# Лабораторная работа № 5

## Исследование методов защиты терминала беспроводной связи Bluetooth

### 5.1. Цель лабораторной работы:

Ознакомление с методами защиты терминала беспроводной связи Bluetooth в системе Android.

Перед выполнением лабораторного задания студенты должны ориентироваться в основных аспектах информатики и иметь основные понятия о функционировании системы беспроводной связи Bluetooth и используемых методах защиты информации.

В результате выполнения лабораторного задания студенты должны получить навыки обеспечения защиты терминала беспроводной связи Bluetooth в системе Android.

### 5.2. Краткие теоретические сведения

В данной работе рассматриваются средства безопасности, используемые при передаче информации посредством технологии Bluetooth.

**Bluetooth** − технология беспроводной передачи данных по радиоканалу между различными типами электронных устройств с целью обеспечения их взаимодействия.

При разработке Bluetooth-интерфейса выдвигались следующие требования: аппаратура должна быть компактной, недорогой и экономичной, т. е. должна быть способна работать при малых значениях потребляемого тока.

Система Bluetooth позволяет объединять в одну беспроводную пикосеть (piconet) от двух до восьми различных электронных устройств, таких как, например, сотовый телефон, беспроводная гарнитура, ноутбук, цифровой фотоаппарат, принтер, клавиатура и др., но общее количество объединяемых устройств (как результат объединения пикосетей) может достигать 71.

По сравнению с интерфейсом беспроводной связи IEEE 802.11, работающим в том же диапазоне частот − 2,4 ГГц, Bluetooth-система обеспечивает меньшую скорость передачи информации (721 Кбит/с против 11 Мбит/с в стандарте IEEE 802.11b), меньшую дальность и меньшее число объединяемых в сеть устройств (максимально до 71 устройства у Bluetooth, 128 на одну сеть у IEEE 802.11). Но система Bluetooth может по трем каналам передавать голосовую информацию, а главное, более дешева (в десятки раз), малогабаритна и экономична.

Bluetooth способна осуществлять передачу данных даже при наличии препятствий и не только по принципу «точка−точка», но и по принципу «точка−много точек», что в положительную сторону отличает Bluetooth от технологии беспроводной инфракрасной связи IrDa, которая обеспечивает связь лишь в зоне прямой видимости и только по принципу «точка−точка».

#### Информационная безопасность системы беспроводной передачи данных Bluetooth

Конкретные средства обеспечения безопасности мобильного терминала зависят от конкретного терминала, наличия или отсутствия в нем предустановленной операционной системы и типа операционной системы, используемой в данном терминале.

Информационная безопасность системы беспроводной передачи данных Bluetooth базируется на использовании частотных шаблонов и необходимости синхронизации процессов приема и передачи данных, возможности реализации односторонней или двусторонней аутентификации, а также на шифровании передаваемых данных. Длина ключа шифрования может варьироваться от 8 до 128 бит, что дает возможность регулировать криптостойкость используемого алгоритма шифрования.

Хотя в Bluetooth предусмотрена криптографическая защита конфиденциальности передаваемых данных, а также процедура аутентификации, предназначенная для защиты от несанкционированного доступа к системе, возможны нарушения информационной безопасности устройств, снабженных Bluetooth.

Через Bluetooth-интерфейс возможна реализация следующих трех основных угроз информационной безопасности связи:

1) проникновение в абонентский аппарат мобильных вирусов и связанные с этим угрозы потери конфиденциальности передаваемой информации, а также целостности, доступности и конфиденциальности информации, хранящейся в абонентском аппарате;

2) перехват информации, передаваемой по радиоканалу системы Bluetooth;

3) дистанционный перехват управления абонентским аппаратом, позволяющий злоумышленнику осуществлять звонки и/или отсылку SMS и MMS сообщений за счет законного владельца аппарата, изменять настройки аппарата, считывать информацию, хранящуюся в памяти аппарата.

