УДК 621.396

ОСНОВНЫЕ ПОДХОДЫ ПРИ ОРГАНИЗАЦИИ SMS-СПАМА И СПОСОБЫ ПРОТИВОДЕЙСТВИЯ

А.С. ШЕЛКОВ, Н.В. НАСОНОВА

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 25 октября 2015

Рассмотрены вопросы, связанные с актуальностью борьбы с SMS-спамом, основные способы организации SMS-спама и основные методы для его блокировки в сетях сотовой связи.

Ключевые слова: SMS-спам, сотовая связь, блокировка спама.

Введение

Статистика последних лет показывает рост SMS-трафика в сетях операторов сотовой связи. В основном данная тенденция наблюдается для трафика, генерируемого различными приложениями для спам-рассылок пользователям сетей сотовой связи. Для SMS-сообщений, которые рассылаются вредоносными программами, действующими на телефонных аппаратах абонентов, напротив, характерен спад из-за широкого распространения программ-мессенджеров: Skype, Viber и т. д.

Актуальность

Из-за особенностей организации сетей сотовой связи, поддерживающих технологию SMS, абоненты практически не защищены от спам-рассылок через SMS-сообщения. Динамика роста SMS-трафика оператора сотовой связи Республики Беларусь (ИП «Велком») изображена на рис. 1-3.

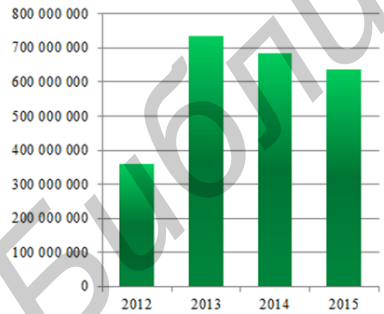

Рис. 1. Динамика роста абонентского SMS-трафика внутри сети

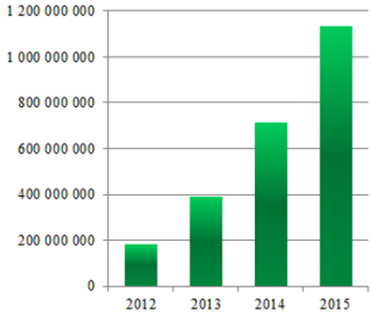

Рис. 2. Динамика роста SMS-трафика от приложений внутри сети

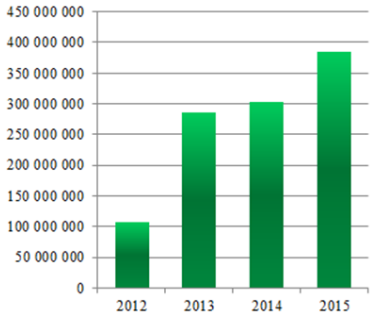

Рис. 3. Динамика роста SMS-трафика из других сетей

Анализ жалоб от абонентов РБ на различных информационных сайтах и порталах подтверждает рост доли SMS-спама среди общего объема трафика.

Угрозы SMS-спама для конечных пользователей:

1) расход памяти на телефонном аппарате (ТА) абонента;
2) заражение ТА вредоносным программным обеспечением (ПО);
3) мошенничество (SMS-викторины, SMS-казино);
4) отслеживание местоположения абонента;

5) причинение неудобств пользователям сетей сотовой связи.

Анализ способов организации спама

SMS-спам – массовая смс-рассылка коммерческого либо другого характера, организованная с использованием технологии SMS. По назначению он подразделяется на спам:

1) коммерческого содержания – используются рекламными организациями (рассылка рекламных сообщений, информаций о ссылках), банками (рассылка SMS онлайн-банкинга), торговыми предприятиями, а также любыми другими организациями, поскольку целевой диапазон использования таких рассылок достаточно широк;

2) вредоносного содержания – используются злоумышленниками для распространения вирусов, передачи бинарного кода на телефонные аппараты (ТА) абонентов, добывание персональных данных абонентов, причинение неудобств.

