УДК 621.392

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОФЕССИОНАЛЬНОЙ ТРАНКИНГОВОЙ СЕТИ СВЯЗИ TETRA*

Р. А. Бельфер, доцент кафедры «Информационная безопасность» МГТУ им. Н. Э. Баумана, старший научный сотрудник, к.т.н.; a.belfer@yandex.ru
Д. В. Суходольский, студент МГТУ им. Н. Э. Баумана; diomids@gmail.com
Н. О. Поздеев, студент МГТУ им. Н. Э. Баумана; Nikitapozdeev@list.ru

Высокие требования отдельных пользователей к безопасности профессиональной мобильной радиосвязи, а также особенности сети стандарта TETRA определяют ряд отличий в обеспечении информационной безопасности этих сетей в сравнении с тем, как это реализуется в других беспроводных сетях связи. Анализируются научные публикации и документы международных организаций, в которых показано, как можно выполнить эти требования с помощью механизмов шифрования и управления ключами шифрования.

Ключевые слова: *информационная безопасность, профессиональная мобильная радиосвязь, TETRA, режим транкинговой радиосвязи, режим прямого вызова, радиоинтерфейс, сквозное шифрование.*

Введение. Профессиональная мобильная радиосвязь (ПМР; Private Mobile Radio — PMR) обеспечивает связь для государственных организаций и профессиональных пользователей [1]. Примеры реализации профессиональной транкинговой сети радиосвязи стандарта TETRA (TErrestrial Trunked RAdio) в нашей стране у всех на слуху: это сеть МЧС России для оперативного взаимодействия служб в зоне стихийного бедствия, сеть зимней Олимпиады в Сочи для координации действий организаторов соревнований, спортсменов, сотрудников служб безопасности, сеть служебной радиосвязи в аэропорту Домодедово и др.

Для сетей TETRA характерно то, что, в отличие от сетей связи общего пользования (ССОП), к ним предъявляются более высокие требования в плане обеспечения информационной безопасности (ИБ) со стороны ряда пользователей. Настоящая статья, основанная на анализе публикаций и стандартов международных организаций, посвящена некоторым особенностям профессиональной транкинговой сети радиосвязи стандарта TETRA в части обеспечения ИБ.

Специфика сети TETRA в обеспечении ИБ. Основными элементами сети TETRA, как следует из рис. 1, являются инфраструктура управления и коммутации (Switching and Management Infrastructure, SwMI) и абонентские терминалы (мобильные и стационарные радиостанции TETRA). К SwMI относится оборудование, которое обеспечивает необходимые режимы функционирования сети TETRA: базовые станции, центры коммутации, центр эксплуатации и технического обслуживания и др. [2].

У сети TETRA много общего с сотовыми сетями связи (терминалы, радиодоступ, базовые станции (БС), коммутаторы и др.), однако имеют место и различия в архитектуре. Отметим те из них, которые напрямую влияют на особенности обеспечения информационной безопасности.

- В сети TETRA, кроме обычных индивидуальных вызовов между двумя пользователями, предусмотрен групповой вызов (точка–многоточка, т.е. радиостанция–группа радиостанций). При групповом вызове устанавливается соединение между вызывающим абонентом и группой вызываемых абонентов. Поэтому в каждой радиостанции сети TETRA, кроме индивидуального идентификатора пользователя, есть один или несколько идентификаторов групп пользователей (групповых идентификаторов).
- В сети TETRA предоставляется возможность установления соединения между радиостанциями напрямую, минуя инфраструктуру управления и коммутации SwMI. В радиостанции предусмотрен специальный интерфейс такого режима прямого вызова (Direct Mode Operation, DMO). Например, прямая связь может быть организована между двумя абонентами в том случае, когда один из абонентов не входит в область охвата базовой станцией. Установление соединения между пользователями через инфраструктуру управления и коммутации SwMI осуществляется в режиме транкинговой радиосвязи (Trunked Mode Operation, TMO).
- Основной трафик в TETRA организуется между пользователями сети через один или несколько ком-

