отримання інформації про будь-які операції, які були виконані з товаром. Головна сторінка цієї інформаційної системи зображена на рисунку 1.

За допомогою даної бази даних була зроблена спроба створити оптимальне управління організацією. Вона забезпечує цілісність збережених даних, перешкоджає їх втрати та спотворення. Забезпечує швидкий пошук необхідної інформації, наочність (тому що всі дані представлені в зручному вигляді для користувача). Дозволяє користувачеві вносити зміни (додавати, видаляти непотрібну інформацію).

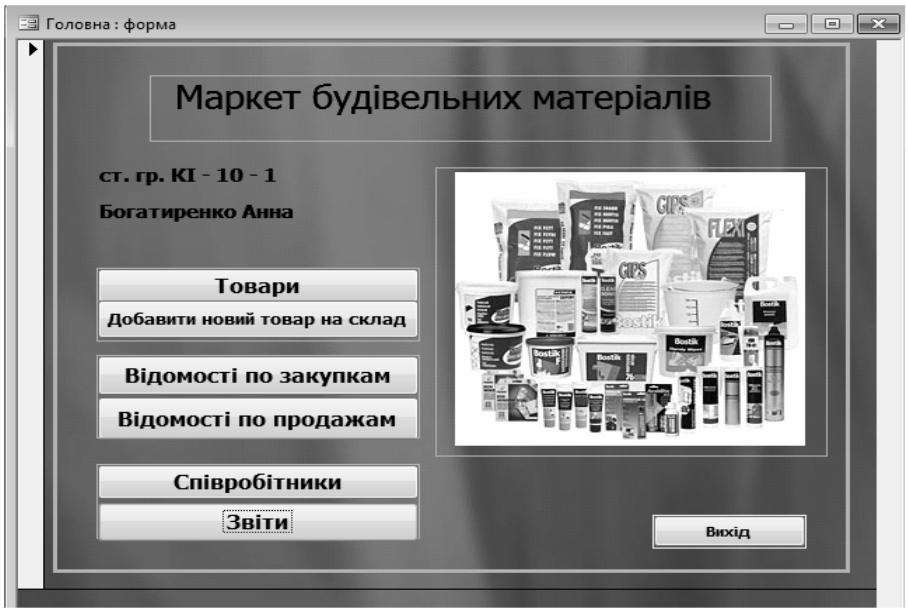

Рисунок 1 – Головна форма будівельної організації

Створена база даних має бути корисна при роботі на будь-якому складі або магазині, що спеціалізується на продажу будівельних матеріалів.

Список літератури

1. Голицина О. Л. Базы данных / Голицина О. Л., Максимов Н. В., Попов И. И. – М.:Форум,2003.–352 с.
2. Рудаков А.В. Технология разработки программных продуктов – М.: Академия, 2005. – 208 с.
3. Благодатских В. А. Стандартизация разработки программных средств: Учеб. пособие/ Благодатских В. А., В. А. Волнин, К. Ф. Поскакалов; Под ред. О. С. Разумова.– М.: Финансы и статистика, 2003.–288с.

УДК 004.42:004.057.4

Р.А. Бондаренко
Науковий керівник – До́ренський О.П., викладач
Кіровоградський національний технічний університет

Передача даних мережею за протоколом SSL

Сьогодні Інтернет використовується не тільки для роботи й дозвілля, але й як зручний засіб для укладання угод, у тому числі й фінансових. За допомогою сервісів всесвітньої мережі можливо здіснювати продаж й купувлю товарів і послуг, переказувати кошти, тобто здійснювати транзакції такі ж, як і у банківській системі.

Але для того, щоб убезпечитись та бути впевненим у тому, що після здійснення оплати, гроші надійдуть саме до вказаного одержувача, необхідне застосування SSL-

сертифіката. Це є є гарантією того, що всі дані, які передаються глобальною мережею, перебувають під захистом, а що є важливим та актуальним.

SSL-сертифікат дозволяє переконатися будь-якому користувачеві у тому, що він належить конкретній організації, а передані дані є захищеними. Визначити такий сайт можна за піктограмою замка. Під час входу на такий ресурс, сервер і браузер клієнта обмінюються ключами. Захищене з'єднання завжди здійснюється за протоколом https, тому вся інформація передається в зашифрованою й розшифровуються за допомогою спеціального ключа.

Таким чином, розробка програмного забезпечення системи передачі даних у мережі за протоколом SSL, є актуальною задачею.

Для програмної реалізації системи запропоновано функціональну схему, що наведена на рисунку 1.

