УДК 681.5
DOI 10.36910/6775-2313-5352-2020-17-14
Мороз С.А., Селепина Й.Р., Приступа С.О., Король О.О.
Луцький національний технічний університет

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДАНИХ В GSM КАНАЛІ МОБІЛЬНОГО ЗВ'ЯЗКУ

Анотація. *В статті проведений аналіз мобільного зв'язку стандарту GSM, зокрема розглянута функціональна будова і інтерфейси взаємодії між структурними елементами стільникової мережі. Для розуміння принципу роботи зв'язку за стандартом GSM наведена структурна схема якій представлені центр комутації мобільного зв'язку (MSC), обладнання базової станції (BSS), центр управління та обслуговування (OMC), мобільні станції (MS). Розглянуті основні алгоритми забезпечення конфіденційності і безпеки даних мобільних абонентів, оскільки GSM канал має свої способи захисту, а також місця вразливості. Зокрема виділено наступні небезпечні види атак, до яких чутливі абоненти стільникових мереж: сніффінг; витік персональних даних; витік даних про місцезнаходження; спуфінг; віддалене захоплення SIM-карти, виконання довільного коду (RCE); відмова в обслуговуванні (DoS). Встановлено, що необхідною функцією мобільної мережі є ідентифікація абонентів, що виконується за IMSI, який записаний в SIM-карті абонента і HLR оператора. Для захисту від спуфінга, мережа виконує аутентифікацію абонента перед тим, як почати його обслуговування. У випадку підтвердження справжності абонента, відбувається захист як абонента так і мережевого оператора від впливу шахрайського доступу. Крім цього користувач повинен бути захищений від підслуховування. Це досягається шляхом шифрування даних, переданих по радіоінтерфейсу.*

Ключові слова: *стандарт GSM, функціональні компоненти мережі, аутентифікація абонента, шифрування даних, радіо інтерфейс.*

Вступ. Стандарт GSM для стільникових мобільних мереж був розроблений Європейським інститутом телекомунікаційних стандартів (ETSI) і визнаний найбільш надійним і масовим по використанню в засобах телекомунікації та мобільного зв'язку. За приблизними підрахунками, число абонентів даного виду зв'язку в Україні та Європі складає понад 500 млн.

Функціональна будова і інтерфейси, прийняті в стандарті GSM, ілюструються за допомогою структурної схеми (рис. 1), на якій MSC (Mobile Switching Centre) - центр комутації мобільного зв'язку; BSS (Base Station System) - обладнання базової станції (БС); OMC (Operations and Maintenance Centre) - центр управління та обслуговування; MS (Mobile Stations) - мобільні станції (МС). Функціональне поєднання елементів системи здійснюється за допомогою декількох інтерфейсів. Всі мережеві функціональні компоненти в стандарті GSM взаємодіють відповідно до системи сигналізації МСЕ-Т.

Центр комутації мобільного зв'язку обслуговує групу сот і забезпечує всі види з'єднань, які необхідні в процесі роботи МС. MSC являє собою інтерфейс між фіксованими мережами (PSTN, PDN, ISDN і т.д.) і мережею мобільного зв'язку. Він забезпечує маршрутизацію викликів і функції управління викликами. Крім виконання функцій звичайної комутаційної станції ISDN, на MSC покладаються функції комутації радіоканалів. До них відносяться "естафетна передача", в процесі якої досягається безперервність зв'язку при переміщенні мобільної станції із соти в соту, і переключення робочих каналів в соті при появі перешкод або несправності. Кожен MSC забезпечує обслуговування мобільних абонентів, розташованих в межах певної географічної зони (наприклад, обласний центр і область). MSC управляє процедурами встановлення виклику і маршрутизації. MSC складає також статистичні дані, необхідні для контролю роботи і оптимізації мережі. MSC підтримує також процедури безпеки, які застосовуються для управління доступами до радіоканалів.

