УДК: 004.738.5

СПОСОБ ПРОАКТИВНОЙ ЗАЩИТЫ ПОЧТОВОГО СЕРВЕРА ОТ НЕЖЕЛАТЕЛЬНЫХ СООБЩЕНИЙ ЭЛЕКТРОННОЙ ПОЧТЫ

METHOD FOR PROACTIVE PROTECTION OF MAIL SERVER FROM UNSOLICITED EMAILS

Канд. техн. наук С.П. Соколовский, А.А. Горбачев

PhD S.P. Sokolovsky, A.A. Gorbachev

Краснодарское высшее военное училище им. С.М. Штеменко

Современные методы борьбы с нежелательными сообщениями электронной почты (спамом) включают: фильтрацию писем, комплексный анализ заголовков, использование запрещенных и разрешенных списков адресов отправителей и другие технические меры. Однако все эти методы являются реагирующими, в связи с чем, они эффективны только при использовании известных шаблонов спам-атак. Кроме того, некоторые из этих методов требуют привлечения значительного вычислительного ресурса, регулярных усовершенствований и значительных затрат на техническое обслуживание. В связи с этим, возникает потребность в разработке методов защиты, реализующих превентивные меры, нивелирующих недостатки существующих методов. Предлагаемый в статье способ защиты позволяет с использованием протокольных возможностей SMTP обеспечить снижение результативности обнаружения злоумышленником факта использования средств защиты, увеличить продолжительность доставки спам-сообщений и затрачиваемый злоумышленником вычислительный ресурс.
Ключевые слова: электронная почта, спам, проактивная защита, компьютерная атака.

Current methods of countering unwanted e-mail messages (spam) include e-mail filtering, comprehensive header analysis, and the use of banned and allowed sender lists, and other technical measures. However, all of these methods are reactive, so they are only effective when using known spam attack patterns. In addition, some of these methods require significant computing resources, regular enhancements and significant maintenance costs. In this regard, there is a need to develop protection methods that implement preventive measures, leveling the disadvantages of existing methods. Proposed in the article method of protection allows by using SMTP protocol capabilities to provide decreased possibility of discovering the fact of use of protection means by an intruder, increase duration of delivery of spam messages and computational resource spent by an attacker.
Keywords: e-mail, spam, proactive protection, computer attack.

Известно, что нежелательная электронная почта (спам), составляет от 60 % до 90 % всех электронных писем, отправленных по всему миру. Под спамом понимается телематическое электронное сообщение, предназначенное неопределенному кругу лиц, доставленное абоненту и (или) пользователю без их предварительного согласия и не позволяющее определить отправителя этого сообщения, в том числе ввиду указания в нем несуществующего или фальсифицированного адреса отправителя. По данным «Лаборатории Касперского» в I квартале 2020 года средняя доля спама в мировом почтовом трафике составила 54,61 %, доля спама в трафике россий-

ского сегмента интернета также достигла максимума в январе 2020 года и составила 52,08 %, а первую пятерку стран по количеству исходящего спама возглавила Россия, на ее долю пришлось 20,74 % всего «мусорного» трафика. Для борьбы со спамом, уже достаточно давно разработаны и применяются ряд систем и методик, а большинство известных методов защиты от спама описаны, например, в [1, 2]. Основными из них являются: байесовская фильтрация, методы на основе формальных протокольных правил, процедурные методы, проверка подлинности отправителя, методы, использующие контрольные сумы и списки блокировки и др. Однако все эти методы основаны, в основном, на обнаружении и блокировании уже принятых спам-сообщений, и, по сути, являются реактивными, реагирующими на факт уже совершенного вредоносного воздействия, в связи с этим, они эффективны только при использовании известных шаблонов спам-сообщений. Кроме того, некоторые из известных методов реализуют попытки, так называемого силового демонстративного блокирования спам-сообщений, например, такие методы как перенаправление спам-сообщений их отправителям, направление выявленным источникам рассылки спама средств лечения вредоносных программ, и т.д. Применение таких методов противодействия, с одной стороны, ведет к компрометации применяемых средств защиты, что способствует их последующему обходу и/или изменению стратегии вредоносного воздействия злоумышленником. С другой стороны, эффективность средств защиты, реализующих эти методы, ограничена их ресурсными возможностями, так как эти методы являются вычислительно интенсивными и требуют для эффективного применения мощных процессоров с большими объемами памяти, в то время как ресурс злоумышленников может быть практически неограничен, что подтверждается их возможностью совершать крупномасштабные DOS и DDOS-атаки на основе массовой спам-рассылки с привлечением спам-ботов [3].

