УДК 004.77

ТЕХНОЛОГИИ ПОЛУЧЕНИЯ ДОВЕРЕННОЙ ЭЛЕКТРОННОЙ ПОЧТЫ. ОБЗОР И РЕАЛИЗАЦИЯ

Г. М. Михайлов[1] [0000-0002-4535-7180], А. М. Чернецов[2] [0000-0001-7655-2395]

[1-2]*Федеральный исследовательский центр «Информатика и управление» РАН, ул. Вавилова д. 44 корп. 2, г. Москва, 119333;*
[2]*Национальный исследовательский университет «МЭИ», ул. Красноказарменная д. 14 стр. 1, г. Москва, 111250*

[1]gmickail@ccas.ru, [2]an@ccas.ru

Аннотация

Представлен обзор современных технологий, применяемых при обработке почтовых сообщений для решения задачи получения доверенной электронной почты, проведено их описание. Приведены рекомендуемые настройки для успешного функционирования.

Ключевые слова*: e-mail, SPF, DMARC, DKIM.*

ВВЕДЕНИЕ

Архитектура электронной почты в интернете состоит из «мира пользователей» в виде почтовых агентов (Message User Agent, MUA) и «мира передачи» в виде службы обработки сообщений (Message Handling Service, MHS), состоящей из агентов пересылки сообщений (Message Transfer Agent, MTA).

Задача обеспечения защиты электронной почты от спама (spam) стоит уже много десятилетий [1]. Технологий для решения этой задачи придумано великое множество. К основным применяемым технологиям можно отнести следующие:

- проверка по DNSBL (DNS black list);
- проверка PTR-записи хоста при входящем подключения по SMTP;
- проверка корректности представления сервера в SMTP HELO заголовке;
- graylisting («серые списки»);
- установка таймаута ответа SMTP сервера, ограничение числа одновременных соединений.

Указанные технологии, как и некоторые другие, применяются именно для защиты от спама. К сожалению, проблема спам-сообщений не единственная проблема, которая существует для сообщений электронной почты.

Последнее десятилетие характеризуется также значительным ростом фишинговых атак (интернет-мошенничество для достижения идентификационных данных пользователей). К таким данным относятся, в том числе: логин, пароль, номер кредитной карты и другая конфиденциальная информация. В рамках фишинговых атак также может производиться запуск вредоносного программного обеспечения на компьютере пользователя.

Механизмы борьбы с фишингом электронной почты условно разделяются на настройку механизмов на стороне отправителя электронной почты и на стороне получателя.

Настройка механизмов на стороне отправителя предполагает предоставление дополнительной информации получателю, которая может быть использована для подтверждения факта отправки почты с данного сервера. Настройки механизмов на стороне получателя предполагают возможное использование нижеуказанной информации для принятия соответствующих мер по противодействию возможному фишингу.

Также на стороне получателя не исключается «ручная» проверка пользователем входящих писем. В этом случае, например, можно сравнить отображаемое имя адресата и реальный адрес электронной почты. Помимо этого, целесообразно при переходах из письма по внешним гиперссылкам проверять, что реальная гиперссылка совпадает с её отображением пользователю.

1. ОБЗОР НЕКОТОРЫХ СУЩЕСТВУЮЩИХ ТЕХНОЛОГИЙ ПОЛУЧЕНИЯ ДОВЕРЕННОЙ ЭЛЕКТРОННОЙ ПОЧТЫ

В [2] введено применение ряда протоколов для решения задачи получения доверенной электронной почты. Для этого описаны и рекомендованы к применению следующие протоколы и стандарты:

- STARTTLS: расширение безопасности SMTP, позволяющее клиенту и серверу SMTP договориться об использовании TLS (Transport Layer Security), чтобы наладить закрытый обмен данными с аутентификацией по интернету.

