УДК 004.773.6

О. Ю. Іохов

О. М. Сальніков

В. Т. Оленченко

О. М. Горбов

МЕТОДИКА ОРГАНІЗАЦІЇ СКРИТОГО ОБМІНУ ДАНИМИ В СИСТЕМІ ОПОВІЩЕННЯ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ НА БАЗІ GSM-ЗВ'ЯЗКУ

Розглянуто порядок використання загальнодоступних програмних та технічних засобів для скритого обміну даними у системі оповіщення Національної гвардії України на основі технологій віртуальної приватної мережі VPN та мобільного зв'язку стандарту GSM. Запропоновано методику організації скритого обміну даними у системі оповіщення НГУ.

Ключові слова: *система оповіщення, віртуальна приватна мережа, мобільний зв'язок GSM, безоплатні загальнодоступні програмні засоби, захищений обмін даними.*

Постановка проблеми. Ефективне функціонування будь-якого військового формування, у тому числі й Національної гвардії України (НГУ), неможливе без ефективної системи управління. Своєю чергою, функціонування системи управління забезпечується системою зв'язку та автоматизації управління. Як правило, у бойових умовах використовуються спеціальні засоби зв'язку та передачі даних, але у повсякденній діяльності, зокрема у системі оповіщення, частіше застосовуються загальнодоступні канали та засоби передачі даних, такі, як дротовий міський телефонний зв'язок та мережі мобільного зв'язку стандарту GSM.

Як відомо, однією з основних вимог до системи передачі даних є скритність.

Скритність – це здатність військового зв'язку зберігати в таємниці факт передачі та зміст інформації при її обміні, обробці, зберіганні та вирішенні інформаційних і розрахункових задач [1]. Іншими словами, скритність полягає у збереженні в таємниці від противника всіх заходів і дій, які здійснюють командири, штаби і підрозділи у період підготовки та у ході бойових дій [2].

Скритність досягається такими заходами, як [1]:

– обмеження доступу до інформації службових осіб;

– застосування засобів засекречування та дотримання правил їх експлуатації;

– виключення несанкціонованого доступу до інформації технічними (апаратними та програмними) й організаційними методами та заходами.

Виконання цих заходів в умовах застосування зв'язку стандарту GSM є утрудненим і практично неможливим.

Аналіз останніх досліджень і публікацій. Проведений аналіз сучасних технологій цифрового стільникового зв'язку і визначення можливості використання його у процесі побудови системи радіозв'язку та оповіщення Національної гвардії України засвідчив, що у мирний час і при підготовці до виконання завдань за призначенням можуть використовуватися загальнодоступні канали передачі даних завдяки їх поширеному розповсюдженню [3–6]. Позитивними рисами цих систем є такі:

– у порівнянні з аналогічними стандартами пристрої мають меншу вагу і розміри;

– високий рівень якості зв'язку;

– завади на заданих частотах знаходяться на нижчому рівні;

– поширення на території значних розмірів;

– доступність і можливість використання роумінгового зв'язку (переміщення з однієї мережі в іншу без втрати присвоєного номера);

– розповсюдженість, доступність та порівняльно низька вартість технічного обладнання і програмного забезпечення.

Проте внаслідок проведеного аналізу виявлено, що жодна з існуючих технологій в чистому вигляді не може бути основою системи

мобільного радіозв'язку Національної гвардії України через їх недостатню захищеність від прослуховування та несанкціонованого доступу.

Для реалізації захищеного обміну даними пропонується використовувати технологію VPN [7, 8]. VPN (англ. Virtual Private Network – віртуальна приватна мережа) – технологія, за допомогою якої на базі існуючої мережі (наприклад Інтернет) створюється одне або кілька мережевих з'єднань (логічна мережа), у межах якої може забезпечуватися захист від зовнішнього втручання.

