Безопасность систем электронной почты: проблемы и решения

С. К. Ганиев, email: sharofidinov1990@gmail.com
Ш. Ж. Хамидов, email: hamidov.sherzod.1990@mail.ru

Ташкентский университет информационных технологий имени Мухаммада ал-Хоразмий

Аннотация. *В данной работе рассматривается система, угрозы и протоколы безопасности электронных почтовых служб, проводиться анализ протоколов, а также исследуется методы фильтрации спам писем проводиться сравнительный анализ методов фильтрации.*

Ключевые слова: *электронная почта, протокол, целостность, конфиденциальность, спам, черный-лист, белый-лист, фильтрация, Байес, нейронные сети.*

Введение

Электронная почта - это быстрый, эффективный и дорогой метод обмена сообщениями через Интернет. Сегодня все больше и больше людей используют электронную почту для связи со своими друзьями, семьей, коллегами, клиентами и деловыми партнерами. В современных реалиях сложно представить человека, который не пользуется электронной почтой. Во всем мире люди владеют одним или несколькими адресами электронной почты, на которые ежедневно приходят миллионы писем.

В последние годы широкое использование электронной почты привело к возникновению и дальнейшему обострению проблем, вызванных нежелательными массовыми сообщениями электронной почты, обычно называемыми спамом.

1. Система электронной почты

Система электронной почты состоит из двух основных компонентов, которые находятся в ИТ-инфраструктуре организации: почтовых клиентов и почтовых серверов.

Стандарты (например, SMTP, ESMTP, POP, IMAP) для форматирования, обработки, передачи, доставки и отображения электронной почты гарантируют взаимодействие между множеством различных почтовых клиентов и серверов [1].

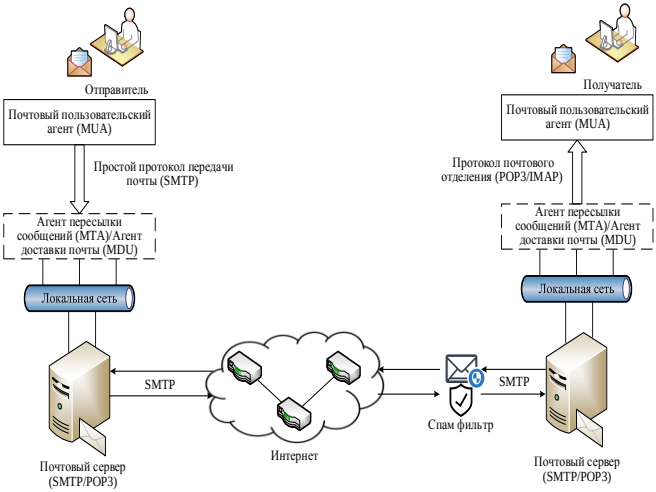

Рис. 1. Архитектура пересылки электронными письмами

Основные виды электронных почтовых сервисов

Веб-служба электронной почты - электронные письма хранятся на другом устройстве в Интернете, для пользования услугами вам нужно иметь учетную запись и подключение к Интернету. Хранение ваших электронных писем в Интернете означает, что вы можете получить к ним доступ из любого места, просто подключившись к Интернету. Почтовая веб-служба использует многоуровневую архитектуру, и, что наиболее важно, вам не нужно иметь дело с какими-либо конфигурациями.

Клиентская электронная почта - электронные письма хранятся на сервере, а не в сети, так что вы можете перечитывать их без доступа в Интернет. Однако у вас должно быть приложение, подключенное к службе и управляющее конфигурациями, и вы можете получить доступ к своей электронной почте только со своего устройства, в отличие от веб-службы электронной почты. Более того, клиентская почтовая служба использует двухуровневую архитектуру, поэтому проблем с безопасностью меньше по сравнению с веб-почтовой службой.

2. Угрозы безопасности электронной почты

Безопасность электронной почты основывается на принципах хорошего планирования, управления и ИТ-инфраструктуры. При правильном планировании, управлении системой и постоянном

мониторинге организации могут реализовать и поддерживать эффективную безопасность.

