Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1246

Поправка 1
(05/2022)

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Безопасность киберпространства – Противодействие спаму

Технологии, используемые в организациях электросвязи для противодействия голосовому спаму

Поправка 1

Рекомендация МСЭ-Т X.1246 (2015) − Поправка 1

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (1)	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды (1)	X.1140–X.1149
Безопасность приложений (1)	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	X.1200–X.1229
Противодействие спаму	**X.1230–X.1249**
Управление определением идентичности	X.1250–X.1279
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (2)	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1319
Безопасность умных электросетей	X.1330–X.1339
Сертифицированная электронная почта	X.1340–X.1349
Безопасность интернета вещей (IoT)	X.1350–X.1369
Безопасность интеллектуальных транспортных систем (ИТС)	X.1370–X.1399
Безопасность технологии распределенного реестра (DLT)	X.1400–X.1429
Безопасность приложений (2)	X.1450–X.1459
Безопасность веб-среды (2)	X.1470–X.1489
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589
Киберзащита	X.1590–X.1599
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699
КВАНТОВАЯ СВЯЗЬ	
Терминология	X.1700–X.1701
Квантовый генератор случайных чисел	X.1702–X.1709
Структура безопасности QKDN	X.1710–X.1711
Проектирование безопасности QKDN	X.1712–X.1719
Методы обеспечения безопасности QKDN	X.1720–X.1729
БЕЗОПАСНОСТЬ ДАННЫХ	
Безопасность больших данных	X.1750–X.1759
Защита данных	X.1770–X.1789
БЕЗОПАСНОСТЬ СЕТЕЙ IMT-2020	X.1800–X.1819

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т X.1246

Технологии, используемые в организациях электросвязи для противодействия голосовому спаму

Поправка 1

Резюме

Голосовая связь является базовой услугой, предоставляемой сетями электросвязи. С развитием голосовой связи все более широкое распространение получает голосовой спам, связанный с многочисленными отрицательными последствиями для конечных пользователей и операторов сетей. Как правило, содержание голосового спама варьируется от коммерческой рекламы до оскорбительного порнографического материала, что оказывает различные виды негативного воздействия на конечных пользователей и операторов сетей. Голосовой спам может соблазнять, раздражать, угрожать и даже запугивать пользователей, а также отрицательно сказываться на сетевых ресурсах. Для того чтобы избежать этого негативного влияния, защитить права пользователей и обеспечить стабильность сети, операторам предлагается активизировать свои усилия по противодействию голосовому спаму.

Задачей Рекомендации МСЭ-Т X.1246 является обзор технических решений по противодействию голосовому спаму без учета риска аутентичности идентификационных данных спамера. В настоящей Рекомендации дается общее представление о голосовом спаме и приводится краткое описание существующих технологий противодействия спаму, которые используются пользователями и применяются в сетях электросвязи, а также механизма взаимодействия между ними. Кроме того, рекомендуются дополнительные предложенные технические решения, основанные на этих технологиях противодействия и механизмах взаимодействия.

Поправка 1 вводит механизм обратной связи от клиента, который принимает возможный спам-вызов (содержащий голосовое, короткое (SMS) или мультимедийное (MMS) сообщение), со своим оператором. Приведены технические требования к системам управления электросвязью и/или службам поддержки клиентов для получения уведомлений о входящих спам-вызовах, содержащих голосовые или SMS/MMS-сообщения. Представлены сценарии взаимодействия клиентов с операторами/поставщиками услуг сетей телефонной связи по вопросам входящих спам-вызовов, а также технические меры, необходимые для поддержания этого взаимодействия. Такое взаимодействие основано на осуществлении вызова на анти-спам номер, который заранее предоставляет оператор, получателем спам-вызова немедленно по завершении этого вызова.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1246	17.09.2015 г.	17-я	11.1002/1000/12448
1.1	МСЭ-Т X.1246 (2015 г.) Amd. 1	20.05.2022 г.	17-я	11.1002/1000/14988

Ключевые слова

Голосовой спам, Спам.

---

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL: http://handle.itu.int/, после которого укажите уникальный идентификатор Рекомендации.
Например, http://handle.itu.int/11.1002/1000/11830-en.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами/авторскими правами на программное обеспечение, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к соответствующим базам данных МСЭ-Т, имеющимся на веб-сайте МСЭ-Т по адресу: http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т X.1246

Технологии, используемые в организациях электросвязи для противодействия голосовому спаму

Поправка 1

Редакционное примечание. – Данная публикация содержит полный текст [Рекомендации]. Изменения, вносимые настоящей Поправкой, показаны в режиме отображения исправлений в тексте Рекомендации МСЭ-Т X.1246 (2015 г.).

1 Сфера применения

В настоящей Рекомендации дается общее представление о голосовом спаме и приводится описание существующих технологий, используемых для противодействия этому спаму, включая технологии, которые применяются в сетях электросвязи и используются пользователями, а также механизма взаимодействия между ними. Кроме того, в данной Рекомендации предлагаются дополнительные практические решения по противодействию спаму, такие как учетные данные о сигнализации, интерактивная верификация, меры пресечения и т. д.

В настоящей Рекомендации рассматриваются только вопросы противодействия голосовому спаму, исходящему из сетей электросвязи с коммутацией каналов, с учетом конкретных характеристик сетевой инфраструктуры. За информацией о технологиях противодействия голосовому IP-спаму следует обращаться к [ITU-T X.1244], [b-ITU-T X.1245] и [b-IETF RFC 5039]. Технологии, предотвращающие имитацию идентичности пользователей, не входят в сферу применения настоящей Рекомендации.

Перед введением в действие методов противодействия спаму, описанных в настоящей Рекомендации, следует проверить их соответствие всем актуальным законам и нормативным положениям.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие справочные документы могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

[ITU-T X.1240] Рекомендация МСЭ-Т X.1240 (2008 г.), *Технологии, применяемые при противодействии спаму, рассылаемому по электронной почте*.

[ITU-T X.1244] Рекомендация МСЭ-Т X.1244 (2008 г.), *Общие аспекты противодействия спаму в мультимедийных IP-приложениях*.

[ITU-T X.1247] Рекомендация МСЭ-Т X.1247 (2016 г.), *Техническая основа противодействия спаму при передаче сообщений на мобильные устройства*.

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах.

3.1.1 сеть с коммутацией каналов (circuit-switched network) [b-ITU-T M.60]: Сеть, предоставляющая соединения пользователям на эксклюзивной основе на время осуществления вызова или оказания услуги путем соединения каналов передачи или каналов электросвязи между собой.

3.1.2 IP-сеть (IP-based network) [b-ITU-T E.370]: Сеть, в которой протокол Интернет используется в качестве протокола ИСО третьего уровня (эталонная модель ВОС).

3.1.3 оператор (operator) [b-ITU-T M.1400]: Организация, ответственная за определение ресурсов электросвязи и управление ими. Оператор должен быть признан на законном основании администрацией электросвязи страны или ее делегацией. Оператор может соответствовать или не соответствовать торговому партнеру.

3.1.4 служба отчетов (reporting service) [ITU-T X.1247]: Служба, которая обеспечивает сбор и накопление отчетов о спаме абонента при наличии разрешения пользователя, а также в соответствии с нормативами и национальными законами.

3.1.5 услуга передачи коротких сообщений (SMS) [b-ITU-T X.1231]: Услугой передачи коротких сообщений называется один из видов услуг передачи сообщений, который позволяет мобильному телефону и другим объектам коротких сообщений передавать и принимать текстовые сообщений с помощью устройства, называемого центром обслуживания, которое реализует такие функции, как хранение и доставка.

3.1.6 спам-SMS (SMS spam) [b-ITU-T X.1242]: Спам, переданный через SMS.