Упровадження VPN на практиці передбачає такі дії. Одному з комп'ютерів локальної обчислювальної мережі надаються функції сервера VPN. Як клієнти можуть виступати віддалені користувачі або маршрутизатори інших локальних мереж. При цьому використовується спеціальне клієнтське програмне забезпечення VPN, яке забезпечує з'єднання із сервером. Першим кроком встановлення з'єднання є аутентифікація користувача – перевірка достовірності права користувача до приєднання до мережі і надання йому доступу до інформації. У разі успішної аутентифікації між клієнтом і сервером узгоджуються деталі забезпечення безпеки з'єднання. Після цього між клієнтом і сервером встановлюється VPN-з'єднання і здійснюється обмін інформацією. При цьому інформація подається у формі набору пакетів. Для захисту від несанкціонованого доступу кожен пакет з даними проходить процедури шифрування/дешифрування і перевірки цілісності.

Для організації VPN використовуються кілька протоколів, серед яких найбільш поширеним є протокол тунельного зв'язку Point-to-Point Tunnelling Protocol (PPTP) – тунельний протокол зв'язку між двома точками. Згідно із цим протоколом створюється Point-to-Point з'єднання – тунель "один-до-одного". Тобто між кожною парою тих, хто передає та отримує інформацію, встановлюється логічне з'єднання (тунель), що дозволяє упакувати (вставити) дані одного протоколу в пакети іншого (це називається інкапсулюванням). Сутність цього полягає в тому, щоб "упакувати" пакет даних разом зі службовою інформацією у новий "конверт". При цьому пакет протоколу нижчого рівня поміщується у поле даних пакета протоколу більш високого або такого ж самого рівня.

Для забезпечення конфіденційності даних вихідний пакет шифрується, "упаковується" у зовнішній пакет і передається транзитною мережею.

Дані, які передаються і приймаються VPN-сервером, ідуть по шифрованому каналу, захист якого забезпечує безпеку й анонімність. Шифрування і дешифрування даних відбуваються як на сервері, так і на клієнтській машині.

Протокол PPTP гарантує, що ніхто не зможе отримати доступ до інформації, яка передається через Інтернет.

На цей час використовуються два основних методи шифрування:

– протокол шифрування або Microsoft Point-to-Point Encryption (MPPE) – шифрування "точка-точка";

– EAP-TLS (Extensible Authentication Protocol – розширюваний протокол аутентифікації, Transport Layer Security – протокол передачі даних) автоматично вибирає довжину ключа шифрування під час узгодження параметрів між клієнтом і сервером.

Ці протоколи можуть працювати з ключами довжиною 40, 56 або 128 біт.

Для кожного прийнятого пакета протокол PPTP формує новий ключ шифрування. При цьому PPTP для зміни ключа шифрування використовує порядкові номери пакетів, що дає змогу здійснювати дешифрування незалежно від порядку приймання пакетів.

Таким чином, послідовність процедур тунелювання, аутентифікації та шифрування дозволяє здійснювати обмін даними між двома точками через мережу загального користування, моделюючи роботу приватної (локальної) захищеної мережі.

Метою статті є визначення порядку та розроблення методики організації скритого обміну даними у системі оповіщення НГУ на основі існуючої загальнодоступної системи мобільного GSM-зв'язку та мережі Інтернет з використанням технології захищеного обміну даними VPN за допомогою відкритого програмного забезпечення.

Виклад основного матеріалу. Однією з реалізацій технології VPN є її безоплатна версія OpenVPN [9, 10]. OpenVPN – вільна реалізація технології VPN з відкритим вихідним кодом для створення зашифрованих каналів типу "точка-точка" або "сервер-клієнт" між комп'ютерами. OpenVPN використовується в

операційних системах Solaris, OpenBSD, FreeBSD, NetBSD, GNU/Linux, Apple Mac OS X, QNX, Microsoft Windows, Android.

