інциденту. Повинні реалізуватись такі вимоги до курсів навчання.

Функціональні керівники повинні:

1. Розуміти важливість політики безпеки СУТ і те, як ця політика впливає на рішення, прийняті щодо захисту СУТ. Розуміти важливість визначення адекватного ступеня безпеки для різноманітних типів інформації, якою володіє функціональне керівництво.

2. Розуміти, що СУТ має цінні ресурси. Розуміти важливість забезпечення адекватного захисту (через фінансування, укомплектовування персоналом тощо).

Адміністратори СУТ повинні:

1. Розуміти усі аспекти роботи СУТ. Мати здатність відрізняти нормальну роботу системи від ненормальної.

2. Розуміти роль адміністратора СУТ в реалізації політики безпеки СУТ.

3. Розуміти, як працюють служба і механізми безпеки. Бути спроможними розпізнати неправильне використання механізмів захисту користувачами.

4. Розуміти, як треба ефективно використовувати можливості з улагоджування інцидентів.

Користувачі СУТ повинні:

1. Розуміти політику безпеки й обов'язки користувача. Розуміти, чому важлива підтримка безпеки СУТ.

2. Розуміти, як використовувати служби і механізми захисту, забезпечувані СУТ, щоб підтримувати безпеку СУТ і захищати критичну інформацію.

3. Розуміти, як використовувати можливості з улагоджування інцидентів, знати, як повідомляти про інцидент тощо.

4. Відрізняти нормальну роботу автоматизованого робочого місця або ПК від неправильної роботи.

Розглянуті аспекти політики безпеки корисно враховувати при її розробці для всіх об’єктів на кожному рівні СУТ.

Література: 1. Кононович В. Г. Класифікація інформації у мережах загального користування відносно технічного захисту інформації // Зв’язок. – 2000. - № 4. 2. В. Б. Булгак, Э. В. Евреинов, И .А. Мамзелев Теория и проектирование управляющих систем электросвязи. – М.: Радио и связь, 1995. – 384 с. 3. Кононович В. Г., Голобородько Д. В. Методи та засоби захисту від несанкціонованого доступу в системі управління мережами електрозв’язку України // - К.: Зв’язок, № 2, 1999, с. 13 - 16. 4. ETSI publications ETR 340. Telecommunications security. Guidelines for security management techniques.

УДК 621.396.2

ИНФОРМАЦИОННАЯ И ТЕХНИЧЕСКАЯ БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТРАНКИНГОВЫХ СИСТЕМ

Виктор Иванов

Украинский научно-исследовательский институт радио и телевидения (УНИИРТ)

Анотація: **Дано порівняльний аналіз можливостей гарантування інформаційної та технічної безпеки в цифрових транкінгових системах стандартів TETRA та TETRAPOL.**

Abstract: **The article deals with comparative analysis of informational and technical security guaranteeing possibility in digital trunking systems of TETRA and TETRAPOL systems.**

Ключевые слова: **Транкинговые системы, TETRA, TETRAPOL, угрозы системам подвижной связи, угрозы системным связям, угрозы связям пользователя, угрозы сообщениям связи.**

Введение

Необходимость в техническом перевооружении корпоративно-ведомственных систем связи и внедрении новейших радио технологий подтверждается реалиями функционирования систем связи государственных структур Украины. Наиболее полно специфическим требованиям к услугам подвижной связи в интересах государственных структур, министерств и ведомств отвечают современные цифровые транкинговые системы, имеющие возможности организации оперативных групповых и экстренных вызовов, гибкого перераспределения канальной емкости в соответствии с информационной нагрузкой, организации прямой радиосвязи в отдаленных и труднодоступных районах и т.д.

Учитывая необходимость обеспечения всех условий межведомственного взаимодействия в рамках единых корпоративно-ведомственных сетей подвижной связи целесообразным видится разворачивание не наложенных сетей отдельных министерств, ведомств и организаций, а Единой Национальной Сети

Конфиденциальной Оперативной Подвижной Радиосвязи (ЕНС КОПРС) как составляющей Единой Национальной сети связи Украины. При этом в качестве базовой системы при построении ЕНС КОПРС необходимо выбрать современный стандарт цифровой транкинговой связи.

В то же время одним из главных вопросов функционирования корпоративно-ведомственных сетей подвижной связи специального назначения является обеспечение полной информационной и технической безопасности и конфиденциальности информационных потоков.

