



УКРАЇНА

(19) UA (11) 89784 (13) C2  
(51) МПК (2009)  
H04L 9/08

МІНІСТЕРСТВО ОСВІТИ  
І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ  
ІНТЕЛЕКТУАЛЬНОЇ  
ВЛАСНОСТІ

## ОПИС ДО ПАТЕНТУ НА ВІНАХІД

**(54) СПОСІБ ШИФРУВАННЯ ТА ПЕРЕДАЧІ ДАНИХ МІЖ ВІДПРАВНИКОМ І ОДЕРЖУВАЧЕМ ЗА ДОПОМОГОЮ МЕРЕЖІ**

1

2

(21) а200613642

(22) 18.04.2005

(24) 10.03.2010

(86) PCT/GB2005/001479, 18.04.2005

(31) 0411560.6

(32) 24.05.2004

(33) GB

(46) 10.03.2010, Бюл.№ 5, 2010 р.

(72) ОЛКУЛУМБР МАЙКЛ, GB

(73) ДЖИКРИПТ ЛІМІТЕД, GB

(56) US 2003/172262 A1, 11.09.2003

EP 0869652 A, 07.10.1998

US 2003/046533 A1, 06.03.2003

(57) 1. Спосіб шифрування та передачі даних між відправником і одержувачем за допомогою мережі, який містить наступні етапи:

- отримання сервером від відправника ідентифікатора одержувача;
- встановлення спеціального ключа шифрування передачі, спеціально для передачі;
- шифрування даних за допомогою спеціального ключа шифрування передачі;
- організація доступу сервера до спеціальної інформації одержувача відповідно до отриманого ідентифікатора одержувача та виконання шифрування спеціальної інформації одержувача вказаним спеціальним ключем шифрування передачі;
- передача зашифрованих даних і зашифрованого спеціального ключа шифрування передачі через мережу для приймання одержувачем;
- виконання прийому сервером від одержувача зашифрованого спеціального ключа шифрування передачі;
- організація доступу сервером до спеціальної інформації одержувача для розшифрування зашифрованого спеціального ключа шифрування передачі; і
- виконання розшифрування зашифрованих даних, за допомогою розшифрованого спеціального ключа шифрування передачі.

2. Спосіб за п. 1, який включає встановлення лінії зв'язку між відправником і сервером та відправку згаданого ідентифікатора одержувача до сервера.

3. Спосіб за п. 2, який включає встановлення лінії зв'язку між відправником і сервером, яка має бути захищеною лінією.

4. Спосіб за п. 2 або п. 3, який включає встановлення лінії зв'язку між відправником і сервером, яка є об'єктом перевірки сервером за допомогою пароля відправника.

5. Спосіб за будь-яким з попередніх пунктів, який включає встановлення лінії зв'язку між одержувачем і сервером та відправку згаданого ідентифікатора одержувача до сервера.

6. Спосіб за п. 5, який включає встановлення лінії зв'язку між одержувачем і сервером, яка має бути захищеною лінією.

7. Спосіб за п. 5 або 6, який містить встановлення лінії зв'язку між одержувачем і сервером за умови перевірки сервером пароля одержувача.

8. Спосіб за будь-яким попереднім пунктом, де встановлення спеціального ключа шифрування передачі має місце у відправника і де встановлений спеціальний ключ шифрування передачі посилається до сервера.

9. Спосіб за будь-яким попереднім пунктом, де шифрування даних за допомогою спеціального ключа шифрування передачі має місце у відправника.

10. Спосіб за п. 9, де відправник отримує від сервера зашифрований спеціальний ключ шифрування передачі та відправник передає зашифровані дані та даний зашифрований спеціальний ключ шифрування передачі одержувачу через мережу.

11. Спосіб за будь-яким з пп. 1-7, де одержувач отримує від сервера розшифрований спеціальний ключ шифрування передачі та має місце розшифрування зашифрованих даних за допомогою використання розшифрованого спеціального ключа шифрування передачі в одержувача.

12. Спосіб за будь-яким з пп. 1-7, де має місце встановлення спеціального ключа шифрування передачі на сервері.

13. Спосіб за п. 12, де має місце шифрування даних за допомогою спеціального ключа шифрування передачі на сервері.

14. Спосіб за п. 13, де сервер передає зашифровані дані і зашифрований спеціальний ключ шифрування передачі одержувачу через мережу.

15. Спосіб за будь-яким з пп. 1-10 та 12-14, де розшифрування зашифрованих даних за допомогою розшифрованого спеціального ключа шифрування

(13) C2

(11) 89784

(19) UA

передачі має місце на сервері та сервер передає розшифровані дані одержувачу.

16. Спосіб за будь-яким з попередніх пунктів, який включає відправку ідентифікатора одержувача від відправника до сервера.

17. Спосіб за будь-яким з попередніх пунктів, який включає відправку ідентифікатора одержувача від одержувача до сервера.

18. Спосіб за будь-яким з попередніх пунктів, який включає наступне:

- встановлення значення коду підтвердження дійсності повідомлення для даних перед шифруванням;

- передачу значення коду підтвердження дійсності повідомлення разом з зашифрованими даними та зашифрованим спеціальним ключем шифрування передачі; і

- встановлення значення коду підтвердження дійсності повідомлення для даних після розшифрування та підтвердження цього шляхом порівняння з переданим значенням коду підтвердження дійсності повідомлення.

19. Спосіб за будь-яким з попередніх пунктів, де шифрування спеціального ключа шифрування передачі використовує декілька способів, тобто спосіб шифрування відкритим ключем, Blowfish алгоритм і секретний код сервера.

20. Спосіб управління сервером для шифрування та передачі даних між відправником і одержувачем за допомогою мережі, який включає наступні етапи:

- отримання від відправника ідентифікатора одержувача;

- організація доступу до специфічної інформації одержувача відповідно до отриманого ідентифікатора одержувача та шифрування спеціальної інформації одержувача спеціальним ключем шифрування передачі, який використовується для шифрування даних;

- отримання від одержувача зашифрованого спеціального ключа шифрування передачі після того, як зашифровані дані та зашифрований спеціальний ключ шифрування передачі передаються через мережу для прийому одержувачем;

- організація доступу до спеціальної інформації одержувача для розшифрування зашифрованого спеціального ключа шифрування передачі.

21. Спосіб управління сервером за п. 20, який містить встановлення на сервері спеціального ключа шифрування передачі спеціально для передачі.

22. Спосіб управління сервером за п. 20, який включає отримання від відправника спеціального ключа шифрування передачі, спеціально для передачі;

- передачу зашифрованого спеціального ключа шифрування до відправника.

23. Спосіб управління сервером за будь-яким з пп. 20-22, який включає шифрування даних на сервері за допомогою спеціального ключа шифрування передачі.

24. Спосіб управління сервером за будь-яким з пп. 20-23, який включає передачу зашифрованих даних і зашифрованого спеціального ключа шифрування передачі через мережу для прийому одержувачем.

25. Спосіб управління сервером за будь-яким з пп. 20-24, який включає передачу розшифрованого спеціального ключа шифрування передачі одержувачу.

26. Спосіб управління сервером за будь-яким з пп. 20-24, який включає розшифрування зашифрованих даних на сервері за допомогою розшифрованого спеціального ключа шифрування передачі.

27. Комп'ютерний носій для способу шифрування та передачі даних між відправником і одержувачем за допомогою мережі, де середовище містить наступне:

- набір команд для отримання від відправника ідентифікатора одержувача і встановлення спеціального ключа шифрування передачі спеціально для передачі;

- набір команд для шифрування даних за допомогою спеціального ключа шифрування передачі;

- набір команд для організації доступу до спеціальної інформації одержувача відповідно до отриманого ідентифікатора одержувача та шифрування спеціальної інформації одержувача вказаним спеціальним ключем шифрування передачі;

- набір команд для передачі зашифрованих даних і зашифрованого спеціального ключа шифрування передачі через мережу для прийому одержувачем;

- набір команд для отримання від одержувача зашифрованого спеціального ключа шифрування передачі та організації доступу до спеціальної інформації одержувача для розшифровки зашифрованого спеціального ключа шифрування передачі; і

- набір команд для дешифрування даних за допомогою розшифрованого спеціального ключа шифрування передачі.