OpenVPN передає дані по мережі за допомогою протоколів UDP або TCP із застосуванням драйвера TUN/TAP. Протокол UDP і драйвер TUN дозволяють підключатися до сервера OpenVPN клієнтам, розташованим за межами локальної мережі.

Безпека і шифрування в OpenVPN забезпечуються бібліотекою OpenSSL і протоколом транспортного рівня Transport Layer Security (TLS). Замість OpenSSL у нових версіях OpenVPN можна використовувати бібліотеку PolarSSL. Протокол TLS – це засіб оптимізації протоколу захищеної передачі даних рівня захищених сокетів Secure Socket Layers (SSL).

В OpenSSL може використовуватися симетрична і асиметрична криптографія. У першому випадку перед початком передачі даних на всі вузли мережі необхідно помістити однаковий секретний ключ. При цьому виникає проблема безпечної передачі цього ключа через небезпечний Інтернет.

У другому випадку у кожного учасника обміну даними є два ключі – публічний (відкритий) і приватний (секретний). Публічний ключ використовується для шифрування даних, а приватний – для розшифрування. В основі шифрування лежить досить складна математика. Вибраний у SSL/TLS алгоритм шифрування публічним ключем забезпечує можливість розшифрування тільки за допомогою приватного ключа.

Щоб уникнути підроблення відкритого ключа, якась авторитетна третя сторона повинна його завірити. У результаті цієї процедури створюється так званий *сертифікат відкритого ключа*. Як така третя сторона виступає так званий центр сертифікації CA (CA – Certification authority). Якщо створюється відкритий ключ для публічного використання, то центром сертифікації повинна виступати комерційна або державна організація з безперечною репутацією. Для мереж VPN, які створюються для себе, є можливість самостійно створити свій центр CA і випустити так звані *самопідписані сертифікати*. Звісно, довіра до таких сертифікатів не буде виходити за межі організації, яка їх створює, але, по-перше, цього буде цілком достатньо, а по-друге, – самопідписані сертифікати абсолютно безоплатні. Самопідписані сертифікати і будуть відігравати роль публічних ключів, за допомогою яких вузли вашої мережі OpenVPN зашифровуватимуть дані. Для розшифрування даних будуть використані приватні ключі.

Захищений обмін даними здійснюється за допомогою алгоритмів симетричного шифрування, для чого потрібен спільний секретний ключ. Такий ключ отримується протоколом, який реалізується за допомогою так званого файлу Діффі-Хелмана. Цей файл створюється на сервері OpenVPN.

Для додаткового захисту інформації та перевірки її достовірності створюється ще так званий статичний ключ аутентифікації повідомлень (Hash-based Message Authentication Code, HMAC). Він також створюється на сервері OpenVPN.

У системі оповіщення НГУ треба організувати обмін даними та голосове спілкування кількох абонентів одночасно, оскільки необхідними є їх спілкування та координація дій. Крім того, таке спілкування має здійснювалися не тільки між комп'ютерами, а й між іншими пристроями – телефонами, смартфонами, планшетами. Є кілька програм із схожим набором функцій, таких, як наприклад, усім відомий Skype. Для організації системи оповіщення НГУ найбільш підходить TeamSpeak [11, 12]. Від класичного телефона відрізняється практично необмеженою кількістю абонентів, що розмовляють одночасно. Найбільше це схоже на багатоканальну радіостанцію, в якій можна водночас користуватися кількома каналами. При цьому доступні всі опції, розроблені раніше для зручності використання радіостанцій у польових (бойових) умовах. Програми цього типу можуть використовуватися скрізь, де необхідні голосовий зв'язок та координація великої групи людей.

До складу програмного комплексу обміну даними, звісно, мають входити програмні засоби. Але для реалізації можливостей цих засобів необхідна відповідна технічна платформа. Оскільки мова йде про використання недорогих або зовсім безкоштовних програмних засобів, то і технічні засоби теж мають бути такими. Тому доцільно скористатися тим, що вже є, тобто наявною комп'ютерною технікою для використання як сервера. У ролі клієнтів тоді використовують мобільні телефони або планшети.