Настоящая статья является продолжением дискуссии о выборе целесообразного стандарта цифровой транкинговой связи для ЕНС КОПРС [1, 2] и посвящена сравнительному анализу механизмов обеспечения безопасности в современных цифровых транкинговых системах стандартов TETRA (разработка Европейского института стандартов электросвязи – ETSI) и TETRAPOL (разработка французской фирмы “Matracom”).

I Классификация угроз системам подвижной связи

ЕНС КОПРС должна рассматриваться как важный элемент системы национальной безопасности Украины, в связи с чем ее создание должно осуществляться под управлением государственных органов, отвечающих за обеспечение конфиденциальности всех видов информации, которые составляют специализированный трафик системы. Неотъемлемым требованием построения ЕНС КОПРС является обеспечение полной информационной и технической безопасности от угроз, классифицированных на рисунке 1 [3].

Основываясь на полном пакете стандартов ETSI на цифровую транкинговую систему TETRA, а также пользуясь технической документацией фирмы “Matracom” на цифровую транкинговую систему TETRAPOL [4–11], проведем сравнительный анализ их возможностей противостоять рассмотренным типам угроз в аспекте целесообразности использования этих систем в качестве базовых при построении ЕНС КОПРС для силовых структур Украины.

Рисунок 1 – Классификация угроз в системах подвижной связи

II Угрозы сообщениям связи

Этот класс угроз включает те угрозы, которые направлены в первую очередь на индивидуальные сообщения, переданные в системе. Типичным объектом нападения может служить информационный обмен между двумя (или больше) пользователями системы, между операторами сети, между пользователем и поставщиком обслуживания.

Общая классификация угроз сообщениям связи представлена на рис. 2.

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

II.1 Перехват

Перехват представляет собой ситуацию несанкционированного изучения информации, переданной или сохраненной в системе подвижной связи, и относится как к государственным, так и частным сетям и ко всем видам информационного трафика.