В настоящее время все большую актуальность приобретают принципиально новые подходы борьбы со спамом, основанные на предотвращении самой доставки спам-сообщений от злоумышленника на почтовый сервер. Эти подходы смещают акцент борьбы со спамом в сторону проактивной защиты, накладывающей ограничение на используемый злоумышленником вычислительный ресурс и вызывающей «истощение» его ресурсов в процессе почтовой транзакции без значительных вычислительных затрат со стороны защищаемого почтового сервера. В соответствии с [4], под проактивной защитой понимают активные воздействия на средства, применяемые злоумышленником в процессе проведения компьютерной атаки, с целью получения информации о злоумышленнике, противодействия проводимой компьютерной атаке, а также выведения из строя применяемых злоумышленником средств.

Однако известные технические решения, реализующие вопросы проактивной защиты почтовых серверов от массовой рассылки спам-сообщений, еще недостаточно проработаны и обладают существенными недостатками, а задачи приведения в соответствие таких мер защиты к централизованному замыслу противодействия спаму только начинают формулироваться отдельными авторами и их кооперациями [5].

В связи с этим, возникает ряд противоречий между результативностью защиты почтовых серверов от спам-сообщений и возможностями злоумышленников по компрометации средств защиты, а также между наличием необходимости управления ресурсными возможностями злоумышленника по организации массовой рассылки спам-сообщений и отсутствием технических решений по динамическому управлению параметрами почтовой транзакции со злоумышленником. На устранение указанных противоречий направлен способ проактивной защиты, предложеннный авторами статьи.

Известные подходы к защите почтовых серверов от нежелательных сообщений электронной почты обладают рядом существенных недостатков. К этим недостаткам можно отнести отсутствие учета возможностей злоумышленника по блокированию и перенаправлению пересылаемых ему средств лечения программы, рассылающей спам, а также отсутствие учета возможностей злоумышленника по спам-рассылке с поддельных адресов электронной почты, что повышает вероятность успешной реализации некоторых видов NDR-атак (Non Delivery Report) [6]. Отсутствие учета возможностей использования злоумышленником множества поч-

товых ящиков на территориально распределенных компьютерах, под управлением спам-ботов резко повышает его возможности, а также компрометация применяемых средств защиты за счет перенаправления спам-сообщений их отправителю вынуждает злоумышленника продолжать вредоносное воздействие и (или) изменять свою стратегию [7].

Разработанный способ проактивной защиты почтовых серверов от нежелательных сообщений электронной почты позволяет повысить результативность защиты за счет снижения возможности обнаружения злоумышленником факта использования средств защиты почтовых серверов, достигаемой имитацией канала связи с плохим качеством на различных этапах почтовой транзакции, посредством разбиения ответного отклика злоумышленнику на фрагменты и направления этих фрагментов через многочисленные малые интервалы времени задержки, направления ответного отклика злоумышленнику после множества промежуточных откликов через многочисленные малые интервалы времени задержки, а также направления злоумышленнику заведомо ложных сообщений о временной или постоянной невозможности продолжения почтовой транзакции.

Реализация предлагаемого способа защиты поясняется обобщенной структурно-логической последовательностью, представленной на рис. 1, где на начальном этапе формируют модуль хранения, модуль обнаружения и анализа, модуль проактивной защиты (блок 1). Модуль хранения предназначен для хранения в ячейках памяти разрешенных идентификаторов отправителей (клиентов) и получателей (серверов) сообщений электронной почты, предназначенных для идентификации несанкционированных клиентов, а также значений счетчиков количества подключений для каждого конкретного клиента и общего количества подключений клиентов к почтовому серверу, для предотвращения реализации атак отказа в обслуживании на почтовый сервер. Модуль обнаружения и анализа предназначен для сравнения количества сетевых подключений с их максимально допустимыми значениями, а также сравнения считанных идентификаторов отправителей и получателей сообщений электронной почты с санкционированными, и выдачи команды на блок проактивной защиты в случае их несовпадения. Модуль проактивной защиты предназначен для формирования управляющего воздействия, имитирующего канал связи с плохим качеством, значительно увеличивающего продолжительность времени почтовой транзакции с несанкционированным отправителем сообщений и расход его вычислительного ресурса, без блокирования или разрыва установленного сетевого соединения со злоумышленником.

