Международный союз электросвязи

МСЭ-Т X.1249

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(01/2019)

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

Безопасность киберпространства – Противодействие спаму

Техническая основа противодействия рекламному спаму в приложениях для мобильных устройств

Рекомендация МСЭ-Т X.1249

Международный союз электросвязи

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	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности	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	
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.1360–X.1369
Безопасность интеллектуальных транспортных систем (ИТС)	X.1370–X.1389
Безопасность технологии распределенного реестра	X.1400–X.1429
Протоколы безопасности	X.1450–X.1459
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
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

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

Рекомендация МСЭ-Т X.1249

Техническая основа противодействия рекламному спаму в приложениях для мобильных устройств

Резюме

Рекомендация МСЭ-Т X.1249 обеспечивает техническую основу противодействия рекламному спаму в приложениях для мобильных устройств. Рекламный спам в приложениях для мобильных устройств – это рассылка нежелательной рекламы, которая отображается в приложении для мобильного телефона. Эта незапрашиваемая реклама может отображаться на экране мобильного устройства в виде баннера в верхней или нижней части экрана, подвижного окна или всплывающего окна. Наряду с быстро растущим количеством мобильных приложений стремительно растет и объем рекламы в приложениях для мобильных устройств, и необходима фильтрация вредоносной рекламы для удобства и даже безопасности пользователей. Вследствие этого, может оказаться полезным создание практической основы для противодействия рекламному спаму в приложениях для мобильных устройств, которая позволит рациональным образом объединить преимущества всех мер противодействия.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1249	30.01.2019 г.	17-я	11.1002/1000/13605

Ключевые слова

Реклама в приложениях для мобильных устройств, 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, 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 патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т X.1249

Техническая основа противодействия рекламному спаму в приложениях для мобильных устройств

1 Сфера применения

Настоящая Рекомендация обеспечивает техническую основу противодействия рекламному спаму в приложениях для мобильных устройств. В рамках этой основы определены функциональные компоненты, правила фильтрации и рабочие процессы. Кроме того, в настоящей Рекомендации предлагается платформа обратной связи для противодействия рекламному спаму в приложениях для мобильных устройств.

Настоящая Рекомендация предназначена для поставщиков приложений и услуг мобильного интернета.

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.

Отсутствуют.

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 мобильный телефон (mobile phone) [b-ITU-T X-Sup.19] – электронное устройство, используемое для осуществления телефонных вызовов и отправки текстовых сообщений на обширной территории с помощью радиодоступа к сетям подвижной связи общего пользования и при этом обеспечивающее мобильность пользователя.

3.1.2 смартфон (smartphone) [b-ITU-T X-Sup.19] – мобильный телефон с большими вычислительными возможностями, поддержкой различных типов соединений и усовершенствованной операционной системой, предоставляющей платформу для сторонних приложений.

3.1.3 спам (spam) [b-ITU-T X.1242] – электронная информация, переданная от отправителей к получателям при помощи оконечных устройств, таких как компьютеры, мобильные телефоны, телефоны и т.д., которая, как правило, не затребована, нежелательна или вредна для получателей.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяются следующие термины.

3.2.1 асинхронная фильтрация (asynchronous filtering) – метод обработки файлов в целях выявления объявлений, являющихся спамом, который позволяет выполнять несколько процессов идентификации одновременно.

3.2.2 приложение для мобильных устройств (mobile application) – прикладная программа, предназначенная для работы на мобильных устройствах, таких как смартфоны и планшеты.

3.2.3 реклама в приложении для мобильных устройств (mobile in-application advertising) – реклама, отображаемая в приложении для мобильных устройств. Она может отображаться на экране мобильного устройства в виде баннера в верхней или нижней части экрана, подвижного окна, всплывающего окна и т. д.

3.2.4 рекламный спам в приложении для мобильных устройств (mobile in-application advertising spam) – реклама в приложении для мобильных устройств, которая, как правило, не затребована, нежелательна или вредна для получателей.

ПРИМЕЧАНИЕ 1. – В данном контексте "не затребована" означает "не запрошена пользователем", а "нежелательна" означает, что пользователем были предприняты какие-либо действия, для того чтобы четко заявить о своем отказе, например путем отключения опции получения некоторых видов рекламы.

