Использование статистических данных при построении алгоритма противодействия террористической угрозе в сетях сотовой связи

Пановицын А.М.
Кафедра АСУ, электротехнический факультет
ГУВПО «Белорусско-Российский университет»
г. Могилев, Беларусь
e-mail: ykm@tut.by

***Аннотация* – Предложена процедура построения системы безопасности в сетях сотовой связи снижающая вероятность проведения террористических актов с использованием мобильных устройств в качестве радио-взрывателей. Показано, что допустимо использовать статистические данные учета стоимости разговоров в мобильной сети, хранящиеся в центре коммутации в качестве основного критерия определяющего активность абонентов и как следствие их потенциальную террористическую угрозу. Предложен критерий деления абонентов сотовой связи на группы, составляющие потенциальную угрозу.**

Ключевые слова: центр коммутации (MSC), опорный регистр местоположения (HLR), визитный регистр (VLR)

I. Введение

Одной из актуальных проблем современного общества является борьба с терроризмом. Большинство террористических актов, совершаемых в странах СНГ и на территории Республике Беларусь, связаны с использованием взрывчатых веществ. Для приведения в действие зарядов террористами часто используются радио-взрыватели, активируемые по каналам сотовой связи. Ярким примером тому служит последний террористический акт, произошедший 11 апреля 2011 года в Минске на станции метро «Октябрьская». Видеозапись камеры наблюдения метро, на которой террорист активирует взрывное устройство с помощью мобильного телефона, демонстрировалась по всем государственным телеканалам.

Сегодня ввиду повсеместного распространения сотовой связи актуальна проблема организации противодействия возможности использования GSM каналов в экстремистских целях. Для противодействия GSM радио-взрывателям в арсенале органов внутренних дел имеются подавители сигналов сотовых телефонов. Данные устройства предназначены для блокирования (подавления) радиоуправляемых взрывных устройств, выполненных на основе сотовых телефонов.

Подавители сигналов мобильных устройств эффективно работают по заданным диапазонам частот, не мешая другим устройствам связи. Но все эти устройства имеют одинаковый и очень существенный недостаток, они не подходят как средство профилактики и предупреждения террористической угрозы в местах большого скопления людей. Постоянное использование в общественных местах GSM подавителей лишит граждан связи, что противозаконно в большинстве стран мира.

Статья 13 Закона Республики Беларусь «О борьбе с терроризмом» позволяет в служебных целях использовать средства связи, принадлежащие гражданам, государственным органам и иным организациям независимо от форм собственности [1]. Данная статья допускает использование ресурсов операторов сотовой связи для реализации мероприятий, по снижению вероятности проведения террористических актов с использованием мобильных телефонов, что в свою очередь позволяет рассмотреть вопрос построения систем безопасности использования GSM сетей на платформе операторов сотовой связи.

II. Организационные мероприятия

Анализ информационных технологий применяемых в работе сетей сотовой связи позволяет использовать их возможности для значительного снижения вероятности проведения террористических актов с использованием мобильных устройств сотовой связи в качестве радио-взрывателей. В этой связи целесообразно говорить о комплексном подходе, включающем взаимодействие организационных и технических мероприятий.

Организационные мероприятия в первую очередь направлены на определение места и времени большого скопления граждан. Если общественно-массовое мероприятие планируется заранее (демонстрация, митинг, спортивный матч и т.д.) заявка подается в соответствующие органы с уведомлением операторов сотовой связи. В местах постоянного скопления граждан (ключевые станции метро, концертные залы, кинотеатры и т.п.) зоны местоположения стационарных объектов известны заранее. Зона местоположения (LA — Location Area) — группа сот. Это область, в которой вероятнее всего может в данный момент перемещаться абонент. Каждая зона местоположения обслуживается одним или более контроллерами базовых станций и только единственным центром коммутации мобильной связи. Каждой зоне местоположения назначен идентификатор зоны нахождения абонента (LAI — Location Area Identity) [2]. Информация о географическом положении используется при определении идентификационного номера групп сот для активации в них алгоритма системы безопасности.

