

УДК 004.056.55

Клоков А.О.<sup>1</sup>, Зайко Т.А.<sup>2</sup>

<sup>1</sup>студ. гр. КНТ-118 НУ «Запорізька Політехніка»

<sup>2</sup>канд. техн. наук, доц. НУ «Запорізька Політехніка»

## **ПРОБЛЕМИ ТА МЕТОДИ ШИФРУВАННЯ ДІЛОВОГО ДОКУМЕНТООБІГУ**

Для кожного підприємства, без сумніву, пропорційно його розвитку збільшується обсяг документації, що використовується. Фізичне поширення, розмноження та пошук документів значно знижує швидкість та якість прийняття рішень у цілому. Через це все більше підприємств впроваджують системи електронного документообігу (СЕД). Такі системи мають забезпечувати цілісність, доступність та конфіденційність корпоративної інформації, але в силу того, що СЕД набули широкого застосування відносно недавно, їх робота недостатньо налагоджена, і незважаючи на переваги від використання таких систем, залишаються певні невирішені проблеми.

Одна з наймасштабніших проблем СЕД – захист інформації від несанкціонованого доступу. Адже є багато бажаючих перехопити конфіденційну інформацію, задля використання у своїх інтересах, або пошкодження її, для зменшення конкурентоспроможності підприємства.

Рішенням таких проблем є криптографічне шифрування. Загалом шифрування – це оборотне перетворення даних, з метою приховування інформації. Шифрування відбувається із застосуванням криптографічного ключа. Ключ – це певна кількість символів, сформованих вільним чином з символів, що доступні у системі шифрування.

Першою відомою пам'яткою шифрування прийнято вважати єгипетський текст, який було створено напевно десь в 1900 році до нашої

ери., у якому використовувались другі символи замість відомих єгипетських ієрогліфів.

До нашого часу, криптографія займалася виключно забезпеченням конфіденційності повідомлень (тобто шифруванням) – перетворенням повідомлень із зрозумілої форми в незрозумілу і зворотнє відновлення на стороні одержувача, роблячи його неможливим для прочитання для того, хто перехопив або підслухав без секретного знання (а саме ключа, необхідного для дешифровки повідомлення). В останні десятиліття сфера застосування криптографії розширилася і включає не лише таємну передачу повідомлень, але і методи перевірки цілісності повідомлень, ідентифікування відправника/одержувача (аутентифікація), цифрові підписи, інтерактивні підтвердження, та технології безпечного спілкування, тощо.

Виділяють два методи криптографічного шифрування: симетричне та асиметричне.

У симетричному шифруванні один ключ, який зберігається в секреті, служить і для шифрування, і для дешифрування. Переваги симетричних методів шифрування:

- велика пропускна здатність;
- ключі мають невеликий розмір;
- застосовуються, як основа для різних криптографічних механізмів.

Серед недоліків даного шифрування:

- необхідно використовувати значну кількість ключів;
- необхідно досить часто змінювати ключі;
- при використанні кількома клієнтами ключ слід засекречувати на двох кінцях.

К симетричним алгоритмам шифрування відносять: Twofish, Serpent, AES, Blowfish, CAST5, RC4, TDES, та IDEA.

Асиметричне шифрування, або метод відкритого ключа, передбачає застосування в парі двох відмінних ключів, а саме секретний та відкритий. В асиметричному шифруванні інформація шифрується відкритим ключем, а розшифровування відбувається тільки відповідним секретним ключем та навпаки. Неможливим є використання відкритого ключа із однієї пари та секретного ключа із іншої пари. Найбільшою перевагою є вищий рівень захисту цілісності даних. Але при цьому вагомими є вади швидкості дії асиметричних методів. До асиметричних алгоритмів шифрування належать RSA та ECC.

Оскільки існує запит не тільки на максимальний захист інформації, а й на швидкість її поширення та обробки, у новітніх крипто системах, застосовуються комбінації симетричних та асиметричних алгоритмів, з метою отримання переваг обох схем.

Захищений документообіг не тільки допомагає у боротьбі зі зловмисниками та «брудною» конкуренцією, а й лежить в основі успішного розвитку підприємств, дозволяє більш ефективно використовувати часові та фінансові ресурси, забезпечує стабільність і надійність в очах партнерів. У цьому важливу роль має галузь кібербезпеки, що вважається перспективною та затребуваною як для підприємств, що розвиваються, так і для цілих держав.