Угрозы безопасности электронной почты продолжают оставаться одними из самых больших рисков для организаций по всему миру. В системах электронной почты существует много угроз, таких как:

- Конфиденциальность сообщений;
- Блокировка доставки сообщения;
- Изменение содержания и источника сообщения;
- Изменение содержания и источника сообщения посторонним или получателем;
- Отказ передачи сообщения;
- Перехват сообщений и последующее использование [2].

Вредоносные электронные письма

Вредоносные электронные письма – содержащий программы или файл, который может повлиять на работу устройства или нанести ущерб данным без разрешения. Это опасно для безопасности электронной почты, они могут включать вирусы, троянские программы, черви и шпионское программы. Злоумышленник обычно использует электронную почту, чтобы обеспечить их доставку целевому пользователю. Опасность заключается в его способности, в случае успешного использования, взять под контроль устройство или даже всю сеть, применив повышенные привилегии к системе.

Фишинговые электронные письма – вид интернет-мошенничества, цель которого получить идентификационные данные пользователей. Представляет собой пришедшие на почту поддельные уведомления от банков, провайдеров, платежных систем и других организаций о том, что по какой-либо причине получателю срочно нужно передать / обновить личные данные. Если мошенники получат эту информацию, они могут получить доступ к вашей электронной почте, банку или другим счетам.

Спам письма - это рассылка писем без согласия получателя. Спам - одна из основных проблем сегодняшнего дня, приносящая финансовый ущерб компаниям и раздражающая пользователей электронной почты. Щелчок по ссылкам в спам-сообщениях может направить пользователей на фишинговые веб-сайты или места, зараженные вредоносными программами. Спам - серьезная проблема, которая потенциально угрожает дальнейшему использованию услуг электронной почты. Спам, являющийся носителем вредоносного ПО, вызывает распространение нежелательной рекламы, схем мошенничества, фишинговых сообщений, откровенного содержания, пропаганды и т.д.

По результатам отчетов лаборатории Касперского доля спам писем в мировом почтовом трафике распределяется следующим образом:

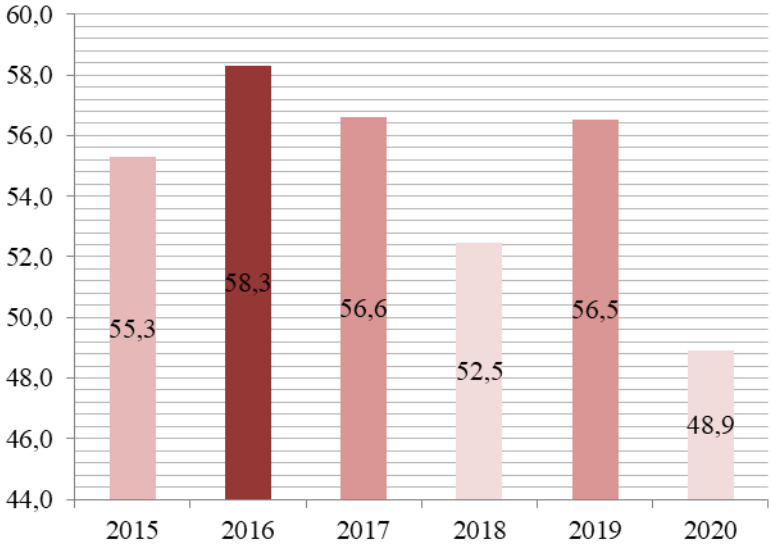

Рис. 2. Статистика доли спама в мировом трафике

3. Протоколы безопасности почтовых сервисов

Протокол безопасности электронной почты отвечает за защиту сообщений электронной почты и паролей. Это обеспечивает конфиденциальность клиентов. Некоторые провайдеры электронной почты поддерживают безопасные почтовые протоколы. Протокол защиты транспортного уровня предотвращает спуфинг и перехват сообщений между почтовыми серверами. Он используется для обеспечения конфиденциальности в Интернете и аутентификации конечного пользователя.

