k	2	3	4	5	6	7	8	9	10
2^k	4	8	16	32	64	128	256	512	1024
Теор. O_S	2,77	3,62	6,76	12,98	25,30	49,67	97,98	193,89	384,47
Эксп. O_S	–	2,33	4,42	9,34	19,55	40,55	82,62	169,32	339,48

Рисунок 3 – Сравнительный анализ средней кратности тестов (MATS ++) и *March C−*

Анализ эксперимента показывает, что значения среднего количества итераций O_S являются реализуемыми , поэтому можно сделать вывод о применимости многократных вероятностных тестов с изменяемыми исходными состояниями для псевдо исчерпывающего тестирования ОЗУ.

Список использованных источников:

1. Barzilai, Z. Exhaustive Generation of Bit Pattern with Application to VLSI Self–Testing / Z. Barzilai, D. Coppersmith, A. Rozenberg // IEEE Transactions on Computers. –1983. – Vol. C–31, № 2. – P.190–194.
2. Nicolaidis, M. Theory of transparent BIST for RAMs // IEEE Transactions on Computers. – 1996. – Vol. 45, № 10. – P. 114.
3. Ярмолик, В.Н. Псевдоисчерпывающее тестирование ОЗУ / В.Н. Ярмолик, И. Мрозек, В.А. Леванцевич// Информатика. – 2017. – №2(54). – С.58–69.
4. Д. Кнут Устойчивые паросочетания и другие комбинаторные задачи / Д.Э.Кнут / МЦМНО. 2014, с 26-28

ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА ЗАЩИТЫ ПРИВАТНОСТИ И ФИЛЬТРАЦИИ НЕЖЕЛАТЕЛЬНЫХ ПИСЕМ В ЭЛЕКТРОННОЙ ПОЧТЕ

Литвинко П.М.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Лапицкая Н.В. – к.т.н.,доцент

В настоящей работе предлагается новый подход к решению проблемы фильтрации спама за счёт распознавания массовых рассылок и дополнительной проверки отправителя при обнаружении сообщений личного характера. Проверка осуществляется при помощи автоматизированного теста Тьюринга. Разработанная модель позволяет добиться высокой точности распознавания (98.81%) и эффективно осуществлять фильтрацию писем, а также защиту от утечек личной информации.

Электронная почта остаётся неотъемлемой частью социального взаимодействия и повсеместным средством коммуникации. По данным исследования Radicati Group, число активных пользователей электронной почты составляет 3,9 млрд на 2019 год [1]. По прогнозам, общее количество отправляемых и получаемых электронных писем в день к концу 2023 года вырастет до 347 миллиардов, а число пользователей - до 4,3 миллиардов.

По мере того, как число пользователей и объём пересылаемых сообщений неуклонно растёт с годами, несанкционированное использование электронной почты в маркетинговых и мошеннических целях, распространения вредоносного ПО и кражи личной информации становится одной из самых серьёзных проблем в почтовых службах. По оценкам, в 2010 году более 97% писем были классифицированы как спам [2]. При этом становится всё более распространённым феномен «перегрузки электронной почтой», впервые описанный ещё в 1996 году [3]. Именно поэтому многие исследования, изучающие или анализирующие электронные письма, сосредоточены на аспекте категоризации электронных писем, а также поиске эффективных инструментов управления почтой и снижения информационной перегрузки. Однако борьба между спамерами и инструментами защиты от спама продолжается, поскольку каждая сторона пытается создать новые способы преодоления методов, разработанных другой.

Традиционные методы определения спама включают применение байесовского классификатора [4], системы оценки на основе правил [5], проверку DNS MX-записей и обратный поиск по адресу [6], ведение чёрных списков IP и DNS (DNSBL) [7]. Однако каждый из приведённых объективных методов классификации при достижении заданного предела точности приводит к ложным положительным или неверным отрицательным срабатываниям. Идеальное решение не может быть найдено, поскольку каждая сторона использует уязвимости прежних алгоритмов для разработки новых способов доставки писем.

Принципиальная сложность разработки эффективных систем фильтрации спама заключается в том, само определение спама является субъективным и получателем электронных писем также является субъект. В то же время общей характеристикой спама является массовый характер рассылок, поскольку отправитель рассчитывает лишь на заданный процент доставки и открытия электронных писем, что является уже объективным критерием.

В настоящей работе для решения задачи фильтрации нежелательных писем, предлагается сместить область применения объективных методов классификации для решения задачи распознавания рассылки массового характера и использовать принципиально новый подход для проверки легитимности доставки электронного письма. Использование комбинации двух методов позволит более эффективно решить общую задачу определения и фильтрации спама.