3.1.7 спам [ITU-T X.1240]: Значение слова "спам" зависит от того, что понимается под конфиденциальностью в каждой стране, и от того, что представляет собой спам в техническом, социально-экономическом и практическом аспекте в национальном контексте. В частности, значение этого слова изменяется и расширяется с развитием технологий, открывающих все новые возможности для злоупотреблений электронными сообщениями. И хотя согласованного на международном уровне определения спама не существует, этот термин обычно используется для обозначения рассылаемых в массовом порядке по электронной почте или на мобильные устройства незапрашиваемых сообщений, целью которых является, как правило, маркетинг коммерческих продуктов или услуг.

3.1.8 спамер [ITU-T X.1240]: Объект или лицо, создающее и рассылающее спам.

~~**3.1.4 спамер (spammer)** [b-ITU-T X.1231]: Спамером называется объект или лицо, создающие и отправляющие спам.~~

3.2 Термины, определяемые в настоящей Рекомендации

В настоящей Рекомендации определяются следующие термины.

3.2.1 анти-спам номер (anti-spam number): Специальный заранее определенный домашним/собственным поставщиком услуг/оператором электросвязи телефонный номер (этот номер может быть уникальным в рамках страны или индивидуальным для каждого оператора), по которому пользователь уведомляет о спам-вызове, поступившем на его телефонный номер непосредственно перед осуществлением вызова на этот анти-спам номер. Уведомлением является сам факт вызова на анти-спам номер; пользователь не должен предоставлять какую-либо информацию.

3.2.2 программа-ловушка (honeypot): Программа (может устанавливаться в терминале), которая имитирует работу терминала или группы терминалов для выявления подозрительных голосовых спамеров и даже для содействия их верификации. Результаты работы этих систем можно использовать для сбора доказательств.

3.2.3 интерактивный отчет пользователя (interactive user report): Жалоба абонента, который получил на свой телефонный терминал вызов, содержащий спам или являющийся спамом. В целом, отчетом является вызов (факт вызова) на анти-спам номер или переадресация на анти-спам номер потенциального спам-вызова вместе с сообщением.

3.2.4~~3~~ управляющая структура (management entity): Структура, которая может иметь одну или несколько обязанностей по управлению, проверке или руководству деятельностью по противодействию голосовому спаму.

3.2.5 спам-вызов (spam-call): Телефонный вызов, содержащий голосовое, текстовое или мультимедийное незапрашиваемое сообщение, целью которого является, как правило, сбыт коммерческих продуктов или услуг.

3.2.6 потенциальный спам-вызов (suspicious spam call): Неопределенный телефонный вызов, который, как предполагается, является спам-вызовом.

3.2.74 сторонняя организация (third party organization): Организация, которая может проводить консультации, оказывать помощь или координировать работу в области противодействия голосовому спаму.

3.2.~~1~~8 голосовой спам (voice spam): Незапрашиваемые, автоматически набираемые, предварительно записанные телефонные вызовы, как правило, в целях продвижения коммерческих товаров или услуг. Содержание голосового спама варьируется от рекламы товаров до оскорбительных порнографических материалов. Голосовой спам может оказывать на пользователей и операторов вредное воздействие различного рода.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

Caller ID	Caller Identification	Идентификация вызывающей стороны
CAMEL	Customized Applications for Mobile Enhanced Logic	Специализированные приложения для расширенной логики подвижной связи
CCLTP	Call Clear Time Point	Момент отбоя вызова
CCOTP	Call Continued Time Point	Момент продолжения соединения
CDMA	Code Division Multiple Access	Многостанционный доступ с кодовым разделением каналов
CDR	Call Detail Record	Подробная запись о вызове
CDR_n	initial Call Detail Record	Подробная запись о первоначальном вызове
CDR_{n+1}	interactive Call Detail Record back from the user to its operator	Интерактивная подробная запись о вызове обратной связи, осуществляемом пользователем к своему оператору
CLI	Calling Line Identification	Идентификации линии вызывающей стороны
CLI_n	Calling Line Identification of initial caller to the user	Идентификация линии вызывающей стороны первоначального вызова к пользователю
CLI_{n+1}	Calling Line Identification of the user, when it makes feedback call to an anti-spam number	Идентификация линии вызывающей стороны – пользователя, осуществляющего вызов обратной связи на анти-спам номер
COSN	Call Originated Subscriber Number	Номер абонента, инициирующего вызов
COTP	Call Originating Time Point	Момент инициации вызова
CRBT	Customized Ring Back Tone	Специализированный сигнал контроля посылки вызова
CS	Circuit-Switched	С коммутацией каналов
CTSN	Call Terminated Subscriber Number	Номер абонента, завершающего вызов
DMP	Device Management Platform	Платформа управления устройством
GMSC	Gateway Mobile Switching Centre	Шлюзовой центр коммутации подвижной связи
GSM	Global System for Mobile communications	Глобальная система подвижной связи
HLR	Home Location Register	Домашний регистр местоположения

ID	Identification	Идентификатор
ISIS	Information Sharing System	Система совместного использования информации
IMS	IP Multimedia Subsystem	Мультимедийная IP-подсистема
IN	Intelligent Network	Интеллектуальная сеть
INAP	Intelligent Network Application Protocol	Прикладной протокол интеллектуальной сети
IP	Internet Protocol	Протокол Интернет
IVR	Interactive Voice Response	Интерактивный речевой ответ
MMS	Multimedia Messaging Service	Служба передачи мультимедийных сообщений
MSC	Mobile Switching Centre	Центр коммутации подвижной связи
OTAP	Over-the-Air Platform	Платформа беспроводной связи
PSTN	Public-Switched Telephone Network	Коммутируемая телефонная сеть общего пользования (КТСОП)
QoS	Quality of Service	Качество обслуживания
SCP	Service Control Point	Пункт управления услугами
SIM	Subscriber Identity Module	Модуль идентификации абонента
SLETP	Signalling Link Establishment Time Point	Момент установления канала сигнализации
SLRTP	Signalling Link Release Time Point	Момент освобождения канала сигнализации
SMS	Short Message Service	Служба коротких сообщений
SS7	Signalling System No. 7	Система сигнализации № 7
STP	Signalling Transfer Point	Пункт передачи сигнализации
UMTS	Universal Mobile Telecommunications System	Универсальная система подвижной электросвязи
VLR	Visitor Location Register	Визитный регистр местоположения
VMS	Voice Mail Server	Сервер голосовой почты
VoIP	Voice over Internet Protocol	Передача речи по протоколу Интернет

5 Условные обозначения

Отсутствуют.

6 Общее описание голосового спама

Голосовой спам – это незапрашиваемые, автоматически набираемые, предварительно записанные телефонные вызовы, как правило, в целях продвижения коммерческих товаров или услуг. Содержание голосового спама варьируется от рекламы товаров до оскорбительных порнографических материалов. Голосовой спам оказывает на пользователей и операторов вредное воздействие различного рода.

6.1 Сценарии голосовой связи

Голосовая связь – это основополагающая услуга, оказываемая операторами электросвязи. Изначально голосовая связь базировалась на традиционных сетях с коммутацией каналов (CS). С развитием интернета система голосовой связи расширилась, включив в себя передачу речи по протоколу Интернет (VoIP) в сетях на базе протокола Интернет (IP).

Ниже рассматриваются четыре сценария голосовой связи в зависимости от используемых технологий:

- сценарий 1: CS-CS – голосовая связь по традиционным сетям подвижной/фиксированной связи с коммутацией каналов;
- сценарий 2: CS-IP – голосовой вызов, инициированный пользователем сети подвижной/фиксированной связи с коммутацией каналов и завершенный пользователем IP-телефонии;
- сценарий 3: IP-CS – голосовой вызов, инициированный пользователем IP-телефонии и завершенный пользователем сети подвижной/фиксированной связи с коммутацией каналов;
- сценарий 4: IP-IP – голосовая связь между пользователями IP-телефонии.

Эти четыре сценария голосовой связи и соответствующие технологии показаны на рисунке 1.