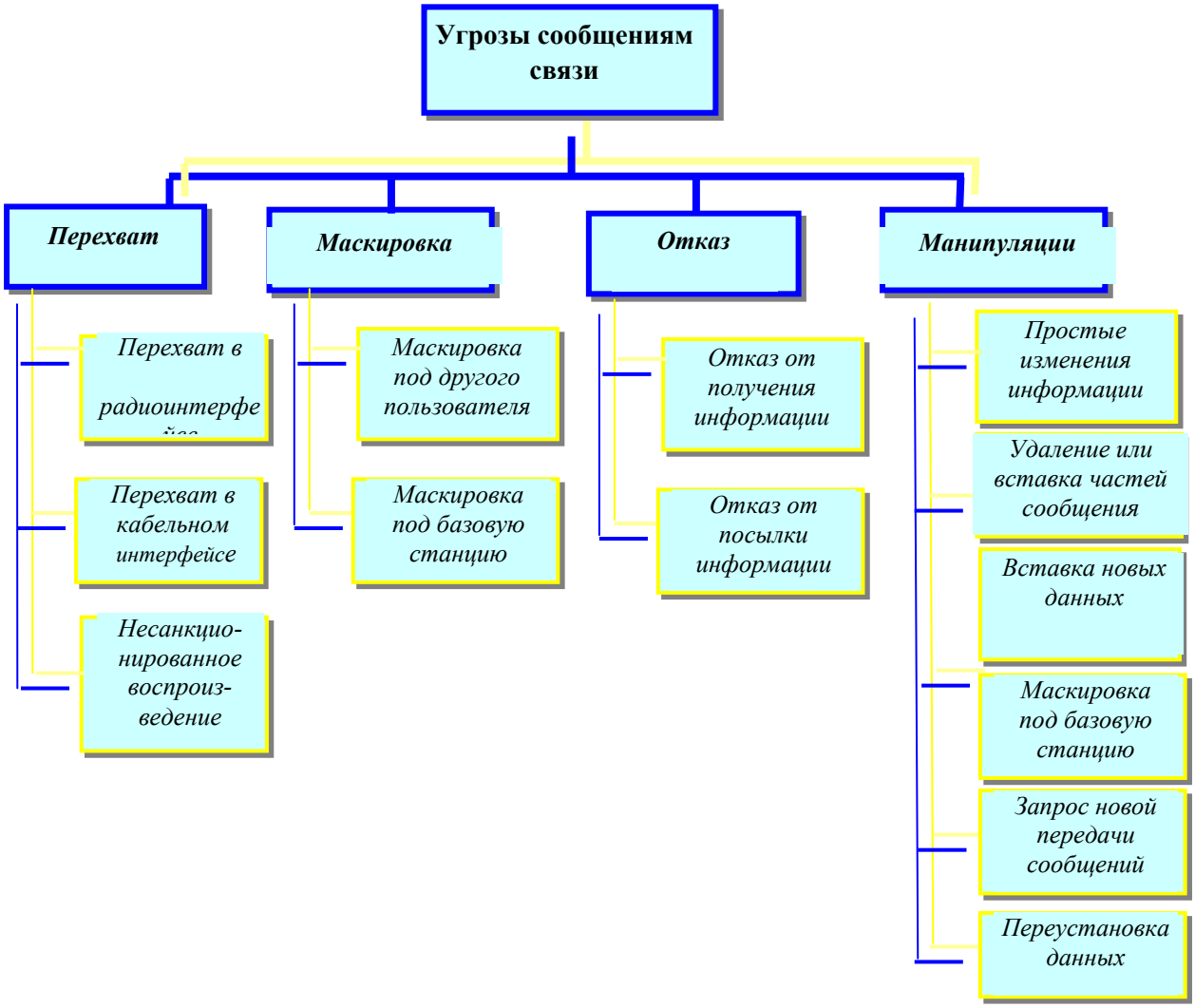

Рисунок 2 – Классификация угроз сообщениям связи

II.1.1 Перехват в радио интерфейсе

Перехват в радио интерфейсе является преобладающим типом угрозы из-за относительной простоты и доступности информации о характеристиках системы подвижной связи. Возможные нападения могут заключаться в желании получить доступ к важным данным и данным управления в интерфейсе между базовой станцией (БС) и мобильной станцией (МС) или маскировка под один из сетевых объектов на обеих сторонах радио интерфейса. При этом информация в режиме интегрированной передачи речи и данных на интерфейсе между БС и МС может быть перехвачена без нарушения первоначальной связи. Как и в случае аналоговых радио интерфейсов, перехват осуществляется с помощью сканеров, обладающих возможностью декодирования цифровых радиосигналов соответствующих протоколов. Помимо этого, пользователь системы мог бы использовать свою (возможно, с измененными параметрами или украденную) МС с целью прослушивания информационных каналов.

Эффективность этого рода нападения напрямую зависит от вида перехватываемой информации. В случае перехвата пользовательской речи или данных злоумышленникам становится известной конфиденциальная информация. При перехвате же данных управления злоумышленник может получить доступ к

идентификации пользователя или группы пользователей, его местоположении или уровне приоритета, идентификации или местоположении используемого терминала, перечне требуемого обслуживания и т. д. К тому же перехвату может подвергаться и информация о работе сети, связях с другими сетями и др. При этом интерес злоумышленников может представлять и информация, связанная с механизмами безопасности сети, например ключи, используемые для шифрования и аутентификации.

Подчеркнем, что результаты перехвата могут использоваться для поддержки других нападений, в частности при маскировке под другого пользователя или для управления некоторыми данными. Важно отметить, что несанкционированный перехват данных на интерфейсе между БС и МС систем подвижной связи никогда не может быть обнаружен или полностью предотвращен механизмами системной безопасности. В то же время применение шифрования дает возможность удостовериться, что перехваченная информация не понятна другим, несанкционированным для ее получения пользователям.

В таблице 1 представлен полный перечень механизмов борьбы с перехватом в радио интерфейсе, обеспечиваемых системами цифровой транкинговой связи стандартов TETRA и TETRAPOL [4], [5].

Таблица 1

Механизмы борьбы с перехватом в радиоинтерфейсе
1. взаимная аутентификация через интерфейс между БС и МС;
2. шифрование интерфейса между БС и МС;
3. шифрование между оконечными точками;
4. механизм передачи ключей шифрования по интерфейсу между БС и МС (OTAR).

На первый взгляд системы предоставляют одинаковый уровень защиты от перехвата в радио интерфейсе, используя как аутентификационные механизмы, так и ключи шифрования. Тем не менее, система TETRAPOL обладает рядом недостатков:

- использование механизма автоматической смены ключей (OTAR) приводит к окончанию информационной передачи и необходимости ее повторной инициализации;
- согласно документации [6] передача ключей (с аутентификацией и без) по радио интерфейсу для системы TETRAPOL не является обязательной функцией;
- механизмы аутентификации терминального оборудования инициируются периодически или по запросу оператора;
- идентификация пользователя осуществляется на основании псевдонима, данного системой после регистрации. При использовании мультисайтового открытого канала (в момент его освобождения) пользователю потребуется регистрация, осуществление которой приведет к присвоению абоненту нового псевдонима. Очевидно, что частое использование мультисайтового открытого канала, особенно, с целью экстренных вызовов, может привести к отказу работы всей системы шифрования;
- для шифрования между оконечными точками используются разные алгоритмы, например, в зависимости от процедур роуминга (национального или международного) используется свой тип алгоритма. Тем самым мигрирующий между различными зонами пользователь не сможет в полной мере использовать механизмы шифрования.