На следующем этапе (блок 2), устанавливают сетевые соединения клиентов с почтовым сервером. Способы проактивной защиты клиент-серверных вычислительных сетей, реализуемые на транспортном уровне, на этапе установления сетевого соединения, предшествующие непосредственно обмену сообщениями на уровне приложений в процессе почтовой транзакции, которые также могут быть применимы для защиты почтовых серверов от нежелательных сообщений электронной почты, достаточно полно изложены в [8–10], в связи с чем, в настоящей статье не рассматриваются. Далее в модуле обнаружения и анализа (блок 3) сравнивают количество сетевых подключений с их максимально допустимыми значениями, для этого после установления сетевого соединения сервера с клиентом увеличивают значения количества подключений счетчиков на единицу и сравнивают их полученные значения с максимально заданными значениями. В случае выхода количества сетевых подключений к почтовому серверу из разрешенных пределов, по команде с модуля проактивной защиты, уменьшают значения счетчиков количества подключений клиента и общего количества подключений к почтовому серверу на единицу (блок 20) и разрывают сетевое соединение с клиентом (блок 21).

В ином случае, после обмена приветственными сообщениями сервера и клиента, получения (блок 4) от клиента команды EHLO (HELO), содержащей полное доменное имя клиента SMTP, если такое имя доступно, идентифицируют отправителей и получателей сообщений электронной почты (блок 5) в модуле обнаружения и анализа. Если идентифицирован санкционированный отправитель, обращающийся к санкционированному получателю сообщений электронной почты, то переходят к следующему этапу почтовой транзакции (блок 9). Иллюстрация процесса установления сетевого соединения