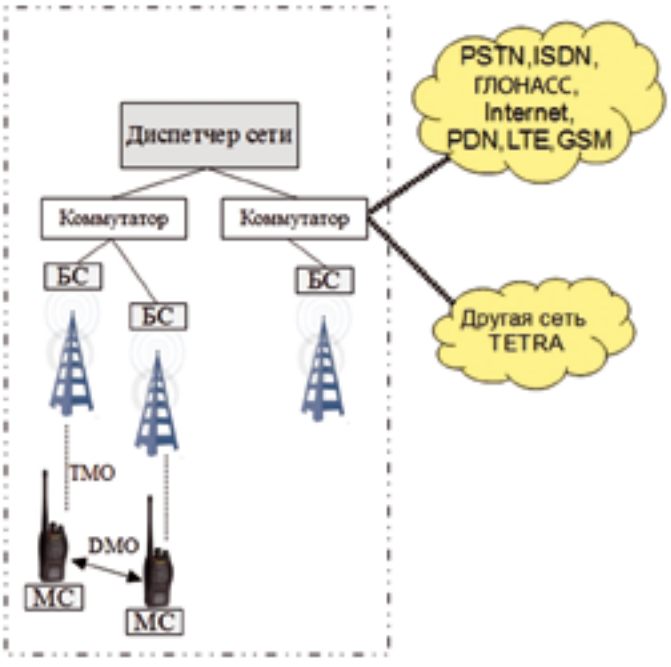

Рис. 1. **Схема сети TETRA**

* Анализ информационной безопасности профессиональных транкинговых сетей был внесен в учебный план 6-го семестра 2012 г. по предложению первого проректора кафедры ИБ, проректора по учебной работе МГТУ им. Н. Э. Баумана Е. Г. Юдина (1940—2012).

мутаторов, а не на участке доступа в сети связи ТфОП, Интернет и др. В сочинской сети таких коммутатора два — в Краснодаре и Сочи. Некоторые сети TETRA могут быть даже автономными [2].

● Высокие требования отдельных пользователей к безопасности профессиональной сети и отмеченные выше особенности сети TETRA обусловили некоторые отличия в обеспечении ИБ в сравнении с другими сетями связи. Одним из механизмов выполнения этих требований является предоставление возможности сквозного шифрования сообщений между радиостанциями («из конца в конец», end-to-end).

Шифрование в сети. Выполнить высокие требования спецпотребителей к уровню информационной безопасности позволяют такие механизмы, как управление ключами и шифрование в сети TETRA [3, 4]. В зависимости от запросов пользователей шифрованию подлежат идентификаторы индивидуальных пользователей (Individual TETRA Subscriber Identity, ITSI) и идентификаторы групп пользователей (Group TETRA Subscriber Identity, GTSI). На беспроводном участке радиоинтерфейса шифруются сообщения сигнализации, речи и данных не только индивидуальных, но и групповых пользователей. При высоких требованиях к информационной безопасности эти сообщения подвергаются сквозному шифрованию.

Управление ключами шифрования. Для индивидуальных и групповых вызовов на беспроводном участке между радиостанцией и инфраструктурой SwMI требуется шифрование сигнального и пользовательского трафика. Механизм этого шифрования предусматривает возможность работы в режиме как TMO, так и DMO**.**

Ключ шифрования сессии (Derived Cipher Key, DCK) служит для поточного шифрования на участке радиодоступа при *индивидуальном вызове*. Он создается при взаимной аутентификации на этом участке. Принцип работы поточного шифрования в сети TETRA такой же, как в сетях GSM, UMTS и LTE [5]. DCK используется также при создании безопасного канала для распределения радиостанциям ключей группового вызова. Для этого в SwMI генерируется общий ключ шифрования (Common Cipher Key, CCK), который распределяется в радиостанции с помощью DCK. CCK используется для шифрования сообщений, которые направляются в группы мобильных радиостанций, расположенных в одной или нескольких областях местонахождения LA (Local Area) [6]. Когда CCK распределяется по радиостанциям через участок радиодоступа, реализуется так называемый механизм смены ключей по эфиру (Over The Air Re-keying, OTAR), использующий ключ шифрования сессии DCK этих радиостанций [7]. CCK позволяет также шифровать сообщения групповых вызовов в режиме транкинговой радиосвязи TMO.