HLR є довідковою базою даних про постійно прописаних в мережі абонентів. У ній містяться розпізнавальні номера та адреси, а також параметри автентичності абонентів, склад послуг зв'язку, спеціальна інформація про маршрутизацію. Ведеться реєстрація даних про роумінгу абонента, включаючи дані про тимчасовий ідентифікаційний номер мобільного абонента (TMSI) і відповідний VLR. До даних, що містяться в HLR, мають дистанційний доступ всі MSC і VLR мережі і, якщо в мережі є кілька HLR, в базі даних міститься тільки один запис про абонента, тому кожен HLR являє собою певну частину загальної бази даних мережі

про абонентів. Доступ до бази даних про абонентів здійснюється за номером IMSI або MSISDN (номеру мобільного абонента в мережі ISDN). До бази даних можуть отримати доступ MSC або VLR, що відносяться до інших мереж, в рамках забезпечення міжмережевого роумінгу абонентів.

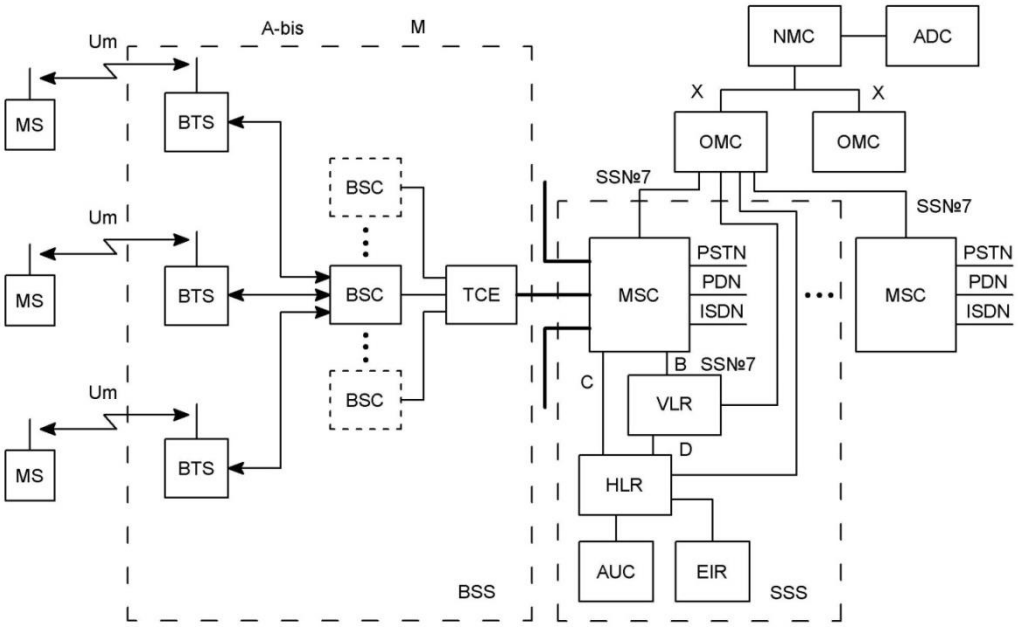

Рис. 1. Функціональна будова і інтерфейси стандарту GSM

VLR містить такі ж дані, як і HLR, проте ці дані містяться в VLR тільки до тих пір, поки абонент знаходиться в зоні, контрольованій VLR. У мережі мобільного зв'язку GSM стільники групуються в географічні зони (LA), яким присвоюється свій ідентифікаційний номер (LAC). Кожен VLR містить дані про абонентів декількох LA. Коли мобільний абонент переміщається з однієї LA в іншу, дані про його місцезнаходження автоматично оновлюються в VLR. Якщо стара і нова LA перебувають під управлінням різних VLR, то дані на старому VLR стираються після їх копіювання в новий VLR. Поточна адреса VLR абонента, що міститься в HLR, також оновлюється.