Даний винахід стосується способу шифрування і передачі даних між відправником і одержувачем за допомогою мережі, який надає можливість передавати дані захищеним чином.

У даний час збільшується кількість конфіденційних даних, які надсилаються в електронному вигляді від відправника до одержувача. При таких обставинах становиться все більш і більш важливим гарантування того, що дані не можуть бути перехоплені, або прочитані особами, які не є вповноваженими, тобто дані повинні передаватися

захищеним чином так, щоб зміст даних міг бути доступний тільки відправнику і одержувачу.

В одному з варіантів, захищена лінія зв'язку може бути встановлена між відправником А і одержувачем В до того, як має відбутися передача даних. Однак, в ситуаціях, коли скажемо в одному офісі 10 осіб бажають встановити зв'язок та передати конфіденційні дані один одному, або бажають встановити зв'язок та передати дані, які потребують захисту 10 особам, які знаходяться в іншому віддаленому офісі в дуплексному режимі, то ма-

ються незручності, щодо створення таких умов оскільки захищені лінії зв'язку вимагають додаткового апаратного та програмного забезпечення. На додаток потрібно сказати, що треба залучати значні апаратні та часові ресурси для обслуговування таких ліній та систем пов'язаних з встановленням справжності паролю. Це особливо справедливо, коли особи в кожному офісі проводять зв'язок між собою за допомогою одного з видів Intranet або Ethernet мережі, а офіси встановлюють зв'язок через Internet мережу. Також необхідно мати складне програмне забезпечення для шифрування та розшифрування як у відправника так і в одержувача, що у свою чергу вимагає додаткового апаратного та програмного забезпечення, причому тягне за собою витрати, які потрібні на технічне обслуговування спеціалістом.

В іншому випадку, один відправник може бажати передати різні дані до багатьох окремих одержувачів. Однак, це має ті ж недоліки які згадані вище. Зокрема, для відправника необхідно підготувати складні заходи забезпечення безпеки для підтримки систем встановлення дійсності паролю в безпеці. Більш того, додаткове апаратне та програмне забезпечення повинне бути встановлене для створення резерву та для виконання технічного обслуговування таких систем.

Дійсно, у добу малих кишенькових приладів, таких як, наприклад, пристрої для зберігання особистих даних, мобільні телефони, які мають доступ до Internet мережі та мають можливості електронної пошти, при чому мають обмежену пам'ять та продуктивність обробки, часто з технічної точки зору не практично мати засоби для захищеного дуплексного зв'язку, коли залучаються високі рівні шифрування і розшифрування.

Все це впливає на вартість, яка часто не може бути виправдана для одержувача, навіть коли ця вартість мала, тому поки можуть використовуватися цифрові посвідчення для зменшення потреб на технічні ресурси як для відправника так і одержувача.

Для відправника маєтсья одна з альтернатив, яка полягає в тому, щоб виконати шифрування даних, що підлягають передачі, а потім передавати зашифровані дані через мережу. Однак, знову таки одержувач повинен мати апаратні ресурси обробки разом із наявною пам'яттю для відповідного програмного забезпечення, яке може виконувати розшифрування зашифрованих даних. Більш того, в ситуаціях, де пристрій одержувача має відносно слабкі ресурси апаратного забезпечення, придбання значних ресурсів для надання можливості захищеної передачі даних є часто не прийнятним на практиці.

Використання складних способів шифрування і розшифрування вимагає встановлення спеціального програмного забезпечення на апаратних засобах відправника і одержувача. Це є як незручним так і коштовним. Крім того, процедура встановлення може бути складною та потребувати багато часу при чому може привести до конфліктів з іншим програмним забезпеченням на їх відповідних апаратних засобах. До того ж, додаткове програмне забезпечення може вимагати відповідного рівня обчислювальної потужності, який відсутній в

даному пристрої та може вимагати значного обсягу пам'яті; це все особливо справедливо для випадку раніше згаданих малих кишенькових приладів.

З вищевикладеного ясно, що відомі способи та системи для передачі даних захищеним чином вимагають значної підготовки до роботи, а також значної обчислювальної потужності та локальних ресурсів пам'яті. Зрозуміло що це не підходить для тих ситуацій, де відправник і/або одержувач має пристрій просто з обмеженою кількістю вищезгаданих технічних ресурсів.

Тобто є потреба в способі та системі для передачі даних захищеним чином, що може зменшити рівень технічних ресурсів, які потрібні для апаратних засобів відправника і/або одержувача. Також у випадку, коли використовується відкритий/секретний ключ шифрування, відправник повинен бути впевненим, що відкритий ключ, який вони вважають належним одержувачу, не буде замінений відкритим ключем втручальника. Відповідно до одного варіанту даного винаходу забезпечується спосіб шифрування і передачі даних між відправником і одержувачем з використанням мережі, причому даний спосіб містить наступні етапи:

- отримання сервером від відправника ідентифікатора одержувача;
- встановлення спеціального ключа шифрування передачі, спеціально для передачі;
- виконання шифрування даних за допомогою спеціального ключа шифрування передачі;
- виконання організації доступу сервера до спеціальної інформації одержувача відповідно до отриманого ідентифікатора одержувача та виконання шифрування вказаним спеціальним ключем шифрування передачі спеціальної інформації одержувача;
- виконання передачі зашифрованих даних і зашифрованого спеціального ключа шифрування передачі через мережу для приймання одержувачем;
- виконання прийому сервером від одержувача зашифрованого спеціального ключа шифрування передачі;
- виконання доступу сервером до спеціальної інформації одержувача для розшифрування зашифрованого спеціального ключа шифрування передачі; і
- виконання дешифрування зашифрованих даних за допомогою розшифрованого спеціального ключа шифрування передачі.

Окрім цього переважним чином спосіб містить створення лінії зв'язку між відправником і сервером та відправку згаданого ідентифікатора одержувача до сервера.

В одному з варіантів виконання даного винаходу, окрім цього спосіб містить встановлення лінії зв'язку між відправником і сервером, яка має бути захищеною лінією.

В одному випадку окрім цього даний спосіб містить створення лінії зв'язку між відправником і сервером за умови виконання перевірки сервером пароля відправника.

В іншому варіанті виконання даного винаходу спосіб окрім цього містить встановлення лінії зв'я-

зку між одержувачем і сервером та відправку згаданого ідентифікатора одержувача до сервера.

В одному випадку спосіб окрім цього містить встановлення лінії зв'язку між одержувачем і сервером, яка має бути захищеною лінією.

В окремому випадку, даний спосіб окрім цього містить встановлення лінії зв'язку між одержувачем і сервером за умови виконання перевірки сервером пароля одержувача.

Переважним чином, встановлення спеціального ключа шифрування передачі має місце у відправника та виконується відправка встановленого спеціального ключа шифрування передачі до сервера.

В іншому випадку, шифрування даних з використанням спеціального ключа шифрування передачі має місце у відправника.

В іншому варіанті виконання даного винаходу відправник отримує від сервера зашифрований спеціальний ключ шифрування передачі та відправник передає зашифровані дані та зашифрований спеціальний ключ шифрування передачі одержувачу через мережу.

В іншому варіанті виконання даного винаходу одержувач приймає від сервера розшифрований спеціальний ключ шифрування передачі та виконує розшифрування зашифрованих ця них з використанням розшифрованого спеціального ключа шифрування передачі, що має місце в одержувача.

В ще одному варіанті виконання даного винаходу встановлення спеціального ключа шифрування передачі спеціально має місце на сервері.

В окремому випадку, шифрування даних із використанням спеціального ключа шифрування передачі має місце на сервері.

В одному з варіантів виконання даного винаходу, сервер передає зашифровані дані та зашифрований спеціальний ключ шифрування передачі до одержувача через мережу.

В іншому варіанті виконання даного винаходу дешифрування зашифрованих даних із використанням розшифрованого спеціального ключа шифрування передачі має місце на сервері і сервер передає розшифровані дані одержувачу.

Переважним чином даний спосіб окрім цього містить відправку ідентифікатора одержувача від відправника до сервера.