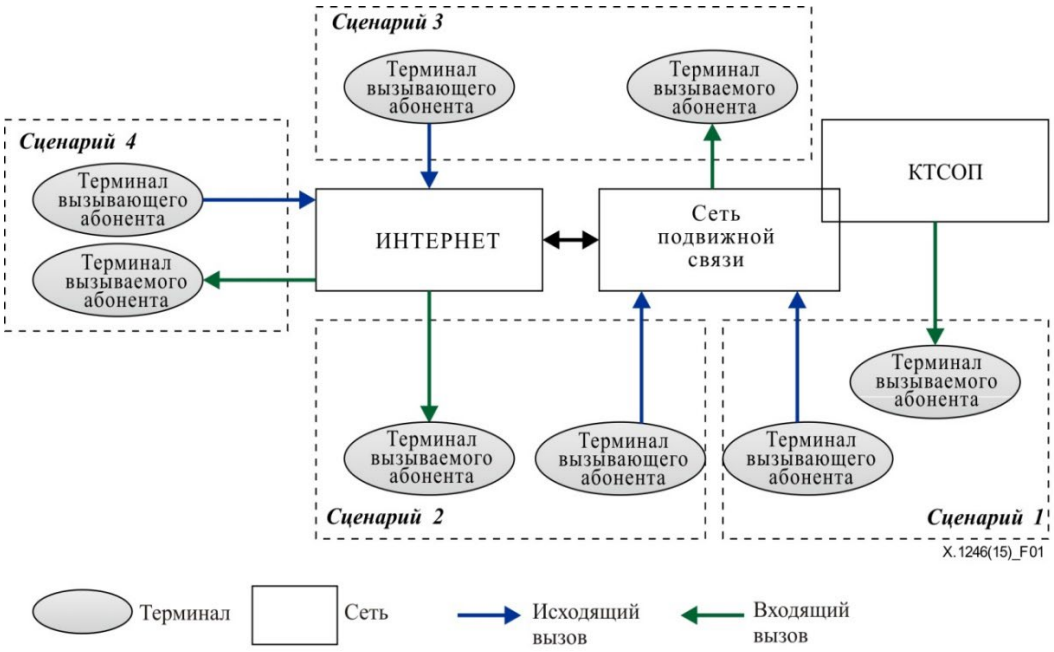

Рисунок 1 – Сценарии голосовой связи в сетях электросвязи

ПРИМЕЧАНИЕ. – Под термином "терминал", используемым здесь, на рисунке 1, могут подразумеваться мобильные телефоны, стационарные телефоны, ноутбуки, персональные компьютеры и т. п., при помощи которых можно получить доступ к сетям с коммутацией каналов/IP-сети. В целом большинство пользователей доверяют источнику голосовой связи. Соответственно, голосовые спамеры готовы использовать традиционную голосовую связь в сетях с коммутацией каналов для отправки голосового спама. Кроме того, следует отметить, что технологии противодействия голосовому спаму в сценариях 3 и 4 представлены в Рекомендации [ITU-T X.1244]. Поэтому настоящая Рекомендации посвящена лишь противодействию голосовому спаму в сценариях 1 (CS-CS) и 2 (CS-IP).

6.2 Характеристики голосового спама

С помощью голосового спама может распространяться различная информация – от рекламы товаров до оскорбительных порнографических материалов, – которая может оказать вредное воздействие на пользователей и операторов сетей электросвязи:

– голосовой спам может содержать информацию навязчивого, обманного, запугивающего или угрожающего характера;

– ресурсы пользователей и операторов могут расходоваться напрасно;

– пользователи и операторы могут быть вынуждены тратить время, деньги и усилия на противодействие голосовому спаму.

Наиболее широко признанные формы голосового спама делятся на два следующих типа (но не ограничиваются ими).

– **Первый тип ("молчаливый" вызов)**. "Молчаливый" вызов – это телефонный вызов в целях телемаркетинга, осуществляемый системой (или системами) автоматического обзвона и не предназначенный для его немедленной обработки агентом. В случае немедленного ответа система обзвона может завершить вызов, и тогда вызываемый абонент услышит в трубке тишину (прерванный сигнал) или сигнал телефонной компании, свидетельствующий о сбросе вызова. Термин "несостоявшийся вызов" обозначает то же самое. Как правило, в таких случаях следует ожидать повторного вызова.

– **Второй тип (беспокоящий вызов)**. Телефонный вызов в целях телемаркетинга, который может причинять беспокойство абонентам, раздражать, тревожить или запугивать их и содержать информацию порнографического характера, угрозы, незаконную информацию, ложную рекламу и т. д. Как правило, такие вызовы не прекращаются, пока их не примут.

7 Технологии противодействия голосовому спаму

7.1 Общие аспекты

Ни одно из решений само по себе не способно гарантировать полного успеха. Для смягчения негативного воздействия голосового спама необходимо реализовать широкий спектр решений с использованием соответствующих технологий, подразделяемых на сетевые и пользовательские, охватив сценарии 1 и 2, описанные в пункте 6.1.

В целях выработки рекомендаций по конкретным практическим технологиям необходимо углубленное рассмотрение характеристик сети с коммутацией каналов, включая архитектуру сети, топологию сети, стек протоколов сигнализации и т. д. Кроме того, рассматриваются процессы оказания услуг голосовой связи и тенденции развития функций терминалов. Предлагаемые технологии можно подразделить на сетевые и пользовательские.

Сетевые технологии имеют ключевое значение для операторов, то есть для коммутируемых телефонных сетей общего пользования (КТСОП), сетей универсальной системы подвижной электросвязи (UMTS), глобальной системы подвижной связи (GSM) и многостанционного доступа с кодовым разделением каналов (CDMA). По сравнению с сетевыми технологиями пользовательские технологии являются гораздо более гибкими и зависят от инициатив пользователей. Обратная связь с пользователями – необходимое дополнение к сетевым технологиям. Поэтому следует также создать эффективный механизм взаимодействия между этими двумя видами технологий.

7.2 Сетевые технологии

Каждый телефонный вызов начинается в сети доступа с сигнализации. Основной метод, который может быть использован для выявления подозрительного голосового спамера, заключается в сборе, анализе и проверке данных сигнализации. Этот метод следует подвергнуть всестороннему рассмотрению. В самом общем виде этап установления соединения включает подтверждение установления связи между двумя конечными точками соединения. На этапе установления соединения происходит только идентификация (ID) вызывающего абонента без идентификации вызываемого абонента. В связи с этим необходимо отметить следующее.

1) Любые решения по обработке вызовов необходимо принимать в режиме реального времени до завершения этапа установления соединения.

Спам ставит сложные технические проблемы, и поэтому решения по его устранению должны быть подкреплены соответствующими процедурами в сочетании с техническими мерами. В базовую процедуру по противодействию голосовому спаму на стороне сети можно было бы включить следующие процессы, представленные на рисунке 2.

Рисунок 2 – Процедура противодействия голосовому спаму на стороне сети

– **Запись и сбор данных сигнализации** – запись и сбор исходных данных сигнализации в режиме реального времени.

– **Анализ** – выявление подозрительных голосовых спамеров и составление списка их номеров.

– **Интерактивная верификация** – проведение прямой верификации для обнаружения реально существующих голосовых спамеров в списке подозрительных номеров.

– **Пресечение** – ограничение или блокирование действий голосовых спамеров, обнаруженных в процессе верификации в целях защиты правомерных пользователей.

В процедуру противодействия на стороне пользователя входят почти те же процессы, но на каждом этапе применяются более простые меры. В некоторых случаях можно пренебречь интерактивной верификацией.

Согласно данной процедуре, на каждом этапе применяется несколько технологий. Необходимо отметить, что ни одна из технологий, которые рассматриваются в следующих пунктах, не станет "серебряной пулей" или единственным решением проблем голосового спама. Напротив, все эти технологии дополняют друг друга и будут более эффективны при их использовании в комплексе.

