5. *Петраков А. В., Основы практической защиты информации. 2-е изд. Учебн. Пособие. – М.: Радио и связь, 2000. – 376 с.* ***6.*** *"Положення про порядок здійснення криптографічного захисту інформації в Україні" затверджене Указом Президента України від 22 травня 1998 року № 505/98.* ***7.*** *Указ Президента України від 6 жовтня 2000 року № 1120 "Питання Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України".* ***8.*** *Порядок проведення сертифікації засобів криптографічного захисту інформації.* ***9.*** *"Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту конфіденційної інформації", затверджено наказом ДСТСЗІ СБ України від 30.11.99 № 53.* ***10.*** *"Положення про державну експертизу у сфері криптографічного захисту інформації", затверджено наказом ДСТСЗІ СБ України від 25.12.2000 року № 62.* ***11.*** *Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, НД ТЗІ 2.5-004-99, затверджено наказом ДСТСЗИ СБ України від 28.04.99 № 22.* ***12.*** *Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу, НД ТЗІ 1.1-003-99, затверджено наказом ДСТСЗИ СБ України від 28.04.99 № 22.* ***13.*** *Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі, НД ТЗІ 3.7-001-99, затверджено наказом ДСТСЗИ СБ України від 28.04.99 № 22.* ***14.*** *Харин Ю. С., Берник В. И., Матвеев Г.В. Математические основы криптологии. – Минск.: БГУ, 1999. – 182 с.* ***15.*** *Феллер В. Введение в теорию вероятностей и ее приложения. – М.: Мир, 1964. – 498 с.* ***16.*** *Tetrapol News. PMR: Digital radio standardisation update/ № 6, September 1996.* ***17.*** *Radio Equipment and Systems (RES)/ Trans-European Trunked Radio (TETRA)/Voice plus Data (V+D)/Part 7: Security/ ETS 300 392-7 December 1996.* ***18.*** *Trans-European Trunked Radio (TETRA) systems; Technical requirements specification Part 3: Security aspects ETR 086-3 January 1994.*

УДК 621.395, 621.391.82

ПУТИ ПОВЫШЕНИЯ БЕЗОПАСТНОСТИ РАДИОИНТЕРФЕЙСА В СЕТЯХ ОПОВЕЩЕНИЯ

Александр Романов, Сергей Ливенцев, Игорь Столяр
Научный центр связи и информатизации, г. Киев

Анотація: **Рассмотрены пути повышения безопасности радиоинтерфейса в сетях оповещения. Произведен анализ и систематизация угроз безопасности информации. Предложены методы борьбы с ними.**
Summary: **In the article considered way of raising safety радиоинтерфейса in networks of notification. Made analysis and systematization of threats of safety information.. Offered methods of struggle with them.**
Ключові слова: **система радиосвязи, радиоинтерфейс, защищенность.**

Одной из задач, которая требует своего развития на базе достижений современных телекоммуникационных технологий, является совершенствование сетей передачи сигналов оповещения и сопровождающих их сообщений и команд. Эта задача актуальна для Вооруженных Сил Украины, Министерства по Чрезвычайным ситуациям, Министерства Внутренних дел и ряда других министерств и ведомств.

При решении этой задачи необходимо учитывать ряд особенностей и специфических требований, предъявляемых к функционированию систем такого типа.

1. Для достижения высокой вероятности доведения сигналов с требуемой степенью достоверности целесообразно обеспечивать передачу и прием сигналов параллельно по нескольким каналам связи, образованным различными средствами связи.

2. Сообщения, с помощью которых передаются сигналы оповещения, имеют малый объем. Это дает возможность вводить достаточно большую избыточность с целью достижения высокой надежности и достоверности доведения сигналов до абонентов.

3. Интенсивность возникновения сигналов очень мала, поэтому необходимо применять специальные меры для повышения эффективности использования оборудования.

4. Сигналы несут особо важную информацию, что требует принятия специальных мер по скрытности, достоверности, высокой степени безопасности, надежности и защите передаваемой информации, а так же исключения приема ложных сигналов.

5. Жесткие требования ко времени доставки сообщений и тенденции его уменьшения по мере совершенствования средств поражения и их носителей.

6. Сигналы, как правило, передаются по принципу "сверху вниз" с постоянным увеличением количества абонентов на каждом участке системы. Это усложняет создание обратной связи для передачи подтверждения приема переданного сигнала.