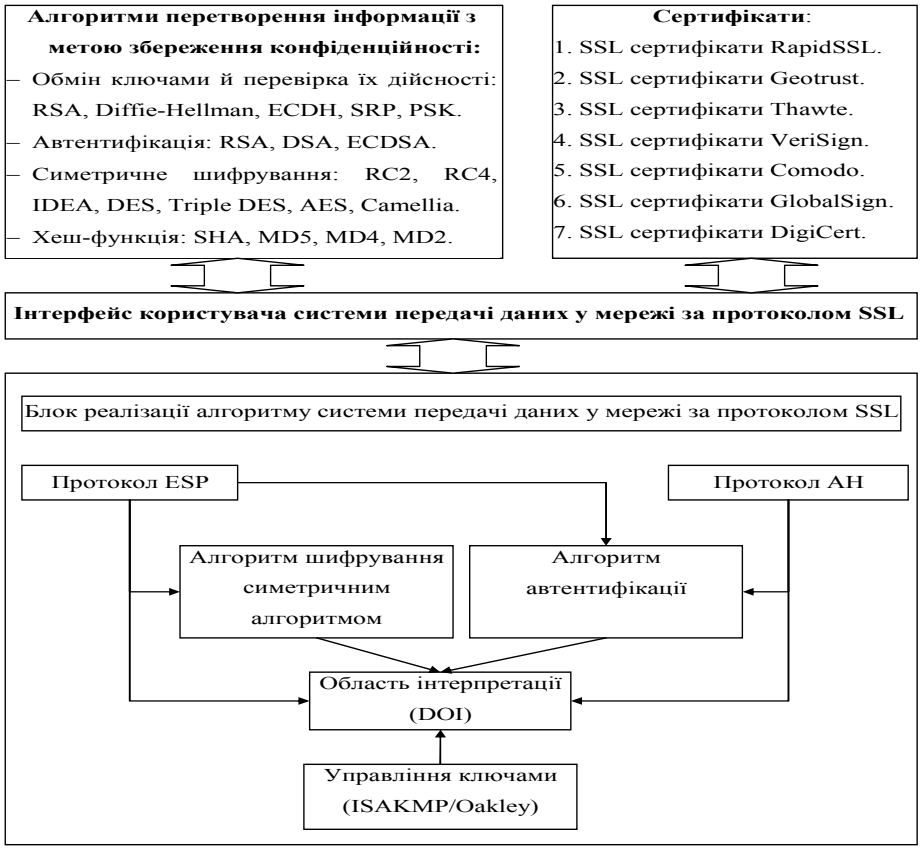

Рисунок 1 – Функціональна схема системи передачі даних у мережі за протоколом SSL

Функціональні блоки розробленого програмне забезпечення системи передачі даних у мережі за протоколом SSL реалізовано на основі наступних алгоритмів: RSA, Diffie-Hellman, ECDH, SRP, PSK для обміну ключами й перевірки їхньої дійсності; RSA, DSA, ECDSA для автентифікації; RC2, RC4, IDEA, DES, Triple DES або AES, Camellia для симетричного перетворення інформації з метою збереження конфіденційності; SHA, MD5, MD4 і MD2 для хеш-функцій.

Для здійснення SSL-з'єднання необхідно, щоб сервер мав інстальований цифровий сертифікат – файл, що унікально ідентифікує користувача і сервер. Це – свого роду електронний паспорт, що проводить автентифікацію сервера до того, як встановлюється сеанс SSL-з'єднання. Цифровий сертифікат незалежно підписується й засвідчується третьою стороною, що гарантує його достовірність. У ролі такої третьої сторони виступають центри сертифікації, наприклад, компанія "Thawte".

Запропоноване ПЗ для встановлення захищеної сесії забезпечує перевірку, щоб доменне ім’я в сертифікаті відповідало тому домену, від якого йде запит на захищене з’єднання; сертифікат не був прострочений; сертифікації, що підписала сертифікат домену, входив до числа довірених Web-браузера.

Список літератури

1. Балакирский В.Б. Безопасность электронних платежей. Защита информації – Конфидент, № 5, 1996.
2. Бернет С., Пэйн С. Криптография. Официальное руководство RSA Security. М.: Бином-пресс, 2002.
3. Бруно Л. Certificate Authorities: Кому Вы доверяете? Data Communications (Russian edition). № 3, 1998.
4. Галатенко В.А. Информационная безопасность. Обзор основних положений. Jet Info. № 1-3, 1996.
5. Галатенко В.А. Стандарты в области безопасности распределенних систем. Jet Info, № 5, 1999.
6. Галатенко В.А. Основы информационной безопасности. – М.: ИНТУИТ.РУ – "Интернет-университет информационних технологий", 2003.

УДК 004.056.55

В.О. Гаража
Науковий керівник – До́ренський О.П., викладач
Кіровоградський національний технічний університет

Створення архівів у файловій системі NTFS з розмежуванням доступу за допомогою алгоритму AES

Програми для стиснення даних почали розроблятися одночасно зі створенням перших персональних комп’ютерів, адже ще тоді постійно відчувалася недостача вільного місця на жорстких дисках. Як правило, користувачі стискують текстові документи, рідше – фотографії і відеодані, тому що в останньому випадку виграш у вільному місці виявляється зовсім невеликим. Процес створення архіву називають архівацією або упакуванням, а зворотній процес – розпакуванням або екстракцією [1].

Проте під час перенесення архівів портативними носіями або передачі їх мережею гостро постає питання безпеки заархівованої інформації. Тому задача забезпечення розмежування доступу до архівів є актуальною.

Метою роботи є розробка програмного забезпечення створення архівів у файловій системі NTFS з розмежуванням доступу.

Аналіз [2-5] показав, що серед найпоширеніших алгоритмів шифрування оптимальними з погляду специфіки їх роботи, рівня захисту та простоти імплементації є алгоритми AES та RSA. Водночас, симетричний алгоритм AES, наприклад, відповідно до дослідження [4], має значно кращу часову характеристику: якщо 1 Мб даних асиметричний RSA шифрує за 7,5 сек., то AES – за 0,51 сек. Тобто програмна реалізація криптографічних перетворень над даними на основі алгоритму AES є більш ніж в 10 разів швидша ніж при використанні RSA. Таким чином, алгоритм AES можна вважати доцільним для програмної реалізації з метою подальшого впровадження і використання, що є актуальною задачею. Також слід відзначити, що Rijndael стандарту AES – це швидкий і компактний алгоритм з простою математичною структурою, завдяки чому він є простим для аналізу під час оцінювання рівня захисту.

Отже, можна впевнено зробити висновок, що для розробки програмного забезпечення створення архівів у файловій системі NTFS з розмежуванням доступу є доцільним застосування саме алгоритму AES, відомого ще під назвою Rijndael [3].