В SwMI генерируется общий групповой ключ шифрования (Common Cipher Key, GCK). Внутри области местонахождения мобильной радиостанции LA ключ GCK используется в модифицированном виде. Этот модифицированный групповой ключ шифрования MGCK (Modified Group Cipher Key) создается с помощью специального алгоритма, учитывающего, кроме GCK, также ключ CCK [8]. MGCK обеспечивает шифрование сообщений определенной группы пользователей. Быстрая смена CCK позволяет осуществить частую смену ключей шифрования MGCK, что гарантирует высокую степень шифрования.

Когда GCK распределяется к радиостанции с помощью механизма OTAR на участке радиоинтерфейса (air interface, AI), шифрование этого ключа производится с помощью ключа шифрования сессии DCK.

Статический ключ шифрования (Static Cipher Key, SCK) может быть использован в режиме прямого вызова для шифрования сообщений индивидуальных и групповых пользователей. Эти ключи статические в том смысле, что в сети TETRA предусмотрен набор 32 таких фиксированных ключей. Новые ключи шифрования SCK не создаются, они могут только заменяться. Ключ SCK распределяется радиостанциям по беспроводному доступу, подобно GCK. Используя механизм OTAR, он шифруется ключом шифрования сессии DCK. Ключ SCK используется также для шифрования в режиме транкинговой радиосвязи TMO [7].

Шифрование на участке радиоинтерфейса. Шифрование сообщений на участке AI сети TETRA осуществляется поточным методом, как и в сотовых сетях связи. Посмотрим, чем отличается шифрование в режиме транкинговой радиосвязи TMO сети TETRA [7, 8] от шифрования в сети GSM [5].

В обоих случаях на вход алгоритма формирования псевдослучайной последовательности для шифрования открытого текста по модулю 2 поступают два значения. Одно из них — номер кадра (в сети GSM), другое — ключ шифрования. В сети TETRA принята более длинная нумерация кадров, что обеспечивает больший период повтора нумерации, а следовательно, и повтор псевдослучайной последовательности. Изменение иерархии кадров потребовало усиления конфиденциальности сообщений из-за групповых вызовов [1]. В сети TETRA к нумерации кадра добавлены еще три бита, один из которых определяет восходящий или нисходящий поток, а два других — номер слота. В результате на формирование псевдослучайной последовательности поточного шифрования в сети TETRA поступает значение вектора инициализации (IV) длиной 29 бит.

Ключ шифрования в сети GSM один, он соответствует ключу шифрования сессии DCK в сети TETRA. Ключ шифрования ECK (Encryption Cipher Key) в режиме транкинговой радиосвязи TMO сети TETRA создается с помощью соответствующего алгоритма TB5, посредством одного из ключей шифрования, таких как DCK, SCK, MGCK или CCK, в зависимости от выполняемой функции. Для шифрования сообщений индивидуальных вызовов, например, используется ключ шифрования сессии DCK, для шифрования сообщений групповых вызовов — MGCK. Алгоритм TB5 при создании ключа шифрования ECK, кроме одного из указанных ключей шифрования для защиты от некоторых угроз ИБ, использует следующие параметры: идентификатор области местонахождения, несущую частоту (Carrier Number, CN) и др.

На основе ключа шифрования ECK и с помощью алгоритма шифрования формируется псевдослучайная последовательность для поточного шифрования открытого текста по модулю 2. В сети TETRA стандартизированы четыре алгоритма шифрования TEA (TETRA Encryption Algorithm): TEA1–TEA4. Они обеспечивают пользователям разные степени защиты в зависимости от требований к уровню ИБ. В [9—12] отмечается, что сами алгоритмы TEA1–TEA4 являются конфиденциальными, причем TEA1, TEA3 и TEA4 распределяет ETSI, а TEA2 — ИТ-департамент полиции Германии [6].