EIR - регістр ідентифікації устаткування, містить централізовану базу даних для підтвердження автентичності міжнародного ідентифікаційного номера обладнання мобільної станції (IMEI). Ця база даних відноситься виключно до обладнання мобільної станції. База даних EIR складається зі списків номерів IMEI, організованих таким чином: «Білий список» - містить номери IMEI, про яких є відомості, що вони закріплені за санкціонованими мобільними станціями. «Чорний список» - містить номери IMEI мобільних станцій, які вкрадено або яким відмовлено в обслуговуванні з іншої причини. «Сірий список» - містить номери IMEI мобільних станцій, у яких існують проблеми, виявлені за даними програмного забезпечення, що не є підставою для внесення до "чорного списку". До бази даних EIR отримують дистанційний доступ MSC даної мережі, а також MSC інших мобільних мереж.

OMC - центр експлуатації і технічного обслуговування, є центральним елементом мережі GSM, який забезпечує контроль і управління іншими компонентами мережі та контроль якості її роботи. OMC з'єднується з іншими компонентами мережі GSM каналами пакетної передачі протоколу X.25. OMC забезпечує функції обробки аварійних сигналів, призначених для оповіщення обслуговуючого персоналу, і реєструє відомості про аварійні ситуації в інших компонентах мережі. Залежно від характеру несправності OMC дозволяє забезпечити її усунення автоматично або при активному втручанні персоналу. OMC може забезпечити перевірку стану обладнання мережі та проходження виклику мобільної станції. OMC дозволяє здійснювати управління навантаженням в мережі. Функція ефективного управління включає збір статистичних даних про навантаження від компонентів мережі GSM, записи їх в дискові файли та виведення на дисплей для візуального аналізу. OMC забезпечує управління змінами програмного забезпечення і базами даних про конфігурацію елементів мережі. Завантаження програмного забезпечення в пам'ять може проводитися з OMC в інші елементи мережі або з них в OMC.

NMC - центр управління мережею, дозволяє забезпечувати раціональне ієрархічне

управління мережею GSM. Він забезпечує експлуатацію і технічне обслуговування на рівні всієї мережі, підтримуваної центрами OMC, які відповідають за управління регіональними мережами. NMC забезпечує управління графіком у всій мережі і забезпечує диспетчерське управління мережею при складних аварійних ситуаціях, як наприклад, вихід з ладу або перевантаження вузлів. Крім того, він контролює стан пристроїв автоматичного управління, задіяних в устаткуванні мережі, і відображає на дисплеї стан мережі для операторів NMC. Це дозволяє операторам контролювати регіональні проблеми і, при необхідності, надавати допомогу OMC, які відповідають за конкретний регіон. Таким чином, персонал NMC знає стан всієї мережі і може дати вказівку персоналу NMC змінити стратегію рішення регіональної проблеми.

BSS - обладнання базової станції, складається з контролера базової станції (BSC) і приймально-передавальних базових станцій (BTS). Контролер базової станції може керувати кількома приймально-передавальними блоками. BSS управляє розподілом радіоканалів, контролює з'єднання, регулює їх черговість, забезпечує режим роботи зі змінною частотою, модуляцію і демодуляцію сигналів, кодування і декодування повідомлень, кодування мови, адаптацію швидкості передачі для мови, даних і виклику, визначає черговість передачі повідомлень персонального виклику [4, 5].

Розглянемо основні алгоритми забезпечення конфіденційності і безпеки даних мобільних абонентів, оскільки GSM канал має свої способи захисту, а також місця вразливості.

Експериментальні результати та їх обговорення. Проаналізуємо основні вектори атак [5]. Оскільки GSM-інтерфейс є радіоінтерфейсом, весь його трафік «видно» будь-кому, що знаходиться в радіусі дії BTS. Причому аналізувати дані, що передаються через радіоефір, можна навіть не виходячи з дому, використовуючи спеціальне обладнання і персональний комп'ютер.

Виділяють два види атаки: пасивна та активна. У першому випадку атакуючий ніяк не взаємодіє ні з мережею, ні з абонентом, що атакується - виключно прийом і обробка інформації. Виявити таку атаку майже не можливо, але й перспектив у неї не так багато, як у активної. Активна атака має на увазі взаємодію атакуючого з абонентом, що атакується і / або мережею.