SMS-спам по способам организации подразделяется на:

1) MO-MT (Mobile Originated – Mobile Terminated) – SMS-трафик, формируемый вредоносными программами на ТА абонентов;

2) AO-MT (Application Originated – Mobile Terminated) – SMS-трафик, формируемый приложениями, которые имеют подключение к SMS-центру (SMSC) оператора сотовой связи.

На рис. 4, 5 изображены схемы организации MO-MT и AO-MT SMS-спама соответственно.

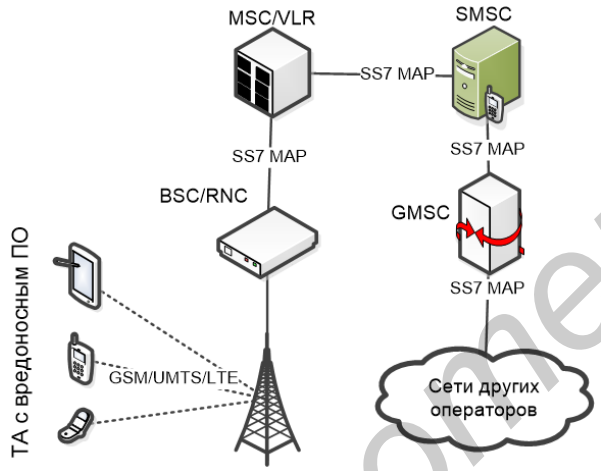

Рис. 4. Схема организации MO-MT SMS-спама

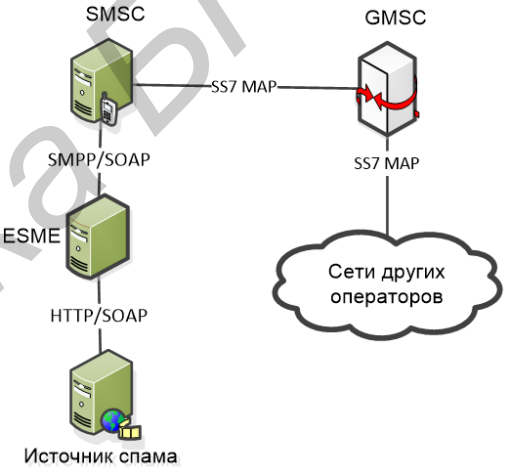

Рис. 5. Схема организации AO-MT SMS-спама

Обозначения на рисунках:

GSM (Global System for Mobile Communications) – технология сотовой связи второго поколения (2G);

UMTS (Universal Mobile Telecommunications System) – технология сотовой связи третьего поколения (3G);

LTE (Long-Term Evolution) – технология сотовой связи четвертого поколения (5G);

BSC (Base Station Controller) – контроллер базовых станций в 2G-сетях;

RNC (Radio Network Controller) – контроллер радиосети в 3G-сетях;

MSC (Mobile Switching Center) – коммутатор в сетях сотовой связи;

VLR (Visitors Location Register) – временная база данных абонентов;

SMSC (SMS Center) – сервер обработки и отправки SMS-сообщений;

GMSC (Gateway MSC) – коммутатор, который обрабатывает вызовы из внешних сетей и наоборот [1, 2];

SS7 MAP (Signalling System №7 Mobile Appication Part) – протокол системы общеканальной сигнализации №7 для обеспечения работы мобильных приложений в сетях сотовой связи, в частности SMS [3];

SMPP (Short Message Peer-to-peer Protocol) – протокол передачи коротких сообщений между приложением (ESME) и SMSC;

ESME (External Short Messaging Entities) – приложения рассылок коротких сообщений в спецификации протокола SMPP [4];

SOAP (Simple Object Access Protocol) – протокол обмена структурированными сообщениями в распределенной вычислительной среде;

HTTP (HyperText Transfer Protocol) – протокол прикладного уровня передачи данных.

