ЗАХИСТ КОНФІДЕНЦІЙНИХ ДАНИХ ПРИ ПЕРЕДАЧІ ЇХ ПО ВІДКРИТОМУ КАНАЛУ ЗВ'ЯЗКУ В ON-LINE ДОКУМЕНТОВЕДЕННІ

Товкач І. О., Піддубний В. О., к.т.н., доц.
Національний технічний університет України
«Київський політехнічний інститут», м. Київ, Україна

На сучасному етапі розвитку нашого суспільства актуальною є задача введення електронного документообігу в роботу державних управлінських структур, забезпечення зв'язку між державними органами управління та громадянським суспільством.

Ця задача вирішується шляхом впровадження в їх роботу систем електронного документообігу (СЕД), наприклад таких, як АСКОД, архівна справа, «*Megapolis*. Документообіг», система електронного архіву *STOR-M* та інші [1–4]. Такі системи досить непогано працюють, але й мають свої недоліки, оскільки більшість з них необхідно встановлювати на кожен комп'ютер індивідуально, що потребує значних часових затрат та залучення для їх налаштування спеціалістів високого кваліфікаційного рівня. Такий порядок унеможливлює їх розгортання та обслуговування співробітниками самої установи, де використовується СЕД, а це призводить до додаткових фінансових затрат. У більшості проаналізованих СЕД бази даних є уніфікованими, тобто незмінними для кожної конкретної установи або галузі. Тому їх не можна без суттєвої переробки перенести з однієї установи чи галузі в іншу. Такі бази даних зберігаються на кожному комп'ютері окремо, а відтак не існує єдиної бази для перегляду всіх даних в цілому, що значно ускладнює статистичні дослідження роботи установи. Це вимагає утримувати у штаті державних установ висококваліфікованих системних адміністраторів, що є досить затратним.

Тому була розроблена система електронного документоведення «ПОЛІДАР» (рис. 1), робота якої базується на паралельній обробці лінійних ірраціональних даних алгоритмами рекомбінації (від чого й походить її назва). Дана СЕД не потребує спеціалізованого обслуговування, не містить уніфікованих шаблонів для формування баз даних, а натомість дає можливість користувачам 1 самостійно створювати форми та шаблони під власні потреби. СЕД «ПОЛІДАР» включає в себе інтерактивний режим користування, зручний інтерфейс, можливість формування бази даних під різні галузі, а також має шифровану передачу даних. Веб-сайт для управління системою розміщено на *SaaS*-сервері 2 і використовується для передачі шифрованих даних з комп'ютера працівника 1 установи до бази даних установи 3, тобто всі робочі місця знаходяться в одній мережі.

Для шифрування застосовується оптимізований метод шифрування *MHED*-2 [5].

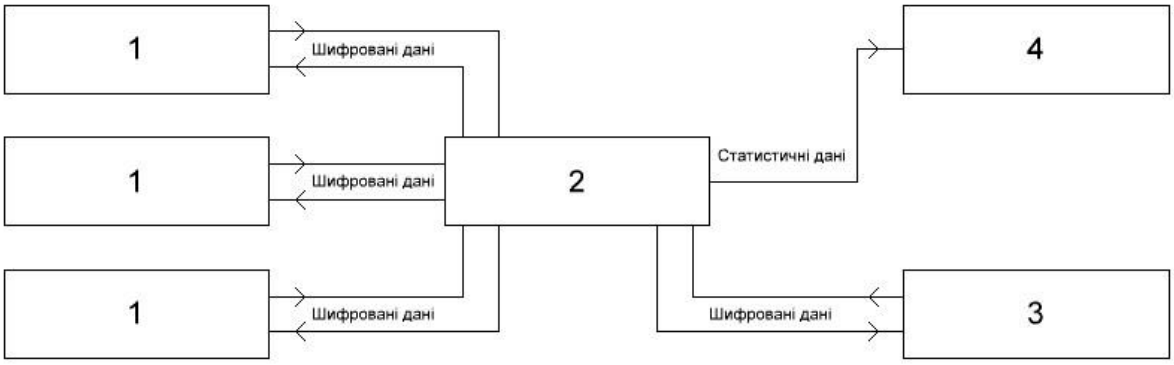

Рисунок 1. Структурна схема взаємодії в СЕД «ПОЛІДАР»: 1 — комп'ютери користувачів, який дозволяють шифрування даних, 2 — SaaS сервер з розміщеним веб-сайтом, 3 — база даних установи, 4 — портал з можливістю отримання статистичних даних.

Його особливість полягає в тому, що в шифруванні одночасно задіяні чотири алгоритми: три симетричні (*AES*, *Serpent*, *Twofish*) та один асиметричний (*RSA*). Коротка характеристика алгоритмів наведена нижче.