II.1.2 Перехват в кабельном интерфейсе

Перехват информации в кабельных интерфейсах систем подвижной связи характеризуется теми же самыми видами нападений**,** что и перехват в радио интерфейсе. Сам термин "кабельный интерфейс" используется для описания всех узлов и связей сети за исключением МС и радио интерфейса между МС и БС. Единственное различие заключается в необходимости получения доступа к физическим объектам или проводным линиям системы или связанной сети, например к телефонной сети общего пользования.

Перехват в кабельном интерфейсе как тип нападений может реализовываться следующим образом: злоумышленник может выявлять любой проводной интерфейс системы и, используя коммерчески доступный (и возможно измененный) анализатор протокола, принимать посланную информацию. Интересно обратить внимание на тот факт, что этот тип нападения нуждается в физическом доступе к узлу сети, например БС, в отличие от пассивного прослушивания, описанного выше.

Перечень основных механизмов борьбы с перехватом в кабельных интерфейсах представлен в таблице 2. Важно отметить, что на сегодняшний день на квантовом уровне возможно обнаружение (хотя и не предотвращение) с высокой степенью достоверности перехвата данных в кабельных интерфейсах систем подвижной связи.

Анализ документации на систему TETRAPOL выявляет следующие особенности обеспечения этой системой борьбы с перехватом в кабельных интерфейсах. В целях улучшения качества связи в системе

Таблица 2

Механизмы борьбы с перехватом в кабельных интерфейсах	
TETRA	TETRAPOL
1. шифрование между оконечными точками; 2. обеспечение защиты информации на БС.	1. шифрование между оконечными точками.

TETRAPOL происходит скремблирование служебной информации, что в совокупности с различным цифровым и канальным кодированием речевых и служебных сигналов существенно затрудняет применение элементов безопасности на БС [7], [8].

II.1.3 Несанкционированное воспроизведение информации

Несанкционированное воспроизведение информации является следствием осуществления перехвата и стоит в раскрытии злоумышленниками конфиденциальной пользовательской или служебной информации. Защита против воспроизведения обеспечивается при помощи инициализации переменных во времени ключей шифрования информационных потоков. К тому же регистрация и воспроизведение полного сеанса вызова может быть предотвращена при помощи введения в информационный поток дополнительных данных.

Таблица 3

Механизмы борьбы с несанкционированным воспроизведением информации
1. использование ключей шифрования; 2. механизм автоматической смены ключей по интерфейсу между БС и МС (OTAR).

В вопросе предотвращения несанкционированного воспроизведения информации (табл. 3) системы TETRA и TETRAPOL обеспечивают одинаковые уровни защиты, за исключением негибкости механизма OTAR для системы TETRAPOL. Как и в случае с перехватом в радио интерфейсе использование этой системой механизма автоматической смены ключей (OTAR) приводит к окончанию информационной передачи и необходимости ее повторной инициализации [5, 9].

II.2 Маскировка

Для маскировки существуют следующие возможности:

1) маскировка под другого пользователя (или терминал) с целью получения информации**,** предназначенной этому пользователю.

2) маскировка под БС для получения интересующих вызовов от МС.

Маскировка под другого пользователя может осуществляться как на радио- та и на проводном интерфейсе, и является более сложным вариантом, нежели маскировка под БС в радио интерфейсе. Специальным случаем маскировки выступает маскировка под объект системы на интерфейсе, который не постоянно устанавливает соединение, типа межсистемного интерфейса между двумя системами подвижной связи разных стандартов, связанных через транзитную сеть. Важно отметить, что при маскировке интерес для злоумышленника представляют прежде всего служебные данные, отвечающие за безопасность системы, то есть аутентификационные данные МС.

Возможными контрмерами против обоих типов маскировок, по существу, являются те же самые процедуры (табл. 4), что и в случае перехвата в радио интерфейсе, то есть шифрование и аутентификационные механизмы. К тому же маскировка под другого пользователя может быть выявлена с помощью переустановки данных.