Можна виділити найбільш небезпечні види атак, до яких чутливі абоненти стільникових мереж: сніффінг – використання програми або пристрою для перехоплення і аналізу мережевого трафіку; витік персональних даних, SMS і голосових дзвінків; витік даних про місцезнаходження; спуфінг (FakeBTS або IMSI Catcher) – в контексті безпеки мережі, це випадок, коли особа або програма маскується під іншу за допомогою фальсифікації даних, і тим самим отримує незаконну перевагу; віддалене захоплення SIM-карти, виконання довільного коду (RCE); відмова в обслуговуванні (DoS).

Необхідною функцією мобільної мережі є ідентифікація абонентів, що виконується за IMSI, який записаний в SIM-карті абонента і HLR оператора. Ідентифікація мобільних телефонів виконується за серійним номером - IMEI. Однак, після аутентифікації ні IMSI, ні IMEI у відкритому вигляді по мережі «не літають». Після процедури Location Update абоненту присвоюється тимчасовий ідентифікатор - TMSI (Temporary Mobile Subscriber Identity), і подальшу взаємодію здійснюється саме з його допомогою. В ідеальному випадку, TMSI абонента відомий тільки мобільному телефону і мережі. Однак, існують і способи обходу такого захисту. Якщо циклічно дзвонити абоненту або відправляти SMS-повідомлення, спостерігаючи за каналом PCH і виконуючи кореляцію, можна з певною точністю виділити TMSI абонента, що атакується. Крім того, маючи доступ до мережі міжопераційної взаємодії SS№7, за номером телефону можна дізнатися IMSI і LAC його власника. Проблема в тому, що в мережі SS№7 всі оператори «довіряють» один одному, тим самим знижуючи рівень конфіденційності даних своїх абонентів.

Для захисту від спуфінга, мережа виконує аутентифікацію абонента перед тим, як почати його обслуговування (рис. 2).

Використання пароля (або PIN-код - персонального ідентифікаційного цифрового коду) - один з простих методів аутентифікації. Він дає дуже низький рівень захисту в умовах використання радіозв'язку. Досить почути цей персональний код всього лише один раз, щоб обійти засоби захисту. Насправді GSM використовує PIN-код в поєднанні з SIM (Subscriber Identify Module): даний PIN-код перевіряється на місці самим SIM без передачі в ефір.

Крім IMSI, в SIM-карті зберігається випадково згенерована послідовність, що називається «Ki», яку вона повертає тільки в хешированому вигляді. Також Ki зберігається в

HLR оператора і ніколи не передається у відкритому вигляді. В цілому, процес аутентифікації заснований на принципі «чотиристоронього рукостискання»: 1. Абонент виконує Location Update Request, потім надає IMSI. 2. Мережа надсилає псевдовипадкове значення RAND. 3. SIM-карта телефону хешує Ki і RAND за алгоритмом A3. A3 (RAND, Ki) = SRAND. 4. Мережа теж хешує Ki і RAND за алгоритмом A3. 5. Якщо значення SRAND з боку абонента збіглося з обчисленим на стороні мережі, значить абонент пройшов аутентифікацію (рис. 2.).

