УДК 681.327.8

В.Ніконенко
Тернопільська академія народного господарства

МОЖЛИВОСТІ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ІНТЕРНЕТ ДЛЯ ПЕРЕДАЧІ ЗВІТНОЇ ІНФОРМАЦІЇ У БАНКІВСЬКІЙ СИСТЕМІ З УРАХУВАННЯМ ПИТАНЬ ЇЇ ЗАХИСТУ

Розглядається можливість передачі у банківській системі звітної інформації засобами мережі Інтернет. При цьому здійснюється огляд існуючих та вибір найбільш ефективних засобів захисту інформації для забезпечення конфіденційності, цілісності та достовірності її передачі. Наведено пропозиції щодо запровадження та використання нової технології подачі та формування звітності з урахуванням питань її захищеності.

Перехід до ринкової економіки, розвиток нових інформаційних технологій, посилення конкурентної боротьби вимагає нових підходів до системи управління банком. Зокрема, одним з перспективних напрямів є створення корпоративної інформаційно-аналітичної мережі, здатної забезпечити комплексне розв'язання задач збору, систематизації, аналізу інформації, прийняття управлінських рішень в усіх підрозділах і на всіх рівнях структури банку [1].

Наявна методика подання оперативної звітності з використанням засобів електронної пошти характерна низкою організаційних і технологічних недоліків, що ускладнює механізм своєчасного отримання, обробки та систематизації необхідної інформації й спричинює надлишкові витрати.

Так, подекуди не уніфіковано форми подання звіту, що вимагає їх роздрукування та ручної чи механізованої обробки, що є надзвичайно неефективним і супроводжується суттєвими затратами часу. Стандартна форма звіту дозволяє її автоматизовану обробку та зведення одержаної інформації, але, в свою чергу, вимагає розробки та супроводу відповідних програмних засобів. Потрібно враховувати, що інформація передається електронною поштою окремими файлами, тому відповідальний працівник повинен спочатку створити та заповнити певний файл, далі підготувати його (назвати, заархівувати) і відправити, що вимагає наявності певних знань і навиків у роботі з різними форматами даних та з файловою системою. Багато часу також витрачається на конвертацію цього файла поштовою програмою, його пересилання та розконвертацію. Все це спричинює значні затримки, а деколи і порушення необхідних строків подання звітності.

Неефективним є використання звичайних комутованих каналів зв'язку. Оскільки вони мають низьку швидкість та надійність передачі даних, можлива зайнятість конкретних номерів чи "зашумленість" лінії. При цьому необхідно оплачувати міжміські телефонні з'єднання, що призводить до значних телекомунікаційних витрат.

Неврегульованим є питання захисту звітної інформації, що передається фактично відкрито, оскільки поштові програми, що використовуються для передачі електронної пошти мають відповідні засоби або не ефективні, або не мають їх зовсім. А якщо врахувати важливість інформації, що передається в банківській системі, зацікавлена сторона може дозволити собі фінансові витрати на злам захисту і, відповідно, використати кращі та потужніші методи – спостереження за трафіком, криптоаналіз перехопленої інформації, а також різні імітовставки, диверсії та шахрайство.

Треба пам'ятати, що конфіденційні дані повністю захищені від посягань лише тоді, коли вони розміщені на дисках, що зняті з комп'ютера і перебувають під охороною. Навіть їх підключення до комп'ютера створює одразу декілька каналів, якими зловмисник може отримати доступ до таємної інформації, не кажучи вже про передачу даних каналами зв'язку. Поряд з цим система повинна мати певний рівень відкритості, щоб забезпечити доступ до даних, їхню передачу, тобто можливість

їхнього корисного використання. Потрібно вибирати такий баланс між захищеністю системи та її відкритістю, який забезпечував би високий рівень обох цих характеристик.

Розв'язання цих питань та усунення недоліків можливе шляхом створення корпоративної інформаційно-аналітичної системи у вигляді централізованих баз даних та інтерфейсів доступу до них на основі технології Інтернет/Інтранет на закритих сайтах. Переваги полягають у поширеності та загальнодоступності мережі Інтернет, простоті та наочності роботи з нею, існуванні стандартних засобів передачі, зберігання та обробки інформації, що забезпечує достатню відкритість системи. З іншого боку існують такі методи та засоби, які дозволяють надійно захищати інформацію, що передається. Взагалі термін "закритий сайт" означає, що доступ до цього сайту можливий лише для обмеженого числа зареєстрованих користувачів, а для всіх інших він недоступний – закритий.

Згідно з організаційною структурою банку та ієрархічною системою подання звітної інформації виникає необхідність трирівневого розподілу цієї інформаційної системи. На першому рівні перебувають районні відділення, що формують звітні дані для передачі їх обласному управлінню (другий рівень). В обласному управлінні обробляються, узагальнюються одержані дані та передаються Правлінню банку (третій рівень) для їх консолідації, обробки та використання.