Таблица 4

Механизмы борьбы с маскировкой
1. взаимная аутентификация через интерфейс между БС и МС; 2. шифрование интерфейса между БС и МС; 3. шифрование между оконечными точками; 4. механизм передачи ключей (OTAR).

Отметим, что в режиме защиты от маскировки система TETRAPOL обладает теми же недостатками, что и в режиме защиты от перехвата в радио интерфейсе [6, 9].

II.3 Манипуляции

В общем случае манипуляции представляют собой вид угроз, заключающихся в возможности несанкционированного изменения информации в системе. Это относится как к государственным, так и частным сетям связи и ко всем видам передаваемой информации. Согласно степени проникновения манипуляционных механизмов в систему подвижной связи могут различаться следующие угрозы.

II.3.1 Манипуляции в радио интерфейсе

Типичный сценарий манипуляции данными в радио интерфейсе системы подвижной связи выглядит так: передатчик одной МС настроен на тот же самый канал, что и передатчик другой МС, но с большим уровнем мощности передачи. Подобная ситуация может произойти и случайно, когда МС №1 посылает сигнал к БС № 1 в то время как МС №2 посылает сигнал к БС №2 на той же самой частоте и временном слоте. Вполне вероятно, что, не имея возможности различить пакеты от разных МС, БС № 1 воспринимает данные от МС № 1 как информацию, поступившую от МС №2. Конечно, это может быть выполнено и преднамеренно, и в зависимости от технических возможностей злоумышленника модификация может достигать очень высокого уровня.

Характерной особенностью модификации является то, что не все ее виды могут осуществляться в радио интерфейсе системы подвижной связи. Во-первых, у злоумышленника отсутствует возможность повторного запроса речевой информации и данных пользователя, поэтому удалить ее можно лишь косвенным путем, например, переполнением декодера ошибочными сообщениями. Во-вторых, умышленные вставки новых данных и речевых сигналов возможны только в паузах передачи, для чего применяется маскировка под пользователя или БС. При этом даже не обязательно расшифровывать сообщения, можно просто их воспроизводить со вставками. Этот тип нападения может распространяться и на механизмы аутентификации, когда путем переустановки некоторых аутентификационных данных (например, идентификаторов и паролей) происходит срыв опознавательных процедур.

В случае осуществления речевого вызова, когда обе стороны знают друг друга, единственно возможным нападением видится запись некоторых данных, и затем (возможно, после некоторой переустановки) - речи. Тем не менее, для вызовов, когда стороны сообщения не знают друг друга или не гарантирована точная идентификация голоса, возможна вставка собственного голоса злоумышленника.

Типичными объектами модификаций становятся данные управления, как то идентификация отправителя и/или получателя, его местоположение, идентификация уровня приоритета, заголовки некоторых данных. Эти модификации могут использоваться для нарушения маршрутизации некоторой информации или с целью маскировки под другого пользователя. Злоумышленник может изменять данные управления, например, организовывать изоляцию некоторых системных узлов, что может использоваться для финансовых махинаций.

К сожалению, приходится констатировать, что нападения манипуляции не могут быть предотвращены алгоритмическими механизмами безопасности. Все, что может быть выполнено, это применение механизмов, позволяющих получателю информации обнаруживать манипуляции с высокой вероятностью (табл. 5).

Таблица 5

Механизмы борьбы с манипуляциями в радио интерфейсе
1. взаимная аутентификация через интерфейс между БС и МС; 2. шифрование интерфейса между БС и МС; 3. шифрование между оконечными точками; 4. автоматическая смена ключей (OTAR)

II.3.2 Манипуляции в кабельном интерфейсе

В отличие от радио интерфейса в кабельных интерфейсах систем подвижной связи возможны все виды манипуляции – удаление, повторный запрос и вставка данных без ограничения. Типичные сценарии нападений, в принципе, те же самые, что и манипуляции в радио интерфейсе, но со следующими добавлениями. В первую очередь, манипуляции в кабельном интерфейсе возможны при использовании оборудования, обеспечивающего доступ к управлению данными и речевыми сигналами, например, на БС. Такое нападение требует хорошего знания внутренней работы системы, поэтому злоумышленником может быть лицо из штата обслуживающего персонала.

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

Таблица 6

Механизмы борьбы с манипуляциями в кабельном интерфейсе
1. взаимная аутентификация через интерфейс между БС и Центром коммутации;
2. шифрование между оконечными точками.

