СОВРЕМЕННЫЕ СИСТЕМЫ ОБНАРУЖЕНИЯ ВРЕДОНОСНЫХ СООБЩЕНИЙ ЭЛЕКТРОННОЙ ПОЧТЫ

Ломонос Г. В., Захарьев В. А.
Кафедра информационных систем и технологий,
Белорусский государственный технологический университет
Кафедра систем управления,
Белорусский государственный университет информатики и радиоэлектороники
Минск, Республика Беларусь
E-mail: lomonosg07@gmail.com, zahariev@bsuir.by

Статья посвящена исследованию современных систем и методов обнаружения вредоносных сообщений в электронной почте. В ней представлен обзор наиболее эффективных подходов и технологий, а также рассмотрены ключевые особенности их реализации.

Введение

В современном мире, где интернет стал неотъемлемой частью повседневной жизни, компьютерные технологии служат ключевым инструментом доступа к информации. Эти технологии обеспечивают обмен данными, включая электронную почту и мгновенные сообщения.Согласно статистике, к 2023 году число пользователей интернета достигло 4,8 миллиарда, что привело к увеличению нагрузки на сетевые инфраструктуры и к росту объема отправляемой корреспонденции [1]. Однако с ростом использования этих средств коммуникации возникают различные проблемы. Одной из наиболее актуальных является проблема фильтрации спам-писем. Спам-письма можно определить как нежелательные сообщения, которые доставляются на электронные адреса без предварительного согласия получателя. В большинстве случаев это рекламные материалы, распространяемые незаконными методами массовой рассылки [1].

I. Современные методы обнаружения вредоносных сообщений

Существует программное обеспечение (ПО) для автоматического определения спама (т. н. спам-фильтры). Оно может быть предназначено для конечных пользователей или для использования на серверах. Программы автоматической фильтрации используют статистический анализ содержания письма для принятия решения, является ли оно спамом. Наибольшего успеха удалось достичь с помощью алгоритмов, основанных на теореме Байеса. Для работы этих методов требуется предварительное «обучение» фильтров путем передачи ему рассортированных вручную писем для выявления статистических особенностей нормальных писем и спама.

Метод очень хорошо работает при сортировке текстовых сообщений (в том числе HTML). После обучения на достаточно большой выборке удаётся отсечь до 95—97 процентов спама. Для обхода таких фильтров спамеры иногда помещают содержательную часть в картинку, вложенную в письмо, текст же либо отсутствует, либо случаен, что не позволяет фильтру составить статистику для распознавания таких писем. В этом случае необходимо пользоваться программами распознавания текста (большинство современных почтовых программ этого не поддерживают), либо использовать другие методы [2]. Залог надежной работы байесовского метода – постоянное дообучение фильтра и указание ему на совершаемые ошибки. В почтовых программах для этого вводится возможность ручной пометки сообщения «спам/не-спам», а в почтовых сервисах в интернете – кнопка «пожаловаться на спам».

Многие программы и почтовые сервисы в интернете позволяют пользователю задавать собственные фильтры. Такие фильтры могут состоять из слов или, реже, регулярных выражений, в зависимости от наличия или отсутствия которых сообщение попадает или не попадает в мусорный ящик. Однако такая фильтрация трудоёмкая и негибкая, кроме того, требует от пользователя известной степени знакомства с компьютерами. С другой стороны, она позволяет эффективно отсеять часть спама, и пользователь точно знает, какие сообщения будут отсеяны и почему.

Например, одним из методов неавтоматической фильтрации являются черные списки, которые как метод широко используются и поэтому будут кратко освещены, однако не относятся к методам классификации текстовой информации.

Чёрные списки. DNSBL – DNS blacklist или DNS blocklist – списки хостов, хранимые с использованием системы архитектуры DNS. Обычно используются для борьбы со спамом. Почтовый сервер обращается к DNSBL, и проверяет в нём наличие IP-адреса клиента, с которого он принимает сообщение. При положительном ответе считается, что происходит попытка приёма спам- сообщения. Серверу отправителя сообщается ошибка 5xx (неустранимая ошибка) и сообщение не принимается. Почтовый сервер отправителя создаёт «отказную квитанцию» отправителю о недоставке почты. Раньше такие списки назывались RBL, Real-time Blackhole List, но сейчас это название яв-

ляется торговой маркой, принадлежащей MAPS LLC [3].