Описание и классификация технологий в настоящей Рекомендации даются по месту их применения (то есть сетевые и пользовательские технологии) и по процессам, указанным на рисунке 2.

7.2.1 Запись и сбор данных сигнализации

Запись и сбор данных сигнализации – это сбор подробной информации о вызове в режиме реального (квазиреального) времени для проведения анализа. Сюда могут относиться данные, связанные со временем вызова или номером телефона, такие как:

– момент инициации вызова (COTP) – момент времени, в который вызывающий абонент инициирует вызов;

– момент установления канала сигнализации (SLETP) – момент установления канала сигнализации между вызывающим и вызываемым абонентами;

– момент продолжения соединения (CCOTP) – момент продолжения вызова и соединения с вызываемым абонентом;

– момент отбоя вызова (CCLTP) – момент завершения вызова вызывающим или вызываемым абонентом;

– момент освобождения канала сигнализации (SLRTP) – момент освобождения канала сигнализации после отбоя вызова;

– номер абонента, инициирующего вызов (COSN) – обычно называется номером вызывающего абонента и представляет собой номер, с которого осуществляется вызов, инициированный вызывающим абонентом;

– номер абонента, завершающего вызов (CTSN) – обычно называется номером вызываемого абонента и представляет собой номер, с которого вызываемый абонент завершает вызов.

Значение одних и тех же данных, особенно данных, связанных со временем вызова, может слегка различаться в зависимости от места нахождения пунктов сбора данных. Тем не менее на практике эти вышеупомянутые различия всегда можно не принимать во внимание.

Следует отметить, что источником всех перечисленных в этом пункте данных являются каналы передачи сигналов, а не служебные каналы. В рамках этого процесса записи данных сигнализации все подлежащие сбору данные в большинстве случаев уже существуют в системе управления сигнализацией для учета и анализа качества работы, поэтому их можно использовать повторно, учитывая соотношение выгод и затрат.

ПРИМЕЧАНИЕ. – Ниже будут перечислены только широко используемые источники данных (на основе системы сигнализации № 7 (SS7), интеллектуальной сети (IN), мультимедийной IP-подсистемы (IMS), специализированного сигнала контроля посылки вызова (CRBT), сервера голосовой почты (VMS) и т. д.), хотя существуют и другие альтернативные источники данных, такие как система сигнализации R2 и системы уведомлений о пропущенных вызовах.

7.2.1.1 Сигнализация SS7

Сигнализация SS7 может стать полезным источником данных, помогающим отслеживать голосовой спам. Практичным решением выглядит установка пункта сбора данных сигнализации для копирования информации и параметров сигнализации и их записи. Пункт сбора данных сигнализации параллельно соединен с каналом сигнализации, так что сигнал фактически "расщепляется", однако этот пункт забирает лишь малую долю мощности сигнала. В этих условиях отказ пункта сбора данных сигнализации не ведет к отрицательным последствиям для канала сигнализации.

Существует еще один метод сбора данных сигнализации SS7, заключающийся в установке скрытого узла сигнализации между двумя явными узлами сигнализации. Подразумевается, что скрытый узел сигнализации сначала "заблокирует" сигнал с целью записать его, а затем передаст сигнал без изменений, но с короткой задержкой. Однако у этой технологии есть слабая сторона – риск образования единой точки отказа. Поэтому она нуждается в обеспечении высокой отказоустойчивости и резервной емкости.

Большим преимуществом использования записей данных сигнализации SS7 является то, что в них содержится подробная информация о вызовах, позволяющая определить различные показатели, см. пункт 7.2.2. Однако в случае увеличения голосового трафика и расширения сети должно быть одновременно увеличено количество пунктов сбора данных сигнализации, с тем чтобы охватить все/основные источники данных сигнализации в целях сохранения приемлемого масштаба мониторинга. Это может привести к росту затрат на противодействие спаму.

Рекомендуется размещать пункты сбора данных сигнализации в базовых/местных сетях. Для обеспечения полного сбора информации такие пункты должны охватывать все интерфейсы MC- и NC-коммутаторов. Кроме того, для обеспечения сбалансированного сбора данных достаточно обеспечить охват такими пунктами только всех интерфейсов NC-коммутаторов. Если же речь идет лишь о междугородних вызовах в пределах одной страны или о международных вызовах, то надлежит обеспечить охват междугородних/международных транзитных пунктов передачи сигнализации (STP).

ПРИМЕЧАНИЕ. – Пункт сбора данных сигнализации является элементом логической сети, которая может быть сформирована из различных системных элементов.

7.2.1.2 Интеллектуальная сеть (IN)

Метод, основанный на использовании пунктов управления услугами (SCP), заключается в сборе данных сигнализации от специализированных приложений для расширенной логики подвижной связи (CAMEL) или прикладного протокола интеллектуальной сети (INAP) и их последующего анализа. SCP является одним из важнейших узлов интеллектуальных сетей (IN) и определяющим фактором принятия решения о порядке обработки телефонных вызовов.

Если абонент заключил соглашение о пользовании услугами интеллектуальной сети, при исходящем вызове запускается SCP, запрашивающий информацию о визитном регистре местоположения (VLR) вызываемого абонента, и лишь после этого устанавливаются каналы связи. Поскольку некоторые операторы охотно используют услуги IN, сбор и запись данных сигнализации по вызовам, инициируемым абонентами, заключившими соглашение о пользовании услугами IN, не представляют затруднений.

Поскольку пункты сбора данных сигнализации могут находиться на SCP или вблизи него, при использовании этого метода требуется меньше пунктов сбора данных сигнализации, чем для сбора данных в системе SS7. Этот метод позволяет без труда осуществлять мониторинг абонентов, заключивших соглашение о пользовании услугами IN, независимо от того, находятся ли они в роуминге или в домашней сети.

Однако у этого метода есть одно ограничение. Если уровень распространения услуг IN остается низким, отслеживать можно лишь незначительную долю действий абонентов. Тем не менее эту проблему можно решить путем содействия косвенной подписке каждого абонента на специализированную услугу IN, благодаря которой при инициировании исходящего вызова система IN будет в безусловном порядке направлять в SCP запрос на проверку.

Этот метод ограничен общей процедурой оказания услуг IN, поэтому собирать можно лишь определенные виды данных, такие как COTP, SLETP, COSN и CTSN, см. пункт 7.2.1. Тем не менее эту ситуацию можно улучшить в случае внедрения более сложной процедуры оказания услуг IN, как, например, передача всех сигналов телефонной сигнализации через SCP.

Метод, основанный на использовании мультимедийной IP-подсистемы (IMS), аналогичен рассмотренному выше, поскольку процедуры сигнализации в IMS схожи с применяемыми в IN.

7.2.1.3 Специализированный сигнал контроля посылки вызова (CRBT)

CRBT – это особая ориентированная на пользователя услуга, предоставляемая некоторыми операторами. Если абонент подписан на услугу CRBT, другие абоненты вместо вызывного тонального сигнала слышат заранее заказанную абонентом мелодию. В результате появляется возможность записи и сбора данных сигнализации на CRBT-хостах.

Этот метод ограничен процедурой оказания данной услуги, поэтому собирать можно лишь определенные виды данных, такие как COTP, CCOTP, CCLTP, COSN и CTSN, см. пункт 7.2.1. Никакие дальнейшие усовершенствования процедуры оказания услуги CRBT в целях расширения спектра собираемых данных практически невозможны.

Однако если голосовой спамер беспокоит пользователя CRBT, возможен мониторинг действий такого спамера. Поэтому для того, чтобы данный метод стал применимым на практике, требуется высокий уровень распространения этой услуги. При выполнении этого условия для налаживания записи и сбора данных сигнализации потребуются сравнительно незначительные инвестиции.