Анализ механизмов борьбы с манипуляциями (табл. 6) в TETRA и TETRAPOL говорит о том, что ни одна из систем не имеет решающего преимущества в этом вопросе [10, 11].

II.4 Отказ

Отказ характеризует тот тип угроз, при котором одна из сторон, вовлеченных в информационный обмен, отвергает (возможно, частично) участие в связи. Отказ как тип угроз интересен тем, что потенциальные злоумышленники являются обычными пользователями системы, отправителями или получателями некоторых сообщений.

Могут различаться два вида угроз отказа:

1. отказ от получения информации;
2. отказ от посылки информации.

II.4.1 Отказ от получения информации

Эта угроза возникает в следующей ситуации: один абонент послал некоторое сообщение другому абоненту, и сообщение получено вторым абонентом. Однако, впоследствии получатель отрицает факт приема сообщения. С точки зрения внешнего пользователя это аналогично случаю, когда злоумышленник выдает себя за отправителя сообщения. Отказ от получения информации может быть предотвращен как криптографическими мерами безопасности, так и не криптографическими, как то: всесторонняя регистрация трафика заслуживающим доверия центром в комбинации с надежным установлением подлинности пользователей и др.

II.4.2 Отказ от посылки информации

Эта угроза возникает в следующей ситуации: один абонент послал некоторое сообщение другому абоненту, и сообщение получено вторым абонентом. Однако, впоследствии пославший сообщение абонент отрицает свое участие в связи. С точки зрения внешнего пользователя это адекватно выдаче себя за получателя сообщения.

Меры по борьбе с отказом от посылки информации являются аналогичными рассмотренным выше мерам предотвращения отказа от получения информации (см. табл. 7).

Таблица 7

Механизмы борьбы с отказом от участия в связи
1. взаимная аутентификация через интерфейс между БС и МС;
2. использование криптографических алгоритмов;
3. всесторонняя регистрация трафика.

III Угрозы связям пользователей

Этот класс угроз включает те типы нападений, которые направлены на изучение общего поведения пользователей системы. Общая классификация угроз связям пользователей представлена на рис. 3.

III.1 Анализ трафика

Для этого типа угроз первоочередной интерес представляет информация о характере передаваемой информации, а также о некоторых сообщениях, посланных в определенное время и на определенном интерфейсе. При этом в общем случае злоумышленники могут пользоваться теми же самыми средствами, что и в случае перехвата.

Конечно, шифрование содержания сообщения и, в максимально возможной степени - данных управления, являются достаточной предпосылкой для предотвращения анализа информационного трафика. Однако, даже если информационный трафик подвергнут шифрованию, возможны варианты использования его отдельных фрагментов для статистического анализа. Поэтому во избежание несанкционированного анализа

информационного трафика шифрование должно дополняться другими механизмами безопасности, например, вставкой фиктивных сообщений (см. табл. 8).

В режиме защиты от анализа трафика система TETRAPOL обладает теми же недостатками, что и в режиме защиты от перехвата в интерфейсе между БС и МС [4, 5].

Рисунок 3 – Классификация угроз связям пользователя

Таблица 8

Механизмы борьбы с анализом трафика
1. взаимная аутентификация через интерфейс между БС и МС;
2. шифрование интерфейса между БС и МС;
3. шифрование между оконечными точками;
4. механизм передачи ключей по интерфейсу между БС и МС (OTAR);
5. вставка фиктивных сообщений;
6. дополнение сообщений.

III.2 Наблюдаемость

Наблюдаемость в системах подвижной связи означает, что поведение определенных (не обязательно известных) пользователей в системе может находиться под постоянным наблюдением. Злоумышленник может изучать, например, типичное время осуществления вызовов, местоположение пользователя, его принадлежность к абонентским группам, уровень приоритета и т.д. С точки зрения внешнего пользователя наблюдаемость является просто специальным случаем анализа информационного трафика. Однако, этот тип угроз также охватывает случаи, когда пользователи или операторы системы пробуют собрать информацию относительно других пользователей, к которым они не имеют доступа.

Основным инструментом противодействия наблюдаемости является использование псевдонимов для анонимной посылки и получения сообщений (табл. 9). В то же время во избежание подбора злоумышленником пользовательской идентификации современные системы подвижной связи должны

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

обеспечивать механизмы периодической смены данных абонентской идентификации.