В іншому варіанті виконання даного винаходу даний спосіб окрім цього містить відправку ідентифікатора одержувача від одержувача до сервера.

Вочевидь, даний спосіб окрім цього містить наступне:

- встановлення значення коду підтвердження дійсності повідомлення (MAC- message authentication code) для даних перед шифруванням;

- передача значення коду підтвердження дійсності повідомлення разом з зашифрованими даними і даним зашифрованим спеціальним ключем шифрування передачі; та

- встановлення значення коду підтвердження дійсності повідомлення для даних після дешифрування і підтвердження їх шляхом порівняння зі

значенням переданого коду підтвердження дійсності повідомлення.

В одному з варіантів виконання даного винаходу шифрування спеціального ключа шифрування передачі використовується кілька способів з наступного: спосіб шифрування відкритим ключем, Blowfish алгоритм, секретний код сервера.

Відповідно до іншого варіанту даного винаходу забезпечується спосіб управління сервером для виконання шифрування і передачі даних між відправником і одержувачем за допомогою мережі, при чому спосіб містить етапи:

- отримання від відправника ідентифікатора одержувача;

- доступу до спеціальної інформації одержувача відповідно до отриманого ідентифікатора одержувача та виконання шифрування спеціальної інформації одержувача спеціальним ключем шифрування передачі, який використовується для шифрування даних;

- отримання від одержувача зашифрованого спеціального ключа шифрування передачі після передачі зашифрованих даних та зашифрованого спеціального ключа шифрування через мережу для приймання одержувачем;

- доступу до спеціальної інформації для розшифрування зашифрованого спеціального ключа шифрування передачі.

В одному з варіантів виконання даного винаходу спосіб управління сервером окрім цього містить встановлення на сервері спеціального ключа шифрування передачі, спеціально для передачі.

В іншому варіанті виконання даного винаходу спосіб управління сервером окрім цього містить прийом від відправника спеціального ключа шифрування передачі, спеціально для передачі;

і передачу зашифрованого спеціального ключа шифрування передачі до відправника.

Переважним чином спосіб управління сервером окрім цього містить шифрування даних на сервері за допомогою спеціального ключа шифрування передачі.

В іншому варіанті виконання даного винаходу спосіб управління сервером окрім цього містить передачу зашифрованих даних і зашифрованого спеціального ключа шифрування передачі через мережу для прийому одержувачем.

Переважним чином, спосіб управління сервером окрім цього містить передачу розшифрованого спеціального ключа шифрування передачі до одержувача.

В іншому варіанті виконання даного винаходу спосіб управління сервером окрім цього містить розшифрування зашифрованих даних на сервері за допомогою використання розшифрованого спеціального ключа шифрування передачі.

Відповідно до іншого варіанту виконання даного винаходу забезпечується комп'ютерний носій для способу шифрування і передачі даних між відправником і одержувачем за допомогою використання мережі, причому носій містить наступне:

- набір команд для отримання від відправника ідентифікатора одержувача та встановлення на сервері спеціального ключа шифрування передачі, спеціально для передачі;

- набір команд для шифрування даних за допомогою використання спеціального ключа шифрування передачі;
- набір команд для доступу до спеціальної інформації одержувача відповідно до отриманого ідентифікатора одержувача та шифрування спеціфічної інформації одержувача вищезгаданим спеціальним ключем шифрування передачі;
- набір команд для перенесення зашифрованих даних і даного зашифрованого спеціального ключа шифрування передачі через мережу для прийому одержувачем;
- набір команд для отримання від одержувача зашифрованого спеціального ключа шифрування передачі та для доступу до спеціальної інформації одержувача для розшифровки зашифрованого спеціального ключа шифрування передачі; і
- набір команд для розшифрування зашифрованих даних за допомогою використання розшифрованого спеціального ключа шифрування передачі.

Тепер один з прикладів даного винаходу буде описаний за допомогою креслень, де:

- на Фігурі 1 показана принципова схема системи функціонування способу даного винаходу шифрування та передачі даних між відправником і одержувачем за допомогою використання мережі;
- на Фігурі 2 показана принципова блок-схема виконуючих модулів сервера, які використовуються на фігурі 1;
- на Фігурі 3 представлена блок-схема процесу, який має місце у відправника та сервера для даного винаходу відправки даних від відправника до сервера;
- на Фігурі 4 представлена блок-схема процесу, який має місце у одержувача та даного сервера у відповідь на електронну пошту, яка отримується від сервера.

Тепер звертаючись до фігур 1 і 2 побачимо, що на них представлено функціонування системи одного з варіантів виконання даного способу шифрування та передачі даних між відправником і одержувачем за допомогою використання мережі. Звертаючись до малюнків, побачимо, що дана система функціонує для виконання шифрування та передачі даних між апаратним засобом відправника 100 і апаратним засобом одержувача 200.

У цьому прикладі, апаратні засоби відправника 100 містять комп'ютер 101, який з'єднується з клавіатурою 107, джерело даних 108 і зовнішній прилад відображення 105. Джерело даних може містити один зі зчитуючих пристроїв з диску або наскрізне з'єднання з бібліотекою даних, джерело даних, яке зберігає дані, які повинні бути передані до одержувача. Комп'ютер 101 має загальну шину доступу 106, з'єднану з мікропроцесором 102, пам'ять 103, інтерфейс відображення 104, інтерфейс вхідного пристрою 109 і один з веб-браузерів 110 для приєднання до Internet мережі через з'єднання 111.

Інтерфейс відображення 104 приєднується до зовнішнього приладу відображення 105 в той час як вхідний прилад інтерфейсу 109 приєднується до клавіатури 107 і джерела даних 108. Звичайно, пам'ять 103 зберігає ідентифікаційний код відправника та пароль відправника, хоч все це може бу-

ти введене через клавіатуру 107 у відповідь на показ підказки на приладі відображення 105.

У цьому прикладі, апаратні засоби одержувача 200 містять деякий мобільний телефон, який має можливість доступу до Internet мережі за допомогою веб-браузера 210, який виконує приєднання до Internet мережі через з'єднання 211.

Деталі того, як таке з'єднання встановлюється добре відомі спеціалістам в даній галузі і тому не буде описуватися в даній заявці. Даний веб-браузер приєднується до загальної шини доступу 206, яка приєднується до мікропроцесору 202, пам'яті 203, інтерфейсу відображення 204 і інтерфейсу вхідного пристрою 209. Інтерфейс відображення 204 приєднується до інтегрального приладу відображення 205 в той же час інтерфейс вхідного пристрою 209 приєднується до інтегральної клавіатури 207. Пам'ять 203 зазвичай зберігає, ідентифікаційний код одержувача та пароль одержувача, хоча все це може бути введене за допомогою клавіатури 207 у відповідь на показ підказок на приладі відображення 205. Окрім цього апаратний засіб 200 містить електронну пошту користувача 212 для відправки та отримання електронної пошти через з'єднання 213 до Internet мережі.

Сервер 300 також приєднується до Internet мережі через з'єднання 302. Докладна блок-схема структури сервера показана на фігурі 2. Ця структура сервера буде пояснена в комбінації з описом дії системи даного винаходу. Як видно завдяки фігурі 1 і фігурі 2 перед використанням даної системи, як відправник, так і одержувач з самого початку проходять реєстрацію на сервері 300 та їх деталі зберігаються в модулі бази даних сервера 306. В іншому варіанті виконання даного винаходу інформація, яка зберігається, включає щонайменше ідентифікаційний код і пароль для кожного відправника і одержувача.

Відправник має намір передати дані, які утримуються в джерелі даних 108 до одержувача. Для того, щоб відправник передав дані відправнику потрібно знати ідентифікаційний код одержувача і веб-адрес сервера 300. Ця інформація може зберігатися в пам'яті 103 відправника або може бути введена вручну за допомогою клавіатури 107 у відповідь на підказки на приладі відображення 105.

