



ДЕРЖАВНА СЛУЖБА
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ
УКРАЇНИ

УКРАЇНА

(19) **UA**

(11) **110814**

(13) **U**

(51) МПК

H04M 1/68 (2006.01)

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2016 03390**

(22) Дата подання заявки: **01.04.2016**

(24) Дата, з якої є чинними
права на корисну
модель: **25.10.2016**

(46) Публікація відомостей
про видачу патенту: **25.10.2016, Бюл.№ 20**

(72) Винахідник(и):

**Османкіна Ганна Олегівна (UA),
Воробйов Андрій Васильович (UA)**

(73) Власник(и):

**Османкіна Ганна Олегівна,
вул. Молодіжна, 22, с. Базаліївка,
Чугуївський р-н, Харківська обл., 63531
(UA),
Воробйов Андрій Васильович,
пров. Електроінструментальний, 6-б, м.
Харків, 61070 (UA)**

(54) СПОСІБ ПІДВИЩЕННЯ ЗАХИСТУ ДАНИХ В ІР-ТЕЛЕФОНІЇ ДЛЯ ОРГАНІЗАЦІЇ ЗАХИЩЕНОЇ ЛІНІЇ ЗВ'ЯЗКУ МІЖ ФІЛІЯМИ ПІДПРИЄМСТВА

(57) Реферат:

Спосіб організації захищеної лінії ІР-телефонії для зв'язку між філіями підприємства полягає в тому, що голосові дані з виходу вокодера шифрують. Дані після вокодера передаються на вхід симетричного блочного шифру, де шифруються за допомогою унікального ключа, а потім шифруються протоколом SRTP. При цьому у відправника і приймаючої сторони повинен бути один і той же ключ, яким філії підприємства обмінюються заздалегідь, та яким прийняті зашифровані дані з виходу протоколу SRTP розшифровуються і передаються на вхід декодера голосових даних.

UA 110814 U

Корисна модель належить до галузі інформаційних мереж, а саме до області передачі голосових даних по комп'ютерних мережах. Дана модель може використовуватися для підвищення захисту даних, що передаються за допомогою IP-телефонії.

Для захисту конфіденційних переговорів та мінімізації можливості попадання конфіденційної або комерційної інформації до рук зловмисника в IP-телефонії, найчастіше застосовують два типу протоколів, оскільки для здійснення дзвінка клієнт і сервер попередньо обмінюються службовими даними для встановлення з'єднання. Тому як засіб захисту службових даних IP-телефонії використовують протокол TLS (Transport Layer Security) і протокол SRTP (Secure Real Time Protocol) для захисту голосового трафіку.

TLS - криптографічний протокол, що забезпечує захищену передачу даних між вузлами в мережі, є стандартним методом для шифрування SIP-протоколу. TLS забезпечує конфіденційність і цілісність інформації, що передається, та здійснює аутентифікацію. Також протокол TLS забезпечує формування ключа сеансу для шифрування службових та голосових даних.

Протокол SRTP використовується в IP-телефонії для шифрування голосових даних. Для цього застосовується стандарт шифрування AES в потоковому режимі. Для шифрування даних використовується ключ сеансу, що ускладнює атаки повтору для зловмисників, які мають доступ до лінії зв'язку на ділянці між абонентами. Протокол SRTP вважається одним з кращих способів захисту IP-телефонії. Основна перевага цього протоколу - відсутність будь-якого впливу на якість зв'язку. Протокол SRTP може використовуватися як для конфіденційних, так і для звичайних дзвінків (з відключенням шифруванням).

Найбільш близьким до запропонованого технічним рішенням, вибраним як найближчий аналог, є організація зв'язку між абонентами на основі IP-телефонії, при якому голосові дані кодуються вокодером (метод стиску голосових даних з втратами інформації) та передаються до протоколу SRTP, де шифруються за допомогою стандарту AES та ключа сеансу.

Недоліком способу-найближчого аналога є те, що використання стандарту шифрування AES робить схему шифрування вразливою до атак з боку спеціальних підрозділів, які є розробниками цього стандарту та з великою вірогідністю мають спосіб його зламу. Крім того, зловмисник може зламати шифр, якщо якимось чином отримає ключ сеансу (наприклад за рахунок вразливостей протоколу TLS, програмних чи апаратних помилок при його реалізації, вразливостей протоколу аутентифікації тощо).

В основу корисної моделі поставлена задача створення методу, який був би позбавлений вищезгаданих недоліків способу-найближчого аналога.

Поставлена задача вирішується завдяки тому, що в схему обробки даних вводиться ще один метод шифрування (МШ). Це може бути симетричний блочний шифр, наприклад, оснований на мережі Фейстеля, або будь-який інший шифр, що задовольняє вимоги по швидкості шифрування даних в IP-телефонії. Цей шифр пропонується вбудувати в схему кодування даних між вокодером та протоколом SRTP (або іншим прийнятним протоколом, наприклад, SRTCP). Дані з вокодера передаються на МШ та кодуються за допомогою унікального ключа, після чого передаються на вхід протоколу SRTP. На приймальній стороні дані з виходу протоколу SRTP передаються на дешифрування МШ з використанням того ж самого унікального ключа, а потім на дешифрування вокодером. При використанні IP-телефонії для організації зв'язку між філіями одного підприємства є можливим одноразово забезпечити доставку цього унікального ключа на всі філії підприємства (наприклад, відповідальною особою з керівництва підприємства). Таким чином, цей ключ не буде передаватись по лініях передачі даних і є захищеним від викрадення.

Таким чином, запропонований спосіб організації зв'язку IP-телефонії між філіями підприємства дозволяє підвищити криптостійкість шифрування голосових даних, що передаються по лінії зв'язку.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Спосіб організації захищеної лінії IP-телефонії для зв'язку між філіями підприємства, який полягає в тому, що голосові дані з виходу вокодера шифруються, який **відрізняється** тим, що дані після вокодера передають на вхід симетричного блочного шифру, де їх шифрують за допомогою унікального ключа, а потім шифрують протоколом SRTP, при цьому відправник і приймаюча сторона мають один і той же ключ, яким філії підприємства обмінюються заздалегідь, та яким прийняті зашифровані дані з виходу протоколу SRTP розшифровують і передають на вхід декодера голосових даних.

Комп'ютерна верстка М. Мацело

Державна служба інтелектуальної власності України, вул. Василя Липківського, 45, м. Київ, МСП, 03680, Україна

ДП "Український інститут інтелектуальної власності", вул. Глазунова, 1, м. Київ – 42, 01601