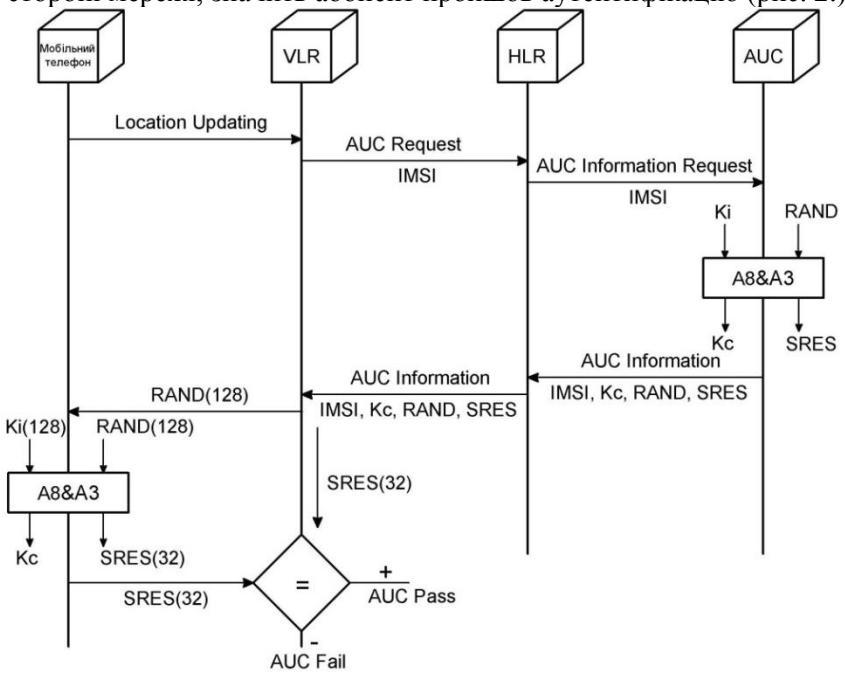

Рис.2. Обчислення аутентифікації

Для того щоб досягти необхідного рівня безпеки, алгоритм A3 має бути односпрямованої функцією, як її називають експерти криптографи. Це означає, що обчислення SRES при відомих Ki і RAND має бути простим, а зворотна дія - обчислення Ki при відомих RAND і SRES - має бути максимально ускладненою. Безумовно, саме це і визначає в кінцевому підсумку рівень безпеки. Значення, що обчислюється за алгоритмом A3, повинно мати довжину 32 біта. Ki може мати будь-який формат і довжину. Криптографічні методи дають можливість за допомогою відносно простих засобів домогтися високого рівня безпеки. У GSM використовуються єдині методи для захисту всіх даних, будь то інформація для користувача, передача сигналів, пов'язаних з користувачем (наприклад, повідомлень, в яких містяться номери телефонів, що викликаються), або навіть передача системних сигналів (наприклад, повідомлень, що містять результати радіовимірювань для підготовки до передачі). Необхідно усвідомлювати різницю тільки між двома випадками: який зв'язок виявляється захищеним (тоді всю інформацію можна відправляти в зашифрованому вигляді), який зв'язок є незахищеним (тоді вся інформація відправляється у вигляді незашифрованої цифрової послідовності).

Як тільки справжність абонента була перевірена, таким чином захищаючи і абонента і мережевого оператора від впливу шахрайського доступу, користувач повинен бути захищений від підслуховування. Це досягається шляхом шифрування даних, переданих по радіоінтерфейсу, з використанням другого ключа Kc і спочатку секретного алгоритму A5 (рис. 3).

Kc генерується в ході перевірки автентичності, використовуючи Ki, RAND і секретний алгоритм A8, який також зберігається на SIM-карті. Подібно до алгоритму A3, A8 не унікальний, і він може також бути обраний оператором. Ключі Kc для кожного користувача обчислюються AuC домашньої мережі і передаються в VLR у складі набору триплетів, де кожному триплету і, відповідно – ключу Kc, присвоюється номер ключа – CKSN. У деяких реалізаціях алгоритми A3 і A8 об'єднані в єдиний алгоритм A38, який використовує RAND і Ki, щоб згенерувати Kc і SRES. На відміну від A3 і A8, які, можливо, різні для кожного індивідуального оператора, A5 вибирається з списку із 7 можливих варіантів.