- S/MIME (Secure Multipurpose Internet Mail Extensions): обеспечивают аутентификацию, целостность, невозможность отказа (nonrepudiation, посредством цифровых подписей) и конфиденциальность (посредством шифрования) сообщений SMTP.
- DANE (DNS-Based Authentication of Named Entities): предназначен для исправления недостатков системы центров сертификации (CA) за счет создания альтернативного канала аутентификации открытых ключей на основе DNSSEC. При применении такого механизма те же самые отношения доверия, которые используются для сертификации IP-адресов, используются для сертификации серверов, работающих по этим адресам.
- SPF (Sender Policy Framework) [3] позволяет владельцу домена указать IP-адреса MTA, уполномоченных отправлять почту от имени домена. SPF использует DNS, чтобы владельцы доменов могли создавать записи, связывающие доменное имя с конкретным диапазоном IP-адресов или уполномоченных MTA. Получатель просто сличает текстовую запись SPF (типа TXT) в DNS, чтобы проверить, имеет ли право предполагаемый отправитель сообщения использовать такой исходный адрес. Почта, поступающая не с уполномоченных IP-адресов, может отбрасываться.
- DKIM (DomainKeys Identified Mail) [4]: позволяет «акторам» электронной почты (авторам или операторам) надежно приписать к сообщению свое доменное имя с помощью криптографических методов, чтобы механизмы фильтрации могли выработать точную репутацию домена. MTA могут подписывать выбранные заголовки и тело сообщения. Такая подпись подтверждает исходный домен письма и обеспечивает целостность тела сообщения.
- DMARC (Domain-based Message Authentication, Reporting, and Conformance) [5]: публикует требование, чтобы доменное имя автора было аутентифицировано по DKIM и/или SPF, чтобы владелец домена затребовал от получателя обработку неаутентифицированной почты с помощью этого домена, а также механизм отчетности для отправки отчетов от получателей владельцам доменов. DMARC сообщает отправителям о пропорциональной эффективности их политик SPF и DKIM, а также сигнализирует получателям, какие действия нужно предпринять в различных ситуациях индивидуальных и массовых атак.

Остановимся подробнее на особенностях трех технологий – SPF, DKIM и DMARC. С остальными технологиями можно ознакомиться в работе [6].

Наличие SPF снижает вероятность попадания письма в спам при приеме почтового сервера адресата. Важно помнить, что SPF-запись может быть только одна для одного почтового домена. В рамках одной SPF может быть несколько записей серверов.

Использование SPF решает следующую проблему: в нынешней инфраструктуре электронной почты любой хост может поставить любое доменное имя в любой идентификатор в заголовке письма: не требуется, чтобы хост ставил обязательно имя домена, где он сам находится. SPF заставляет почту идти по определенному пути и ломается, когда легитимная почта отклоняется от этого пути – в частности, когда сообщение проходит через список рассылки.

Подпись DKIM добавляется в служебные заголовки письма и не видна для пользователя. DKIM использует два ключа шифрования – открытый и закрытый [7]. С помощью закрытого ключа формируются заголовки для всей исходящей почты, а открытый ключ как раз добавляется в DNS в виде записи типа TXT. Подпись создается автоматически в MTA, т. е. SMTP-сервером [8].

Проверка DKIM происходит автоматически на стороне получателя. Если домен в письме не авторизован для отправки сообщений, то письмо может быть помечено как «подозрительное» или помещено в спам в зависимости от политики получателя.

Технология DMARC (аутентификация сообщений, предоставление отчётов и проверка соответствия на базе доменного имени) помогает помечать «подозрительными» сообщения по принципу наличия записей SPF и DKIM. DMARC – это подпись, которая позволяет принимающему серверу решить, что делать с полученным письмом. DMARC использует DKIM и SPF. Если отправленное сообщение не прошло проверку DKIM и SPF, то оно не пройдет и DMARC. Если же сообщение успешно прошло хотя бы одну проверку (DKIM или SPF), то и проверку DMARC сообщение пройдет успешно.

2. НАСТРОЙКА ДЛЯ ВЦ ФИЦ ИУ РАН

В 2023 году Минобрнауки издало распоряжение по подведомственным организациям о необходимости использования для почтовых серверов технологий

SPF, DKIM и DMARC вместе (Письмо Минобрнауки России от 17 августа 2023 г. № МН-19/634 «О направлении типовых рекомендаций»). Соответственно сервера ВЦ ФИЦ ИУ РАН были перенастроены с использованием указанных технологий.