7.2.1.4 Сервер голосовой почты (VMS)

Серверы голосовой почты (VMS) обслуживают вызовы в случае переадресации вызова при отсутствии ответа или при занятости, в случае безусловной переадресации и т. д. В большинстве случаев VMS не реагирует на "молчаливые" вызовы, если только не установлена безусловная переадресация. VMS может предоставлять запись голоса вызывающего абонента, если осуществляющий вызов голосовой спамер намерен добиться установления соединения и передать спам-сообщение непосредственно вызываемому абоненту. Тогда VMS может существенно помочь процессу интерактивной верификации, выступая источником записей, предоставляемых в порядке обратной связи с абонентами или с их разрешения, см. пункт 7.3.3.

Как и в случае CRBT, применимость этого метода на практике зависит от уровня проникновения и использования услуг VMS.

7.2.1.5 Программа-ловушка

Метод с применением программы-ловушки используется для организации определенного количества следующих друг за другом либо отобранных в случайном порядке телефонных номеров в целях привлечения голосовых спамеров. В дополнение к сбору данных этот метод может также облегчить процедуры анализа и интерактивной верификации.

Поскольку при данном методе с ловушкой может соединиться любой вызывающий абонент (исходящий вызов), он позволяет собирать определенные виды данных, такие как COTP, CCOTP, CCLTP, COSN и CTSN, см. пункт 7.2.1. Метод программы-ловушки обеспечивает расчет и передачу данных для принятия некоторых аналитических мер, описанных в пункте 7.2.2.

7.2.2 Анализ

Для проведения анализа противодействия голосовому спаму с помощью системы мониторинга собранные исходные данные необходимо пересчитать и преобразовать в значимые показатели, такие как скорость соединения, число случаев завершения вызова, продолжительность сигнала вызова и т. д. Для отличения голосовых спамеров от обычных пользователей исчисление этих показателей следует вести непрерывно в течение определенного периода времени, обычно называемого временным интервалом (отрезком времени). Операторы могут соответствующим образом корректировать продолжительность этого интервала исходя из опыта эксплуатации сети.

На основе всех этих показателей можно вывести логическим путем комплексный показатель "закономерность", который может быть использован в определенных алгоритмах для более точного анализа поведения голосового спамера. Модель закономерностей для выявления голосовых спамеров приведена на рисунке 3.

Рисунок 3 – Модель закономерностей

Модель закономерностей выводится на основе нескольких показателей с помощью логической функции "И". Поскольку данные поступают из различных источников и могут быть сведены воедино, одновременно могут поддерживаться не все показатели. Возможное решение этой проблемы состоит в том, чтобы присвоить неподдерживаемым показателям значение "ИСТИНА" или "1" и не учитывать их. Например, после сбора данных и их преобразования в показатели программе-ловушке для проведения необходимой процедуры анализа требуется лишь показатель продолжительности сигнала вызова, а остальные показатели должны быть установлены в значение "ИСТИНА" или "1", чтобы их не учитывать.

Ниже перечисляются показатели, содержащиеся в модели закономерностей, и приводятся их определения:

– частота вызовов – число вызовов за определенный период времени;

– показатель соединения – количество голосовых вызовов или случаев установления канала сигнализации;

– число случаев отбоя вызова – количество случаев, когда вызывающий или вызываемый абонент завершает вызов по собственной инициативе;

– продолжительность сигнала вызова – длительность тонального сигнала вызова;

– статистические данные по вызываемым абонентам – статистические данные по характеристикам вызываемых абонентов, например равномерное распределение, арифметическая прогрессия и т. д.

Пороговые значения показателей должны корректироваться операторами исходя из реалистичных сценариев обслуживания для обеспечения баланса между точностью и затратами. Кроме того, должны быть определены конкретные закономерности, соответствующие различным типам голосового спама.

Например, широко признанные формы голосового спама подразделяются на два типа – "молчаливые" вызовы и беспокоящие вызовы, см. пункт 6.2. "Молчаливый" вызов (известный также как "несостоявшийся вызов") – это телефонный вызов, инициированный устройством набора номера без возможности его немедленной обработки агентом. В этом случае такое устройство может завершить вызов, и тогда вызываемый абонент услышит в трубке тишину (прерванный сигнал) или сигнал телефонной компании, свидетельствующий о сбросе вызова. Как правило, в таких случаях ожидается обратный вызов. Беспокоящий вызов – это вызов, призванный беспокоить, раздражать, тревожить или запугивать пользователей и содержащий информацию порнографического характера, угрозы, незаконную информацию, ложную рекламу и т. д. Как правило, такие вызовы не прекращаются, пока их не примут.

В рамках предлагаемой модели закономерностей для "молчаливых" и беспокоящих вызовов (см. пункт 6.2) могут быть характерны различные значения показателей. Более высокое значение показателя частоты вызовов или числа случаев отбоя вызова и более низкое значение показателя соединения или продолжительности сигнала вызова указывают на то, что речь идет о спамере, использующем "молчаливые" вызовы. С другой стороны, беспокоящий вызов может быть ориентирован на конкретного вызываемого абонента – в этом случае продолжительность сигнала вызова больше, а показатель соединения – сравнительно выше.

В определенных условиях группа тех, кто осуществляет "молчаливые" вызовы, может инициировать услугу "безусловная переадресация" для выдачи сети указания о безусловной переадресации входящих вызовов на определенный номер, к которому подключена платформа интерактивного речевого ответа (IVR). По сигналу вызова такая платформа IVR может даже отправлять голосовые спам-сообщения обратно звонящему. В ходе анализа полезно проверять, не инициировали ли подозрительные вызывающие абоненты услугу безусловной переадресации и на какой номер она направляется.

Известно, что для противодействия голосовому спаму применяются некоторые более сложные и действенные модели анализа, такие как модель, объединенная с анализом человеческого общества, анализом платежных документов вызывающих абонентов и т. д. В любом случае модель закономерностей могла бы стать основой для разработки комплексных моделей.

7.2.3 Интерактивная верификация

По требованию управляющих структур или в соответствии с договором об обслуживании пользователя до принятия мер пресечения производится верификация номера вызывающего абонента, занесенного в список подозрительных номеров. Верификацию по такому требованию можно провести двумя различными способами.

Первый способ состоит в том, что организации электросвязи ведут постоянно обновляемый список подозрительных номеров, представляют его управляющим структурам и поддерживают с ними обратную связь.

Второй способ – если это предусмотрено договором об обслуживании пользователя или разрешено управляющей структурой – заключается в том, что оператор может осуществить тестовый набор номера вызывающего абонента, занесенного в список подозрительных номеров, в целях проведения прямой верификации. Используя результаты тестового набора номера, обычно именуемые "файл голосовой записи", уполномоченные контролеры попытаются определить, является ли данная запись спамом.

Между тем точность и качество интерактивной верификации влияют на процесс принятия мер пресечения.

Как упоминалось выше, программа-ловушка способна самостоятельно провести интерактивную верификацию, то есть если расчет значений показателей указывает на то, что исходящий вызов принадлежит к категории "молчаливых" (см. пункт 6.2), то программа-ловушка выполнит обратный вызов для фактического подтверждения результата верификации; напротив, если анализ показателей подтвердит факт беспокоящего вызова, программа-ловушка выполнит вызов и запишет его.

Кроме того, координация действий группы тех, кто осуществляет "молчаливые" вызовы, и одной или нескольких платформ IVR может ввести операторов в заблуждение относительно истинного источника голосового спама. Иногда платформы IVR и те, кто осуществляет "молчаливые" вызовы, относятся к разным операторам. Выполнив запись голосового спама, целесообразно отследить потенциальное соединение между тем, кто осуществляет "молчаливые" вызовы, и платформой IVR, для чего, например, направить запрос в домашний регистр местоположения (HLR).

7.2.4 Пресечение

Меры пресечения призваны ограничить или заблокировать действия голосовых спамеров, принадлежность которых к этой категории подтверждена в процессе верификации с целью защитить от них обычных пользователей. Ниже рассматриваются два метода пресечения.