Схема работы системы представлена на рисунке 1. При получении входящего сообщения происходит извлечение текста и разделение его на n-граммы. Затем, с помощью многослойного персептрона (MLP) осуществляется предсказание класса письма: рассылка (Newsletter) – информационные сообщения, не требующие ответа или личное сообщение (Personal) – письма, предполагающие ответ или взаимодействие. В ходе исследования, данная модель показала наивысшую точность распознавания на тестовой выборке (98.81%), для обучения использовалось 37800 размеченных писем. Далее, для личных сообщений, которые и представляют угрозу оказаться спамом, происходит проверка адреса отправителя по списку контактов и в случае, если письмо отправлено с неизвестного адреса, запускается процедура проверки легитимности доставки электронного письма.

Данная процедура включает следующие шаги:

1) подозрительное письмо помечается как небезопасное и удаляется из списка непрочитанных сообщений на почтовом сервере пользователя;

2) генерируется ответное письмо, содержащее инструкции и уникальную ссылку для прохождения автоматизированного теста Тьюринга отправителем;

3) в случае успешного прохождения теста, письмо помечается как проверенное, переносится в список входящих сообщений, а отправитель получает подтверждение доставки.

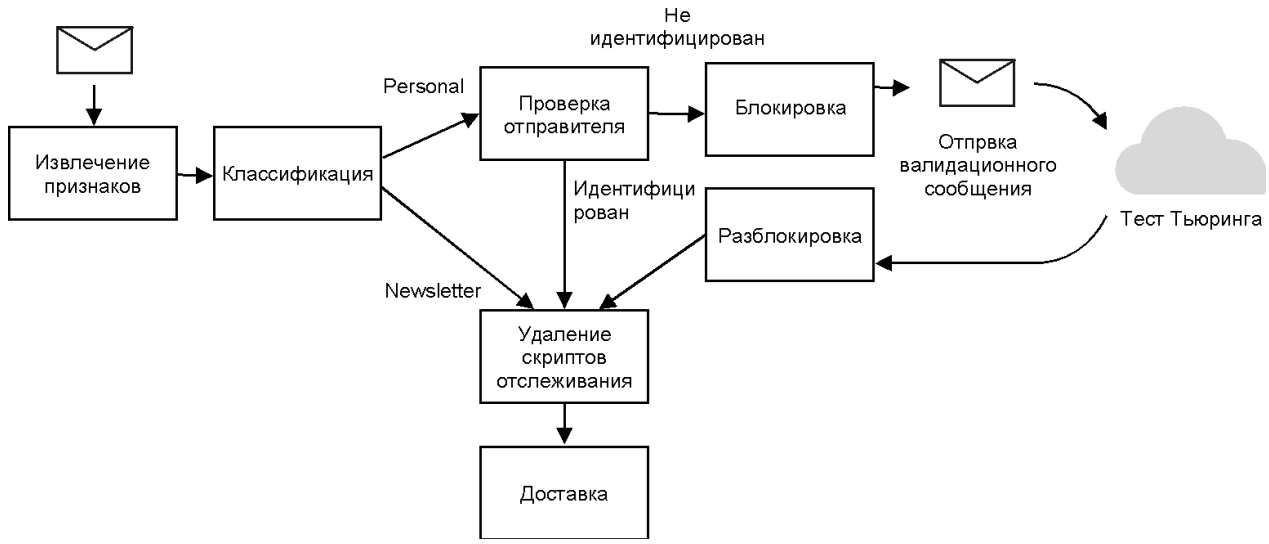

Рисунок 1 – Схема работы интеллектуальной системы фильтрации спама

В качестве автоматизированного теста Тьюринга в настоящей работе используется сервис reCAPTCHA от Google, обеспечивающий необходимый уровень сложности и в то же время позволяющий пропустить или упростить проверку для авторизованных пользователей. Для массовых спам-рассылок прохождение теста становится нецелесообразным и слишком трудоёмким для автоматизации, обеспечивая необходимую уверенность в том, что письмо было предназначено конкретно этому пользователю. Кроме того, на данном этапе может быть дополнительно осуществлена проверка личности отправителя для минимизации риска целенаправленного мошенничества (фишинга, вымогательства, попыток шантажа).

Помимо фильтрации спама, система выполняет также и проверку содержимого для предотвращения утечек персональной информации (IP адрес, местоположение пользователя, используемый браузер, почтовый клиент, операционная система и др.) и отслеживания таких действий пользователя как открытие/повторное открытие письма, переход по ссылке, открытие/просмотр вложений, пересылка письма и другие, широко применяющиеся в маркетинговых и мошеннических целях. В ходе работы было обнаружено более 40 различных способов внедрения скрытого кода отслеживания, каждый из которых был протестирован в 8 наиболее популярных клиентских приложениях электронной почты: Gmail (веб-версия), Gmail (Android), Gmail (iOS), Яндекс.Почта (веб-версия), Яндекс.Почта (iOS), Mail (Mac OS), Outlook (веб-версия), Mail.ru (веб-версия). В 44% случаев была зафиксирована утечка персональной информации при получении электронного письма. После внедрения разработанной системы этот показатель снизился до 3%.