Рассмотрим основные принципы шифрования в режиме прямого вызова (DMO), отличные от приведенных выше для шифрования в транкинговой радиосвязи (TMO) сети TETRA. Как отмечено в Приложении А документа ETSI

[13], главное различие в формировании псевдослучайной последовательности шифрования сообщений по модулю 2 заключается в формировании ключа шифрования ECK (Encryption Cipher Key), который в режиме транкинговой радиосвязи DMO сети TETRA создается с помощью алгоритма TB6, используя только ключ шифрования SCK. Алгоритм TB6 при создании ключа шифрования ECK поддерживает еще два параметра: несущую частоту и короткий идентификатор абонента (незашифрованный SSI или зашифрованный EDSI). Другой особенностью является использование вместо вектора инициализации параметра временного варианта (Time Variant Parameter, TVP), выполняющего ту же функцию. Первоначальное значение TVP устанавливается в пакете синхронизации. При каждой транзакции TVP увеличивается на единицу. Все эти функции подробно изложены в [13].

Сквозное шифрование. Некоторым пользователям для обеспечения ИБ подчас недостаточно обязательного шифрования сигнальных и пользовательских сообщений на участке радиоинтерфейса. Им требуется сквозное шифрование сообщений от радиостанций через всю сеть (между базовыми станциями и коммутаторами, между отдельными коммутаторами) [6, 14]. В ответ на этот запрос рабочая группа по защите от фрода (Security and Fraud Prevention Working Group, SPFG) разработала стандарт [15], включающий алгоритмы сквозного шифрования в сети TETRA, рекомендации по использованию одного из стандартных алгоритмов AES и IDLE для совместимости сетей разных операторов.

В то же время этот стандарт сети TETRA оставляет оператору свободу выбора реализации сквозного шифрования в зависимости от требований пользователя. Так что разные группы потребителей могут использовать разные алгоритмы шифрования в соответствии с политикой безопасности.

Стандарт сквозного шифрования изложен в виде следующих четырех функций [14]:

- шифрование трафика пользователя (алгоритм E1);
- шифрование ключа шифрования трафика (алгоритм E2);
- обеспечение целостности кадра синхронизации (алгоритм E3);
- сообщения ключа управления (алгоритм E4).

Шифрование трафика пользователя (алгоритм E1.) Как следует из приведенной на рис. 2 функциональной диаграммы механизмов шифрования/дешифрования речи [16], псевдослучайная ключевая последовательность поточного шифрования формируется по алгоритму E1 на базе ключа шифрования трафика (Traffic Encryption Key, TEK) и вектора инициализации (IV). В результате противоположному пользователю передается зашифрованное сообщение C. По алгоритму E1 создается также вектор синхронизации SV (Synchronization Vector), который передается в устройство управления синхронизацией (УС). УС формирует кадр синхронизации (КС), который передается вместе с зашифрованным сообщением (C). На приеме устройство обнаружения синхронизации выделяет кадр синхронизации, с его помощью определяет вектор инициализации IV, посредством которого и ключа TEK расшифровывается сообщение.

Для того чтобы на приеме расшифровать зашифрованное сообщение, в поток данных вставляется вектор синхронизации SV. Вектор инициализации IV выполняет здесь ту же функцию, что и в протоколах WEP и TKIP в беспроводной локальной сети группы стандартов 802.11 [5].

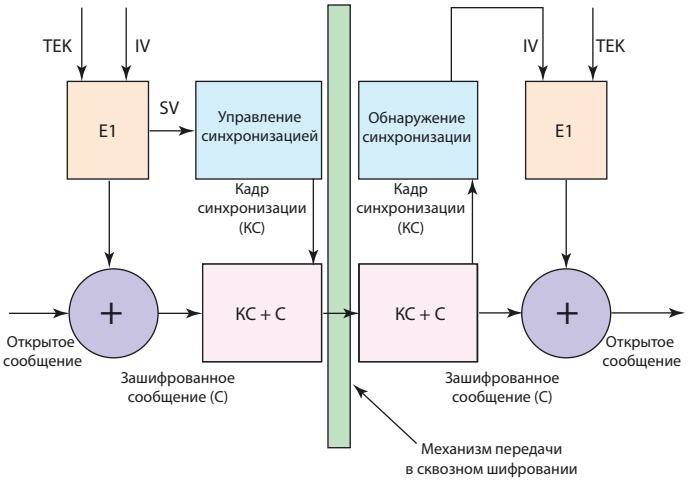

Рис. 2. **Функциональная диаграмма механизмов шифрования/дешифрования речи [16]**