III. Технические мероприятия

Технические мероприятия опираются на принцип работы центра коммутации обслуживающего определенную группу сот. Центр коммутации (MSC) является мозговым центром и одновременно диспетчерским пунктом системы сотовой связи, на который замыкаются потоки информации со всех базовых станций и через который осуществляется выход на другие сети связи – стационарную телефонную сеть, сети междугородной связи, спутниковой связи, другие сотовые сети [3]. MSC формирует данные, необходимые для выписки счетов за предоставленные сетью услуги связи, накапливает данные по состоявшимся разговорам и передает их в центр расчетов (биллинг-центр). MSC составляет также статистические данные, необходимые для контроля работы и оптимизации сети; он поддерживает

процедуры безопасности, применяемые для управления доступом к радиоканалам [2].

Следовательно, для статистического анализа активности абонентов и последующего их деления на группы, можно использовать статистические данные учета стоимости разговоров в сети. Маловероятно, что пренебрегая элементарной конспирацией и рискуя быть легко идентифицированным, потенциальный террорист станет активировать взрывное устройство с мобильного телефона, используемого для ежедневного общения. Вероятнее всего будет применяться устройство ранее не использовавшееся, приобретенное за границей или зарегистрированное на подставных лиц. Поэтому именно статистика использования услуг связи абонентом и будет являться главным критерием, определяющим его потенциальную угрозу.

Используя методы статистической обработки информации и анализа полученных данных, абонентов сотовой связи целесообразно классифицировать по группам:

1. Абоненты, ранее не пользовавшиеся услугами связи или использующие телефон крайне редко;
2. Абоненты, находящиеся в роуминге;
3. Абоненты, зарегистрированные в других регионах;
4. Абоненты, постоянно использующие услуги связи в данной местности.

Результатом анализа статистических данных будет временное изменение коммутационных возможностей определенной группы абонентов на момент их нахождения в зоне повышенной террористической опасности. Для удобства восприятия введем цветовую шкалу классификации абонентов сотовой связи:

1. Красный (абонент полностью исключается из обслуживания оператором сотовой связи на момент проведения мероприятия или нахождения в данной зоне обслуживания);
2. Оранжевый (временно отключается услуга голосового вызова, доставка SMS и MMS сообщений откладывается до окончания мероприятия или нахождения в данной зоне обслуживания, выход в интернет без ограничений);
3. Желтый (временно отключается услуга голосового вызова, допускается доставка SMS, MMS и доступ в интернет);
4. Зеленый (абонент пользуется услугами связи без ограничений).

Построение систем сотовой связи на основе информационных технологий позволяет включить в состав алгоритма безопасности специальную компьютерную программу. Основной задачей программы будет анализ и статистическая обработка данных об абонентах, поступающих с определенного визитного регистра центра коммутации обслуживающего потенциально опасный участок и выработка команд временной корректировки данных, о коммутационных возможностях, хранящихся в опорных регистрах операторов связи.

Результатом применения информационных технологий в борьбе с террористической угрозой в местах большого скопления людей будет снижение вероятности использования взрывных устройств активируемых по каналам сотовой связи. Наличие такой системы безопасности, возможно, могло предотвратить указанную ранее трагедию, произошедшую в Минском метро.

[1] О борьбе с терроризмом: Закон Респ. Беларусь, 3 янв. 2002 г., № 77-З: в ред. Закона Респ. Беларусь от 03.06.2011 г. // Консультант Плюс: Беларусь. Технология 3000 [Электронный ресурс] / ООО «ЮрСпектр». – Минск, 2011.

[2] А.Н. Берлин Цифровые сотовые системы связи. – М: Эко-Трендз, 2007. – 296 с: ил.

[3] Ратынский М. В. Основы сотовой связи / Под ред. Д. Б. Зимина. - 2-е изд., перераб. и доп. – М.: Радио и связь, 2000. – 248 с.: ил.