Для використання як сервера може підійти будь-який персональний комп'ютер, який задовольняє вимоги до його потужності та швидкодії на середньому рівні, але необхідною умовою є підключення до Інтернету. За операційну систему (ОС) можуть

використовуватися: будь-яка ОС із сімейства Windows починаючи з Windows XP; усі сучасні версії Linux-подібних ОС; сімейство MacOS.

Як клієнтські засоби можуть використовуватися будь-які мобільні пристрої (смартфони або планшети) з операційними системами сімейств iOS або Android.

Програмна частина комплексу: OpenVPN; TeamSpeak. Алгоритм дій під час організації обміну голосовими повідомленнями подано на рисунку.

Отже, спочатку слід створити та налаштувати серверну частину комплексу, тобто вибрати комп'ютер і встановити на нього програми OpenVPN та TeamSpeak. Вибраний комп'ютер має бути підключений до мережі Інтернет і мати зовнішню IP-адресу.

Для обміну файлами необхідно встановити VPN-канал між сервером та комп'ютером користувача (VPN-клієнт), як показано на рисунку. Для цього на комп'ютері користувача треба встановити і налаштувати клієнтські програми OpenVPN та TeamSpeak.

Після підключення до каналу групи абонентів між ними встановлюється голосовий зв'язок. Також абоненту надаються такі додаткові можливості (за допомогою відповідних кнопок): передача текстових повідомлень, відімкнення мікрофона, відімкнення гучномовця, режим підпису до каналів (вибір каналів зв'язку).

Для створення VPN-підключення за допомогою додатка OpenVPN на Android-пристрої знадобляться: смартфон або планшет на базі ОС Android; програма OpenVPN connect для ОС Android; конфігураційні файли із сертифікатами клієнта та сервера.

Завантажити і встановити програму OpenVPN for Android можна за допомогою сервісу Google Play Store, програма розповсюджується безоплатно і може бути налаштована у будь-якому пристрої на базі Android. Установка TeamSpeak здійснюється за допомогою вбудованого в ОС Android інсталятора APK-файлів шляхом натискання на відповідний файл у файловому менеджері або за допомогою Google Play.

Для роботи ПЗ необхідним є підключення до серверу TeamSpeak. Параметри підключення задаються закладками (Bookmarks). Для підключення до нового сервера треба задати відповідні параметри: назву сервера (для відображення), адресу (URL/IP-адреса), пароль, ідентифікатор абонента, параметри окремого каналу для підключення.

Алгоритм дій під час організації обміну голосовими повідомленнями

Для забезпечення голосового зв'язку в групі абонентів (каналів) необхідно підключитися до відповідної групи (каналу) або створити нову групу (канал). Для підключення до існуючого каналу використовуються відповідні задані параметри. Під час створення нового каналу треба задати: назву каналу, пароль, тему та опис каналу (не обов'язково), тип каналу, параметри якості каналу.

Виходячи з викладеного у Національній академії Національної гвардії України (НАНГУ) було розроблено методику створення, налаштування та експлуатації захищеної системи обміну даними та повідомленнями, яка детально описана в Інструкції [13]. Ця методика передбачає таку послідовність кроків.

1. Створення та налаштування серверної частини комплексу програмних засобів на вузлі зв'язку військової частини:

– встановлення і налаштування на спеціально виділеному як сервері VPN комп'ютері серверної частини прорами OpenVPN;

– встановлення та налаштування на тому ж самому комп'ютері серверної частини програми TeamSpeak Server 3.

2. Створення та налаштування клієнтської частини програмного комплексу:

– встановлення та налаштування на комп'ютерах вузлів зв'язку підпорядкованих підрозділів клієнтської частини програм OpenVPN та TeamSpeak;

– підключення клієнтів TeamSpeak до сервера.