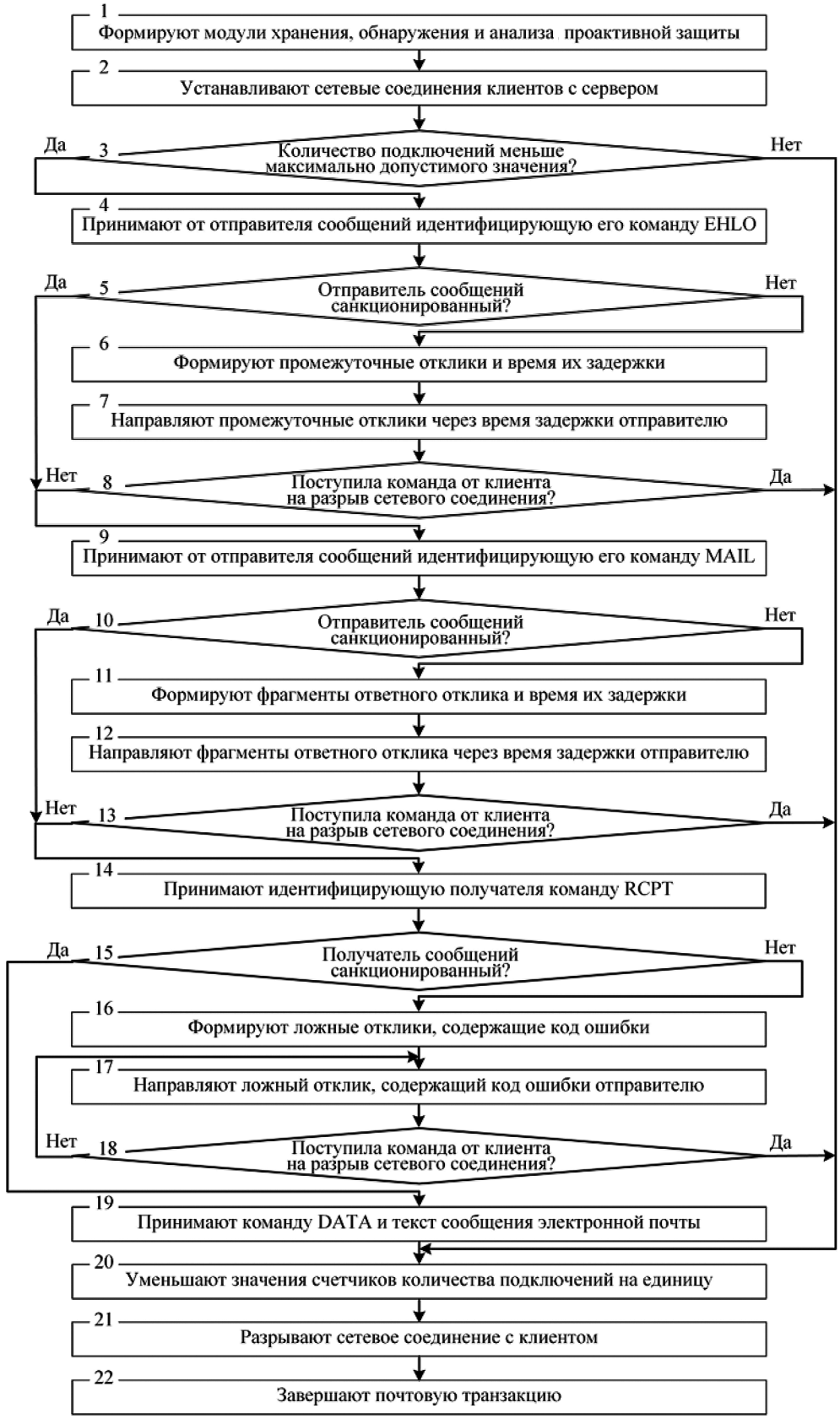

Рис. 1. Обобщенная структурно-логическая последовательность способа проактивной защиты почтовых серверов от нежелательных сообщений электронной почты

и почтовой транзакции SMTP представлена на рис. 2.

В ином случае, при несоответствии выделенных идентификаторов отправителя сообщений электронной почты санкционированным, по команде с модуля проактивной защиты, формируют (блок 6) множество промежуточных откликов и направляют (блок 7) каждый из них через предварительно сформированные значения времени задержки отправителю сообщений электронной почты перед ответным откликом. Многострочный отклик, в соответствии с [11], имеет следующий вид:

– 250 Первая строка;
– 250 Вторая строка;
– 250–234 Текст, начинающийся с числа;
– 250 Последняя строка.

Количество промежуточных откликов в соответствии со спецификацией протокола SMTP [11] не ограничено, а значения времени задержки перед отправкой каждого из промежуточных откликов в разработанном способе защиты выбираются исходя из анализа стратегий злоумышленника по преодолению средств проактивной защиты, основанных на установлении малых значений времени тайм-аута ожидания ответных откликов [12].