ПРИМЕЧАНИЕ 2. − Рекламный спам в приложении для мобильных устройств, как правило, рассылается беспорядочно, методом массовой рассылки и многократно. К примерам фактического и ощутимого вреда относятся мошенничество или передача вредоносного кода.

3.2.5 Синхронная фильтрация (synchronous filtering) – метод обработки файлов для выявления объявлений, являющихся спамом, при котором каждый процесс начинается по завершении предыдущего.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

AD	Advertisement	Реклама
API	Application Program Interface	Интерфейс прикладного программирования
ID	Identity	Идентификатор
IP	Internet Protocol	Протокол Интернет
URL	Uniform Resource Locator	Универсальный указатель ресурса

5 Соглашения по терминологии

Отсутствуют.

6 Общие аспекты

Ввиду быстрого развития мобильного интернета и открытого характера операционных систем для мобильных устройств стремительно растет и количество рекламных объявлений в приложениях для таких устройств. Обычно для доставки рекламы приложение для мобильных устройств вызывает интерфейс прикладного программирования (API), предоставляемый платформой обслуживания. Поскольку реклама, доставляемая приложениями для мобильных устройств, бесплатна или почти бесплатна, она становится чрезвычайно популярной. Бóльшая часть этой рекламы законна и приемлема для пользователей, но некоторая ее часть представляет собой спам. Для блокирования рекламного спама принимаются разнообразные меры, такие как разрешение или запрет.

При том что реализованы многие меры противодействия такой рекламе, техническая основа для борьбы с рекламным спамом в приложениях для мобильных устройств по-прежнему отсутствует. Рекламный спам в приложениях для мобильных устройств способен вызвать множество негативных последствий для поставщиков приложений и услуг. Рекламный спам в приложениях для мобильных устройств может занимать значительную часть полосы пропускания или вызывать задержку трафика данных, он даже может использоваться для мошенничества посредством мобильных устройств. Не существует какой-либо одной меры, обеспечивающей абсолютно эффективное решение для борьбы со спамом. Настоящая Рекомендация является попыткой создать практическую основу для противодействия рекламному спаму в приложениях для мобильных устройств, способную рационально объединить преимущества всех мер противодействия.

7 Техническая основа

Системы фильтрации для противодействия рекламному спаму в приложениях для мобильных устройств (например, система фильтрации спама) реализуются главным образом на платформах обслуживания, предоставляющих API-интерфейсы для приложений. Приложения могут вызывать эти API для доставки рекламных объявлений и других сообщений. Техническая основа для противодействия рекламному спаму в приложениях для мобильных устройств показана на рисунке 1.