Таблица 9

Механизмы борьбы с наблюдаемостью	
TETRA	TETRAPOL
Применение временной идентификации (псевдонимов)	

Как и в случае борьбы с перехватом в радио интерфейсе система TETRAPOL обладает недостатками при осуществлении вызовов на открытом канале. Идентификация пользователя осуществляется на основании псевдонима, присвоенного системой после регистрации. При использовании мультисайтового открытого канала (в момент его освобождения) пользователю потребуется регистрация, осуществление которой приведет к присвоению абоненту нового псевдонима. Второй негативной особенностью является гарантированное участие абонентов системы TETRAPOL всего лишь в одной абонентской группе [10, 11].

IV Угрозы системным связям

Главное отличие угроз системным связям состоит в том, что они направлены не на определенных пользователей или отдельные сообщения, а на систему подвижной связи в целом или на ее отдельные части. Нападения этого класса служат для того, чтобы повредить целостность системы, получить доступ к системным ресурсам или внести изменения в ее функциональные возможности (см. рис. 4).

Рисунок 4 – Классификация угроз системным связям

IV.1 Повреждение обслуживания

Угроза преднамеренной блокировки обслуживания или вывода его из строя злоумышленником как в

рамках сети, так и вне ее представляет собой класс угроз повреждения обслуживания. Наиболее простыми для злоумышленника являются удаление и задержка сообщений в радио- и кабельных интерфейсах, которые могут осуществляться теми же методами, что и при манипуляциях. Другие типы угроз повреждения обслуживания, как то изменение конфигурации системы, преднамеренное создание «заторов» или злоупотребление дополнительным обслуживанием требуют дополнительных технических средств и достаточных знаний работы системы.

Приходится констатировать, что оператору бывает очень трудно защитить систему подвижной связи от многочисленных возможных нападений, которые ведут к повреждению обслуживания, так как вышеупомянутый список сценариев угроз является далеко не полным. Тем не менее, наиболее эффективными способами защиты системы против угроз подобного рода являются те же методы, которые используются для поддержки общей безопасности в случае отказа, то есть избыточность и системная гибкость. В дополнение к этому, эффективным средством борьбы против потенциальных злоумышленников может стать периодическая всесторонняя ревизия системной работы (табл. 10).

Таблица 10

Механизмы борьбы с повреждением обслуживания
1. применение информационной избыточности;
2. обеспечение гибкости системы;
3. всесторонняя ревизия функционирования сети.

IV.2 Несанкционированное и запрещенное использование ресурсов

Под ресурсами в данном случае понимается весь комплекс технических средств систем подвижной связи, например, радиоканалы, оборудование, обслуживание или базы данных системы. В случае, когда пользователь не обладает правом использования определенных ресурсов, возможными нападениями могут быть следующие сценарии. Во-первых, злоумышленник может маскироваться под другого пользователя и реализовывать права доступа этого пользователя для получения доступа к запрещенным ресурсам, например доступ к системе в целом, или доступ к определенным услугам. Во-вторых, злоумышленник может использовать украденное или не сертифицированное оборудование. Наконец, злоумышленник с достаточным знанием внутренней работы системы может приобретать дополнительные права доступа или обходить механизмы управления доступом. Использования запрещенных ресурсов можно избежать надежными механизмами пользовательской и операторской аутентификации, администрированием прав доступа и осуществлением управления доступом [8].

IV.2.1 Использование неуполномоченных ресурсов

В общем случае этот тип угроз возникает тогда, когда пользователь имеет право использования некоторых системных ресурсов, однако он начинает превышать предоставленные ему полномочия. Так, злоумышленник может использовать по своему усмотрению некоторую системную информацию, например сетевой оператор или поставщик обслуживания, может неправильно использовать некоторые персональные данные пользователей. К тому же возможен вариант использования системного оборудования вне уполномоченных прав доступа и обслуживания. Наконец, нападения этого типа могут быть направлены против организации доступа к системе с целью перераспределения уровней приоритетности, несанкционированное создание льготных прав доступа некоторым категориям пользователей и т. д.

Средства защиты против этого типа угроз включают в дополнение к методам аутентификации и механизмам управления доступом всестороннюю ревизию чрезвычайных действий в системе (табл. 11).

Таблица 11

Механизмы борьбы с использованием запрещенных и несанкционированных ресурсов
– взаимная аутентификация через интерфейс между БС и МС;
– управление доступом;
– администрирование функций и прав доступа;
– всесторонняя ревизия работы системы

Преимущества системы TETRA в вопросе защиты от использования запрещенных и неуполномоченных ресурсов связаны с более гибкими алгоритмами управления как системой в целой, так и процедурами доступа в частности, более эффективная организация администрирования сетей (огранизация приоритетности) [10, 11].