Як показано на фігурі 2, сервер 300 містить веб-сервер 301, який приєднується до Internet мережі через зв'язок 302. Веб-сервер приєднується до вхідної шини 303 і управляється мікропроцесором 304. Коли відправник звертається за веб-адресою сервера, то захищена лінія, як наприклад лінія з протоколом захищених з'єднань (SSL - Secure Sockets Layer - протокол захищених з'єднань) встановлюється, деталі чого добре відомі спеціалістам в даній галузі техніки. Мікропроцесор 304 не дозволяє організувати доступ до даної системи відправнику, поки не буде завершена перевірка пароля модулем 305 в поєднанні з доступом до модуля бази даних 306. Подробиці таких перевірок пароля добре відомі спеціалістам в даній галузі техніки і отже не описуються в даній заявці.

Після завершення перевірки пароля інформація, яка відображається на екрані, посиляється сервером 300 до відправника. Для завершення

цього тесту, відправник посилає до сервера підтвердження ідентичності ідентифікаційного коду одержувача разом з даними, які потрібно передати, та які отримуються з джерела даних 108. Ці вхідні дані обробляються за допомогою модулів у напрямку до верхнього краю даної фігури.

При отриманні ідентифікаційного коду одержувача та даних, які потрібно відправити, мікропроцесор 304 сервера направляє дані до модулю генератора коду підтвердження дійсності повідомлення 307. Як відомо спеціалістам в даній галузі такий генератор виробляє частину коду, який вираховується за допомогою використання частини або повних даних в комбінації з криптографічним алгоритмом представлення повідомлення в стислій формі. У даному випадку використовується відомий хеш-алгоритм повідомлення в стислій формі для того, щоб генерувати значення хеш-функції повідомлення в стислій формі з даних. Значення хеш-функції повідомлення в стислій формі направляється до електронної пошти користувача 312, приєднаної до Internet мережі через лінію 316 таким чином, щоб бути готовим для обробки в частину електронної пошти.

Отримані дані стискаються в модулі 308 перед тим, як здійснюється шифрування модулем 309, який використовує ключ сеансу, отриманий від модуля 310. Як відомо спеціалістам в даній галузі ключ сеансу генерується за допомогою генератора випадкового числа 311. Цей ключ сеансу є спеціальним до цих даних і відповідної передачі, таким чином, завдяки чому він стає спеціальним ключем шифрування передачі. Зашифровані дані послідовно перенаправляються до електронної пошти користувача 312 у готовому вигляді для обробки в частину електронної пошти.

Також ключ сеансу від модуля 310 шифрується в модулі 313 за допомогою відкритого ключа одного з способів шифрування відкритим/секретним ключем шифрування, наприклад, шифрування методом RSA, який добре відомий спеціалістам в даній галузі. Відповідно, окрім цього результат від модуля 313 шифрується в модулі 314 за допомогою Blowfish алгоритму, який приєднує пароль одержувача, який отримується з бази даних 306. Цей пароль є результатом відповідно до ідентифікаційного коду одержувача, направлено від мікропроцесору на шину 315. Зашифрований ключ сеансу направляється до електронної пошти користувача 312 у готовому вигляді для обробки в частину електронної пошти.

Електронна пошта користувача 312 обробляє значення хеш-функції повідомлення в стислій формі, зашифровані дані та зашифрований ключ сеансу відомим чином для створення електронної пошти, яка потім посилається на відповідну адресу одержувача, що забезпечується мікропроцесором на шині 315 з наступним доступом до бази даних 306. Відомим способом користувач електронної пошти розміщує унікальну мітку до електронної пошти та, таким чином реєструє відправку. Підтвердження відправки електронної пошти також відправляється до відправника або за допомогою веб-сервера 301 або електронної пошти користувача 312.

Електронна пошта, що відправляється за допомогою сервера 300, може бути отримана звичним чином електронною поштою користувача 212 мобільного телефону 200. Зміст електронної пошти приводить одержувача у стан готовності передачі даних за допомогою системи даного винаходу, або автоматично приводить у дію веббраузер 210, щоб ініціювати лінію зв'язку з сервером 300. В усякому випадку під управлінням мікропроцесору 202, одержувач встановлює зв'язок з веб-адресою сервера та встановлюється захищена лінія наприклад, така як лінія з протоколом захищених з'єднань, причому деталі цього добре відомі спеціалістам в даній галузі техніки. Мікропроцесор 304 сервера не дозволяє доступ до даної системи, поки не буде завершена перевірка пароля модулем 305 в поєднанні з доступом до модуля бази даних 306. Подробиці таких перевірок пароля добре відомі спеціалістам в даній галузі та, таким чином, не описуються в даній заявці.

Тільки після успішного завершення перевірки пароля, зашифровані дані, зашифрований ключ сесії та значення хеш-функції стислої форми повідомлення, які містяться в електронній пошті відправляються по захищеній лінії до сервера 300 через веб-сервер 301. Все це виконується за допомогою модулів в напрямку до нижнього краю фігури.

Зрозуміло, якщо вибраний спосіб відправки та зчитування електронної пошти виконується за допомогою веб-пошти, то тоді нема потреби в окремій електронній пошті користувача 213.

Завдяки чому при прийманні, даний мікропроцесор 304 сервера перенаправляє зашифрований ключ сесії до модуля 320, який застосовує зворотній Blowfish алгоритм в комбінації з паролем одержувача, який отримується від бази даних 306 завдяки шині 315 відповідно до ідентифікаційного коду одержувача. Окрім цього даний результат від модуля 320 розшифровуються в модулі 321 за допомогою секретного ключа шифрування по способу RSA, використаного для відправки даних. За допомогою цих модулів відтворюється первинний ключ сеансу модуля 310.

Отримані зашифровані дані, які знаходяться в стисnutій формі розшифровуються в модулі 323 за допомогою розшифрованого ключа сеансу до виконання розвороту в модулі 324.

Як в модулі 307, генерується одне із значень хеш-функції стислої форми повідомлення в модулі 325 з розшифрованих і розвернутих даних та під управлінням мікропроцесору 304, при чому модуль 326 проводить порівняльну перевірку для підтвердження відповідності заново генерованого значення хеш-функції стислої форми повідомлення значенню хеш-функції стислої форми повідомлення, яке отримується від одержувача, для того щоби гарантувати збіг.

Допускаючи, що значення хеш-функції стислої форми повідомлення правильним чином підтверджується на відповідність в модулі 326, то розшифровані дані від модуля 324 відправляються назад до одержувача через захищену лінію.

На фігурі 3 представлена блок-схема завдяки чому демонструються процеси, які мають місце у даного відправника та на сервері відповідно до

даного винаходу при відправці даних від відправника до сервера.

Спочатку відправник бажає передати спеціальні дані до конкретного одержувача, маючи відомий ідентифікаційний код одержувача. На етапі S1A, відправник встановлює зв'язок з сервером, роблячи спробу встановити захищену лінію зв'язку, наприклад, лінію яка використовує протокол захищених з'єднань. Встановлення даної лінії містить виконання конкретних протоколів зв'язку та вищезгаданої перевірки пароллю та може мати місце у вигляді відображення веб-сторінки на приладі відображення 105, вводу відповідних даних реєстрації на веб-сторінці і такого іншого. Як згадувалося раніше, встановлення такої лінії зв'язку та організація перевірки пароллю добре відомі спеціалістам в даній галузі тому не буде детально описуватися в даній заявці.

Сервер у відповідь на встановлення зв'язку зі сторони відправника, також пробує на етапі S1B установити лінію зв'язку за допомогою виконання відомих протоколів зв'язку та вищезгаданої перевірки пароллю. Потім на етапі S2B сервер буде виконувати контроль для того, щоб переконатися чи дійсна лінія була встановлена, тобто, чи всі протоколи зв'язку були узгоджені і чи всі перевірки пароллю були виконані. Якщо лінія не була встановлена, або перевірка пароллю показала його невідповідність, тоді сервер приходить до помилки при виконанні етапу S3B. Такий етап може включати подальші спроби установити лінію зв'язку. Допускаючи, що дійсна лінія зв'язку встановлена, то тоді процес пересувається до етапу S4B тобто чекання прийому ідентифікаційного коду одержувача та даних, які потрібно передати. Якщо потрібно в цей момент можна включити етап закінчення часу очікування.

