

МЕТОДИ СТВОРЕННЯ ТА ВБУДОВУВАННЯ ЕЛЕКТРОННИХ ЦИФРОВИХ ПІДПИСІВ

Заглада В. І.

Науковий керівник - ст. викл., к.т.н. Барішев Ю. В.

Використання електронного документообігу відкриває нові можливості для підприємства, але також несе велику кількість загроз. Одним із методів забезпечення захисту електронного документообігу є електронний цифровий підпис. Він дозволяє гарантувати автентичність документів і користувачів.

Відомі задачі, в яких постає необхідність пошуку місць вбудовування електронного цифрового підпису. Так як після зміни документа існує певна ймовірність його подальшої зміни, а також зміни електронного цифрового підпису, тому є необхідність в розгляді можливих місць вбудовування в електронних документах.

При розробці електронного цифрового підпису була досліджена структура *.pdf файлу щодо наявності можливих місць вбудовування електронного цифрового підпису. Даний формат електронного документу складається з таких частин:

- заголовок – в даному розділі міститься інформація про версію PDF;
- тіло – послідовність об'єктів, опис яких як заголовка представлені в текстовому вигляді;
- таблиця перехресних посилань – текстова таблиця і у своєму тілі має посилання на всі непрямі об'єкти в документі;
- блок зв'язків між таблицями.

Для вбудовування найкраще підходить тіло даного файлу. Електронний цифровий підпис вбудовується між об'єктами, які визначаються в тілі електронного документу.

Для створення електронного цифрового підпису необхідно використовувати асиметричний алгоритм шифрування. Аналіз показав, що алгоритм DSA забезпечує основні вимоги до захисту, а також забезпечує високу швидкість порівняно з іншими алгоритмами асиметричного шифрування.

Іншою складовою електронного цифрового підпису є геш-функція. На основі проведеного аналізу геш-функцій було визначено, що для розв'язання даної задачі найкращим чином підходить геш-функція КЕСАК, яка є фіналістом конкурсу SHA-3. Дана геш-функція використовує конструкцію «губки», яка забезпечує підвищену стійкість до загальних атак, що базуються на мультиколізіях.

В подальшому планується розвиток методів щодо розширення можливостей вбудовування у електронні документи різних форматів.