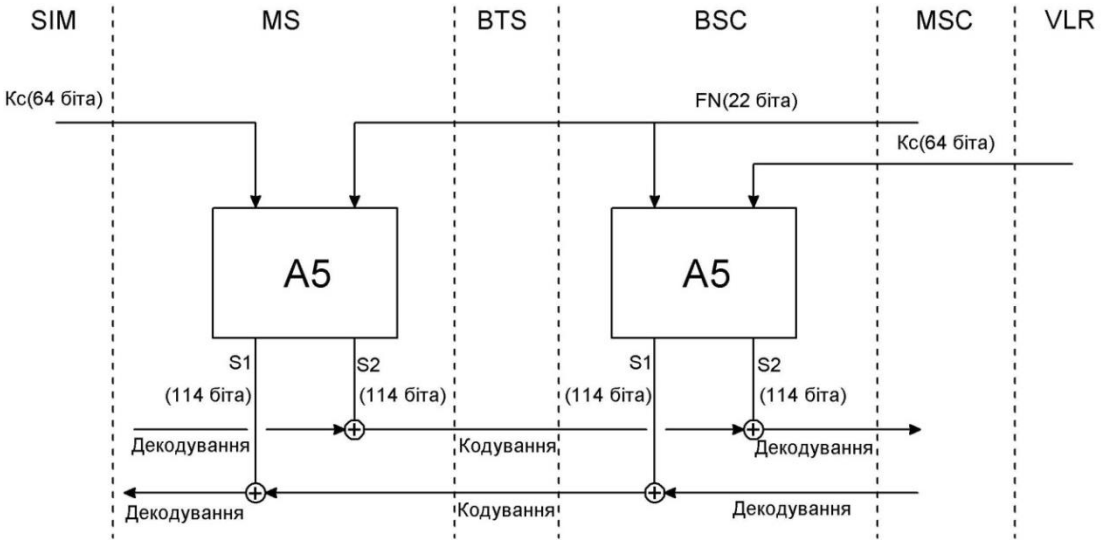

Рис.3. Шифрування і розшифрування в стандарті GSM

Перед шифруванням відбувається фаза переговорів, в ході якої визначається, яка версія A5 буде використана. Якщо мережа і мобільна станція не мають загальних версій A5, зв'язок має продовжитися у відкритому режимі або з'єднання повинне бути розірвано. Алгоритм A5 використовує 64-бітний ключ Kc і 22-бітний номер TDMA кадру для обчислення двох 114-бітних слів шифрування – BLOCK1 і BLOCK2, що використовуються при передачі і прийомі відповідно. Слова шифрування – EXORed зі 114 бітами даних в кожній посилці. Оскільки зашифровані дані обчислені, використовуючи номер TDMA кадру, то слова змінюються від посилки до посилки і не повторюються протягом гіперфрейма (приблизно 3,5 години).

Перед тим, як почати шифрування, мобільна станція (MS) відправляє в VLR номер ключа шифрування CKSN, який зберігається в її пам'яті з моменту останньої процедури аутентифікації. CKSN не містять секретних даних, а служить лише для того, щоб MS могла повідомити мережі, який ключ Kc вона «пам'ятає». Після цього VLR відправляє в MS команду на включення шифрування і передає в базову станцію (BTS) ключ Kc з того триплету, який відповідає номеру CKSN, отриманого від MS. Таким чином між MS і VLR досягається домовленість про вибір ключа шифрування без передачі самого ключа по радіоінтерфейсу.

Особливо варто відзначити, що в наземному каналі передачі дані передаються по проводах в незашифрованому вигляді, і перехоплення інформації йде саме з них.

Висновки. Отже, на GSM-інтерфейс може здійснюватися зовнішній вплив. Серед найбільш небезпечних видів атак виділяють: сніффінг; витік персональних даних, СМС і голосових дзвінків; витік даних про місцезнаходження; спуфінг; віддалене захоплення SIM-карти; відмова в обслуговуванні (DoS).

Для захисту GSM-користувача мережа виконує аутентифікацію абонента перед тим, як почати його обслуговування та здійснює шифрування даних, переданих по радіоінтерфейсу, з використанням ключа Kc і секретного алгоритму A5.