С целью обеспечения удобства пользования и своевременности доведения сигналов до адресатов в сетях оповещения достаточно широко используются радиосредства. Радиоинтерфейсы используются как на уровне абонентского доступа, так и при построении выделенных направлений связи. Это требует поиска путей повышения безопасности связи в радиоинтерфейсах.

С целью анализа особенностей обеспечения безопасности радиосвязи рассмотрим ее обобщенную структурную схему, представленную на рис. 1.

Характерной особенностью систем связи ряда министерств и ведомств, например Вооруженных Сил, является наличие преднамеренных помех в радио тракте, а также возможное радиоэлектронное противодействие противника.

В настоящее время развитие защищенной радиосвязи является неотъемлемой частью повышения эффективности систем управления и передачи информации подвижным объектам. Одним из требований, предъявляемых к защищенной радиосвязи, является требование обеспечения защищенности [1].

Под угрозами понимают пути реализаций действий, которые считаются опасными. В [2-4] определено, что угрозы информации рассматриваются с точки зрения их нежелательного влияния на свойство системы и возможного его нарушения.

Таким образом, угроза – это потенциально возможное неблагоприятное воздействие на информацию, которое приводит к нарушению: конфиденциальности, целостности информации, доступности либо отказу в обслуживании, управляемости.

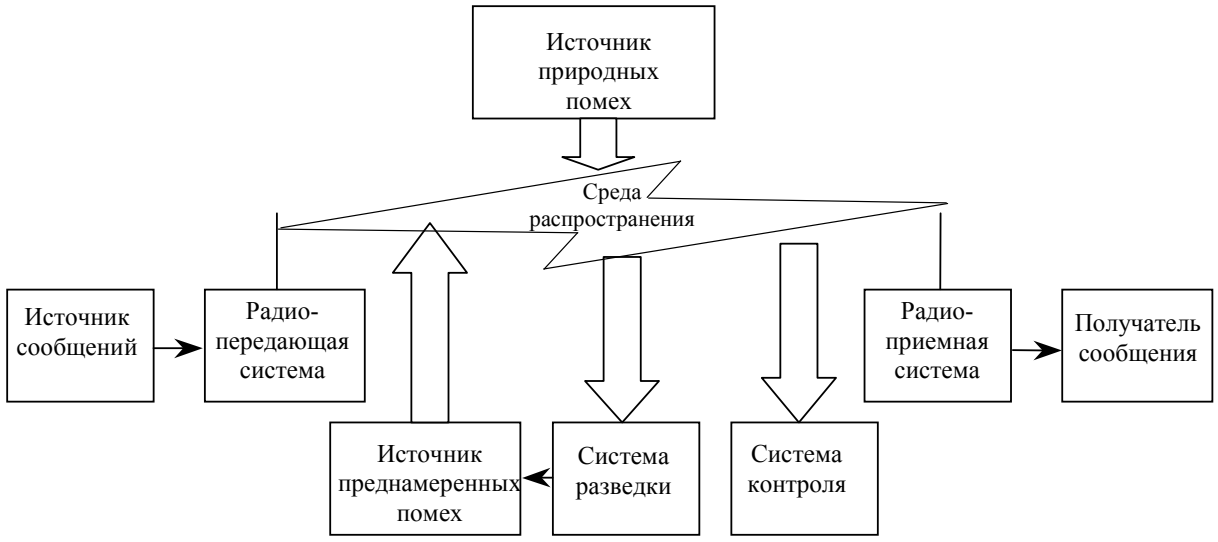

Рисунок 1 – Упрощенная обобщенная структурная схема системы радиосвязи, ее контроля, разведки и противодействия

Анализ угроз является одним из наиболее важных вопросов при построении защищенных систем связи. Функционирование систем радиосвязи военного назначения должно обеспечивать полную информационную и техническую безопасность и конфиденциальность информационных потоков.

Под полнотой защиты при обмене следует понимать множество типов угроз, от которых обеспечивается защита.

Среди способов повышения защищенности можно выделить следующие:

введение избыточности в саму информацию (использование корректирующих кодов);

введение избыточности в процесс обработки информации (использование аутентификации);

введение системной избыточности (повышение живучести системы).

Проведем анализ возможностей систем радиосвязи противостоять различным типам угроз с точки зрения целесообразности использования их в качестве базовых при построении системы связи для силовых структур Украины.

Рассмотрим 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 услуг обслуживания [5-7].

Такими угрозами являются: перехват, несанкционированное воспроизведение информации, маскировка, манипуляции данными в радио интерфейсе, радиоэлектронное подавление.