**Защита от атак на систему беспроводной передачи данных Bluetooth**

Технология Bluetooth предполагает выполнение 6-ти основных рекомендаций по ее безопасному использованию:

1) не следует оставлять систему Bluetooth включенной постоянно, включать Bluetooth рекомендуется только при необходимости (особенно опасно держать Bluetooth включенным в общественных местах: метро, торговых центрах, на вокзалах, в аэропортах и т. п.);

2) обязательным требованием является использование парольной защиты; рекомендуется использовать при соединении более длинные PIN-коды, чем четырехзначный код, желательно не менее, чем из восьми символов;

3) необходимо внимательно отслеживать сообщения системы о запросе устройств на подключение по каналу Bluetooth и разрешать подключение только, если есть уверенность в его безопасности;

4) осуществлять контроль за использованием устройств с Bluetooth-системой для подключения к локальным Wi-Fi сетям, так как их использование может быть эквивалентом созданию непредусмотренных дополнительных беспроводных точек входа в защищенную сеть;

5) соблюдать осторожность при соединении устройств, особенно в общественных местах, где выполнение «паринга» вообще нежелательно;

6) использовать защищенные от обнаруженных уязвимостей обновления программного обеспечения для устройств, использующих Bluetooth.

Рекомендация использовать достаточно длинные (не менее восьми символов) персональные идентификационные коды (PIN-коды) связана с тем, что PIN-коды используются при установлении шифрованной связи между Bluetooth-устройствами. Это является существенной уязвимостью в спецификации Bluetooth. Если атакующий имеет возможность контролировать

канал связи во время работы соединенных Bluetooth-устройств, а значит, перехватывать и записывать процесс соединения устройств, то он достаточно легко может определить короткие PIN-коды.

Наиболее вероятна реализация угрозы прослушивания радиоканала Bluetooth в общественных многолюдных местах, поэтому, по возможности, в таких местах следует избегать соединения Bluetooth-устройств.

Особого внимания требует ситуация, когда ранее соединенные устройства неожиданно требуют нового соединения − это может быть атака с попыткой инициировать соединение с целью наблюдения за информационным обменом. Для этого атакующий посылает подложное сообщение, выдавая себя за известное устройство и утверждая, что PIN-код забыт. В результате Bluetooth-устройство, получившее запрос на соединение, пытается повторить соединение, но теперь уже под контролем атакующего.

Если имеется возможность контролировать процесс установления соединения, то атакующий может вклиниться в обмен PIN-кодами и определить PIN-код с целью его последующего использования.

### 5.3. Лабораторное задание

При подготовке к лабораторному занятию следует предварительно изучить: методы передачи информации посредством технологии Bluetooth, основные угрозы безопасности Bluetooth и методы защиты.

1. Включить Bluetooth на двух или более смартфонах, используя их меню.
2. Включить режим обнаружения расположенных вблизи устройств Bluetooth.
3. Выбрать файл данных для его передачи с использованием технологии Bluetooth.
4. Выбрать получателя для передачи данных.
5. Произвести процедуру «спаривания» передающего и принимающего терминалов.
6. Передать файл.
7. Удостовериться в получении файла противоположной стороной.

## ПОРЯДОК ВЫПОЛНЕНИЯ ЗАНЯТИЯ

При выполнении задания рекомендуется соблюдать следующую последовательность:

1. Изучить методические указания к данному лабораторному занятию.
2. Выполнить лабораторную часть.
3. Ответить на контрольные вопросы.

## СОДЕРЖАНИЕ ОТЧЕТА

1. Краткие теоретические сведения по методам кодовой защиты мобильного терминала.
2. Выполненное задание.

## 5.4. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое технология Bluetooth?
2. Какие технические особенности технологии Bluetooth можно выделить?
3. Какие средства безопасности предусмотрены в технологии Bluetooth?
4. Сколько основных угроз и какие возможны при Bluetooth-связи?
5. Сколько основных рекомендаций и какие следует выполнять при Bluetooth-связи?

## 5.5 Библиографический список

### 5.5.1.Основная литература

1.Методические указания к данной лабораторной работе**.**

2. Конспект лекций.

### 5.5.2.Дополнительная литература

1. Варфоломеев А.А. Основы информационной безопасности: Учеб.пособие. – М.: РУДН, 2008. – 412 с.: ил.
2. В.А. Голуб. Информационная безопасность сотовой связи. Учебное пособие для вузов. Изд-во ВГУ. Воронеж 2007. – 43 с.
3. Электронный Интернет-ресурс: http://www.intuit.ru/department/network/lnetint/6/1.html
1. Hernacki Brian. Повышение безопасности технологии Bluetooth: какие меры могут быть приняты менеджерами IT-отделов и пользователями мобильных устройств. Электронный Интернет-ресурс: http://www.infosecurity.ru/_gazeta/content/060309/article01.shtml.