Інформаційні джерела

1. Основы построения телекоммуникационных систем и сетей: учебник для вузов / В.В. Крухмалёв, Н.В. Гордиенко, А.Д. Моченов и др.; под. ред. В.Н. Гордиенко и В.В. Крухмалёва. - М.: Горячая линия - Телеком, 2004. - 510 с.

2. Карташевский В.Г. Сети подвижной связи / В.Г. Карташевский, С.Н. Семенов, Т.В. Фирстова. - М.: Эко-Трендз, 2001.

3. Системы мобильной связи: учебное пособие для вузов / В.П. Ипатов, В.К. Орлов, И.М. Самойлов, В.Н. Смирнов; под ред.В.П. Ипатова. - М.: Горячая линия - Телеком, 2003. - 272 с.

4. Кирилов В.И. Многоканальные системы передачи: учебник / В.И. Кирилов. - 2-е изд. - М.: Новое знание, 2003. - 751 с.

Мороз С.А., Селепина Й.Р., Приступа С.А., Король А.А.
Луцкий национальный технический университет

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДАННЫХ В GSM КАНАЛЕ МОБИЛЬНОЙ СВЯЗИ

Аннотация. *В статье проведен анализ мобильной связи стандарта GSM, в частности рассмотрено функциональное строение и интерфейсы взаимодействия между структурными элементами сотовой сети. Для понимания принципа работы связи по стандарту GSM приведена структурная схема которой представлены центр коммутации подвижной связи (MSC), оборудование базовой станции (BSS), центр управления и обслуживания (OMC), мобильные станции (MS) . Рассмотрены основные алгоритмы обеспечения конфиденциальности и безопасности данных мобильных абонентов, поскольку GSM канал имеет свои способы защиты, а также места уязвимости. В частности выделено следующие опасные виды атак, к которым чувствительны абоненты сотовых сетей: сниффинг; утечка персональных данных; утечка данных о местонахождении; спуфинг; отдаленный захват SIM-карты, выполнение произвольного кода (RCE) отказ в обслуживании (DoS). Установлено, что необходимой функцией мобильной сети является идентификация абонентов, выполняется IMSI, который записан в SIM-карте абонента и HLR оператора. Для защиты от спуфинга, сеть выполняет аутентификацию абонента перед тем, как начать его обслуживания. В случае подтверждения подлинности абонента происходит защита как абонента так и сетевого оператора от воздействия мошеннического доступа. Кроме этого пользователь должен быть защищен от подслушивания. Это достигается путем шифрования данных, передаваемых по радиоинтерфейсу.*

Ключевые слова: *стандарт GSM, функциональные компоненты сети, аутентификация абонента, шифрование данных, радиоинтерфейс.*

Moroz S., Selepina Y., Pristupa S., Korol O.
Lutsk National Technical University

FEATURES OF DATA SECURITY IN THE GSM MOBILE CHANNEL

Abstract. *The article analyzes the mobile communication of the GSM standard, in particular, considers the functional structure and interfaces of interaction between the structural elements of the cellular network. To understand the principle of communication according to the GSM standard, a block diagram of the Mobile Switching Center (MSC), base station equipment (BSS), control and service center (MCC), mobile stations (MS). The main algorithms for ensuring the confidentiality and security of mobile subscribers' data are considered, as the GSM channel has its methods of protection, as well as vulnerabilities. In particular, the following dangerous types of attacks to which cellular network subscribers are sensitive have been identified: sniffing; leakage of personal data; leakage of location data; spoofing; remote SIM card capture, execution of arbitrary code (RCE); denial of service (DoS). It is established that the necessary function of the mobile network is the identification of subscribers, which is performed by IMSI, which is recorded in the SIM-card of the subscriber and the HLR of the operator. To protect against spoofing, the network authenticates the subscriber before starting its service. In the case of authentication of the subscriber, both the subscriber and the network operator are protected from the effects of fraudulent access. In addition, the user must be protected from eavesdropping. This is achieved by encrypting the data transmitted over the radio interface.*

Keywords: *GSM standard, network functional components, subscriber authentication, data encryption, radiointerface.*