УДК: 621.396.712: 004.056

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ РАДИОСЕТИ ВНУТРИ ЗДАНИЯ

***Жакыпбекова Керез Жакыпбековна**, магистрант КГТУ им. И. Раззакова e-mail: z.kerez@list.ru*
***Жумабаев Мыктарбек Жумабаевич**, к.т.н., профессор e-mail: myktarbekjumabaev@yahoo.com*

Целью статьи – является описание структуры радиосети, в которой ведутся защищенные переговоры с использованием радиооборудования, определение типов

потенциальных нарушителей информации безопасности, рассмотрение угроз информационной безопасности, рассмотрение средств защиты информации.

Ключевые слова: Радиосеть, радиооборудование, нарушитель ,безопасность, угроза, защита.

INFORMATION PROTECTION SYSTEM RADIO NETWORK INSIDE THE BUILDING

Zhakypbekova Kerez J., *undergraduate student of KSTU named after I.Razzakov. e-mail: z.kerez@list.ru*
Jumabaev Myktarbek Ju. *PhD (Engineering), Professor e-mail: myktarbekjumabaev@yahoo.com*

The purpose of the article is to describe the structure of the radio network in which secure negotiations are conducted using radio equipment, identifying types of potential infringers of security information, addressing threats to information security, and considering information security.

Keywords: Radio network, radio equipment, intruder, security, threat, protection.

Обеспечение безопасности при ведении переговоров в радиосистеме встает на первое место, когда передаваемая информация имеет конфиденциальный характер или является информацией ограниченного доступа, что особенно актуально для государственных ведомств и крупных коммерческих предприятий. Однако, именно тот факт, что информация представляет некий интерес, может побудить потенциального нарушителя к противоправным действиям.

Структура радиосети

В радиосети осуществляются как общие вызовы, так и индивидуальные вызовы. В радиостанции запрограммированы набор оперативных ключей шифрования.

- В соответствии с рисунком 1 в радиосети используются радиостанции :
- Базовая радиостанция – выполняет функции мониторинга и управления,
- Носимая радиостанция,
- Возимая радиостанция.

Основные технические характеристики радиосети связи:

- прием и отображение на дисплее информации об абоненте радиосети (ID абонента, местоположения абонента, текущего ключа шифрования, времени начала, конца и длительности сеанса связи),
- отображение местоположения абонента радиосети на электронной карте при его выходе на передачу, периодически и по запросам,
- ведение переговоров в радиосети,
- получение информации об абоненте при его выходе на передачу, по запросу с базовой станции или периодически,
- сохранение радио-переговоров и журнала оператора в БД,
- дистанционное прослушивание абонентских радиостанций,
- дистанционное выключение и включение приёмного и передающего трактов абонентских радиостанций,
- дистанционный опрос абонентских радиостанций по заданным ID кодам,
- шифрование информации и имитозащита.