Для обеспечения безопасности сообщений электронной почты используются отдельные протоколы, такие как PGP и S/MIME. Два протокола могут использоваться для обеспечения функций безопасности электронной почты, связанных с целостностью сообщения, конфиденциальностью, аутентификацией и предотвращением отказа от авторства.

Протокол S/MIME(Secure/Multipurpose Internet Mail Extensions) считается расширением MIME, обеспечивает аутентификацию

(цифровая подпись) и конфиденциальность (шифрования). S / MIME - это не специальный программный продукт, а стандарт, предназначенный для внедрения различными поставщиками электронной почты, чтобы любые два почтовых клиента, поддерживающих S / MIME, могли безопасно обмениваться данными.

PGP(Pretty Good Privacy) можно определить как криптографический пакет, который обеспечивает конфиденциальность и аутентификацию данных для передачи. PGP используется для подписи, шифрования и дешифрования текстов, электронных писем, а также для повышения безопасности сообщений электронной почты. Шифрование содержимого сообщения происходит непосредственно на пользовательском устройстве с использованием открытого ключа получателя. Чтобы гарантировать, что содержимое сообщения не изменилось во время передачи, сообщение может быть подписано цифровой подписью. Формирования подписи сообщения происходит в момент отправки и подписывается уникальным закрытым ключом отправителя. Проверка происходит на устройстве получателя с использованием открытого ключа отправителя для проверки подписи, дешифрования производится закрытом ключом пользователя [3].

Почта с идентификацией ключа домена (Domain Keys Identified Mail) это протокол подписи электронной почты на основе криптографии, предназначенный для аутентификации электронной почты, авторизации и целостности на уровне домена в SMTP. Отправитель генерирует пару открытых и закрытых ключей для каждого почтового агента, публикует открытые ключи и политики в DNS. Получатель проверяет подпись, сравнивая ее с открытым ключом отправляющего почтового агента, доступным через DNS. Вполне возможно, что подпись проверяется промежуточными доменами перед ее пересылкой на следующий переход. В протоколе не применяется шифрование [4].

Таблица 1

Сравнение протоколов безопасности электронной почты

Функции	**S/MIME**	**DKIM**
Стандарт	RFC 3851	RFC 4871
Защита от подслушивания	Да	Нет
Прозрачен для пользователя	Нет	Да
Сообщение доступно для ESP	Нет	Да

Продолжение табл.1

Функции	S/MIME	DKIM
Конфиденциальность сообщений	Да	Нет
Тип аутентификации	Индивидуальный	Доменный
Тип сертификата	X.509	Нет спецификаций
Целостность сообщения	Да	Да
Доступ к веб-почте	Ограничено	Да
Неотказуемость	Да	Нет
Мобильность электронной почты	Ограничено	Да

4. Методы фильтрации спам писем

Фильтры спамов реализованы на всех уровнях, брандмауэр расположен перед почтовым сервером или у почтового агента, почтовый сервер обеспечивает интегрированное решение для защиты от спама и вирусов, предлагая полную защиту электронной почты на сетевом уровне. На уровне агента доставки почты также могут быть установлены спам-фильтры в качестве услуги для всех их клиентов. В почтовом клиенте пользователь может иметь персонализированный спам-фильтр, который затем автоматически фильтрует почту в соответствии с выбранными критериями.

Сегодня разработаны ряд технологий для создания методов фильтрации нежелательных писем. Все технологии можно разделить на настраиваемые вручную и интеллектуальные. Настраиваемые вручную фильтры основаны на списках доступа и настраиваются непосредственно пользователем, который выбирает либо нежелательные адреса с политикой пропускания черного списка, либо разрешенные адреса с политикой пропуска белого списка. Однако ручные методы фильтрации спама неэффективны и требуют постоянного обновления списков доступа. Фильтры на основе интеллектуальных технологий требуют обучения только на начальном этапе, далее обучение производится самостоятельно. Другой подход, который в последнее время стал более распространенным, - это использование нейронных сетей [5].