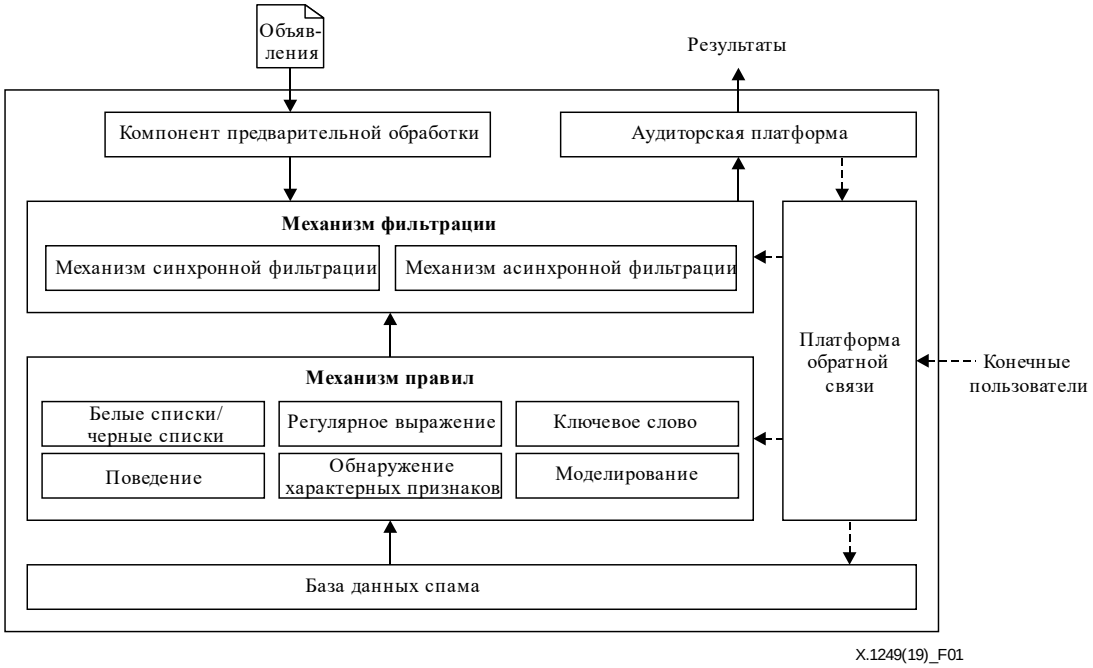

Рисунок 1 − Техническая основа противодействия рекламному спаму в приложениях для мобильных устройств

8 Функциональные компоненты

8.1 Компонент предварительной обработки

Компонент предварительной обработки используется для предварительной обработки исходных файлов рекламных объявлений в целях преобразования их в формат, требуемый механизмами фильтрации, как, например, выделение текста, изображения, универсального указателя ресурса (URL), аудио- и видеоинформации и т. д.

8.2 Механизмы фильтрации

Механизмы фильтрации – это наиболее важные компоненты системы фильтрации рекламного спама в приложениях для мобильных устройств. Их основная цель состоит в выявлении фактического рекламного спама в приложениях для мобильных устройств или возможности такого спама. Исходя из различных способов выявления рекламного спама в приложениях для мобильных устройств механизмы фильтрации можно классифицировать как механизмы синхронной или асинхронной фильтрации. В аспекте эффективности использования времени механизм синхронной фильтрации обычно уступает механизму асинхронной фильтрации.

8.2.1 Механизм синхронной фильтрации

При синхронной фильтрации каждое следующее правило фильтрации запускается по завершении предыдущего. Синхронную фильтрацию относят к онлайновой фильтрации ввиду меньшей сложности и быстрого получения результатов. Обычно ее результаты становятся известны сразу, так что решение принимается немедленно по ее завершении. Если результаты применения правила фильтрации влияют на выполнение последующих правил фильтрации, то предлагается синхронная фильтрация. Такая фильтрация может включать фильтрацию с использованием белых/черных списков, регулярных выражений, моделирования поведения, обнаружения характерных признаков и т. д.

8.2.2 Механизм асинхронной фильтрации

Асинхронная фильтрация позволяет запускать различные рабочие процессы одновременно; другими словами, разные рабочие процессы не зависят от результатов друг друга. Асинхронную фильтрацию относят к офлайновой фильтрации ввиду более высокой сложности фильтрации рекламного спама в приложениях для мобильных устройств и, как правило, длительного ожидания ее результатов.

Асинхронная фильтрация обычно включает распознавание звука, распознавание видеоизображения, сопоставление ключевых слов, глубокое моделирование и т. д.

8.3 Механизмы правил

Механизмы правил обеспечивают выполнение правил фильтрации, включая все правила, которые могут использоваться в механизмах фильтрации. Правила фильтрации имеют несколько источников: конфигурация, выбранная оператором, база данных спама и сторонние источники правил общего пользования. Механизм правил содержит правила принятия решений для выявления рекламного спама в приложениях для мобильных устройств. Некоторые правила принятия решений, если результат фильтрации не определен, основываются на сумме взвешенных значений, полученных из различных тестов спама. Механизм правил выдает пороговое (то есть фиксированное) значение. Если сумма превышает это пороговое значение, то механизм фильтрации решает, является ли объявление спамом. Кроме того, чтобы определить, является ли объявление рекламным спамом в приложениях для мобильных устройств, механизм правил может интегрировать различные факторы выявления механизма фильтрации.

8.4 Аудиторская платформа

Не весь рекламный спам в приложениях для мобильных устройств можно обнаружить с помощью механизмов фильтрации. Поэтому для оценки рекламного спама в приложениях для мобильных устройств следует также использовать ручные методы и добавить аудиторскую платформу. С помощью такой платформы аудитор может выявить неизвестный рекламный спам в приложениях для мобильных устройств, который не распознается механизмами фильтрации. Точность у аудиторской платформы обычно выше, чем у механизмов фильтрации. Поэтому полученные с ее помощью результаты можно ввести в базу данных рекламного спама в приложениях для мобильных устройств для последующего использования.