3. Встановлення та налаштування клієнтської частини комплексу програмного забезпечення на пристроях з ОС Android:

– встановлення на смартфон або планшет абонента програми OpenVPN connect для ОС Android;

– встановлення на смартфон або планшет абонента програми TeamSpeak.

4. Створення групи абонентів та налаштування голосового зв'язку у групі. При цьому кожному з абонентів групи надається можливість голосового спілкування, а також передача текстових повідомлень, відімкнення мікрофона, відімкнення гучномовця, режим підпису до каналів (вибір каналів зв'язку).

За вказівками цієї Інструкції у Національній академії НГУ було створено й апробовано захищену систему обміну даними та повідомленнями, працездатність якої підтверджується її використанням у зоні проведення операції Об'єднаних сил та у навчальному процесі академії під час виїздів на польові заняття.

Висновки

1. Використання запропонованого порядку та методики організації обміну даними у системі оповіщення НГУ забезпечує гарантовану скритність передачі сигналів оповіщення особового складу за умов застосування GSM-зв'язку.

2. Для організації захищених каналів обміну даними у системі зв'язку угруповання НГУ в умовах обмеженого фінансування бажано використовувати відкрите програмне забезпечення, яке розповсюджується безоплатно. Таке програмне забезпечення дозволяє використовувати ефективний захист від несанкціонованого доступу даних, які передаються у системі зв'язку.

3. Як програмне забезпечення для організації захищеної системи обміну даними пропонується використати технологію організації віртуальної приватної мережі VPN. Для її реалізації можливо скористатися безоплатними відкритими програмами: програма створення каналів "сервер-клієнт" OpenVPN; програма голосового спілкування TeamSpeak.

Метою подальших досліджень є підвищення стійкості та скритності обміну даними в системі оповіщення НГУ під час обміну даними за рахунок використання криптографічних технологій захисту інформації від несанкціонованого доступу.

Перелік джерел посилання

1. Організація військового зв'язку: навч. посіб. / В. Г. Шолудько та ін. Київ: ВІТІ, 2017. 282 с.

2. Вимоги до управління військами. URL: https://studopedia.org/10-129031.html (дата звернення: 30.10.2019).

3. Іохов О. Ю. Визначення шляхів побудови перспективної системи мобільного радіозв'язку внутрішніх військ МВС України. *Системи обробки інформації*. 2011. № 4 (94). С. 196–198.

4. Особливості організації зв'язку у військових частинах та підрозділах Національної гвардії України / Г. А. Дробаха та ін. *Честь і закон*. 2016. № 2. С. 19–25.

5. Системы спутниковой связи. Статья в Википедии. URL: www.wikipedia.com (дата звернення: 30.10.2019).

6. Жовноватюк Р. М., Канкін І. О., Умінський В. В. Перспективи побудови безпровідних мереж передачі даних в інтересах Збройних Сил України. *Вісник ЖДТУ*. № 4 (55). С. 39–47.

7. VPN. Стаття у Вікіпедії. URL: https://uk.wikipedia.org/wiki/VPN (дата звернення: 30.10.2019).

8. Что такое VPN или как защитить сеть. URL: http://pro-spo.ru/network-tech/4304-chto-takoe-vpn-ili-kak-zashhitit-set (дата звернення: 30.10.2019).

9. OpenVPN. Стаття у Вікіпедії. URL: https://uk.wikipedia.org/wiki/OpenVPN (дата звернення: 30.10.2019).

10. Руководство по установке и настройке OpenVPN. URL: https://habr.com/post/233971/ (дата звернення: 30.10.2019).

11. TeamSpeak. Стаття у Вікіпедії. URL: https://uk.wikipedia.org/wiki/Teamspeak (дата звернення: 30.10.2019). Инструкция по Teamspeak 3. URL: https://4pda.ru/forum/index.php?showtopic=532362&st=0#entry27989412 (дата звернення: 30.10.2019).