Типы DNSBL

- Списки открытых релеев – база данных почтовых серверов, неправильно сконфигурированных, которые позволяют пересылать через себя почтовые сообщения для всех желающих. Как правило данные хосты автоматически сканируются в Интернете, поэтому попадание такого хоста в руки людей, рассылающих спам сообщения, происходит очень быстро (не более 4 дней). При использовании данных списков существует наименьшая опасность блокирования обычной почты, так как сервер попадает в список, только после проверки его специальным почтовым роботом.
- Списки спам серверов – база данных серверов, через которые было замечено прохождение спам сообщений. Данные списки составляются на основе показаний пользователей, получивших спам с какого-либо сервера, поэтому они могут содержать устаревшую, или просто неверную информацию [4].
- Список Dialup адресов – список ip адресов провайдеров, используемых ими для организации сервиса удалённого доступа, и, следовательно, которые не могут быть адресами почтовых серверов. Использование данных списков практически безопасно для легальной почты.
- Список открытых HTTP/Socks прокси-серверов без контроля доступа позволяющие любому пользователю совершать неавторизованные действия скрывая свой реальный IP адрес, незаконные действия включают не только рассылку спама, но также и многочисленные иные варианты.

II. Современные системы обнаружения вредоносных сообщений

Одним из самых популярных, универсальных и проверенных средств спам-фильтрации является продукт компании Лаборатории Касперского. Kaspersky Anti-Spam – это решение для защиты пользователей корпоративных почтовых систем и публичных почтовых сервисов от массовой незапрошенной корреспонденции – спама.

В данном программном обеспечении применяются следующие алгоритмы распознования спама. Проверка сообщения по спискам. Приложение проверяет IP-адрес отправителя по черным спискам провайдеров и общественных организаций (DNSBL – DNS-based Blackhole List). В случае если адрес занесен администратором в белый список, то сообщение принимается, минуя все этапы анализа [5]. Фильтрация по SPF и SURBL. В процессе фильтрации может учитываться авторизация отправителя по технологии SPF (Sender Policy Framework). В дополнение к спискам DNSBL, выявляющим спамерские IP-адреса, используется также технология SURBL (Spam URI Realtime Block List), распознающая спамерские URL в теле сообщения.

Анализ формальных признаков письма. Программа отсеивает спам по таким типичным для него признакам, как модификация адреса отправителя или отсутствие его IP-адреса в системе доменных имён (DNS), неоправданно большое количество получателей или сокрытие их адресов. Кроме того, оцениваются размер и формат сообщения.

Сигнатурный анализ. Использование круглосуточно обновляемой базы лексических сигнатур позволяет распознавать модифицированные варианты исходного спамерского письма, создаваемые для обхода спам-фильтров.

Лингвистические эвристики. Программа проверяет наличие и расположение в тексте письма слов и фраз, типичных для спама. Анализу подвергается как текст самого письма, так и содержание вложенных файлов. Графические сигнатуры. Используя базу графических сигнатур, приложение блокирует также распространенные в последнее время спамерские письма, которые содержат информацию в виде изображений, а не в виде текста.

UDS-запросы в режиме реального времени. Технология UDS (Urgent Detection System) позволяет получать данные о последних спамерских рассылках уже через секунду после их обнаружения. Эта информация используется для дополнительной проверки тех сообщений, которые не получили однозначной оценки (спам/не-спам) [6].

III. Выводы

В области фильтрации спама используются различные методы распознавания. Однако ни один алгоритм не гарантирует 0 процентов ложноположительных или ложноотрицательных результатов. По мере того, как спамеры совершенствуют свои стратегии рассылки спама, существующие решения по фильтрации спама также должны совершенствоваться.

1. CORMACK, G. V. Email spam filtering: a systematic review. Foundations and Trends® in Information Retrieval, 2006, vol. 1, no. 4, pp. 335–455. https://doi.org/10.1561/1500000006
2. Global Security Map by SAINT [Электронный ресурс]. – Режим доступа: <https://globalsecuritymap.com>
3. Li, Wenbin, Ning Zhong, and Chunnian Liu." Combining multiple email filters based on multivariate statistical analysis." Foundations of Intelligent Systems. Springer Berlin Heidelberg, 2006. 729-738.
4. D.J. Hill, B. S. Minsker, and E. Amir, "Real-time Bayesian anomaly detection in streaming environmental data", Water Resour. Res., 2018, C.45.
5. A. A. Nasr, M. Z. Abdulmaged, "A Learnable Anomaly Detection System using Attributional Rules", International Journal of Computer Network and Information Security, vol. 8(11), 2016, C. 57.
6. M. Zhang, B. Xu and J. Gong, "An Anomaly Detection Model Based on One-Class SVM to Detect Network Intrusions,"11th International Conference on Mobile Ad-hoc and Sensor Networks (MSN), Shenzhen, 2015, C. 157.