Таким образом, разработанная модель позволяет эффективно распознавать массовые рассылки и персональные электронные письма, фильтруя нежелательные письма за счёт дополнительной проверки отправителя. Распознавание и изоляция скриптов отслеживания позволяет обеспечивать защиту личных данных получателя и блокировать триггерные маркетинговые рассылки. Разработанное программное средство может быть внедрено в существующие почтовые сервисы по протоколам SMTP и IMAP.

Список использованных источников:

1. The Radicati Group, Inc [Electronic resource] : Email Statistics Report, 2019-2023 – Executive Summary. – Mode of access: https://www.radicati.com/wp/wp-content/uploads/2018/12/Email-Statistics-Report-2019-2023-Executive-Summary.pdf. – Date of access: 24.03.2019.
2. Salomon, D. Elements of Computer Security / D. Salomon – Springer Verlag, 2010. – 374 P.
3. Email overload: Exploring personal information management of email : in proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI 1996, Vancouver, British Columbia, Canada, April 13-18, 1996 / SIGCHI; ed.: S.Whittaker [et al.]. – Vancouver, SIGCHI 1996. P. 276-283.
4. Zdziarski, J. Ending Spam — Bayesian Content Filtering and the Art of Statistical Language Classification / J. A. Zdziarski – 5th Edition. – No Starch Press, San Francisco, 2005. P – 451.
5. Spam Classification Based on Supervised Learning Using Machine Learning Techniques : papers from the International Conference on Process Automation, Control and Computing, Coimbatore, 20-22 July, 2011 / Coimbatore Institute of Technology; ed.: D. K. Renuka [et al.]. – Coimbatore Institute of Technology, Coimbatore, 2011. P. 1-4.
6. DNS Resource Record Analysis of URLs in E-Mail Messages for Improving Spam Filtering : IEEE/IPSJ 11th International Symposium on Applications and the Internet (SAINT), Munich, 18-21 July, 2011 / IEEE Computer Society; ed.: S. Suwa, N. Yamai, K. Okayama, M. Nakamura – IEEE Computer Society, Munich, 2011. P. 439-444.
7. Improving the Efficiency of Spam Filtering through Cache Architecture : 15th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems, Istanbul, 24-26 October, 2007. P. 303-309.

ОБЗОР РЕШЕНИЙ ПО МОДЕЛИРОВАНИЮ ДВИЖЕНИЯ ПОТОКОВ ЛЮДЕЙ ПРИ ЭВАКУАЦИИ ИЗ ПОМЕЩЕНИЙ

Лихута Е.И.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Парамонов А.И. – к.т.н., доцент

В данной работе представлен сравнительный обзор современных решений, которые используются для разработки планов эвакуации и моделирования эвакуации потоков людей из зданий в случае чрезвычайной ситуации. Рассмотрены преимущества и особенности отдельных программных комплексов.

С точки зрения психологии паника представляет собой одно из самых опасных психологических состояний для жизни человека. Группа людей, которые подверглись панике, способны многократно увеличить общее число жертв в результате чрезвычайной ситуации (ЧС). Это подтверждают проведённые в данной области многочисленные исследования.

На сегодняшний день существует достаточно много математических моделей, на основе которых созданы различные действующие программные комплексы, способные моделировать движения потоков людей при эвакуации из различных зданий и сооружений в случае ЧС.

Использование современных специализированных программных комплексов является показательным способом при расчёте эвакуационных способностей зданий и сооружений. Основное преимущество данного подхода заключается в возможности моделирования чрезвычайной ситуации с учётом весомого числа внешних переменных.

На данный момент существует достаточное количество моделей, которые позволяют настроить детали организации внутренней среды, ключевые особенности движения потоков людей, а также особенности их поведения в условиях ЧС.

Различают следующие модели движения потоков людей:

- упрощенная аналитическая модель,
- имитационно-стохастическая модель,
- индивидуально-поточная модель.

Далее рассмотрим современные программные решения, которые способны эмулировать перечисленные выше модели при моделировании эвакуации из зданий и сооружений.

Программный комплекс «PedGo» способен моделировать перемещение толпы людей при эвакуации людей из зданий, сооружений, а также из самолетов, кораблей и прочих видов общественного транспорта [1]. Модель, используемая в данном комплексе, имитирует решение и движение каждого отдельно взятого человека, поэтому план помещения исследуемого сооружения делится на квадратные ячейки размером 0,4 х 0,4 м. Место, занимаемое человеком, а также стены,