8.5 База данных рекламного спама в приложениях для мобильных устройств

Такая база данных используется для хранения характеристик рекламного спама в приложениях для мобильных устройств. Это логическая база данных, которую может поддерживать каждый поставщик услуг или могут совместно использовать несколько поставщиков услуг. Хранящиеся в базе данных характеристики рекламного спама в приложениях для мобильных устройств можно использовать для сравнения и фильтрации. Расширение базы данных рекламного спама в приложениях для мобильных устройств может способствовать повышению производительности механизма правил. База данных рекламного спама в приложениях для мобильных устройств может быть дополнена платформой обратной связи, которая извлекает характеристики из вновь идентифицированного рекламного спама в приложениях для мобильных устройств.

8.6 Платформа обратной связи

Объектами, жертвами и получателями рекламного спама в приложениях для мобильных устройств являются конечные пользователи. Участие конечных пользователей, наряду с результатами, полученными с помощью аудиторской платформы, способствует эффективному противодействию рекламному спаму в приложениях для мобильных устройств. Поэтому платформа обратной связи также должна учитывать отклики конечных пользователей. Необходимо создать механизмы для этой цели, включая обеспечение обратной связи с базой данных спам-объявлений. Такие процедуры обработки обратной связи должны быть прозрачными, действенными и эффективными. Кроме того, необходимо, чтобы платформы обратной связи регистрировали информацию обратной связи в стандартном формате. Это позволит разным операторам и организациям совместно пользоваться данными обратной связи. Благодаря этому могут быть получены основные адреса спамеров, которые могут быть добавлены в черные списки и использоваться в таких списках.

9 Правила фильтрации

9.1 Ключевые слова

Ключевые слова используются для определения того, соответствует ли содержание (то есть слова) рекламного объявления образцам из базы данных рекламного спама в приложениях для мобильных

устройств. Ключевые слова получают из следующих источников: конфигурация, выбранная оператором, внешние каналы, платформа обратной связи и машинное обучение по базе данных спама. Они позволяют точно выявлять вредоносные объявления за короткий промежуток времени при небольших затратах, поэтому часто используются для синхронной фильтрации. Для повышения эффекта от использования ключевых слов необходимо рассмотреть возможность предварительной обработки исходного текста, чтобы отфильтровать некоторые намеренно вводящие в заблуждение символы и особые типы кодирования ключевых слов, особенно при фильтрации URL-адресов.

9.2 Черные/белые списки

Черные списки основаны на принципе сопровождения IP-адресов или доменов, подозреваемых в рассылке рекламного спама в приложениях для мобильных устройств. Эти списки также могут включать идентификатор (ID) устройств, URL-адреса или учетные записи отправителя на платформе обслуживания. Они могут создаваться организациями для совместного использования или вводиться и поддерживаться платформой обслуживания для удовлетворения собственных потребностей. Белые списки основаны на принципе перечисления источников одобренных или признанных объявлений. Эти списки также могут включать ID устройств или обслуживаемые учетные записи отправителя на платформах обслуживания. Подобно ключевым словам черные и белые списки являются эффективным решением для фильтрации рекламного спама в приложениях для мобильных устройств, хотя они неизбежно содержат неточности, и черные списки могут препятствовать прохождению некоторых законных объявлений через механизмы фильтрации.

9.3 Регулярное выражение

Регулярные выражения обычно используются для точного сопоставления вредоносных объявлений в текстовой форме с некоторыми специальными шаблонами и их фильтрации. Они отличаются гибкостью, логичностью и функциональностью и обычно приводят к конечному результату, который не требует дополнительных обоснований или изменений. В отличие от ключевых слов или черных и белых списков регулярные выражения можно использовать для сопоставления серии объявлений определенной формы, различающихся по содержанию. Они также широко используются при синхронной фильтрации для достижения высокой эффективности. Кроме того, они широко используются при такой фильтрации исходя из того факта, что хорошо продуманное регулярное выражение способно обеспечить высокую точность. Во избежание непредсказуемого потребления ресурсов перед использованием регулярных выражений их следует всесторонне протестировать, в том числе на производительность и точность.