Фильтр черного списка: черные списки - один из самых популярных типов фильтрации спама. Черные списки - это записи адресов электронной почты или IP-адресов, которые ранее

использовались для рассылки спама. Когда приходит входящее сообщение, фильтр спама проверяет, находится ли его IP или адрес электронной почты в черном списке, сообщение считается спамом и отклоняется. В этом методе нельзя сравнивать адрес электронной почты нового отправителя, который не внесен в черный список.

Фильтр белого списка: белые списки - полная противоположность черным спискам. Адреса электронной почты, сохраненные в адресной книге, автоматически попадают в «белый список». Сканирование белого списка помогает блокировать нежелательные сообщения и разрешать только действительные письма, но это не всегда может быть подходящее письмо. В этой системе адрес электронной почты неизвестного отправителя проверяется по базе данных; если у них нет истории спама, их сообщение отправляется в белые списки получателя, которые используются для минимизации ложных срабатываний.

Фильтр серого списка: методы фильтрации спама используют тот факт, что многие спамеры пытаются отправить пакет нежелательной почты только один раз. В системе принимающий почтовый сервер первоначально отклоняет сообщения от неизвестных пользователей и отправляет сообщение об ошибке исходному серверу. Если почтовый сервер пытается отправить сообщение во второй раз, который предпримет большинство легитимных серверов, - метод предполагает, что сообщение не является спамом, и позволяет ему попасть в почтовый ящик получателя. На этом этапе фильтр добавит адрес электронной почты или IP-адрес получателя в список разрешенных отправителей.

Фильтр на основе URL-адреса: метод фильтрации спама на основе URL-адреса. В этом случае входящий URL-адрес сначала проверяется на то, является ли он законным или нет, и, если он обнаружен, ему разрешается отправить почту в почтовый ящик получателей. Таким образом создается репозиторий из этих URL-адресов, который можно время от времени проверять и обновлять.

Фильтрация на основе содержимого выполняет детальную проверку концепции сообщения электронной почты и помогает идентифицировать спам-сообщения. Фильтрация на основе содержимого может быть реализована посредством простого сопоставления текстового шаблона или посредством статистической индикации вероятности. Фильтры на основе содержимого могут классифицировать электронную почту как спам или легитимную, исследуя содержимое электронной почты. Обычно он используется для создания правил автоматической фильтрации и классификации электронных писем с использованием подходов машинного обучения, таких как наивная байесовская классификация, поддержка фильтров на

основе правил, векторная машина, искусственная нейронная сеть. Этот метод обычно анализирует слова, вхождение и распределение слов и фраз в содержимом электронных писем и затем использует сгенерированные правила для фильтрации входящего спама.

Фильтр спама на основе слов - это простейший тип фильтра на основе содержимого. Вообще говоря, фильтры на основе слов просто блокируют любое электронное письмо, содержащее определенные термины. Поскольку многие спам-сообщения содержат термины, которые не часто встречаются в личных или деловых сообщениях, фильтры слов могут быть простым, но действенным методом борьбы с нежелательной электронной почтой. Однако, если они настроены на блокировку сообщений, содержащих более общие слова, эти типы фильтров могут генерировать ложные срабатывания [6].

Байесовская фильтрация спама — метод для фильтрации спама, основанный на применении наивного байесовского классификатора, в основе которого лежит применение теоремы Байеса. При обучении фильтра для каждого встреченного в письмах слова высчитывается и сохраняется его «вес» — оценка вероятности того, что письмо с этим словом — спам. В простейшем случае в качестве оценки используется частота: «появлений в спаме / появлений всего». В более сложных случаях возможна предварительная обработка текста: приведение слов в начальную форму, удаление служебных слов, вычисление «веса» для целых фраз. Теорема Байеса используется несколько раз:

- в первый раз, чтобы вычислить вероятность, того что сообщение - спам, зная, что данное слово появляется в этом сообщении;
- во второй раз, чтобы вычислить вероятность, что сообщение - спам, учитывая все его слова (или соответствующие их подмножества);
- иногда в третий раз, когда встречаются сообщения с редкими словами.