Алгоритм *AES* (*Advanced Encryption Standart*) – симетричний алгоритм блочного кодування. Довжина блоку складає 128 біт, довжина ключа 128 біт. Алгоритм *Serpent* – симетричний алгоритм блочного шифрування, довжина блоку складає 128 біт, довжина ключа 128 біт кількість раундів становить 32. Алгоритм *Twofish* – симетричний алгоритм блочного шифрування, довжина блоку складає 128 біт, довжина ключа 256 біт, кількість раундів становить 16. Алгоритм *RSA* – асиметричний алгоритм шифрування, довжина ключа 1024 біт.

Всі чотири алгоритми використовуються для комплексної обробки даних, при якій три симетричних алгоритми накладаються шар за шаром, послідовно, і після кожного встановлюється ключ за допомогою асиметричного алгоритму, який потім записується в початок зашифрованих даних. Це дозволяє надійно захистити дані навіть при розшифрування одного з симетричних алгоритмів при спробі несанкціонованого доступу до інформації.

Дослідження запропонованого методу шифрування встановило, що послідовність накладання алгоритмів для різних типів даних впливає на швидкодію роботи системи в цілому. Так для текстових даних більш швидкою є обробка в такій послідовності — (*Serpent – Twofish – AES*), для графічних — (*Twofish – Serpent – AES*), для аудіо та відео — (*AES – Serpent – Twofish*).

Використання методу *MHED*-2 дозволило зробити документообіг захищеним від несанкціонованого використання інформації установи.

Таким чином, розроблено програмне забезпечення для здійснення документообігу з можливістю шифрування даних та веб-сайт для взаємодії

користувача з базою даних. Розроблений програмний продукт впроваджений в архівний установах Київської області [6] і нараховує 62 бази даних, які об'єднані в єдину мережу. Він дозволяє працівникам архівних установ, що не мають високої комп'ютерної кваліфікації, самостійно працювати в СЕД і таким чином розвивати електронний документообіг в Україні.

Перелік посилань

1. Вишневський А., Електронне урядування: досвід упровадження в Головдержслужбі України. /А.Вишневський, В.Дунаєв// Вісник державної служби України. — 2008. — №4.

2. Автоматизована система контролю й організації діловодства // веб-сайт компанії АТ "Центр комп'ютерних технологій ІнфоПлюс" [Електронний ресурс]. — Режим доступу: http://infoplus.kiev.ua/index2.php ?products/text_3 — Назва з екрану (08.02.2015).

3. Система автоматизации учета документов архивного фонда «АРХИВНОЕ ДЕЛО» //веб-сайт компанії «ЭОС» [Електронний ресурс]. – Режим доступу: http://www.eos.ru/eos_products/eos_ archive_delo — Назва з екрану (08.02.2015).Мова рос.

4. Megapolis. Документообіг: СЕД для держорганізацій //веб-сайт компанії InBASE [Електронний ресурс]. — Режим доступу: http://inbase.com.ua/ua/produkti/elektronnij-dokumentoobig/megapolis-dokumentoobig — Назва з екрану (08.02.2015).

5. Товкач І.О. Оптимізація взаємодії алгоритмів шифрування в MHED–методі захисту конфіденційних при передачі їх по відкритих каналах зв'язку /І.О.Товкач, В.О.Піддубний// Міжнародна науково-технічна конференція «Радіотехнічні поля, сигнали та системи». Київ, 10 — 16 березня 2014 р.: матеріали конференції — Київ, 2014. — С. 241 — 243.

6. Веб-сайт Електронної мережі архівів Київщини [Електронний ресурс]. — Режим доступу: http://archives.kiev.ua — Назва з екрану (08.02.2015).

Анотація

Розроблено систему електронного документоведення, яка функціонує за допомогою SaaS–технології та забезпечує передачу даних по відкритому каналу зв'язку інтернету за допомогою методу шифрування MHED–2.

Ключові слова: електронне документоведення, SaaS–сервер, відкритий канал зв'язку, метод шифрування MHED–2.

Аннотация

Разработана система электронного документоведения, которая функционирует с помощью SaaS–технологии и обеспечивает передачу данных по открытому каналу связи интернета с помощью метода шифрования MHED–2.

Ключевые слова: электронное документоведение, SaaS–сервер, открытый канал связи, метод шифрования MHED–2.

Abstract

The system Electronic Documentation, which functions using SaaS-technology and provides data on open communication channel – the Internet using encryption method MHED–2.

Keywords: electronic documentation, SaaS–server, open communication channel, encryption MHED–2.