В указанном выше письме приведены настройки для почтовых серверов Postfix, Exim и Exchange. К сожалению, для распространенного почтового сервера Sendmail настроек не приводилось. В ВЦ ФИЦ ИУ РАН почтовый домен ccas.ru работает на Sendmail 8.13.6 на ОС Solaris 10, в качестве SMTP-сервера с 2017 г. используется Sendmail 8.14.4 на ОС CentOS [9].

Для SPF были сделаны следующие настройки: отправка реализуется со всех MX-серверов с явно прописанными адресами SMTP-серверов. Для всех остальных адресов стоит запрет.

Для DKIM, как уже указано выше, необходимо создать для домена пару открытый/закрытый ключ. Открытый ключ публикуется в DNS. Все сообщения автоматически подписываются с использованием закрытого ключа. В силу известных санкционных ограничений по доступу к репозиториям для ОС Solaris провести установку пакета openDKIM не удалось, поэтому наши работы ограничились проведением всех настроек только на SMTP-серверах на базе CentOS. В качестве электронной подписи (ЭП) использовалась запись с ключом длиной 1024 бит.

Настройка для DMARC в нашем случае свелась к созданию единственной записи в отчётах с адресом отправления электронной почты dmarc@frccsc.ru. Если поставить жесткие условия на почту, то возможны ложные отказы в приеме нужной почты, что в нашем случае научной организации неприемлемо. В других случаях можно, например, настроить непрохождение проверки как отказ в приеме письма.

ЗАКЛЮЧЕНИЕ

Представлены настройки записей для почтового сервера научной организации. К сожалению, использование описанных механизмов не дает полной гарантии доверия к доставляемой корреспонденции, но уровень доверия при их использовании может быть повышен.

Благодарности

Работа выполнена в рамках исполнения темы № 0063-2019-0003 «Математические методы анализа данных и прогнозирования 2019-2023 ФИЦ ИУ РАН.

СПИСОК ЛИТЕРАТУРЫ

1. *Копытов М.А., Рогов Ю.П.* Электронная почта. Администрирование и проблемы надежности. Тезисы доклада в сборнике Всероссийской научной конференции «Научный сервис в сети Интернет» (г. Новороссийск, 23–28 сентября 2002 года). М.: Изд-во МГУ, 2002. С. 128–129.

2. National Institute of Standards and Technology, “Trustworthy Email,” NIST Special Publication 800-177, September 2016.

3. SPF RFC.
URL: https://datatracker.ietf.org/doc/html/rfc7208, дата доступа: 11.11.2024.

4. DKIM HomePageю
URL: https://www.dkim.org/, дата доступа: 11.11.2024.

5. DMARC HomePage. URL: https://dmarc.org/, дата доступа: 11.11.2024

6. *Столингс У.* Всеобъемлющая безопасность электронной почты в Интернете (пер. с. англ.)// Интернет изнутри, 2018, №10
URL: https://ii.org.ru/vseobemlyushhaya-bezopasnost-yelektron/, дата доступа: 11.11.2024

7. National Institute of Standards and Technology, “Introduction to Public Key Technology and the Federal PKI Infrastructure,” NIST Special Publication 800-32, February 2001.

8. *Михайлов Г.М., Рогов Ю.П., Чернецов А.М*. Организация внешнего почтового smtp-сервера в научной организации // Научный сервис в сети Интернет: труды XVII Всероссийской научной конференции (21–26 сентября 2015 г., г. Новороссийск). М.: ИПМ им. М.В. Келдыша, 2015. С. 237–239.

9. *Михайлов Г.М., Жижченко М.А., Чернецов А.М.* Обеспечение плавной перенумерации сети при смене провайдера // Научный сервис в сети Интернет: труды XIX Всероссийской научной конференции (18–23 сентября 2017 г., г. Новороссийск). М.: ИПМ им. М.В. Келдыша, 2017. С. 351–355.