Рассылка первым способом возможна при определенном количестве ТА с вредоносным ПО, иначе рассылка не будет массовой.

Наиболее используемый способ рассылки – второй. Источник рассылки (коммерческая организация либо злоумышленники) организовывает подключение с контент-агрегатором (ESME). Контент-агрегатор имеет постоянное подключение к SMSC оператора(ов) сотовой связи по протоколу SMPP (реже SOAP). Контент-агрегаторы – организации, предоставляющие свои услуги различным организациям в организации рассылок. Операторы сотовой связи, как правило, не взаимодействуют напрямую с другими организациями, так как последние не могут обеспечить необходимую интенсивность SMS-рассылок. Далее от SMSC рассылки идут через сети сигнализации SS7 и попадают в сети других операторов сотовой связи. Для транспортировки используется протокол MAP. Уже через сети других операторов SMS-рассылки достигают конечных абонентов [5].

Анализ возможных способов защиты

Перед анализом возможных методов защиты на уровне операторов сотовой связи необходимо отметить следующее: SMS-рассылки незаконного содержания, организованные через SMSC, легко могут быть приостановлены силами владельца этого же SMSC. Именно поэтому в дальнейшем будут рассматриваться SMS-спам из одной сети абонентам другой сети по SS7 MAP.

Путь попадания SMS в сеть сотовой связи извне по SS7 MAP в соответствии со спецификациями ETSI показан на рис. 6.

Рис. 6. Путь попадания SMS из других сетей

В соответствии со спецификациями ETSI для SMS в сети оператора 2 блокировать SMS-спам можно на GMSC и MSC. Реализация блокировки на уровне радиосети более затратная, так как компонентов радиосети во много раз больше и дальнейшая настройка механизмов блокировки будет занимать значительное время. Использование блокировки на уровне GMSC также не является предпочтительным, так как в современных коммутационных сетях каждый MSC является GMSC. Для стабильной и бесперебойной работы коммутационной сети в РБ операторам мобильной связи необходимо иметь от 7 до 10 MSC, поэтому настройка правил блокировки на таком количестве узлов также связана с большими затратами.

На данный момент для решения данной задачи применяется технология «Home Routing». Суть данной технологии для SMS заключается в том, что все SMS маршрутизируются на один MSC, который может одновременно включать в себя функционал SMSC. Такое решение значительно упрощает процесс настройки правил блокировки SMS-спама, поскольку все настройки осуществляются на одном узле сети и этот узел имеет функционал для обработки SMS [6].

SMS в SS7 сетях передаются с использованием протокола MAP. На входе в сеть поступающее SMS сообщение содержит следующую служебную информацию:

1) Originating Address/Destination Address (OA/DA) – номер отправителя/номер получателя;

2) OA/DA Type of Number (TON) – тип номера отправителя/получателя;

3) OA/DA Numbering Plan Indicator (NPI) – индикатор номерного плана отправителя и получателя;

4) Длина SMS в байтах;

5) DCS (Data Coding Scheme) – тип кодировки SMS [7];

6) Global Tittle (GT) SMSC оператора отправителя.

Это основные параметры, которые используются для блокировки SMS-спама. Просмотр текста SMS запрещен в рамках закона «Об информации, информатизации и защите информации» [8].

Методы блокировки SMS-спама.

1. По номеру отправителя.

Достоинства: простая реализация.

Недостатки: организатор спам-рассылки может сменить номер.

2. По TON и NPI номера отправителя. SMS, как правило, имеют следующие значения TON и NPI:

а) TON = 1, NPI = 1 – для абонентских номеров, например «375296452789»;

б) TON = 2, NPI = 1 – для коротких номеров, например «611»;

в) TON = 0, NPI = 5 – для альфанумерических номеров, например «Izbirkom».

SMS-спам обычно рассылается с коротких и альфанумерических номеров.