Відповідно до цієї схеми необхідний закритий сайт на найвищому (третьому) рівні, користувачами якого є уповноважені представники обласних управлінь. Вони повинні передавати дані та вносити зміни у централізовані бази Правління банку. На рівні облуправління також необхідний сайт, користувачами якого є представники відділень, що формують регіональну звітність. При цьому зареєстровані користувачі – це працівники банку, що повністю відповідають за подання оперативної звітності, її зміст та строки.

Закритий сайт та інформаційно-аналітична система повинні забезпечувати:

- авторизацію користувачів;
- передачу та формування оперативної звітності;
- криптозахист інформації, що передається;
- неможливість несанкціонованого доступу до ресурсів;
- розмежування прав користувачів;
- ведення журналів доступу до ресурсів сайту;
- контроль за своєчасністю одержання інформації.

Для захисту сервера, на якому розміщений сайт, від зовнішніх атак з мережі Інтернет, може використовуватись програмно-апаратний засіб FireWall з функціями фільтраційного маршрутизатора. Це дозволяє відповідно із заданою політикою інформаційної безпеки виробити набір правил для фільтрації IP-пакетів, що надходять на сервер. Ця фільтрація виконується за IP-адресами відправника та отримувача IP-пакета, за типом протоколу, портами відправника та отримувача заданого протоколу. Завдяки цьому обмежується доступ до сервера і унеможливлюється зовнішній вплив на нього.

Для одержання доступу до ресурсів закритого сайту користувач повинен бути зареєстрований на ньому. При реєстрації йому присвоюється ім'я ("логін", під яким він заходитиме на цей сайт) та пароль для доступу. Ці реквізити мають зберігатися в таємниці від усіх, крім користувача. Залежно від реєстраційної та службової інформації (посада, відділ) адміністратор сайту надає користувачеві певний вид доступу (перегляд, передача та корегування) до відповідних ресурсів (форм звітності).

Однак слід враховувати, що такі засоби захисту, як запит пароля з наступною передачею його у відкритому вигляді та використання звичайних списків доступу на сьогодні є малоефективними. Для того, щоб бути впевненим, що інформація, яка передається, є захищеною від сторонніх осіб, потрібно використовувати сучасні криптографічні засоби.

Наявні засоби захисту інформації, що передається в мережі Інтернет, можна поділити згідно з належністю до рівнів моделі OSI на три групи:

1) Високорівневі засоби, що використовуються на прикладному рівні (PGP; SHTTP).
2) Засоби, що знаходяться на транспортному рівні (SSL/TLS) .
3) Низькорівневі засоби мережевого рівня (SKIP, IP See).

Використання високорівневих засобів типу відомої та поширеної програми Pretty Good Privacy дозволяє надійно захищати інформацію, однак при цьому постає задача поєднання їх з іншими прикладними системами. При застосуванні низькорівневих засобів спрощується робота з ними для будь-яких застосувань, але поряд з цим виникають обмеження щодо їх апаратної сумісності, рівня захищеності та занадто високої ціни [2].

Досить надійним є застосування протоколу SSL (Secure Socket Layer), що функціонує на транспортному рівні і підтримується основними броузерами Microsoft Internet Explorer, Netscape Navigator та іншими продуктами незалежних компаній. Це універсальний протокол захисту з'єднання, що використовує криптографію з відкритим ключем і дозволяє динамічно захищати будь-яке з'єднання. При цьому процес створення віртуального SSL - з'єднання відбувається за схемою Діффі-Хелмана, яка дозволяє виробити криптостійкий сеансовий ключ, що використовується для шифрування повідомлень, що передаються.

Схема взаємодії користувача та сервера під управлінням протоколу SSL передбачає спеціальний сертифікат, на основі якого виконується аутентифікація та подальше встановлення захищеного з'єднання. Він складається імені сервера, його відкритого ключа, періоду дії сертифікату, імені центру сертифікації та цифрового підпису цього центру. Для кожного сертифікату сервер генерує унікальну пару ключів (таємний і відкритий). На основі відкритого ключа та інформації, що ідентифікує сервер, формується сертифікат, що передається за запитом користувача. Останній, таким чином, отримує можливість аутентифікації сервера. Після цієї процедури встановлюється захищений режим обміну інформацією між користувачем і сервером.

