переваг:

- Відновлення даних після втрати чи поломки пристрою
- Захист від випадкового видалення
- Спрощення переходу на інший пристрій
- Захист від втрати даних при оновленнях системи або програм
- Захист від мережевих атак або вірусів
- Синхронізація даних між пристроями (мобільні телефони, настільні комп’ютери, сервери, хмара, тощо).

Шифрування даних на мобільних пристроях є необхідним заходом безпеки з ряду причин:

Захист від втрати або крадіжки пристрою - шифрування даних гарантує, що навіть у випадку фізичного доступу до пристрою, конфіденційна інформація (контакти, повідомлення, фотографії та інші особисті відомості) залишається недоступною для несанкціонованих осіб. В ОС Android 128 використовується Advanced Encryption Standard (AES) із з’єднанням блоків шифру (CBC) і ESSIV:SHA256. Головний ключ зашифровано за допомогою 128-бітного AES через звернення до бібліотеки OpenSSL

Дотримання нормативів та вимог безпеки - у деяких галузях, таких як охорона здоров'я чи фінанси, дотримання певних нормативів безпеки є обов'язковим. Шифрування даних на мобільних пристроях може бути вимогою для відповідності стандартам та законодавству, наприклад службові пристрої.

Захист корпоративних даних - для пристроїв компанії важливо шифрувати дані, особливо якщо вони містять конфіденційну корпоративну інформацію. Це стає ключовим елементом захисту бізнес-даних в умовах мобільності та роботи на відстані. Зазвичай адміністрування пристрою виконується віддалено, через сервіси Google / Amazon / Microsoft.

Всі сучасні операційні системи мають вбудовані механізми безпеки:

- Кожен додаток працює в власному просторі імен (sandbox), що обмежує його доступ до ресурсів інших додатків.
- Android та iOS використовує модель дозволів, яка дозволяє користувачам контролювати доступ до різних ресурсів, таких як камера, контакти, GPS тощо.
- Для захисту передачі даних між пристроями і серверами використовується шифрування SSL/TLS, забезпечуючи конфіденційність та цілісність даних.

За наявності root-прав (права супер користувача ОС Android) в користувача з'являються додаткові можливості - існує безліч сторонніх додатків, таких як Helium, Titanium Backup, і інші, які дозволяють створювати повну резервну копію, як системи так і окремих програм.

Резервне копіювання виконує ключову роль у запобіганні втраті, відновленні важливих інформаційних ресурсів. Цей процес забезпечує надійність збереження та стійкість даних, допомагає у виконанні переходу між пристроями та дотриманні вимог безпеки. Незалежно від обраного способу резервного копіювання, важливо регулярно перевіряти, чи виконується резервне копіювання, і впевнитися, що ви можете відновити свої дані в разі потреби.

Резервне копіювання є важливим елементом стратегії захисту інформації, забезпечуючи користувачам можливість ефективно управляти своїми даними в умовах постійного ризику втрати чи пошкодження інформації. За допомогою цього процесу користувачі можуть впевнено використовувати свої мобільні пристрої, знаючи, що їхні дані захищені та можуть бути відновлені в разі потреби.

Література

1. Myungseo Park, Okyeon Yi, Jongsung Kim, 2020. A methodology for the decryption of encrypted smartphone backup data on android platform: A case study on the latest samsung smartphone backup system. Vol. 35, 301026, ISSN 2666-2817, Science Direct. https://doi.org/10.1016/j.fsidi.2020.301026.
2. Lance Whitney, 2023. Save Your Stuff: How to Back Up and Restore Your Android Device. PC Mag. https://www.pcmag.com/how-to/how-to-back-up-restore-your-android-device
3. Android Open Source Project, 2023. Full-Disk Encryption., Apache 2.0. https://source.android.com/docs/security/features/encryption/full-disk
4. Shivi Garg a b, Niyati Baliyan, 2021. Comparative analysis of Android and iOS from security viewpoint. Vol. 40, 100372, ISSN 1574-0137, Science Direct. https://doi.org/10.1016/j.cosrev.2021.100372