Нейронные сети - анализ ключевых характеристик нейронной сетью напоминает байесовскую фильтрацию спама, где для каждого слова или словосочетания можно установить коэффициент определения письма как спам. Однако, в отличие от байесовского фильтра, здесь коэффициенты – это веса между нейронами сети, способные динамически изменяться в процессе обучения, что позволяет эффективно обнаруживать новый и ранее неизвестный спам за счет умения нейронной сети обобщать накопленный опыт. Нейронные сети внешне похожи на Наивный байесовский классификатор, но структурно различаются [7].

Таблица 2

Сравнение протоколов безопасности электронной почты

Спам фильтр	**Подходящее состояние**	**Недостаток**
Черный список	если подозреваемые спам IP-адреса являются фиксированными или известными	обнаружение подозреваемых IP-адресов затруднено и содержит ошибки
Список в реальном времени	если IP-адреса, подозреваемые в спаме, являются фиксированными или известными, и третья сторона надежна.	обнаружение подозреваемых IP-адресов затруднено и содержит ошибки
Белый список	если подозреваемые спам IP-адреса исправлены	неизвестная подлинная почта может быть объявлена спамом
Серый список	если доверенный отправитель всегда отправляет сообщение два раза	если доверенный отправитель не отправит сообщение два раза, почта будет потеряна.
Фильтр на основе слов	подозреваемые ключевые слова известны	подлинная почта может содержать подозрительные ключевые слова
Байесовский фильтр	подозреваемые ключевые слова известны своей вероятностью спама	подлинная почта может содержать подозрительные ключевые слова
Нейронные сети	подозреваемые ключевые слова известны и доступна лучшая эвристическая функция	подлинная почта может содержать подозрительные ключевые слова

Заключение

В этой работе были рассмотрены угрозы почтовых служб, протоколы безопасности и методы фильтрации спамов. Систем и методов по обнаружению и распознаванию спам писем электронной почты главной целью является обеспечение целостность данных и конфиденциальность личных данных пользователей. Среди методов, применяемых для фильтрации данных, а в частности электронной почты и сообщений, имеется множество как производительных, но имеющих высокую вероятность ложного срабатывания, так и точных. Совместное использование нейронных сетей с классическими алгоритмами позволяет уменьшить количество спам писем, а также уменьшить вероятность их пропуска фильтром.

Список литературы

1. Stine, K. E-mail security. An overview of threats and safeguards / K.Stine, M.Scholl // Journal of American Health Information Management Association. – United States of America, April 81-4, 2010. – P. 28-30.
2. Choudhary, S. E-mail Security: Issues and Solutions / S.Choudhary, R.Ghusinga // International Journal of Computer Information Systems. – India, October 7-4, 2013. – P. 42-46.
3. Rawdhan, F. Enhancement of Email Security Services / F.Rawdhan, M.Ibrahim // International Journal of Scientific & Engineering Research. – India, January 8-1, 2017. – P. 2090-2098.
4. Tariq, M. Effectiveness and limitations of e-mail security protocols / M. Tariq // International Journal of Distributed and Parallel Systems. – India, May 2-3, 2011. – P. 38-49.
5. Hasib, S. Anti-Spam Methodologies: A Comparative Study / S.Hasib, M.Motwani, A.Saxena // International Journal of Computer Science and Information Technologies. – India, December 3-6, 2012. – P. 5341-5345
6. Somvanshi, D. Spam e-mails filtering techniques/ D.Somvanshi, K.Doke // International Journal of Technical Research and Applications. – India, December 4-6, 2016. – P. 7-11.
7. Anitha, P. A Survey On: E-mail Spam Messages and Bayesian Approach for Spam Filtering / P. Anitha, C. Guru Rao, T. Sireesha // International Journal of Advanced Engineering and Global Technology. – South Africa, October 1-3, 2013. – P. 124-136.