Достоинства: а) все SMS-рассылки с коротких и альфанумерических номеров из других или определенных сетей можно легко заблокировать; б) нагрузка на MSC/SMSC ниже, чем при блокировке отдельных номеров; в) смена номера при организации рассылок не поможет преодолеть блокировку.

Недостатки: а) SMS-спам можно рассылать с абонентских номеров; б) некоторые интернет-сервисы могут проводить рассылку через внешние SMSC и рассмотренный метод блокировки может привести к отказам для легальных пользователей сети.

3. По GT SMSC отправителя.

Достоинства: а) все подозрительные (серые) маршруты доставки SMS можно блокировать, оставив только разрешенные SMSC (яркий пример – австрийский оператор «A1»); б) нагрузка на MSC/SMSC становится ниже, чем при двух предыдущих методах; в) смена номера при организации рассылок не поможет преодолеть блокировку.

Недостатки: блокируется весь трафик, включая абонентский, а это может привести к большому числу жалоб от абонентов.

Указанный метод максимально эффективен, когда договоры о взаимодействии между операторами сотовой связи включают в себя пункты об ответственности за SMS-спам через свои SMSC.

На сегодняшний день серьезный вклад в борьбу с SMS-спамом вносят SMS-хабы – провайдеры, имеющие договорные отношения с различными операторами мобильной связи на предмет SMS-рассылок и ответственности за рассылку спама [9].

Заключение

Выбор метода блокировки SMS-спама должен основываться на используемых организаторами спама параметрах SMS-сообщений (адрес отправителя, GT SMSC отправителя) и на существующих договорных взаимоотношениях, регулирующих межсетевой обмен SMS-трафиком между различными операторами сотовой связи, SMS-хабами и другими сервис-провайдерами, которые осуществляют передачу SMS-трафика.

BASIC APPROACHES OF SMS-SPAM ORGANISATION AND PROTECTION

A.S. SHELKOV, N.V. NASONOVA

Abstract

SMS-spam protection issues, main approaches of SMS-spamming and basic methods of its blocking in cellular networks are discussed.

Список литературы

1. Specification GSM 03.02 – Network architecture. [Электронный ресурс]. Режим доступа: http://www.etsi.org/deliver/etsi_gts/03/0302/ 05.01.00_60/gsmts_0302v050100p.pdf.
2. Specification 3GPP TS 23.01U – General UMTS architecture. [Электронный ресурс]. Режим доступа: http://www.3gpp.org/DynaReport/2301U.htm.
3. Specification ETS 300 599 – GSM 09.02 version 4.17.1 – Mobile Application Part (MAP) specification. [Электронный ресурс]. Режим доступа: http://www.etsi.org/deliver/etsi_i_ets/300500_300599/300599/07_60/ets_300599e07p.pdf.
4. Short Message Peer to Peer. Protocol Specification v3.4. [Электронный ресурс]. Режим доступа: http://opensmpp.org/specs/smppv34_gsmumts_ig_v10.pdf.
5. Specification ETSI TS 100 901 – Technical realization of the Short Message Service (SMS) – Point-to-Point (PP). [Электронный ресурс]. Режим доступа: http://www.etsi.org/deliver/etsi_ts/100900_100999/100901/07.05.00_60/ts_100901v070500p.pdf.
6. Specification 3GPP TR 23.840 – Study into routeing of MT-SMs via the HPLMN. [Электронный ресурс]. Режим доступа: http://www.3gpp.org/DynaReport/23840.htm.
7. Specification GSM 03.38 – Alphabets and language-specific information. [Электронный ресурс]. Режим доступа: http://www.etsi.org/deliver/etsi_ts/100900_100999/100900/07.02.00_60/ts_100900v070200p.pdf.
8. Закон Республики Беларусь от 10 ноября 2008 г. №455-З «Об информации, информатизации и защите информации»
9. Официальный сайт компании «GMS». [Электронный ресурс]. Режим доступа: http://www.gms-worldwide.com/.