У відправника, перевірка виконується на етапі S2A для того, щоб також переконатися чи дійсна лінія була встановлена, тобто, чи всі протоколи зв'язку були узгоджені та чи всі перевірки пароллю на відповідність були виконані. Якщо лінія не була встановлена або перевірка пароллю показала його невідповідність, то, тоді при виконанні етапу S3A відправник приходить до помилки. Такий етап може включати подальші спроби установлення лінії зв'язку. Допускаючи, що дійсна лінія зв'язку встановлена, процес переходить до етапу S4A для того, щоб виправити ідентифікаційний код одержувача та дані, які підлягають передачі. Якщо потрібно в цей момент можна включити етап закінчення часу очікування.

Як один з прикладів, веб-сторінка даних передачі відображається на приладі відображення 105, який потребує вводу ідентифікаційного коду одержувача та приєднання даних, наприклад, файлу, який розміщується в джерелі даних 108. Потім заповнена сторінка даних передачі відправляється до сервера 300. Вочевидь, що дані, які потрібно зашифрувати можуть бути введені безпосередньо в сторінку передачі даних.

Зміст сторінки передачі даних отримується сервером 300 на етапі S4B, після чого процес переходить до етапу S5B. На цьому етапі сервер виробляє значення хеш-функції стислої форми повідомлення, яке є унікальним до даних і направ-

ляє значення до електронної пошти користувача 312, після чого процес переходить до етапу S6B.

На етапі S6B, дані стискаються, наприклад, за допомогою упаковування. Потім, на етапі S7B отримується випадкове число від генератора випадкового числа 311 для того, щоб генерувати ключ сеансу, який є спеціальним для цієї передачі даних. Потім на етапі S8B, дані шифруються цим ключем сеансу і зашифровані дані направляються до електронної пошти користувача 312.

Потім процес переходить до етапу S9B, на якому ключ сеансу зашифрується, за допомогою відкритого ключа способом RSA. Після цього процес переходить до етапу S10B для того, щоб відновити пароль одержувача, після якого, на етапі S11B результат етапу S9B шифрується за допомогою Blowfish алгоритму, використовуючи пароль, який відновлюється на етапі S10B. Потім даний результатуючий зашифрований ключ сеансу направляється до електронної пошти користувача 312.

У наступному етапі S12B, електронна пошта формується відомим чином за допомогою електронної пошти користувача 312 у відповідний формат для передачі за допомогою протоколу HTML (HyperText Markup Language - мова HTML), наприклад, за допомогою шифрування за способом base 64. Також можна мати прикладений HTML файл або лінійний HTML код для зашифрованих даних і зашифрованого ключа сеансу. Потім електронна пошта відправляється та при цьому відправка електронної пошти реєструється звичайним шляхом і відправляється підтвердження до відправника після чого процес закінчується.

Зрозуміло, що електронна пошта містить значення хеш-функції стислої форми повідомлення, зашифровані дані та зашифрований ключ сеансу переважним чином як приховані поля. Також переважним чином дана електронна пошта включає HTML лінію, щоб дати можливість одержувачу приєднатися назад до сервера. Дана лінія формується таким чином, щоб автоматично приєднати приховані поля в HTML вигляді назад до сервера. Предметний заголовок електронної пошти є предметним заголовком, який вибирається відправником та електронна пошта адресується до електронного адресу одержувача.

На етапі S5A відправник отримує підтвердження відправки електронної пошти і закінчення процесу.

На фігурі 4 представлена блок-схема, яка показує процеси, які мають місце у одержувача та на сервері у відповідь на електронну пошту отриману від сервера.

На етапі S101A одержувач 200 отримує електронну пошту від сервера, яка містить, між іншими речами, зашифровані дані, зашифрований ключ сеансу та значення хеш-функції стислої форми повідомлення. Електронна пошта може бути завантажена або за допомогою електронної веб-пошти або за допомогою електронної пошти користувача 212 через лінію 213. На етапі S102A одержувач відкриває електронну пошту і встановлює зв'язок з сервером в спробі встановлення захищеної лінії зв'язку, наприклад, лінії з протоколом захищених з'єднань. До певної міри подібно до того, що описано вище, встановлення даної лінії містить вико-

нання конкретних протоколів зв'язку та перевірку паролю подібно до того, що обговорювалась вище відносно модулю 305, причому може прийняти форму відображення веб-сторінки на приладі відображення 105, введення відповідних даних реєстрації на веб-сторінці та таке інше. Як згадувалося раніше, встановлення лінії зв'язку та організація перевірки пароля добре відомі спеціалістам в даній галузі і не буде детально описуватися в даній заявці.

Сервер у відповідь на встановлення зв'язку зі сторони одержувача, на етапі S101B також намагається встановити лінію зв'язку за допомогою виконання певних протоколів зв'язку та вищезгаданої перевірки паролю. Потім даний сервер на етапі S102B робить перевірку для того, щоб впевнитися, чи дійсна лінія була встановлена, чи всі протоколи зв'язку були відповідними та, чи всі перевірки пароля були виконані. Якщо лінія не була встановлена або перевірка паролю була не задовільною, то сервер приходить до помилки при виконанні етапу S103B. Такий етап може включати подальші спроби установлення лінії зв'язку. Допускаючи, що дійсна лінія зв'язку встановлена, процес переходить до етапу S104B чекання прийому ідентифікаційного коду одержувача та іншої інформації, включаючи зашифровані дані, зашифрований ключ сеансу і значення хеш-функції стислої форми повідомлення. Якщо потрібно в цей момент можна включити етап закінчення часу очікування.

У одержувача перевірка виконується на етапі S103A, щоб також впевнитися чи дійсна лінія була встановлена, чи всі протоколи зв'язку були відповідними та, чи всі перевірки пароля були пройдені. Якщо лінія не була встановлена, або перевірка паролю була незадовільною, то відправник приходить до помилки при виконанні етапу S104A. Такий етап може включати подальші спроби встановлення лінії зв'язку. Якщо потрібно в цей момент можна включити етап закінчення часу очікування.

Допускаючи, що лінія зв'язку встановлена, то процес переходить до етапу S105A для відправки ідентифікаційного коду одержувача та іншої інформації, яка згадується в попередньому параграфі. Останнє може бути в формі прихованих HTML полів в електронній пошті, які пропонуються серверу 300.

Зрозуміло, що протокол розподілу в часі та компоновки відправки ідентифікаційних кодів, прихованих полів, паролів і такого іншого може змінюватися для того, щоб відповідати вимогам окремих ситуацій.

Потім процес на сервері переходить до етапу S105E, щоб відновити пароль одержувача від модуля 306 після чого, на етапі S106B зашифрований ключ сеансу розшифровується за допомогою Blowfish алгоритму, використовуючи відновлений пароль на етапі S105B. Потім процес переходить до етапу S107B де має місце розшифрування за методом RSA на якому результат етапу S106B розшифровується, використовуючи секретний ключ сервера. Це закінчується ключем сеансу, який треба синтезувати.

Після цього, процес переходить до етапу S108B, в якому все ще стиснуті дані розшифровуються за допомогою розшифрованого ключа сесії,

який синтезується на етапі S107B. Після цього, даний процес переходить до етапу S109B для розпакування даних.

На наступному етапі S110B, сервер виробляє значення хеш-функції стислої форми повідомлення, яке є унікальним до даних етапу S109B. З цього часу на етапі S111B значення хеш-функції стислої форми повідомлення від етапу S110B звіряється зі значенням хеш-функції стислої форми повідомлення отриманого на етапі S104B. Допускаючи, що значення хеш-функції стислої форми повідомлення підтверджується, то процес переходить до виконання етапу S113B і тепер незашифровані дані відправника направляються до одержувача через захищену лінію. Відправка цих даних реєструється та процес закінчується. Якщо значення хеш-функції стислої форми повідомлення не може бути підтверджене, то процес приходить до помилки при виконанні етапу S112B. Це може включати реєстрацію помилки та відправки повідомлення про помилку одержувачу для того, щоб вказати, що дані, можливо, були зіпсовані або компрометовані.

На етапі S106A одержувач, отримує незашифровані дані та процес закінчується.

В одному з варіантів виконання даного винаходу, який описується вище, повний процес шифрування і розшифрування проводиться на сервері 300. Таким чином, відправнику і одержувачу не потрібне ніяке спеціальне програмне забезпечення, яке може захищеним чином відправляти або отримувати дані.