9.4 Выявление характерных признаков

Выявление характерных признаков – это стандартное применение машинного зрения, обычно основанное на распознавании образов и машинном обучении. Наиболее типичной областью его применения является распознавание вредоносных объявлений среди тысяч изображений. Для выявления характерных признаков требуется вычисление, поиск и сохранение характерных признаков известного рекламного спама в приложениях для мобильных устройств в базе данных такого спама. При получении подозрительного изображения функция выявления характерных признаков вычисляет абстрактную информацию об изображения и принимает решение о том, содержится ли в нем вредоносное объявление. Возможность быстро и точно определять вредоносные рекламные изображения зависит от алгоритмов выявления характерных признаков и соответствующих алгоритмов сопоставления. Обычно выявление характерных признаков обеспечивает нечеткое заключение, и для получения конечного результата его требуется объединить с дополнительными процессами принятия решений. Ввиду сложности вычислений и необходимости сравнения всего файла выявление характерных признаков чаще всего используется для асинхронной фильтрации.

9.5 Поведение

Рекламный спам в приложениях для мобильных устройств обычно рассылается методом массовой рассылки, без разбора и неоднократно, и имеет некоторые другие характерные особенности. Механизмы фильтрации могут регистрировать поведение объявлений для мобильных устройств и вычислять их взаимосвязь. Когда поведение принятого объявления соответствует характеристикам, уже хранящимся в базе данных спама, можно установить, что файл скорее всего является вредоносным

объявлением. Поскольку у поведения объявлений нет определенной зависимости от времени, выявление поведения можно использовать для обнаружения неизвестных вредоносных объявлений, и оно больше подходит для асинхронной фильтрации.

9.6 Проверка моделей

Проверка моделей – один из важных подходов, предназначенный для верификации требований. Например, эффективными инструментами обнаружения рекламного спама в приложениях для мобильных устройств служат модель подобия и модель дерева решений. Иногда отдельные модели не позволяют определить, являются ли рекламные объявления вредоносными, и для комплексного обнаружения можно использовать комбинацию из нескольких моделей, такую как группирование моделей. Проверку моделей можно использовать как для синхронной, так и для асинхронной фильтрации.

10 Рабочие процессы

Фильтрация рекламного спама в приложениях для мобильных устройств обычно состоит из последовательных процессов, показанных на рисунке 2. В некоторых случаях механизмы синхронной и асинхронной фильтрации могут работать параллельно.

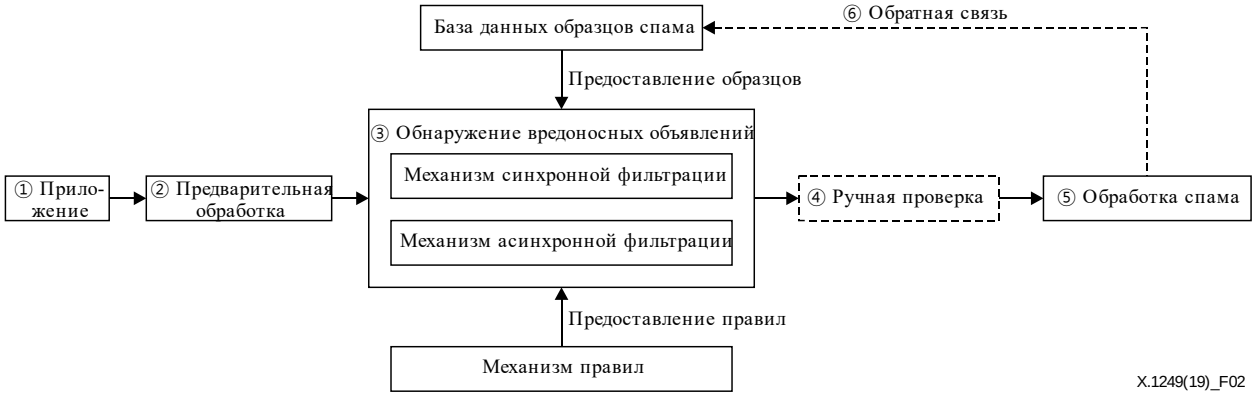

Рисунок 2 − Рабочие процессы фильтрации рекламного спама

Имеют место следующие основные шаги.

1) Объявления рассылаются и доставляются в приложения для мобильных телефонов.

2) Объявления должны быть предварительно обработаны. Например, разделяются разные типы носителей рекламы: URL, текст, аудио, видео и т. д.