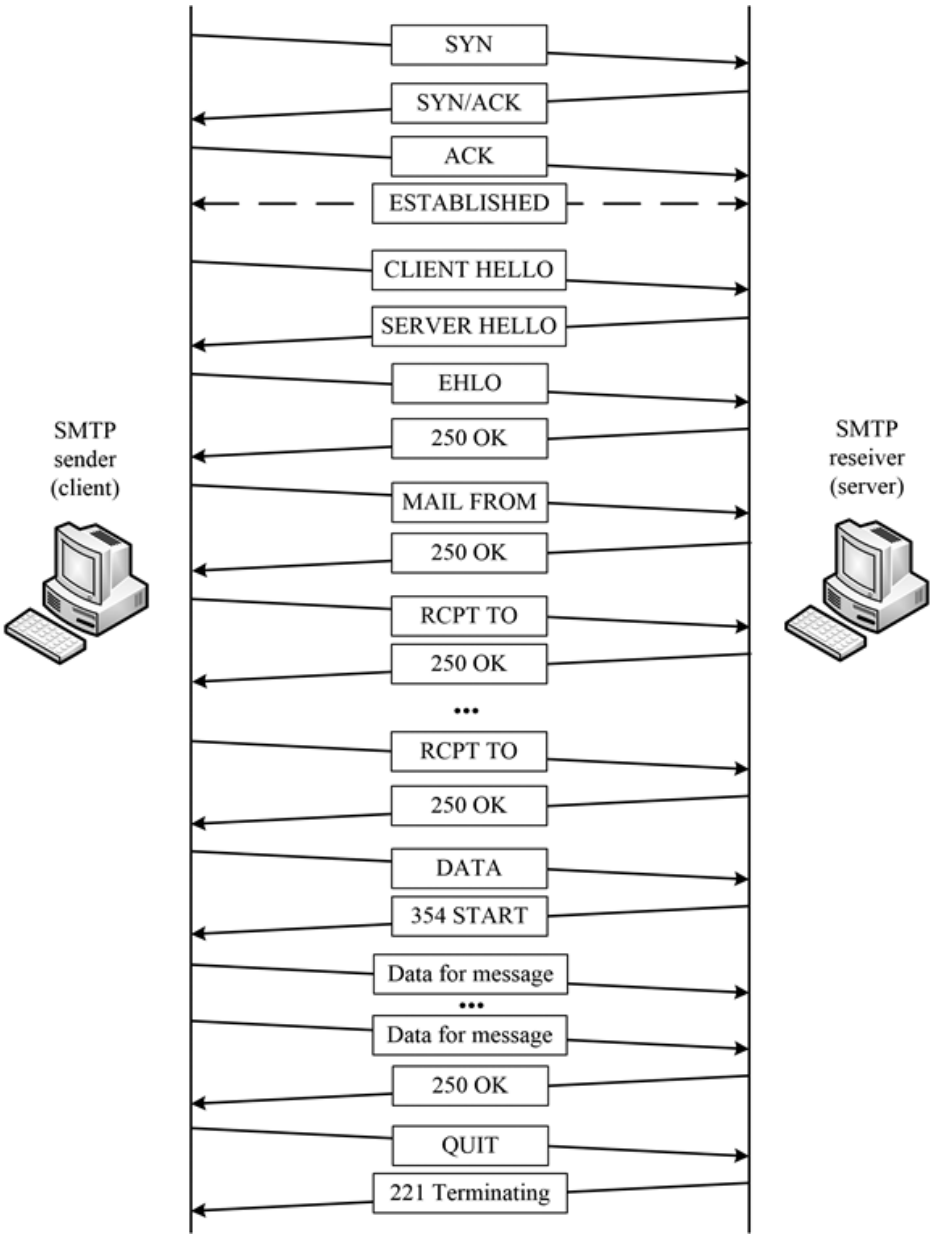

Рис. 2. Иллюстрация процесса установления сетевого соединения и почтовой транзакции SMTP

В соответствии с этим, значение времени задержки для каждого из промежуточных откликов несанкционированному отправителю сообщений электронной почты, перед отправкой ответного отклика, выбирают в пределах от 1 до 10 секунд, а количество промежуточных откликов, направляемых несанкционированному отправителю сообщений электронной почты, перед отправкой ответного отклика получателем выбирают в пределах от 1000 до 20000. Этим значительно увеличивают продолжительность времени диалога с отправителем спам-сообщений, вынуждая его отказаться от их массовой рассылки на атакуемый почтовый сервер из-за низкой интенсивности их получения, одновременно, исключая возможность одностороннего разрыва установленного сетевого соединения злоумышленником, за счет установления им малых значений времени тайм-аутов ожидания ответных откликов. Иллюстрация процесса направления множества промежуточных откликов перед ответным откликом злоумышленнику через заданные значения времени задержки представлена на рис. 3.

На рис. 3 блоками, направленными от клиента к серверу обозначены команды, например, EHLO, MAIL и т.д., а в обратном направлении отклики на них, содержащие трехзначный цифровой код, например, 250 и t — сформированные значения времени задержки промежуточных откликов отправителю сообщений электронной почты, где $t = 1, 2, \ldots, T$, а T — общее количество сформированных значений времени задержки промежуточных откликов отправителю сообщений. В процессе направления промежуточных откликов осуществляют проверку факта одностороннего разрыва соединения злоумышленником. Для этого после каждого отправленного промежуточного отклика сравнивают состояние установленного соединения с активным (блок 8), рис.1. В случае, если клиент (злоумышленник) направил команду на разрыв установленного соединения, то по команде с модуля проактивной защиты сетевое соединение разрывают (блок 21), значения счетчика клиента обнуляют, а счетчика общего количества подключений уменьшают на единицу (блок 20). В ином случае, если установленное соединение с клиентом по-прежнему активно (блок 8), после направления всех промежуточных откликов и ответного отклика переходят к следующему этапу почтовой транзакции (блок 9).