REVIEW OF TECHNOLOGIES FOR ENSURING SECURITY AND PROTECTION OF EMAIL SYSTEMS IN A SCIENTIFIC ORGANIZATION

G.M. Mikhaylov[1] [0000-0002-4535-7180], A.M. Chernetsov[2] [0000-0001-7655-2395]

[1-2]*Federal Research Center "Informatics and Control" RAS, ul. Vavilova, 44 korpus 2, Moscow, 119333;*
[2]*National Research University "MPEI", ul. Krasnokazarmennaya, 14 str.1, Moscow, 111250*

[1]gmickail@ccas.ru, [2]an@ccas.ru

Abstract

The paper provides an overview of modern technologies used in processing email messages to solve the problem of receiving trusted email, and describes them. Recommended settings for successful operation are provided.

Keywords*: e-mail, SPF, DMARC, DKIM.*

REFERENCES

1. *Kopytov M.A., Rogov Iu.P.* Elektronnaia pochta. Administrirovanie i problemy nadezhnosti. Tezisy doklada v sbornike Vserossiiskoi nauchnoi konferentsii "Nauchnyi servis v seti Internet" (g. Novorossiisk, 23–28 sentiabria 2002 goda). M.: Izd-vo MGU, 2002. C. 128–129.

2. National Institute of Standards and Technology, "Trustworthy Email," NIST Special Publication 800-177, September 2016.

3. SPF RFC.
URL: https://datatracker.ietf.org/doc/html/rfc7208, date accessed: 11.11.2024

4. DKIM HomePage.

URL: https://www.dkim.org/, date accessed: 11.11.2024

5. DMARC HomePage.

URL: https://dmarc.org/, date accessed: 11.11.2024

6. *Stolings U.* Vseobieemliushchaia bezopasnost elektronnoi pochty v Internete" (per. s angl.) // Internet iznutri, 2018, №10.

URL: https://ii.org.ru/vseobemlyushhaya-bezopasnost-yelektron/, date accessed: 11.11.2024

7. National Institute of Standards and Technology, "Introduction to Public Key Technology and the Federal PKI Infrastructure," NIST Special Publication 800-32, February 2001.

8. *Mikhailov* G*.M., Rogov Iu.P., Chernetsov A.M.*. Organizatsiia vneshnego pochtovogo smtp-servera v nauchnoi organizatsii // Nauchnyi servis v seti Internet: trudy XVII Vserossiiskoi nauchnoi konferentsii (21–26 sentiabria 2015 g., g. Novorossiisk). M.: IPM im. M.V. Keldysha, 2015. S. 237–239.

9. *Mikhailov G.M., Zhizhchenko M.A., Chernetsov A.M.* Obespechenie plavnoi perenumeratsii seti pri smene provaidera // Nauchnyi servis v seti Internet: trudy XIX Vserossiiskoi nauchnoi konferentsii (18–23 sentiabria 2017 g., g. Novorossiisk). M.: IPM im. M.V. Keldysha, 2017. S. 351–355.

СВЕДЕНИЯ ОБ АВТОРАХ

МИХАЙЛОВ Гурий Михайлович – кандидат физ.-мат. наук, гл. специалист отдела 11 Вычислительного центра им. А.А. Дородницына Федерального исследовательского центра «Информатика и управление» Российской академии наук.

Gury Mikhailovich MIKHAILOV – candidate of physics and mathematics Sciences, Ch. specialist of department 11 of the Computer Center named after. A.A. Dorodnitsyn Federal Research Center "Informatics and Management" of the Russian Academy of Sciences

email: gmickail@ccas.ru

ORCID: 0000-0002-4535-7180

ЧЕРНЕЦОВ Андрей Михайлович – кандидат технических наук, доцент, ведущий инженер Федерального исследовательского центра «Информатика и управление» Российской академии наук; доцент кафедры Прикладной математики и искусственного интеллекта Национального исследовательского университета «МЭИ».

Andrey Mikhailovich CHERNETSOV – Candidate of Technical Sciences, Associate Professor, leading engineer of Federal Research Center "Informatics and Management" of the Russian Academy of Sciences; Associate Professor, Department of Applied Mathematics and Artificial Intelligence, National Research University "MPEI".

email: an@ccas.ru, chernetsovam@mpei.ru

ORCID: 0000-0001-7655-2395

Материал поступил в редакцию 14 ноября 2024 года