3) В зависимости от угроз и сложности фильтрации контент доставляется в механизм синхронной или асинхронной фильтрации, который предварительно настроен, но по мере необходимости может регулироваться. Для комплексного обнаружения иногда бывает необходимо загрузить один и тот же контент в синхронный и асинхронный фильтры. Для определения необходимости фильтрации объявления проверяются по правилам и образцам, полученным от механизма правил и из базы данных рекламного спама в приложениях для мобильных устройств.

   a) После шага 2 механизм синхронной фильтрации выявляет рекламный спам в приложениях для мобильных устройств на основе правил фильтрации, предоставленных механизмом правил. Если модуль синхронной фильтрации обнаруживает рекламный спам в приложениях для мобильных устройств, фильтрация спама завершается, объявление немедленно блокируется, и алгоритм переходит к шагу 6. Если в механизме синхронной фильтрации URL-адреса или учетные записи в приложении относятся к белым спискам, то объявление доставляется. Если оценить рекламу не удалось, алгоритм переходит к шагу 4.

b) После шага 2 механизм асинхронной фильтрации выявляет спам в объявлениях на основе правил фильтрации, предоставленных механизмом правил. Если модуль асинхронной фильтрации обнаруживает спам, фильтрация спама завершается, объявление немедленно блокируется, и алгоритм переходит к шагу 6. Если оценить рекламу не удалось, алгоритм переходит к шагу 4.

4) Иногда требуется ручная проверка и оценка объявления. Если спам обнаружен и подтвержден, алгоритм переходит к шагу 5.

5) Над спам-объявлениями выполняются операции согласно предварительно выбранной конфигурации, такие как запись, замена и т. д.

6) Рекламные спам-объявления в приложениях для мобильных устройств сохраняются в базе данных рекламного спама в приложениях для мобильных устройств. Кроме того, спам-объявления могут извлекаться из базы данных спама как новые правила и загружаться в механизм правил или использоваться для оптимизации этого механизма.

11 Эксплуатационные требования

Точность обнаружения рекламного спама в приложениях для мобильных устройств измеряется сочетанием частоты ложноположительных и частоты ложноотрицательных результатов, которые должны считаться сбалансированными.

11.1 Требования к точности

Частота ложноположительных результатов рассчитывается как отношение количества законных объявлений, которые неверно оценены как спам или вредоносные объявления, к общему количеству законных объявлений. Если данный показатель высок, это означает, что могут блокироваться некоторые законные рекламные объявления в приложениях для мобильных устройств. Таким образом, этот показатель должен быть как можно ниже.

Частота ложноотрицательных результатов рассчитывается как отношение количества рекламных спам-объявлений в приложениях для мобильных устройств, которые неверно оценены как законные, к общему количеству рекламных спам-объявлений в приложениях для мобильных устройств. Если данный показатель высок, это означает, что пользователи приложения для мобильных устройств будут чаще подвергаться воздействию рекламного спама. Таким образом, этот показатель должен быть как можно ниже.

11.2 Требования к эффективности

Эффективность алгоритма фильтрации рекламного спама в приложениях для мобильных устройств можно измерить по пространственно-временной сложности механизма фильтрации. Под временной сложностью понимается время, которое требуется для выполнения процесса фильтрации рекламы, а под пространственной сложностью – требуемое пространство (память). Эти два показателя оказывают существенное влияние на способ применения правила фильтрации. В синхронных фильтрах могут применяться правила фильтрации пониженной пространственно-временной сложности, а в асинхронных – правила фильтрации повышенной пространственно-временной сложности.

Библиография

[b-ITU-T X.509] Recommendation ITU-T X.509 (2016), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*

[b-ITU-T X.800] Рекомендация МСЭ-Т X.800 (1991 г.), *Архитектура безопасности для взаимосвязи открытых систем для приложений МККТТ*.

[b-ITU-T X.805] Рекомендация МСЭ-Т X.805 (2003 г.), *Архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами*.

[b-ITU-T X.1231] Рекомендация МСЭ-Т X.1231 (2008), *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.1254] Рекомендация МСЭ-Т X.1254 (2012 г.), *Структура гарантии аутентификации объекта*.

[b-ITU-T X-Sup.19] ITU-T X-series Recommendations – Supplement 19 (2013), *Supplement on security aspects of smartphones.*

[b-ITU-T X-Sup.24] ITU-T X-series Recommendations – Supplement 24 (2014), *Supplement on a secure application distribution framework for communication devices.*

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	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; 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
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 межсетевого протокола, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2019 г.