Шифрование ключа (алгоритм E2). Подобно тому, как на участке радиоинтерфейса существует механизм OTAR для распределения ключей, на участке между взаимодействующими радиостанциями при сквозном шифровании предусмотрен механизм OTAK (Over The Air Keying) для распределения ключей [6]. Для шифрования трафика используются ключи TEK (Traffic Encryption Key), а для распределения этих ключей по радиостанциям — ключи для индивидуальных соединений (Unique Encryption Keys, UEK) и ключи для групповых соединений (Group Encryption Keys, GEK). В больших системах довольно много пользовательских групп сквозного шифрования с разными ключами.

Принцип обеспечения целостности кадра синхронизации (алгоритм E3) с помощью контрольно-проверочной комбинации (КПК) аналогичен обеспечению по протоколу WEP целостности кадра в беспроводной локальной сети группы стандартов 802.11 [5]. Кадр синхронизации, кроме вектора синхронизации (64 бит), включает дополнительные поля: признак соответствия рекомендации 02 [15] или несоответствия (1 бит), идентификатор подлежащих КПК полей (10 бит) и др. Длина кадра синхронизации составляет 119 бит, длина КПК — 22 бит.

Сообщения управления ключом (алгоритм E4). В сети TETRA предусмотрена услуга передачи коротких сообщений (Short Data Service, SDS). В частности, можно отправлять или получать SDS параллельно с ведением разговора или с передачей данных. SDS реализуются при выполнении требований защиты, связанных с управлением ключами. Алгоритм E4 используется в связке с ключом шифрования сигнализации (Signalling Encryption Key, SEK). Предполагается, что алгоритм E4 предусматривает блочное шифрование, поддерживающее режим сцепления шифрованных блоков CBC.

Конфиденциальность трафика при шифровании из конца в конец не нуждается в шифровании на участке радиоинтерфейса. Однако механизм шифрования радиоинтерфейса усиливает шифрование из конца в конец в таких случаях, как, например, скрытие вектора синхронизации, защита на участке радиоинтерфейса от анализа или атак системы шифрования из конца в конец [1].

Заключение. Таким образом, высокие требования к обеспечению информационной безопасности в широко используемой в нашей стране профессиональной радиосети TETRA говорят о необходимости специальных мер защиты

от угроз. В настоящее время на международных форумах [17, 18] обсуждается возможность создания оборудования широкополосной ПМР, причем рассматривается сеть 4G стандарта LTE. Однако следует учитывать, что в настоящее время такие коммерческие сети не отвечают строгим критериям, предъявляемым ПМР к информационной безопасности.