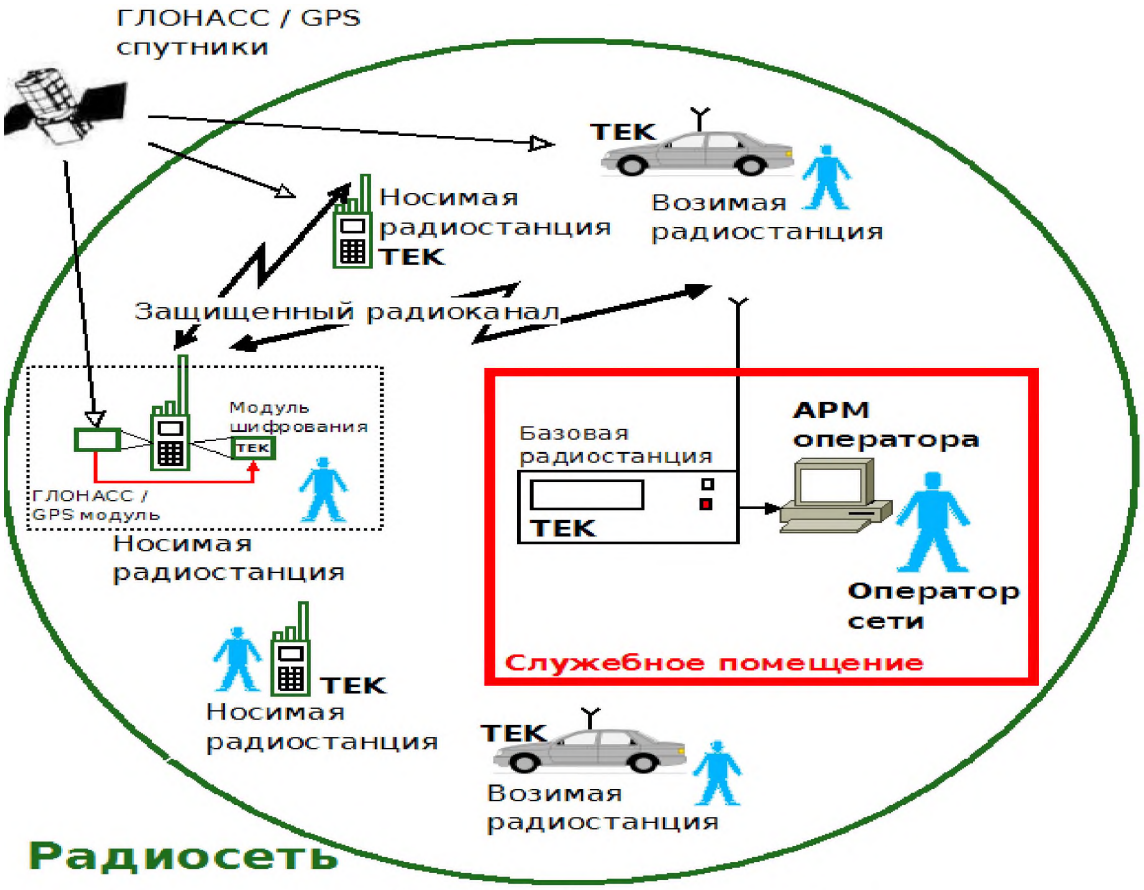

Рисунок 1 – Структура радиосети

Модель нарушителя

Нарушитель – это заинтересованное лицо, которое пытается осуществить НСД к информации или техническим средствам системы радиосвязи.

- Нарушители подразделяются на два типа:
- Внешние нарушители. Данные лица не имеют физического доступа к информации или техническим средствам радиосети
- Внутренние нарушители. Данные лица имеют физический допуск к информации или техническим средствам радиосети, могут являться зарегистрированными пользователями и пытаться получить доступ за пределами своих полномочий.

Угрозы со стороны внешнего нарушителя

Как показано на рисунке 2, внешний нарушитель в зависимости от уровня технической оснащенности может применять различные способы получения информации. Он может перехватить сигнал и попытаться дешифровать закрытое речевое сообщение. Нарушитель также может быть нацелен не на получение информации, а на выведение радиосистемы из работоспособного состояния. Он может перехватывать радиопереговоры, записывать их, может вносить некоторые изменения и снова повторять их в нужный момент в эфире . Нарушитель может создавать помеху, делая невозможным ведение переговоров на данной радиочастоте.

Рисунок 2 – Внешний нарушитель

Информационная безопасность в сетях радиосвязи

Информационная безопасность в сетях радиосвязи разделяется на три части: конфиденциальность, целостность и аутентификация, и управление ключами. Защита информации по этим трем направлениям позволит добиться наилучшего результата в обеспечении безопасности

Таблица 1 – Структура информационной безопасности в радиосетях

Конфиденциальность переговоров	**Целостность и Аутентификация**	**Управление ключами**
Должны применяться СКЗИ (средства криптографической защиты информации) определенного класса (уровня защиты)	Аутентификация и целостность сообщения: выработка имитовставки в режиме алгоритма ГОСТ 28147-89 (в СКЗИ) или MAC в режиме CFB в алгоритмах AES или D	Программирование ключей в радиостанцию с помощью программаторов ключей или устройств Key Loader.
Возможные алгоритмы блочного шифрования ГОСТ 28147-89, Уступ, AES, DES. Возможно применение алгоритмов поточного шифрования, например RC4	Хронологическая целостность используется для предотвращения появления в эфире передаваемых ранее сообщений. Используются окна допустимых номеров и MI	Безопасная передача ключей шифрования трафика ТЕК, применяя технологию OTAR (Over-the-Air Rekeying)
Требуется надежная синхронизация шифраторов на передающей и приёмной стороне	Аутентификация источника сообщения позволяет определить подлинность передающего абонент	Механизм управления ключами определяет момент смены и обновления ключей

Для алгоритмов шифрования и аутентификации требуется своевременная смена криптографических ключей по надежному каналу	При компрометации ключевой информации должна быть запущена процедура установки новых ключей

Заключение

Радиосвязь является основным видом связи с подвижными объектами, обеспечивающим управление органами и подразделениями правоохранительных и силовых министерств и ведомств, а в ряде случаев единственным видом связи, а также при ликвидации последствий стихийных бедствий. Важным преимуществом радиосвязи является ее высокая мобильность, то есть возможность изменения состава сети радиосвязи или полное ее перемещение без нарушения работы. Применение радиосвязи позволяет сконцентрировать в минимальные сроки и в нужном месте необходимое количество оперативных сил и средств для проведения мероприятий, согласовать по времени их действия и осуществлять единое руководство.

Для защиты радиосвязи нужно применять комплексный подход и учитывать все возможные угрозы информационной безопасности и нейтрализовывать их техническими и организационными мерам.

Список литературы

1. Терехов А.В, Чернышев А.В, Чернышев В.Н. Учебное пособие ТГТУ 2007-128 с.
2. Горбенко И.Д., Качко Е.Г., Потий, А.В. Решения и средства защиты информации. М.: «Форум-Инфра М», 2004. 528-533 с.
3. Спесивцев А. В. Защита информации в персональных компьютерах. М.: «Радио и связь», 1992. 140-149 с.
4. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство радиосеть», 2009 – 508 с.