Зокрема, не потрібно мати програмне забезпечення або використовувати апаратну пам'ять і ресурси обробки, щоб дати можливість шифрувати за допомогою способу RSA і Blowfish. Крім того, доступ до паролів підтримується на сервері та не має потреби підтримуватися у відправника. Більш того, оскільки шифрування та розшифрування має місце на сервері, спеціальні заходи, необхідні для шифрування та розшифрування непотрібні відправнику або одержувачу.

Однак, даний винахід також включає альтернативу функціям, які знаходяться всередині рамки 317 фігури 2 причому, які забезпечуються у відправника. Тобто, у даному варіанті генерація ключа сесії генератором послідовності випадкових чисел і упаковка даних та шифрування упакованих даних ключем сеансу цілком ведеться у відправника. Однак, захищена лінія встановлюється з сервером, як вказано вище, але в цьому випадку тільки зашифрований - ключ сеансу, який генерується, відправляється до сервера. Після подібної перевірки паролю, як вказано вище, модулі S313 і S314 знову генерують зашифрований ключ сеансу, який в цьому випадку повертається відправнику. Зашифровані дані, зашифрований ключ сеансу та значення хеш-функції потім доставляються користувачу електронної пошти відправника (не показано), який також приєднується до Internet мережі. Цей користувач електронної пошти створює електронну пошту, як вказано вище до відправки її одержувачу. Отже, як можна побачити етапи з S5B до S8B на фігурі 3 в даний момент мають місце у відправника. Це може зменшити обробку даних по вимозі, які розміщені на сервері.



Одержувач отримує електронну пошту в свого користувача електронної пошти та може обробити дану електронну пошту, як зображено на фігурі 4.

Однак, даний винахід також включає альтернативу функціям, які знаходяться всередині рамки 322 фігури 2, які забезпечуються у одержувача, як тільки отримується електронна пошта від сервера. Тобто, в даному варіанті розшифровка даних розпакування даних, генерування значення хеш-функції стислої форми повідомлення та її підтвердження ведеться цілком у одержувача. Однак, захищена лінія встановлюється з сервером, як вказано вище, але в цьому випадку тільки зашифрований ключ сеансу відправляється до сервера. Після подібної перевірки паролю, як вказано вище, модулі S320 і S321 знову розшифровують ключ сеансу, який в цьому випадку повертається одержувачу. Зашифровані дані розшифровуються за допомогою розшифрованого ключа сеансу, розпаковуються, генерується значення хеш-функції стислої форми повідомлення та перевіряється на відповідність значенню хеш-функції стислої форми повідомлення, яка була отримана електронною поштою. Отже, можна побачити, що етапи з S108B до S113 на фігурі 4 в даний момент мають місце у одержувача. Це може зменшити обробку даних по вимозі, які розміщені на сервері.

Спеціалістам в даній галузі техніки зрозуміло, що обидва варіанти, які згадуються вище, можуть бути здійснені одночасно. Проте, відповідно до даного винаходу, шифрування ключа сеансу в комбінації з паролем одержувача має місце на сервері.

Спеціалістам в даній галузі техніки зрозуміло, що група користувачів може бути зареєстрована для отримання електронної пошти, коли у цьому буде потреба. Наприклад, відділ, який відповідає за інформаційні технології на фірмі може зареєструвати всіх службовців. У даному випадку якщо трапиться так що перевірка пароля не буде завершена успішно на сервері, то посилання до інших паролів в тій групі може бути прийнята до уваги.

В одному з варіантів втілення винаходу потреба встановлення спеціального програмного забезпечення для відправника або одержувача, як відомо спеціалістам в даній галузі техніки, може бути виконана шляхом завантаження з сервера протягом процесу реєстрації та подальшого встановлення відповідним чином.

Спеціалістам в даній галузі техніки зрозуміло, що оскільки правильний пароль одержувача вимагається для розшифрування даних за допомогою Blowfish алгоритму та правильність розшифрування ефективно перевіряється за допомогою підтвердження значення хеш-функції стислої форми повідомлення, то можна звільнити від перевірки паролю протягом зв'язку між одержувачем і сервером на етапі 102A, якщо в цьому буде потреба.

Спеціалістам в даній галузі техніки зрозуміло, що, якщо розшифрування мало успіху, то сервер 300 може бути організованим таким чином, щоб можна було проводити подальші перевірки з ціллю одержання правильного паролю, наприклад, за допомогою перегляду старих паролів одержувача та в свою чергу спроб кожного разу розшифрування даних. У випадку якщо один з тих паролів

виробляє правильне значення хеш-функції стислої форми повідомлення, то тоді розшифрування буде успішним. Однак, якщо ні один з тих паролів не спрацює, то тоді одержувач не є призначеним одержувачем або дані були зіпсовані під час передачі.

Якщо одержувач не має пароля та при цьому ще не є зареєстрованим на сервері 300, то тоді сервер може генерувати один разовий пароль, який відправляється даному одержувачу будь-якими захищеними засобами, які відповідають цьому, наприклад за допомогою наступного: безпечної пошти або захищеної лінії або захищеною електронною поштою, при цьому, вимагаючи від користувача зміни свого паролю на захищений пароль, який буде використовуватися після того.

Завдяки даному винаходу ідентичність як відправника так і одержувача може бути встановлена так, що відправник може відправляти дані одержувачу, який не має спеціального програмного забезпечення, яке встановлюється для того, щоб одержувач був впевненим щодо походження даних. Крім того, спроби шифрування та розшифрування реєструються, що може дозволити відправнику перевірити чи отримав і розшифровував одержувач дані та може дозволити одержувачу перевірити, чи були послані вже дані, які вони очікують отримати.

Апаратні засоби відправника і одержувача можуть бути різними, наприклад, не претендуючи на винятковий перелік, це може бути наступне: комп'ютер, пристрій для зберігання особистих даних або інші кишенькові пристрої, переносний комп'ютер, мобільний телефон. Переважним чином як сервер використовують комп'ютер, хоча це може бути також щось інше, альтернативне до обчислювальної машини.

Спеціалістам в даній галузі техніки зрозуміло, що завдяки даному винаходу ні відправник, ні одержувач не обізнані з паролем іншого, оскільки всі ці дані утримуються на сервері. Отже, рівень безпеки, яка вимагається відправником і одержувачем не такий високий, як інші відомі види передачі даних захищеним чином.

Завдяки даному винаходу сервер обслуговує спеціальну інформацію одержувача, наприклад, таку як пароль, який використовується сервером в процесі шифрування. Сервер отримує цю інформацію зі сховища даних, яке має список ідентифікаційний кодів одержувача та спеціальну інформацію одержувача, яка містить секрет. Спеціальна інформація одержувача може містити пароль, фразу проходу, особистий кодовий номер, значення хеш-функції або будь-яку іншу інформацію, яка може використовуватися для перевірки ідентичності.

Мережа, яка використовується з даним винаходом, це може бути Internet мережа, місцева Intranet мережа, наприклад, така як Ethernet мережа, телефонна мережа, радіомережа, або будь-який інший тип мережі для передачі даних. Переважним чином, коли використовується Internet мережа, то використовується захищений SSL зв'язок (SSL -Secure Sockets Layer - протокол безпечних з'єднань) між сервером і відправником і/або між сервером і одержувачем.

Відправник і одержувач можуть бути ідентифіковані сервером за допомогою своїх адрес електронної пошти (або іншими мережевими адресами). Однак, вони можуть також мати ідентифікаційні коди користувача, які не пов'язані з їх мережевими адресами. Даний сервер може мати список мережових адресів у своїй базі даних, і/або він може мати список ідентифікаційних кодів користувачів, де кожна мережева адреса і/або ідентифікаційний код користувача є пов'язаним з секретною спеціальною інформацією одержувача.

В одному з варіантів даного винаходу, сервер 300 може містити секретний код, унікальний для даного сервера та відомий тільки даному серверу. Цей секретний код може бути включеним в модулі, які виконують шифрування та розшифрування за Blowfish методом. Секретний код може використовуватися в шифруванні на додаток до використання спеціальної інформації одержувача. Ці дві частини інформації можуть просто бути об'єднані для того, щоб використовуватися в процесі шифрування. Використання секретного ключа забезпечує підвищений рівень безпеки даної системи.