Рассмотрим эти угрозы подробнее с точки зрения возможности снижения уровня защищенности.

Перехват. Перехват представляет собой ситуацию несанкционированного изучения информации, переданной или сохраненной в системе радиосвязи, и относится ко всем сетям и ко всем видам информационного трафика.

Перехват может осуществляться как в радиоинтерфейсе, так и в кабельном интерфейсе.

Перехват в радио интерфейсе является преобладающим типом угрозы из-за относительной простоты и доступности информации о характеристиках системы беспроводной связи. Перехвату может подвергаться информация о работе сети, связях с другими сетями и др. При этом интерес противника может представлять и информация, связанная с механизмами безопасности сети, например ключи, используемые для шифрования и аутентификации.

Эффективность угроз такого вида зависит от вида перехватываемой информации. В случае перехвата пользовательской речи или данных противнику становится известной конфиденциальная информация. При перехвате данных управления, противник может получить доступ к данным идентификации пользователя или группы пользователей, данным о его местоположении или уровне приоритета, данным идентификации или местоположения используемого терминала, перечню требуемого обслуживания и т. д.

Результаты перехвата могут использоваться для поддержки и организации других нападений, в частности при маскировке под другого пользователя или для манипуляции некоторыми данными.

Основными способами борьбы с перехватом в радиоинтерфейсе являются:

взаимная аутентификация через интерфейс между базовой станцией (БС) и мобильной станцией (МС);

шифрование интерфейса между БС и МС;

шифрование между оконечными точками;

механизм передачи ключей шифрования по интерфейсу между БС и МС;

использование методов повышения скрытности радиосвязи (применение шумоподобных сигналов (ШПС), сигналов с псевдослучайной перестройкой рабочей частоты (ППРЧ)).

Можно отметить ряд недостатков присущих существующим системам радиосвязи.

1. Использование механизма автоматической смены ключей приводит к окончанию информационной передачи и необходимости ее повторной инициализации.

2. Передача ключей (с аутентификацией и без) по радиоинтерфейсу для системы радиосвязи не является обязательной функцией.

3. Механизмы аутентификации терминального оборудования инициируются периодически или по запросу оператора.

4. Идентификация пользователя осуществляется на основании псевдонима, данного системой после регистрации. При использовании открытого канала системы многостанционного доступа (в момент его освобождения) пользователю потребуется регистрация, осуществление которой приведет к присвоению абоненту нового псевдонима. Частое использование открытого канала в системах многостанционного доступа, особенно с целью экстренных вызовов, может привести к отказу работы всей системы шифрования.

5. Для шифрования между оконечными точками используются разные алгоритмы, поэтому мигрирующий между различными зонами пользователь не сможет в полной мере использовать механизмы шифрования.

Маскировка. Существуют маскировка под другого пользователя (или терминал) с целью получения информации, предназначенной этому пользователю и маскировка под БС для получения интересующих вызовов от МС.

Маскировка под другого пользователя может осуществляться как на радио, так и на проводном интерфейсе. Специальным случаем маскировки выступает маскировка под объект системы на интерфейсе, который не постоянно устанавливает соединение типа межсистемного интерфейса между двумя системами радиосвязи разных стандартов, связанных через транзитную сеть. Важно отметить, что при маскировке интерес для противника представляют, прежде всего, служебные данные, отвечающие за безопасность системы, то есть аутентификационные данные МС.

К основным способам борьбы с маскировкой относятся:

взаимная аутентификация через интерфейс между БС и МС;

шифрование интерфейса между БС и МС;

шифрование между оконечными точками;
механизм передачи ключей;
использование методов повышения скрытности радиосвязи (применение ШПС, сигналов с ППРЧ).

Манипуляции данными в радиоинтерфейсе. В общем случае манипуляции представляют собой вид угроз, заключающихся в возможности несанкционированного изменения информации в системе. Это относится ко всем сетям связи и ко всем видам передаваемой информации.

В зависимости от технических возможностей противника модификация может достигать очень высокого уровня.

Характерной особенностью модификации является то, что не все ее виды могут осуществляться в радиоинтерфейсе системы радиосвязи.

Типичными объектами модификаций становятся данные управления, такие как данные идентификации отправителя и (или) получателя, его местоположения, данные идентификации уровня приоритета, заголовки некоторых данных. Эти модификации могут использоваться для нарушения маршрутизации информации или с целью маскировки под другого пользователя. При этом противник может изменять данные управления, например, организовывать изоляцию некоторых системных узлов.