ЛИТЕРАТУРА

1. **Chater-Lea D. J**. Security considerations in PMR networks. Security in Networks IEE Colloquium, 1995, P. 5/1—5/5.
2. **Stavroulakis P**. Terrestrial Trunked RAdio — TETRA. A Global Security Tool, 2007, P. 314.
3. **Smith T.** High-Grade encryption. IEEE Seminar on Digital Object Identifier, 2000, P. 4/1—4/4.
4. **Yong-Seok, Choon-Soo Kim, JaeCheol Ryou**. The Vulnerability Analysis and Improvement of the TETRA Authentication Protocol. 12-th International Conference on Advanced Communication Technology, 2010, P. 1469—1473.
5. **Бельфер Р. А**. Сети и системы связи (технологии, безопасность): Учеб. пособ. по дисциплине «Сети и системы связи» / Электронное учеб. изд. // ФГБОУ ВПО «МГТУ им. Н. Э. Баумана», 2012.
6. TETRA Security. TETRA MoU Association Ltd., 2006.
7. ETSI EN 300392—7 V3.3.1 (2012—07), Terrestrial Trunked radio (TETRA), Voice plus Data; Part 7: Security.
8. **Shuwen D**. Security Analysis of TETRA. Norwegian University of Science and Technology, 2013.
9. ETSI TR 101053—1: Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard encryption algorithms; Part 1: TEA1, 2006.
10. ETSI TR 101053—2: Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard encryption algorithms; Part 2: TEA2, 2012.
11. ETSI TR 101053—3: Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard encryption algorithms; Part 3: TEA3, 2007.
12. ETSI TR 101053—4: Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard encryption algorithms; Part 4: TEA4, 2006.
13. ETSI EN 300—6 V1.21 (2004—05), Terrestrial Trunked radio (TETRA), Direct Mode Operation (DMO); Part 6: Security.
14. **Murgatroyd B.** W. End to end encryption in public safety TETRA networks. IEE Seminar: Secure GSM and Beyond: End to End Security for Mobile Communications, 2003, P. 7/1—7/12.
15. TETRA MoU SFPG: End-to-End Encryption. Recommendation 02, Edition 4, 2005.
16. ETSI EN 302109 V1.1.1 Terrestrial Trunked Radio (TETRA); Security; Synchronization mechanism for end-to-end encryption, 2003.
17. **Иванов С. М**. От TETRA к LTE для профессионалов // Вестник связи.— 2012. № 6.
18. **Есауленко А.** LTE идет на смену TETRA // Сети/Nerwork World.— 2012.— № 6.

Получено 14.01.14

ИНФОРМАЦИЯ

РЕШЕНИЕ «МФИ СОФТ» ПРИЗНАНО «ПРОЕКТОМ ГОДА-2013» В НОМИНАЦИИ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Система защиты баз данных МТС-Банка на основе решения «МФИ Софт» стала победителем конкурса «Проект года-2013».

Решение, набравшее наибольшее количество голосов ИТ-директоров компаний России и СНГ, признано лучшим в номинации «Информационная безопасность». Организатор конкурса — официальный портал ИТ-директоров России Global CIO.

Проект защиты баз данных дальневосточного филиала МТС-Банка на основе аппаратно-программного комплекса «Гарда БД» был реализован в течение года. Его основная задача — повышение уровня защищенности баз данных от нежелательного разглашения, фальсификации, незаконного тиражирования или уничтожения информации, а также удовлетворение законодательных норм (требования ФЗ «О персональных данных» 152-ФЗ, 161-ФЗ, 781-ФЗ, 382-П, международные стандарты SOX, PCI-DSS и др.). Для реализации проекта была выбрана система «Гарда БД», разработанная российской компанией «МФИ Софт».

Внедрение комплексной системы аудита и защиты информации от неправомочного доступа в автоматизированную банковскую систему (АБС) стало достаточно масштабным проектом, охватывающим более тысячи рабочих мест. В общей сложности проект занял 5800 человеко-часов.

На данный момент в дальневосточном филиале МТС-банка функционирует комплексная система защиты, которая перехватывает информацию по заданным критериям в режиме 24/7 и анализирует в автоматическом режиме полученные данные с уведомлением сотрудников отдела ИБ о выявлении подозрительных событий.

Проект позволил настроить многоуровневый контроль баз данных с градацией по пользователям, включая администраторов. В результате проекта снижены риски, связанные со случайными и умышленными ошибками сотрудников при работе с базами данных при минимальных затратах на проект.

«Обеспечение безопасности баз данных в финансовом предприятии имеет высокое значение для работы предприятия в целом за счет минимизации целого комплекса рисков, а также удовлетворения законодательных норм,— отметил главный специалист отдела информационной безопасности дальневосточного филиала ОАО «МТС-Банк» **К. Щепилов**.— Комплекс защиты информации банка стал более гибким, мы смогли на порядок увеличить оперативность принятия решений при предотвращении инцидентов нарушения политик информационной безопасности».