УДК 004.056

# ЗАЩИТА АКУСТИЧЕСКОЙ РЕЧЕВОЙ ИНФОРМАЦИИ С ОГРАНИЧЕННЫМ ДОСТУПОМ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКОМУ КАНАЛУ ПРИ ИСПОЛЬЗОВАНИИ СРЕДСТВ МОБИЛЬНОЙ СВЯЗИ

Потоцкий С.В.,
Научный руководитель: Войцех С.И.
ГВУЗ «Национальный горный университет», http://bit.nmu.org.ua, E-mail: s90992p@uandex.ua

**Проанализированы методы и средства несанкционированного получения акустической речевой информации с использованием мобильных телефонов и средств мобильной связи, технические устройства противодействия утечке информации.**

**Ключевые слова – сотовая связь, мобильный телефон, канал утечки, блокиратор.**

Защита информации с ограниченным доступом от утечки по техническим каналам на объекте информационной деятельности достигается при применении совокупности организационных, инженерных и технических мероприятий и средств. При озвучивании информации в ходе закрытых совещаний, показов видеоматериалов со звуковым сопровождением особое внимание требует защита от утечки информации по прямому акустическому каналу.

Серьезную угрозу представляет использования возможности сотовой связи путем непосредственного применения мобильных телефонов, характеристики которых постоянно расширяются и модифицируются, и различных технических устройств на базе сотовой связи.

Простейший способ использования мобильного телефона в качестве закладного устройства - набор перед заходом в выделенное помещение номера абонента, который будет вести запись разговора.

Прослушивание также может осуществляться с использование специального приемника, настроенного на частоту стандарта GSM, с последующей записью и расшифровкой трафика.

Широкое распространение смартфонов привело к использованию программного способа прослушивания. Программа может быть установлена удаленно. В программе за ранее записан номер, при входящем звонке по которому мобильный телефон без видимых признаков включает микрофон, и передача информации происходит, как при обычном разговоре.

Возможно применение активного комплекса перехвата GSM-сигнала, представляющего собой ложную базовую станцию, которая становится посредником между реальной базовой станцией и мобильным телефоном. Ложная базовая станция перехватывает параметры соты и аутентифицируется мобильными телефонами в качестве обычной базовой станции. С этого момента возможно управление мобильным телефоном виртуальной базовой станцией, вплоть до перевода телефона в режим передачи без какой-либо индикации и без ведома его владельца (т. н. «полицейский режим»).

Для предотвращения утечки акустической информации через мобильный телефон могут использоваться пассивные и активные средства. К пассивным средствам относятся специальные чехлы, стаканы, сейфы, исключающие возможность воздействия акустического сигнала на телефон. Этот метод не обеспечивает защиту в случае, когда мобильный телефон скрыто установлен или занесен в выделенное помещение.

К активным средствам относится использования различных типов блокираторов, делающих невозможным установления связи с базовыми станциями. Классификация блокираторов представлена на рис. 1. Одной из основных характеристик блокираторов является радиус действия, который зависит от мощности блокиратора и от расстояния до базовой станции. Блокираторы по режиму работы можно разделить на три группы.

Блокираторы с ручным управлением создают шумовую помеху на диапазонах частот соответствующего стандарта работы базовых станций, делающую невозможным прием сигнала мобильными телефонами от базовых станций. Такие блокираторы обычно содержат от двух до четырех генераторов помех, охватывающих различные стандарты с возможностью включения в разных сочетаниях. Выходная мощность каждого генератора варьируется от 0,5 Вт до 2 Вт для портативных блокираторов и от 8 до 10Вт для стационарных. Основной недостаток - непрерывная работа вне зависимости от рабочего или нерабочего состояния мобильных телефонов.