7.2.4.1 "Белые" списки/"черные" списки

Создание "белых" и "черных" списков, обычно известных как ключевые списки учетных записей, требует больших затрат времени и постоянного обновления содержащейся в них информации. Жизненным циклом каждого элемента "белого"/"черного" списка необходимо тщательно управлять в целях обеспечения точности и эффективности списка. Кроме того, на протяжении всего жизненного цикла каждого элемента "белого"/"черного" списка необходимо обеспечивать безопасное ведение такого элемента.

Как описано в Рекомендации [ITU-T X.1240], качество "черных" списков в огромной степени колеблется в зависимости от профессионализма того, кто их составляет. "Черные" списки неизбежно содержат неточности, не позволяющие некоторым правомерным вызовам дойти до вызываемых абонентов. Хотя использование "черных" списков вызывает множество проблем, они являются быстрым решением, позволяющим отказать в установлении соединения между источниками голосового спама и его получателями (абонентами телефонной связи).

"Черные" списки, содержащие абонентские номера или их части, обычно размещаются в шлюзовом центре коммутации подвижной связи (GMSC), в SCP, на коммутаторах и иных сетевых объектах. Как правило, "черные" списки сети одного оператора можно разместить в SCP, на коммутаторах или иных сетевых объектах, тогда как "черные" списки сетей других операторов можно размещать только в GMSC, емкость соответствующего раздела памяти которого может быть недостаточной для хранения "черных" списков большого объема. Простым решением этой проблемы может быть создание скрытых узлов сигнализации (см. подпункт 7.2.1.1) после GMSC.

Может понадобиться обеспечить взаимодействие "белых" списков с официально утвержденной базой данных, которая ведется для уже идентифицированных вызывающих абонентов, действующих на законных основаниях в целях исключения непреднамеренного блокирования реальных абонентов, особенности действий которых сходны с параметрами голосовых спамеров. К таким вызывающим абонентам могут относиться центры обслуживания вызовов, службы уведомлений, службы обратной связи/сбора данных, такие как службы напоминания о непогашенной задолженности, программы обратной связи с абонентами, организованные управляющими структурами, программы повышения информированности, программы оповещения о чрезвычайных ситуациях или стихийных бедствиях и т. д.

7.2.4.2 Механизм отслеживания

Механизм отслеживания позволяет установить реальное физическое местонахождение голосовых спамеров. Иногда он может использоваться для указания, при необходимости, точного местоположения или адреса голосового спамера.

Существующие методики позволяют операторам определить реальное местоположение голосового спамера на основе информации, предоставляемой центром коммутации подвижной связи (MSC); однако определить местоположение этим методом можно лишь приблизительно. Более точное определение местоположения может обеспечить поддерживаемая оператором служба информации о местоположении, например служба адаптивного глобального позиционирования.

7.3 Пользовательские технологии

Пользовательские технологии должны служить эффективным дополнением сетевых технологий. Обратная связь может быть источником подробной информации о голосовых спамерах (см. пункт 7.3.3), что оказывает исключительно важную помощь операторам. Помочь применению пользовательских технологий могут определенные функции некоторых мобильных смартфонов, степень поддержки которых изготовителями может быть неодинаковой.

7.3.1 "Белые" списки/"черные" списки

Абоненты могут воспользоваться функцией управления соединением в своем телефоне для блокирования определенных номеров или частей номеров, создав соответствующий "черный" список, и в то же время функция управления соединением разрешает соединение с определенными номерами (установленными абонентами или синхронизированными с помощью тех или иных мобильных приложений) во всех случаях, включая их в "белый" список.

Этот метод мог бы опираться на "белые"/"черные" списки, синхронизированные на стороне сети, тогда как сторона пользователя подвержена влиянию личных предпочтений, поскольку абоненты могут вести собственные списки.

7.3.2 Задержки вызова

Задержка вызова – это метод на уровне сигнализации, который, в частности, подходит для борьбы с "молчаливыми" вызовами (см. пункт 6.2).

После установления канала сигнализации между вызывающим и вызываемым абонентами периодически генерируется тональный сигнал вызова. Иногда осуществляются "молчаливые" вызовы, в случае которых вызываемый абонент слышит в трубке тишину (прерванный сигнал) или короткий тональный сигнал, свидетельствующий о сбросе вызова.

С помощью мобильных смартфонов абоненты могут блокировать "молчаливые" вызовы на стороне терминала (на стороне пользователя). Поскольку абоненты могут установить значение (порог) продолжительности тонального сигнала для каждого входящего вызова на уровне сигнализации, "молчаливые" вызовы могут быть не пропущены, поскольку продолжительность тонального сигнала у них ниже порогового значения. Однако если обычный вызов с "непродолжительным тональным сигналом" игнорируется, запись о вызове заносится в журнал регистрации соединений мобильного телефона, что позволяет абоненту произвести дополнительную проверку.

7.3.3 Обратная связь

Получив голосовой спам, абоненты могут в порядке обратной связи обратиться к оператору, сообщив ему номер голосового спамера и иную подробную информацию. К каналам обратной связи относятся текстовые сообщения, телефонные звонки, электронная почта и даже официальный веб-сайт отдела обслуживания клиентов (или иного аналогичного отдела) оператора. Необходимо, чтобы все эти каналы обеспечивали удобную и простую процедуру передачи информации абонентами в рамках обратной связи. Удобный для использования канал можно организовать с помощью приложений, установленных в терминалах или на картах модуля идентификации абонента (SIM) и на таких платформах, как платформа управления устройством (DMP) или платформа беспроводной связи (OTAP) в сети.

Кроме того, после получения отделом обслуживания клиентов информации от абонента уполномоченному контролеру необходимо проверить достоверность и фактическую точность такой информации и применить аналогичную процедуру интерактивной верификации до принятия надлежащих дальнейших мер. Если в качестве доказательства фигурирует голосовая запись из VMS и владелец разрешает доступ к этой записи, то верификация может быть более действенной и эффективной.

7.4 Механизм взаимодействия

Операторы могут в сотрудничестве с управляющими структурами, другими операторами или абонентами создать механизм взаимодействия и связи в целях противодействия голосовому спаму.

Операторы могут создать или поддерживать систему совместного использования информации (ISS). Эта конкретная система может обеспечивать обмен с другими организациями основной информацией о голосовом спаме, включая списки подозрительных абонентов/подтвержденных голосовых спамеров, данные о принадлежности каждого спам-сообщения к определенному типу, технологии противодействия и т. д.

Управляющие структуры могут рассмотреть возможность реализации ISS и создания механизма обмена информацией или даже проведения официальных собраний операторов и сторонних организаций для обмена актуальной информацией.

Абоненты могли бы делиться своими "черными" списками с сервером на стороне сети, выгружая или скачивая такие списки. Однако у операторов должен иметься механизм верификации, позволяющий определять, действительно ли тот или иной включенный в личный "черный" список абонент является голосовым спамером. Операторам следует создать интерфейс для выгрузки и скачивания "черных" списков. Можно было бы наладить взаимодействие между этим механизмом и системой обратной связи с абонентами. В то же время управляющие структуры должны проводить проверку обновленной информации во избежание попадания туда ненадлежащих сведений.

В целях реализации механизма совместного использования информации операторы могут регулярно представлять проверенные "черные" списки управляющим структурам и блокировать "черные" списки, составленные управляющими структурами, применение которых они обеспечивают.

Управляющие структуры также могут свести воедино все "черные" списки, полученные от всех операторов, и применять надлежащие меры и процедуры. Управляющие структуры также могут взять на себя дополнительные обязанности, как, например, ограничение голосового спама в самом начале, обеспечивая в то же время выполнение операторами их обязанностей.

7.5 Предлагаемые решения

Ни одно из описанных выше решений само по себе не способно гарантировать полного успеха. Для эффективного противодействия голосовому спаму необходимо комплексное применение сетевых и пользовательских технологий в рамках каждой процедуры.