Отже, процесові аутентифікації та захищеної передачі інформації властива така послідовність дій:

1) користувач надсилає запит на встановлення з'єднання з сервером;
2) сервер передає користувачеві сертифікат;
3) користувач перевіряє цифровий підпис сертифіката і, якщо не отримує підтвердження істинності сервера, розриває з'єднання;
4) користувач генерує сеансовий ключ і шифрує його відкритим ключем сервера, після чого тільки сервер з допомогою свого таємного ключа може виконати дешифрування. Далі цей сеансовий ключ буде використовуватися для шифрування та дешифрування інформаційних потоків і контролю цілісності;
5) сервер дешифрує сеансовий ключ і встановлює з користувачем захищений режим взаємодії.

Протокол SSL застосовує у своїй роботі принцип відкритих ключів, причому асиметричним криптографічним алгоритмом використовуються алгоритм RSA. За цим принципом для шифрування/дешифрування інформації використовує пара асиметричних ключів (відкритий та таємний), а сама процедура шифрування є загальнодоступною. Відкритий ключ роздається учасникам обміну інформацією і кожен може використати його для шифрування/дешифрування інформації. Захищеність системи полягає в тому, що немає ефективного алгоритму, який за відомим відкритим ключем, зашифрованим повідомленням та процедурою шифрування міг би визначити початкове повідомлення. Воно може бути дешифроване лише за допомогою парного, таємного ключа, згенерованого відповідним алгоритмом і відомого лише його власникові [3].

Алгоритм RSA, запропонований у 1977 році Роном Рівестом, Аді Шаміром і Леонардом Эйдельманом, названий на їхню честь. Для цього алгоритму шифрування інформації фактично полягає у піднесенні до степеня за модулем, а його розкриття (злам) вимагає розв'язку задачі добування із заданого числа кореня певного степеня за модулем (тобто його факторизація). На сьогодні для цієї задачі невідомо ніякого ефективного алгоритму і навіть із застосуванням обчислювальної техніки при достатній розрядності (200 десяткових знаків) обраного числа для його розкладу на множники необхідні тисячі років [1].

Звідси випливає, що з допомогою протоколу SSL розв'язуються такі завдання:

- аутентифікація користувачем сервера та навпаки (доменне ім'я в сертифікаті сервера повинно збігатися з доменною адресою в посиланні, яким звертається користувач);
- шифрування всіх даних, що передаються між сервером і користувачем, завдяки чому розв'язується питання конфіденційності передачі даних та усувається можливість перехоплення їх сторонніми особами;
- контроль цілісності даних, які передаються, що дозволяє бути впевненим у незмінності інформації або підтверджує наявність змін у ній.

Доступ до необхідних ресурсів формується з вказанням протоколу HTTPS в посиланні, що означає передачу даних за допомогою одночасного використання HTTP- та SSL- протоколів. Це дозволяє, не розкриваючи конфіденційної інформації, відмовити такому користувачеві, який не підтримує протоколу SSL і не володіє необхідним сертифікатом.

Користувач, вказавши в броузері посилання на закритий сайт, після введення пароля (авторизації) та встановлення захищеного з'єднання, одержує доступ до відповідних ресурсів – форми звітності. Кожна форма є HTML-сторінкою, яка містить засоби для введення, обробки, передачі та відображення інформації. У процесі роботи з формою користувач заповнює необхідні дані і передає їх за призначенням. При цьому передається лише конкретна звітна інформація, що суттєво зменшує трафік та час передачі. При потребі при зміні форм подання звітності корегується відповідна сторінка та процедури обробки інформації, про що повідомляється підпорядкованим установам.

У результаті по мірі надходження даних автоматично формується звітність, що може контролюватися та корегуватися працівником банку. Після завершення формування можливий вивід вихідних форм та підготовка даних для передачі на наступний рівень управління. Ведення журналу роботи дозволяє контролювати функціонування системи, в тому числі своєчасне надання інформації, а при наявності порушень чи помилок інформувати відповідальних осіб .

Таким чином, з допомогою корпоративної мережі, побудованої на основі захищених сайтів і користувачів, що мають доступ до них з використанням засобів мережі Інтернет, з'являється можливість забезпечити оперативну передачу та одержання звітної інформації з урахуванням необхідного рівня захисту цих даних.

Due to means of a Internet network there is a capability to execute transfer of the accounting data in a banking system. The creation of a corporate network, which integrates different bank institution, allows to provide reliable and protected information interchange. Protection of connection and confidential of transfer of the information realized by a means of application SSL- protocol.

Література

1. Задірака В.К., Олексюк О.С., Недашковський М.О. Методи захисту банківської інформації.– К.: Вища школа, 1999.– 261с.
2. Колесников П.В. Обзор протоколов защиты информации в открытых сетях// Радиотехника. Всеукраинский межведомственный научно-технический сборник.– 2000.– Вып. 114.– С.120-123.
3. Вербіцький О.В. Вступ до криптології.– Львів: ВНТЛ, 1998.– 247 с.

Одержано 18.04.01 р.