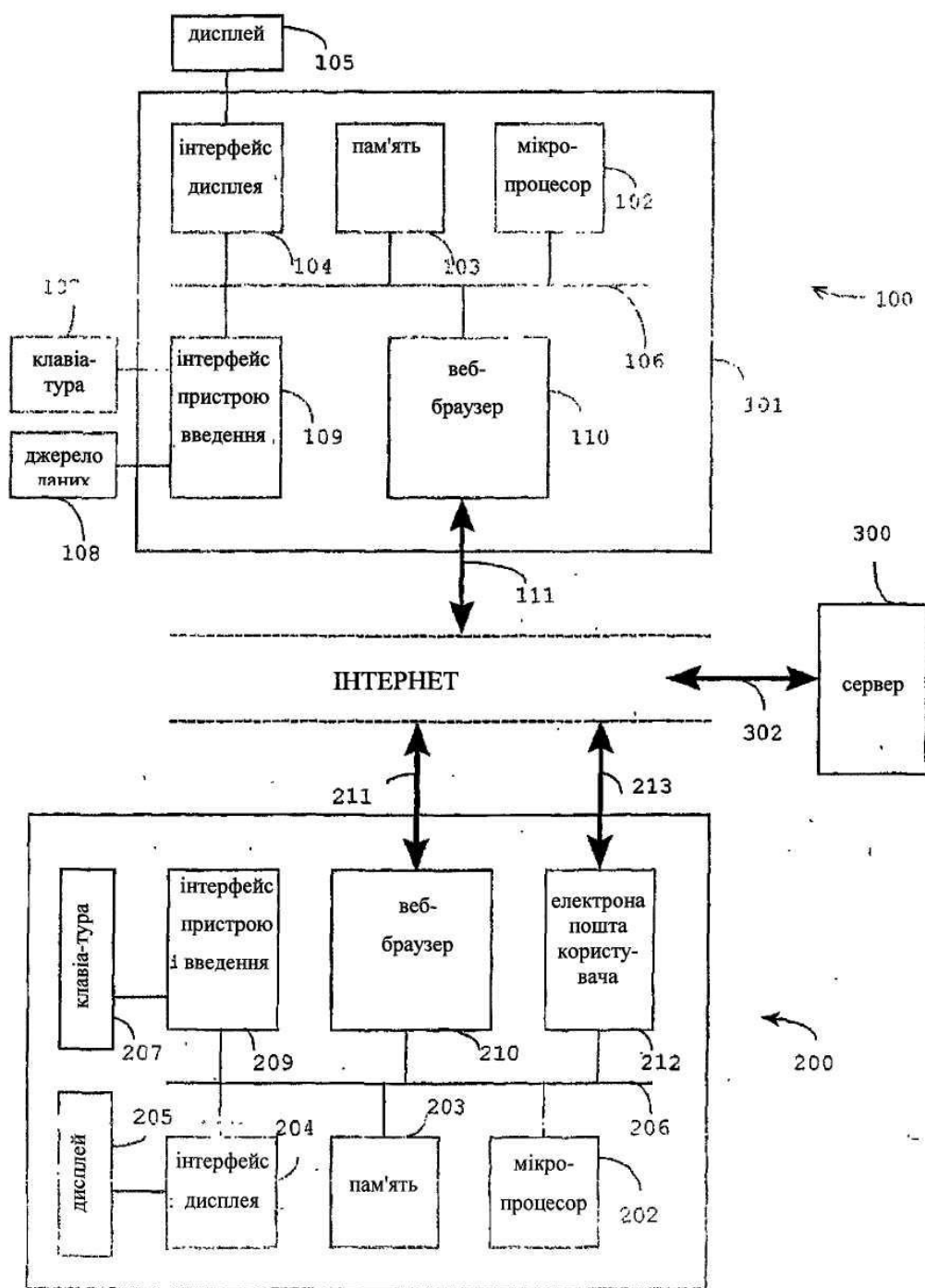
Спеціалістам в даній галузі техніки зрозуміло, що не потрібно зберігати ключ сесії на сервері або зберігати будь-які дані, які повинні бути відправлені одержувачу. Вони можуть зберігатися в енергозалежному запам'ятовуючому пристрої на сервері,

та перезаписуватися тоді, коли додаткові дані та ключі будуть зашифровані. Це має перевагу, яка полягає в тому, що даному серверу не потрібно мати велику кількість пам'яті, доступної для збереження старих і можливо надлишкових даних і/або ключів.

Канал передачі може містити середовище передачі, наприклад, таке як електричне середовище, оптичне середовище, використовувати мікрохвилі, радіочастоти, електромагнітне середовище, звукові або магнітні сигнали (тобто TCP-IP сигнал через IP мережу, наприклад, як через Internet мережу), або несуче середовище, наприклад, таке як дискета, постійний запам'ятовуючий пристрій на компакт-диску, жорсткий диск, або прилад із програмованою пам'яттю.

Викладені вище приклади втілення даного винаходу треба розглядати як переважний варіант виконання, при чому спеціалістам в даній галузі техніки відомо, що різні зміни можуть бути зроблені в межах суті, а також об'єму даного винаходу, який визначається прикладеною формулою винаходу.

Подібним чином, банки можуть розповсюджувати деталі платежів, які поступають до їхніх користувачів, які можуть просто приєднуватися до сервера, як описано вище для того, щоб отримати такі деталі, які розповсюджуються захищеним чином.