Для обеспечения высокой точности в рамках процедуры записи данных сигнализации можно было бы объединить данные из разных источников. Однако создание комплексных источников данных носит в высшей степени затратный характер.

Необходимо рассмотреть следующие ситуации.

Достаточно выбрать только записи сигнализации SS7 (см. пункт 7.2.1), поскольку по сравнению с другими источниками данных сигнализация SS7 охватывает все каналы сигнализации, позволяя получить самые полезные данные, что гарантирует эффективное противодействие голосовому спаму.

С другой стороны, экономически эффективной альтернативой может быть система сбора данных на основе IN, CRBT или VMS, если операторы уже внедрили услуги IN, CRBT или VMS. Однако, как говорилось в пункте 7.2.1, источники данных в сетях с CRBT или IN могут не предоставлять все конкретные данные. Поэтому эти службы можно было бы рассматривать как дополнительный источник данных.

Модель, предложенная в пункте 7.2.2, проста в использовании и не требует больших затрат; она также широко применяется при противодействии голосовому спаму. Для повышения точности анализа можно использовать более сложные модели закономерностей и алгоритмы. Например, заметно уменьшить список подозрительных номеров могут статистические данные о кодах причин завершения вызова и кодах причин отклонения вызова.

Однако использование многосторонних моделей закономерностей или алгоритмов может привести к избыточному усложнению структуры системы и длительным, отнимающим много времени процедурам, что в свою очередь дополнительно замедлит весь процесс противодействия голосовому спаму, а это в конечном счете может снизить уровень удовлетворенности пользователей. С учетом всего этого весьма существенным фактором для оператора является разумный выбор соответствующих моделей закономерностей или алгоритмов.

Процедуры интерактивной верификации могут различаться в разных странах. Поэтому управляющие структуры могут содействовать операторам в создании надлежащей процедуры верификации на основе их национальной практики.

Как видно из описания в пункте 7.2.4 процедуры принятия мер пресечения, для сокращения объема голосового спама следует повышать уровень интеграции методов, применяемых пользователями и сетями. Значительную роль в процедуре пресечения спама и удовлетворении потребностей абонентов могли бы сыграть отделы клиентского обслуживания операторов.

Приложение A

Интерактивные и технические меры борьбы со спам-вызовами

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

Резюме

В настоящем Приложении представлен обзор процессов, которые служат для борьбы со спам-вызовами, а также предложена техническая основа для противодействия таким спам-вызовам с помощью вызовов на номера/номер (специально выделенные оператором электросвязи), которые осуществляются немедленно после получения входящего спам-вызова. В рамках этой структуры определено, что оператор(ы) должен(ны) иметь специальный(е) анти-спам номер(а), а также предназначенные для этих номеров функции обработки подробных записей о вызовах различных уровней. Наряду с этим в настоящем Приложении представлены механизмы обмена информацией для борьбы со спамом в рамках межоператорского взаимодействия.

Настоящее Приложение обеспечивает техническую основу для противодействия спаму, когда абонент уведомляет оператора с помощью короткого вызова на анти-спам номер немедленно после получения спам-вызова. Настоящее Приложение применяется к услуге голосовых вызовов, услуге передачи коротких сообщений (SMS) и услуге передачи мультимедийных сообщений (MMS).

Сценарий службы интерактивных отчетов для взаимодействия абонента с оператором электросвязи/поставщиком услуг с целью борьбы со спам-вызовами, поступающими на телефонные терминалы

В Рекомендации МСЭ-Т X.1247 представлена концепция механизмов обратной связи пользователей и отчетов пользователей, которые используются в обработке сообщений, содержащих спам.

В Рекомендации МСЭ-Т X.1246 представлены различные механизмы интерактивной верификации и обработки спама.

Описанный здесь интерактивный механизм дополняет и расширяет текущие процедуры основной части настоящей Рекомендаций (МСЭ-Т X.1246) и [ITU-T X.1247]. Предлагаемое взаимодействие абонента/получателя спам-вызова с оператором электросвязи/поставщиком услуг заключается в осуществлении абонентом короткого вызова на специальный анти-спам номер этого оператора электросвязи/поставщика услуг или переадресации на этот номер принятого сообщения со спамом.

A.1 Сценарий/алгоритм/вариант использования интерактивной обратной связи

Сценарий использования факта вызова на анти-спам номер для определения спам-вызова с использованием автоматической обработки данных CDR/CLI состоит из описанных ниже шагов.

1) Получатель/клиент/абонент принимает входящий вызов, который он идентифицирует/определяет как спам-вызов или потенциальный спам-вызов (голосовой спам, спам в SMS, спам в MMS).

2) CDR/CLI, относящаяся к этому вызову (а также к любому другому вызову), сохраняется в системе управления электросвязью (или иной системе/системах) оператора электросвязи. В этой CDR_n/CLI_n содержится идентификатор вызывающей стороны (вероятный источник спам-вызова), идентификатор получателя вызова (получатель спам-вызова), время вызова.

3) Немедленно/при первой возможности по завершении этого вызова его получатель/клиент/абонент набирает специальный анти-спам номер, который заранее определен его домашним/собственным поставщиком услуг/оператором электросвязи (в зависимости от национальных правил этот номер может быть уникальным в рамках страны или индивидуальным для каждого оператора), то есть осуществляет исходящий вызов на анти-спам номер в качестве интерактивного отчета пользователя.

4) CDR_{n+1}/CLI_{n+1}, относящаяся к этому вызову, также сохраняется в системе управления электросвязью оператора.

5) Оператор, получив от абонента такой вызов на анти-спам номер, извлекает всю техническую информацию $CDR_{n+1,}$ (CDR и CLI с разной степенью детализации), автоматически находит предпоследний входящий вызов с CDR_n, сделанный абоненту/получателю возможного спам-вызова, и начинает сбор информации о вызывающей стороне, отправившей возможный спам (вероятно обмениваясь информацией с другими операторами/регуляторными органами).

6) Если вызов на анти-спам номер был однократным и/или ошибочным, дальнейшие действия не потребуются.

7) Если на анти-спам номер поступает несколько вызовов от разных получателей возможных спам-вызовов и в каждом случае система обработки CDR определяет одинаковый номер вызывающей стороны или CLI_n последнего входящего вызова к абоненту/пользователю перед его исходящим вызовом на анти-спам номер, это означает высокую вероятность определения реального источника спам-вызовов и, таким образом, обнаружения спамера.

8) Для исключения ложных срабатываний сигнализации факультативно возможно установить разные пороговые уровни для систем обработки CDR.

А.2 Технические требования

А.2.1 Для приема вызовов обратной связи от получателя требуется, чтобы оператор электросвязи/поставщик услуг имел специальный анти-спам номер.

А.2.2 Для обработки большого количества вызовов обратной связи требуется, чтобы система управления электросвязью оператора электросвязи/поставщика услуг обладала возможностью приема и обработки таких вызовов полностью на основе как информации CDR, так и информации CLI более низкого уровня.

А.2.3 Требуется, чтобы система управления электросвязью обладала статистическими данными службы отчетов о качестве обслуживания (QoS).

Дополнение I

Комплексные меры противодействия голосовому спаму

(Данное дополнение не является неотъемлемой частью настоящей Рекомендации.)

Рисунок I.1 отражает технические и нетехнические подходы к противодействию голосовому спаму. Противодействие голосовому спаму – непростая техническая проблема, поэтому необходимо одновременно применять разные подходы.