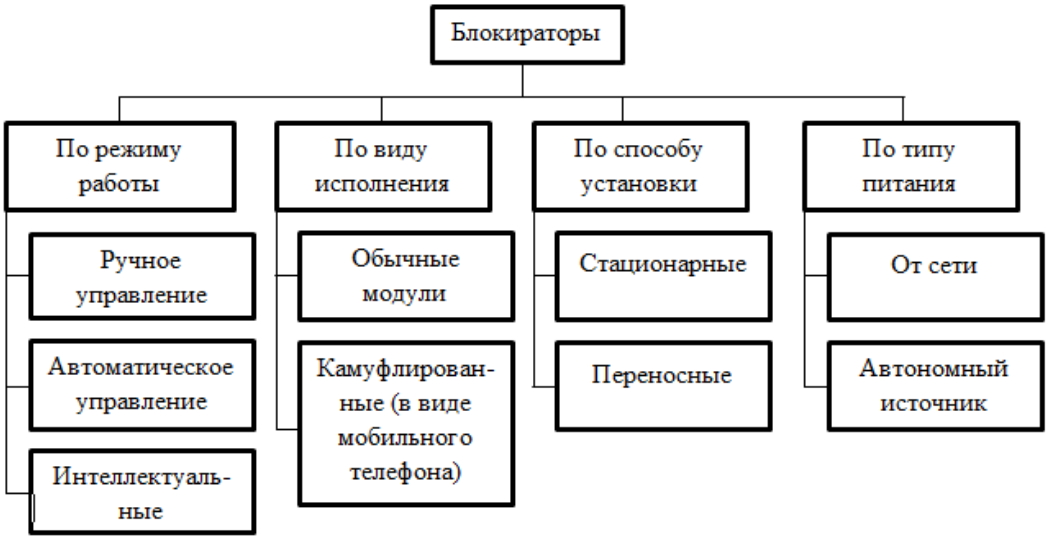


Рисунок 1. Классификация блокираторов

Подавители с автоматическим режимом работы содержат многоканальный приемник, который управляет включением генераторов блокиратора при появлении опасного сигнала. На входе приемника стоят полосовые фильтры, настроенные на частоты определенного стандарта сотовой связи. После выделения сигнала включается соответствующий генератор помех на несколько секунд, срывая установления сеанса связи. Такие блокираторы могут работать в режиме выявления опасного сигнала с постановкой или без постановки помех.

Интеллектуальные блокираторы содержит блок цифровой обработки. Приемник в коротком промежутке времени обнаруживает сигнал от мобильного телефона и вычисляет номер частотного канала и временной слот, выделенный конкретному телефону. Затем формируется заградительная помеха на частоте ответа базовой станции.

## ВЫВОД

Постоянное расширения функциональных возможностей мобильных телефонов и технических средств на основе сотовой связи создает новые возможности для перехвата акустической речевой информации, циркулирующей в выделенных помещениях и делает актуальным проведения работ по совершенствованию блокираторов различных видов.

## СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1. НД ТЗІ 1.1-005-07. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

2. Хорев А.А. Подавители средств сотовой связи и беспроводного доступа Журнал «Защита информации Инсайд» 2012 г.- №1 - с. 8-19.

УДК 004.056.52.001.362:57.087.1

# БІОМЕТРИЧНІ ЗАСОБИ ІДЕНТИФІКАЦІЇ У СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Дем’янюк Максим Юрійович, Мартиненко Андрій Анатолійович
ДВНЗ «Національний гірничий університет», http://bit.nmu.org.ua,
E-mail: jozephpalka@gmail.com

**Однією з головних проблем захисту інформації в сучасних комп'ютерних системах є несанкціонований доступ до ресурсів ІТС. Саме тому, коректна ідентифікація авторизованих користувачів відіграє дуже важливу роль у інформаційній безпеці ІТС.**

***Ключові слова – доступ; авторизація; методи; біометрія.***

## ВСТУП

Біометричні системи ідентифікації дуже добре зарекомендували себе на ринку інформаційної безпеки, але так і не набули широкого розповсюдження окрім дактилоскопічних методів ідентифікації. Це пов'язано з розповсюдженню думкою про високу вартість подібних систем, та відсутністю бажання керівників підприємств зіткатися зі змінами у існуючих системах безпеки. Але, переваги біометричних систем ідентифікації користувачів – незаперечні. Швидкість обробки даних, постійність авторизаційної інформації в поєднанні з доступною ціною, все це беззаперечно повинно схилити підприємців до впровадження біометричних систем ідентифікації.

Дактилоскопія – найбільш відомий та поширений метод встановлення особистості за біометричними параметрами, відмінно зарекомендував себе у криміналістиці 20-го століття і допоміг розкрити не одну сотню злочинів. Проте, технології не стоять на