V Выводы

Общие принципы механизмов безопасности создаваемой Единой Национальной Сети Оперативной Конфиденциальной Подвижной Радиосвязи Украины (ЕНС КОПРС) должны основываться на требованиях законов Украины «О государственной тайне», «О защите информации в автоматизированных системах», Указе Президента Украины «Положение о криптографической защите информации в Украине», а также соответствующих документах ISO [3].

Как следует из проведенного анализа, этим требованиям в большей степени удовлетворяет стандарт на цифровую транкинговую систему TETRA, принятый всеми странами Евросоюза в качестве базового при построении национальных корпоративно-ведомственных сетей подвижной связи специального назначения. Выбор в качестве базовой системы при построении ЕНС КОПРС цифровой транкинговой системы стандарта TETRA будет не только способствовать построению в Украине новейшей высокотехнологичной системы оперативной конфиденциальной подвижной связи, но и заложит прочный фундамент эффективной интеграции отечественной системы связи в европейские и мировые телекоммуникационные структуры.

Литература: А. Г. Мильковский, О. Н. Кононенко. Об эффективности использования частотного спектра в системах стандартов TETRA и TETRAPOL/ ”Зв’язок”, № 4, 1999, с. 17-18. 2. В. Л. Банкет, В. А. Іванов. Аналіз ефективності систем цифрового рухомого радіозв’язку. // Зв’язок, № 6, 1999, с. 21-25. 3. ISO 7498-2 (1989): "Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture". 4. Radio Equipment and Systems (RES) / Trans-European Trounced Radio (TETRA) / Voice plus Data (V+D) / Part 7: Security / ETS 300 392-7 December 1996. 5. TETRAPOL Specifications; Part 16: Security; Part 1: Security services PAS 0001-16-1 Version: 2.1.0 Date: 30 January 1998. 6. TETRAPOL Specifications; Part 16: Security; Part 2: KSW – KMC interface PAS 0001-16-2 Version: 2.1.0 Date: 30 January 1998. 7. TETRAPOL Technical Report; Part 1: Guide to TETRAPOL features; Part 1: System Technical Report; TTR 0001-1-1 Version: 1.0.0 Date: 25 June 1997. 8. Trans European Trounced Radio (TETRA) system; Technical requirements specification Part 3: Security aspects ETR 086-3 January 1994. 9. TETRA security – the fundamental of the high performance system / Gert Roelofsen/ PTT Telecom/KPN Research – Chairman ETSI Project TETRA Working Group. 10. Terrestrial Trounced Radio (TETRA); Security aspects; Subscriber Identity Module to Mobile Equipment (SIM - ME) interface FINAL DRAFT pr ETS 300 812 September 1998. 11. TETRAPOL Specifications; Part 16: Security; +Part 3: Mechanisms, messages and algorithms. PAS 0001-16-3 Version: 2.1.0 Date: 30 January 1998.

УДК 621.391.052

ЗАЩИТА ИНФОРМАЦИИ НА ВОЛОКОННО-ОПТИЧЕСКИХ ЛИНИЯХ СВЯЗИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Александр Манько, Виктор Каток, Михаил Задорожний

Научно-инженерный центр линейно-кабельных сооружений Киевского института связи при Государственном комитете связи и информатизации Украины, г. Киев

Аннотация: **Рассматриваются особенности распространения электромагнитной энергии в оптическом волокне, а также возможности и основные пути обеспечения защиты информации от несанкционированного доступа на волоконно-оптических линиях связи.**

Summary: **In work is considered the features of electromagnetic power propagation in an optic fiber (OF), and also possibility and fundamental ways of provision of protection of the information from the non-authorized access on fiber-optic links of communication.**

Ключевые слова: **Защита информации, волоконно-оптические линии связи, несанкционированный доступ.**

Введение

В последнее время одним из наиболее перспективных и развивающихся направлений построения сети связи в Украине и в мире являются волоконно-оптические линии связи (ВОЛС). В области систем передачи информации с большой информационной емкостью и высокой надежностью работы ВОЛС не имеют конкурентов. Это объясняется тем, что они значительно превосходят проводные по таким показателям, как пропускная способность, длина регенерационного участка, а также помехозащищенность.

Считается, что ВОЛС, в силу особенностей распространения электромагнитной энергии в оптическом