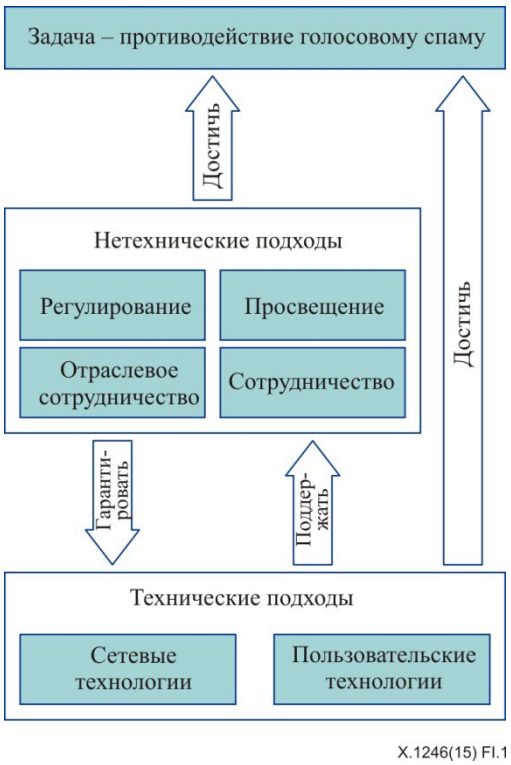

Рисунок I.1 – Структура противодействия голосовому спаму

– Регуляторные положения могут содействовать защите пользователей и операторов от голосового спама.
– Отраслевое сотрудничество необходимо для разработки и внедрения участниками отрасли различных надлежащих технологий.
– Благодаря сотрудничеству операторы и управляющие структуры могут обмениваться информацией об эффективном применении регуляторных положений и о развитии технологий.
– Просвещение имеет важное значение для пользователей с точки зрения минимизации экономических убытков, причиняемых голосовым спамом.

Дополнение II

Предлагаемый подход к проведению интерактивной верификации

(Данное дополнение не является неотъемлемой частью настоящей Рекомендации.)

В сущности говоря, интерактивная верификация в каждом случае заключается в наборе номера подозрительного вызывающего абонента, записи сигнала контроля посылки вызова до начала соединения и голосового сообщения после соединения, а затем – в проверке контента для определения, является он голосовым спамом или нет. Осуществление всех этих операций вручную может привести к серьезному истощению людских ресурсов операторов. Поэтому следует рассмотреть оптимизированный подход в целях балансирования издержек.

Интерактивную верификацию можно проводить централизованно, осуществляя набор номеров и проверку в полуавтоматическом режиме голосовых сообщений подозрительных голосовых спамеров, которые, возможно, рассеяны практически по всем сегментам сети.

При централизованном подходе набор номеров и запись данных осуществляются автоматически, с высокой степенью согласованности, и контролеры могут успешно проводить проверку голосовых сообщений без помех в виде белого шума и других бесполезных сигналов контроля посылки вызова.

Дополнение III

Политические аспекты противодействия голосовому спаму

(Данное дополнение не является неотъемлемой частью настоящей Рекомендации.)

Голосовой спам – это один из опасных инструментов, используемых для рекламы, мошенничества, преследования и т. д., который может применяться в повседневной связи. Для эффективного противодействия голосовому спаму следует рассмотреть различные подходы в разных аспектах групп, участвующих в предоставлении услуг голосовой связи, и в настоящей Рекомендации описаны разные виды соответствующих технологий. К этим участвующим группам относятся пользователи (или абоненты), операторы, управляющие структуры и сторонние организации. В данном дополнении описываются некоторые аспекты участвующих групп, которые необходимо учитывать при противодействии голосовому спаму.

III.1 Пользователи

Пользователи – это жертвы, находящиеся в самом конце коммуникационной цепи голосового спама, поэтому они испытывают большую потребность в блокировании спама. Следовательно, пользователям необходимо применять некоторые из используемых на всех этапах процесса противодействия спаму подходов. Следующие предложения применимы в зависимости от сложившейся ситуации.

– Пользователям следует, по возможности, установить на свои устройства, например на смартфоны, антиспамовые приложения. В целях повышения действенности этих приложений их надлежит постоянно обновлять.

– Пользователям следует сообщать операторам электросвязи или сторонним организациям всю подробную информацию о голосовом спамере сразу же после получения голосового спама.

– Пользователям следует вести себя осмотрительнее в повседневном общении и защищать свою личную информацию от доступа к ней спамеров.

III.2 Операторы

Операторы играют значительную роль во всей процедуре противодействия голосовому спаму. Голосовой спам может привести к резкому снижению уровня удовлетворенности пользователей и масштабной растрате ресурсов сети, поэтому операторы должны знать о голосовом спаме и принимать меры к тому, чтобы защитить свои сети и предоставлять более качественные услуги. Возможные подходы могут включать:

– Операторам следует осуществлять мониторинг всей сети связи для обнаружения потенциального голосового спама, на который могут указывать аномальные передачи сигнализации или структура трафика.

– Операторам следует использовать собственные каналы сбыта или продажи для предварительной установки последних версий антиспамовых приложений во всех устройствах, которые могут стать мишенью голосового спама. В случае использования сторонних каналов сбыта операторам следует гарантировать, что во всех устройствах установлены современные приложения, обеспечивающие полную защиту.

– Операторам следует проводить информационно-разъяснительные кампании и учебные мероприятия, а также рекомендовать пользователям в порядке обратной связи направлять подробную информацию о голосовых спамерах сторонним организациям; такая обратная связь может осуществляться в рамках программ стимулирования.

– Операторам следует участвовать в создании альянсов с управляющими структурами и сторонними организациями в целях объединения усилий по противодействию голосовому спаму.

III.3 Управляющие структуры и сторонние организации

Управляющие структуры и сторонние организации могут осуществлять непосредственный надзор за операторами или руководство их действиями и даже предоставлять необходимую поддержку.

– В целях противодействия голосовому спаму управляющие структуры и сторонние организации могут осуществлять обучение пользователей и операторов или проводить среди них информационно-разъяснительные и просветительские кампании.

– Управляющим структурам и сторонним организациям следует расширять исследования тенденций в сфере голосового спама и стараться найти более эффективные подходы или технологии противодействия новейшим видам голосового спама.

– Управляющим структурам и сторонним организациям следует расчистить каналы рекламы или продвижения товаров и услуг в целях упорядочения современной среды голосовой связи или осуществлять регламентацию используемых рекламными агентствами систем передачи заказных рекламных объявлений по телефонной сети.

– Управляющим структурам и сторонним организациям следует доводить содержание новейших версий "черных" списков до сведения операторов и даже пользователей; эти "черные" списки следует вести при поддержке операторов и пользователей.

– Управляющим структурам следует обеспечить ресурсы для укрепления противодействия голосовому спаму в целях защиты, предлагаемой в рамках коммерческих предложений для пользователей.

Библиография

[b-ITU-T E.370] Recommendation ITU-T E.370 (2001), *Service principles when public circuit-switched international telecommunication networks interwork with IP-based networks*.

[b-ITU-T M.60] Recommendation ITU-T M.60 (1993), *Maintenance terminology and definitions.*

[b-ITU-T M.1400] Рекомендация МСЭ-Т M.1400 (2013 г.), *Обозначения для соединений между сетями операторов*.

[b-ITU-T X.1231] Рекомендация МСЭ-Т X.1231 (2008 г.), *Технические методы противодействия спаму*.

[b-ITU-T X.1242] Рекомендация МСЭ-Т X.1242 (2009 г.), *Система фильтрации спама в услуге передачи коротких сообщений (SMS) на основе определяемых пользователем правил*.

[b-ITU-T X.1245] Рекомендация МСЭ-Т X.1245 (2010 г.), *Структура противодействия спаму в мультимедийных IP-приложениях*.

[b-ITU-T Y.1001] Recommendation ITU-T Y.1001 (2000), *IP framework – A framework for convergence of telecommunications network and IP network technologies*.

[b-IETF RFC 5039] IETF RFC 5039 (2008), *The Session Initiation Protocol (SIP) and Spam*.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация, а также соответствующие измерения и испытания
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты протокола Интернет, сети последующих поколений, интернет вещей и умные города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2022 г.