Угрозы манипуляции не могут быть предотвращены алгоритмическими механизмами безопасности. Все, что может быть выполнено, это применение механизмов, позволяющих получателю информации обнаруживать манипуляции с высокой вероятностью.

Для борьбы с манипуляциями в радиоинтерфейсе применяют:
взаимную аутентификацию через интерфейс между БС и МС;
шифрование интерфейса между БС и МС;
шифрование между оконечными точками;
автоматическую смену ключей;
методы повышения скрытности радиосвязи (применение ШПС, сигналов с ППРЧ).

Радиоэлектронное подавление. Несомненно, что условиями задачи оценки угроз защищенности в системах радио связи специального назначения должны учитываться и определенные факторы, связанные со стратегиями противника по выбору расположения средств радиоэлектронного подавления, маневру ими, маневру видами помех и т. д.

Соответственно в системе радиосвязи для каждого вида помехи необходимо выбрать способ передачи сообщения, обеспечивающий заданную защищенность (например, другой вид передачи, направленную антенну, дублирование направления несколькими видами радиосвязи и т. д.).

Необходимо различать обеспечение защищенности, обусловленное техническими возможностями каналов связи противостоять намеренным и взаимным помехам, и обеспечение защищенности, которая определяется организационными мероприятиями по радиоэлектронной защите системы в целом.

Для систем радиосвязи силовых министерств и ведомств наибольшую угрозу представляют преднамеренные помехи, которые может ставить противник.

Эффект воздействия помех сказывается в ухудшении качества обрабатываемой информации в результате ее разрушения либо старения, что увеличивает степень неопределенности при принятии решений.

Под действием помех радиоэлектронные средства и системы могут перестать быть источниками информации, несмотря на их полную исправность и работоспособность.

Так как подавить разнообразные радиоэлектронные средства помехами одного вида невозможно, то применяют специальные их виды, предназначенные для подавления конкретного вида связи.

Более того, для подавления средств одного и того же класса, но использующих различные виды сигналов способы их обработки, применяются отличающиеся друг от друга виды помех.

Систематизация изложенного материала позволяет произвести классификацию угроз в виде, представленном на рис. 2

Таким образом, проведенный анализ показывает, что повышение уровня безопасности систем военной радиосвязи целесообразно вести по следующим направлениям:

1) введение системной избыточности, а также введение избыточности в саму информацию и в процесс ее обработки.

2) наряду с использованием криптографических методов защиты необходимо принимать меры к повышению скрытности связи.

При этом следует учитывать, что наибольшей угрозой безопасности в сетях радиосвязи силовых министерств и ведомств является радиоэлектронное противодействие противника.

Рисунок 2 – Классификация угроз

Литература: ***1.*** *НД ТЗІ 1.1 002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу 32 с.* ***2.*** *Постанова ВРУ №81/34-ВР Закон України "Про захист інформації в автоматизованих системах"* ***3.*** *НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу 28/40.* ***4.*** *НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.* ***5.*** *ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення. Видання офіційне. ДСТУ. 1996 р.* ***6.*** *ДСТУ 3396.2-96 Захист інформації. Технічний захист інформації. Терміни та визначення. Видання офіційне. ДСТУ. 1997 р.* ***7.*** *ISO/IEC 15408:2000 - Information technology - Security techniques - Evaluation criteria for IT security. – Part 1: Introduction and general model.* ***8.*** *Тези V-ї Міжнародної науково-практичної конференції „Безпека інформації в інформаційно-телекомунікаційних системах". Корнейко О. В., Кувшинов О. В., Лівенцев С. П. Особливості побудови комплексних систем захисту інформації для широкосмугових радіосистем. – Травень 2002. – С. 52.*

УДК 621.395

ПЕРСПЕКТИВЫ ВНЕДРЕНИЯ В УКРАИНЕ СИСТЕМ СОТОВОЙ СВЯЗИ 3-ГО ПОКОЛЕНИЯ

Михаил Гряник, Георгий Карнаухов, Сергей Пасечник, Виктор Фролов
СП ТОВ "ІТС", г. Киев

Аннотация: **Рассматриваются перспективы внедрения систем сотовой связи третьего поколения (3G) в Украине. На основе мирового опыта внедрения систем 3G и анализа технико-экономической эффективности стандартов UMTS и CDMA-2000 сформулирован вывод о наилучшей перспективе**