12. Інструкція з встановлення та налаштування програмного комплексу для організації захищеного обміну голосовими, текстовими повідомленнями та файлами з використанням програмного забезпечення OpenVPN, Teamspeak 3 та PGP / О. Ю. Іохов та ін. Харків: НАНГУ, 2015. 40 с.

Стаття надійшла до редакції 12.12.2019 р.

УДК 004.773.6

А. Ю. Иохов, А. М. Сальников, В. Т. Оленченко, А. М. Горбов

МЕТОДИКА ОРГАНИЗАЦИИ СКРЫТОГО ОБМЕНА ДАННЫМИ В СИСТЕМЕ ОПОВЕЩЕНИЯ НАЦИОНАЛЬНОЙ ГВАРДИИ УКРАИНЫ НА БАЗЕ GSM-СВЯЗИ

Рассмотрен порядок использования общедоступных программных и технических средств для скрытого обмена данными в системе оповещения Национальной гвардии Украины на основе технологий виртуальной частной сети VPN и мобильной связи стандарта GSM. Предложена методика организации скрытого обмена данными в системе оповещения НГУ.

Ключевые слова: *система оповещения, виртуальная частная сеть, мобильная связь GSM, бесплатные общедоступные программные средства, защищенный обмен данными и сообщениями, технология кодирования с открытыми ключами.*

UDC 004.773.6

O. Iokhov, O. Salnikov, V. Olenchenko, O. Gorbov

METHODOLOGY OF THE ORGANIZATION OF THE HIDDEN DATA EXCHANGE IN THE NOTIFICATION SYSTEM OF THE NGU BASED ON THE USE OF GSM-COMMUNICATION

The effective functioning of any military unit, including the National Guard of Ukraine, is impossible without an effective system of government. In turn, the operation of the control system is ensured by the communication and control automation systems. As a rule, special means of communication and data transmission are used in combat conditions, but in daily activities, in particular in the alert system, publicly available channels and data communication facilities are more commonly used, such as wired city telephony and GSM mobile networks. An analysis of modern digital cellular communication technologies and determining the feasibility of using it in the construction of a radiocommunication system and alerting the National Guard of Ukraine showed that public channels of communication can be used in peaceful times and in preparation for their intended purpose due to their widespread distribution. The use of the proposed

methodology for organizing the communication system in the NSU alert system ensures the secrecy of transmitting alert signals to personnel, subject to the use of GSM communication. It is advisable to use open source software, which is distributed free of charge, for the organization of secure communication channels in the NSU grouping system under limited funding conditions. Such software enables efficient cryptographic protection of files and messages transmitted through the communication system. It is proposed to use VPN virtual private network technology as a software for organizing a secure data exchange system. For its implementation it is suggested to use free open source programs: the program of creating channels for the client-server OpenVPN; TeamSpeak Voice Dialer; program for encrypting messages, files and other information for electronic exchange between VPN subscribers. To provide the necessary degree of secrecy of the alert system, it is proposed to use data and message encryption systems with PGP public keys.

Keywords: *notification system; virtual private network; GSM mobile communication; free publicly available software tools; secure exchange of data and messages; public key coding technology.*

Іохов Олександр Юрійович – кандидат технічних наук, старший науковий співробітник, завідувач кафедри військового зв'язку та інформатизації Національної академії Національної гвардії України
https://orcid.org/0000-0002-1718-0138

Сальніков Олександр Михайлович – кандидат технічних наук, доцент, професор кафедри військового зв'язку та інформатизації Національної академії Національної гвардії України
https://orcid.org/0000-0003-4973-9634

Оленченко Віктор Тимофійович – кандидат технічних наук, заступник начальника кафедри військового зв'язку та інформатизації Національної академії Національної гвардії України
https://orcid.org/

Горбов Олексій Михайлович – кандидат технічних наук, доцент кафедри озброєння та стрільби Військового інституту танкових військ НТУ "ХПІ"
https://orcid.org/0000-0002-8326-9413