Фіг. 1

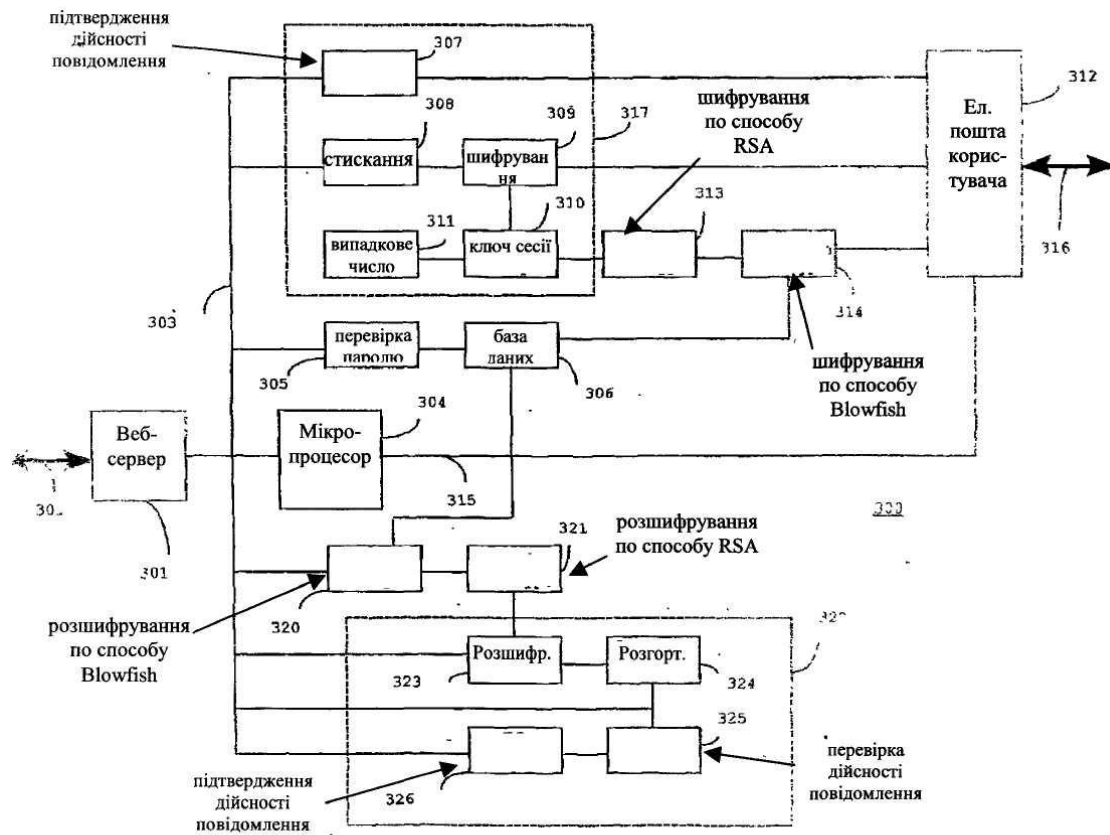
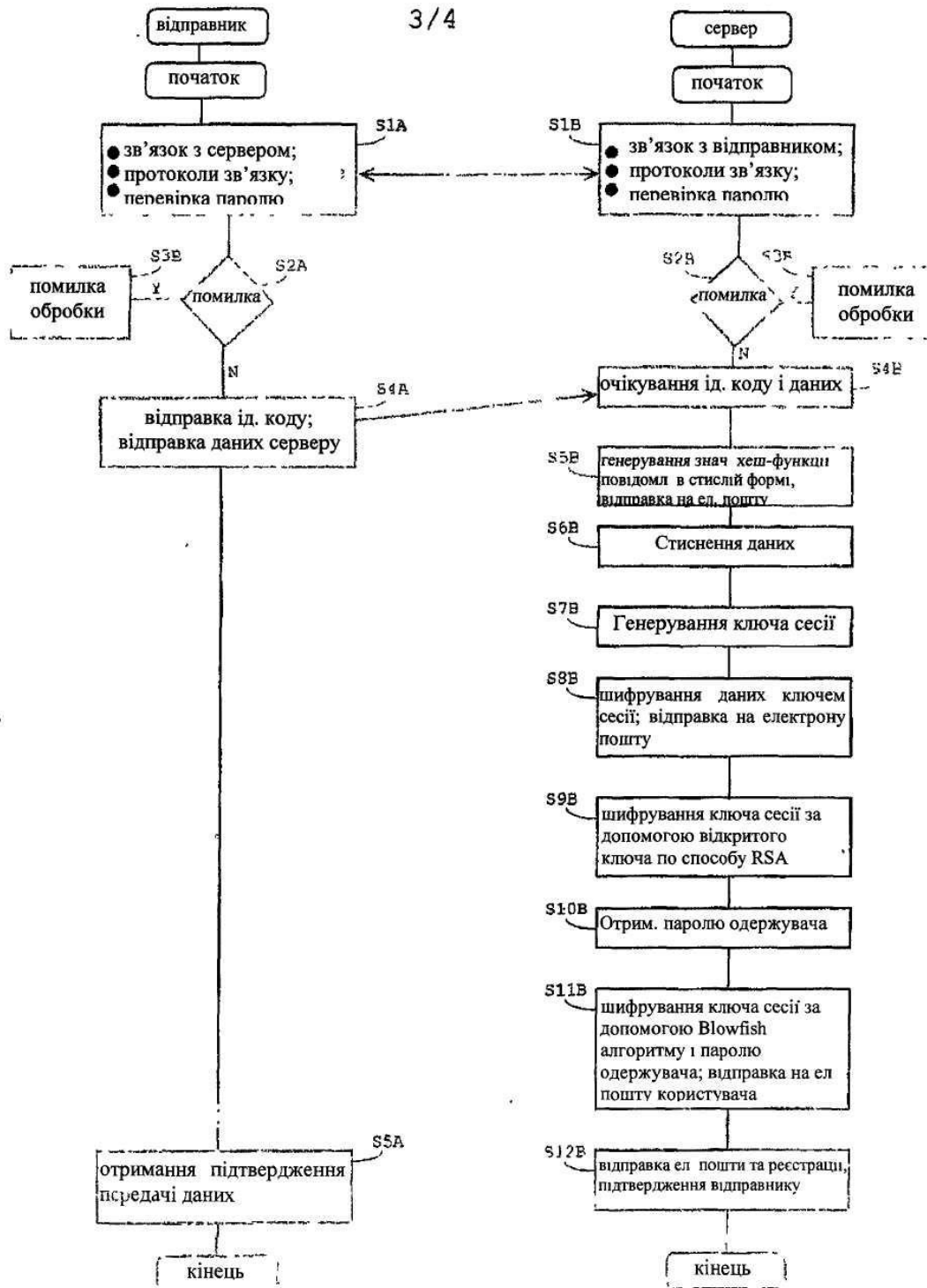


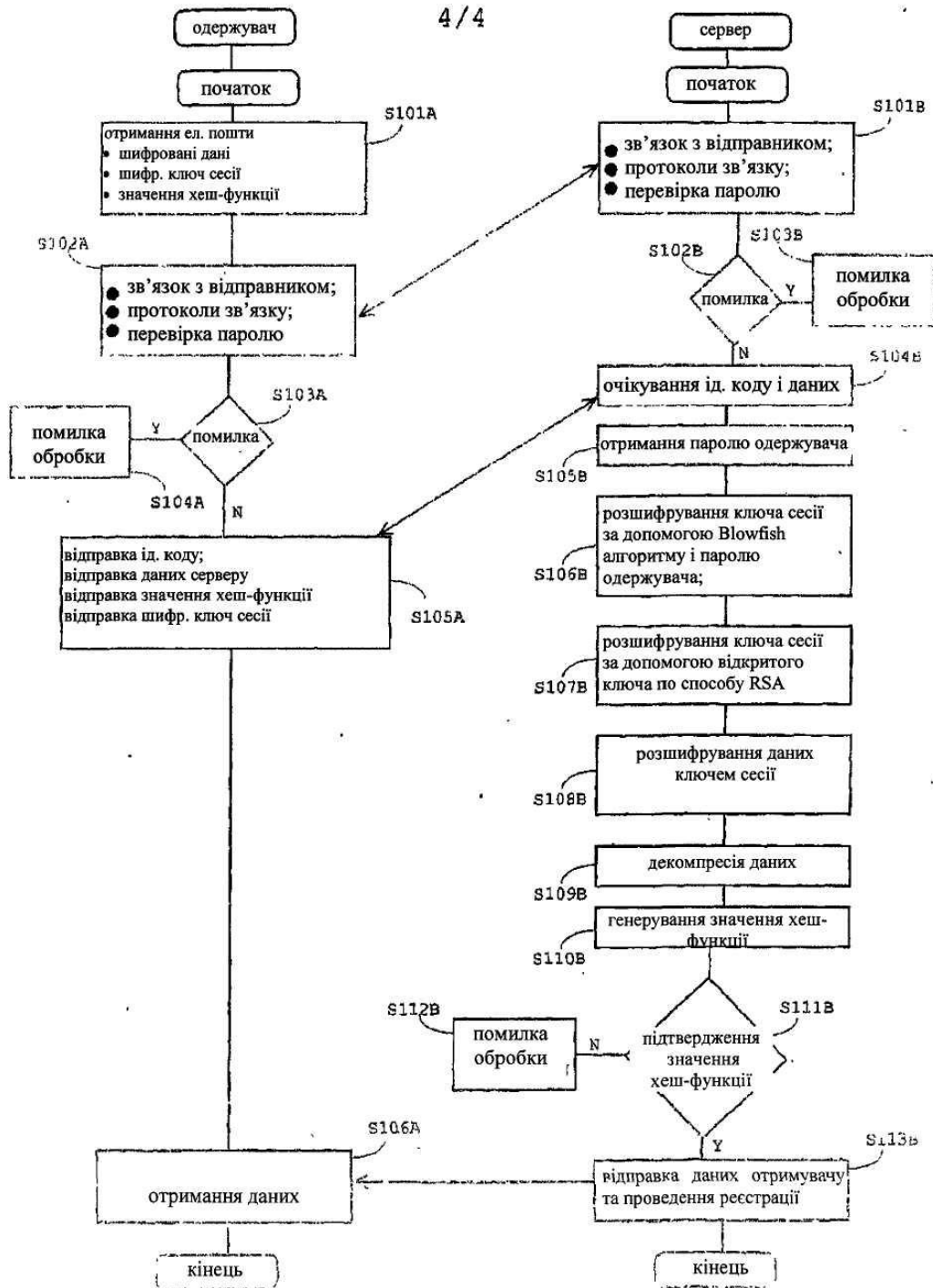
Fig. 2

3/4



Фіг. 3

4 / 4



Фіг. 4