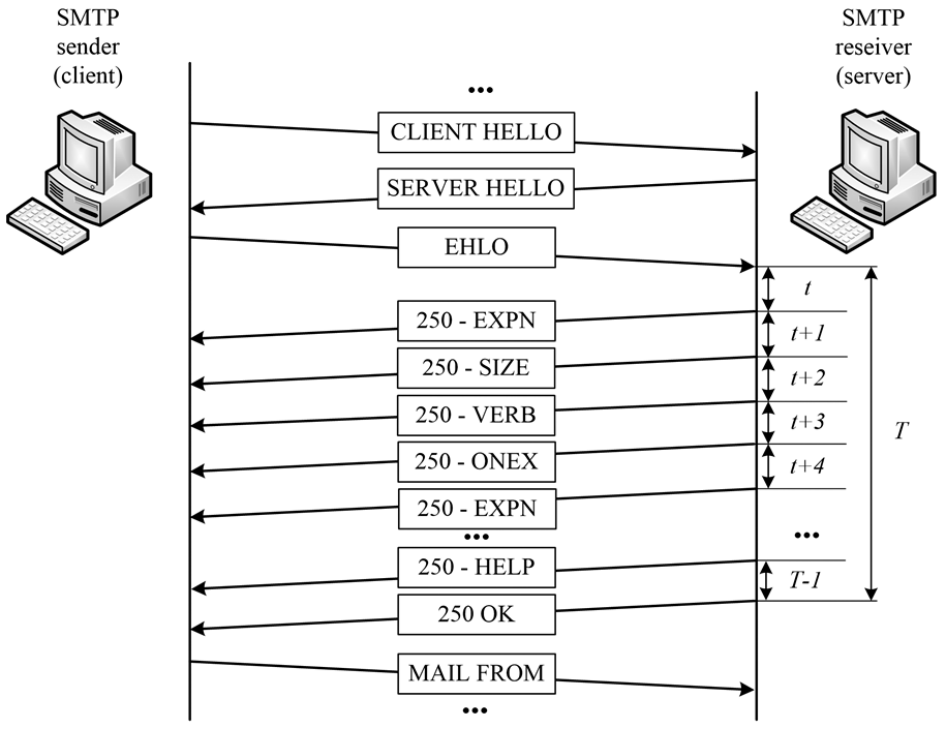

Рис. 3. Иллюстрация процесса почтовой транзакции в момент направления несанкционированному отправителю промежуточных откликов перед ответным откликом через заданные значения времени задержки

На следующем этапе процесса почтовой транзакции принимают очередную команду (команда MAIL), идентифицирующую отправителя сообщений электронной почты (блок 9). После выделения в модуле анализа идентификаторов отправителя сообщений (почтовый ящик отправителя, а также других параметров) сравнивают их с санкционированными отправителями (блок 10) и в случае их совпадения переходят к следующему этапу процесса почтовой транзакции RCTP (блок 14). В противном случае, по команде с модуля проактивной защиты, формируют множество фрагментов, на которые разделяют ответный отклик, а также множество значений времени задержки их отправления (блок 11). Значение времени задержки для каждого из фрагментов ответного отклика, направляемого несанкционированному отправителю сообщений электронной почты, выбирают в пределах от 1 до 15 секунд. Величину фрагментов, на которые разбивают ответный отклик несанкционированному отправителю сообщений электронной почты, выбирают в пределах от 1 до 3 байт. После этого, направляют несанкционированному отправителю сообщений электронной почты ответный отклик, разделенный на множество фрагментов через временные интервалы задержки, сформированные для каждого фрагмента (блок 12). Иллюстрация процесса направления множества фрагментов ответного отклика злоумышленнику через заданные значения времени задержки представлена на рис. 4.

На рис. 4 блоками, направленными от клиента к серверу, обозначены команды, например, MAIL, а в обратном направлении блоки, изображающие g фрагментов, на которые разделяют ответный отклик, направляемый отправителю сообщений, где $g = 1, 2, \ldots, G$, а G — общее количество сформированных фрагментов на которые разделяют ответный отклик и f сформированных значений времени задержки передачи фрагментов ответного отклика отправителю сообщений электронной почты, где $f = 1, 2, \ldots, F$, а F — общее количество сформированных значений времени задержки направления фрагментов ответного отклика отправителю сообщений электронной почты. В процессе направления фрагментов ответного отклика осуществляют проверку факта одностороннего разрыва соединения злоумышленником. Для этого, после каждого отправленного промежуточного отклика сравнива-

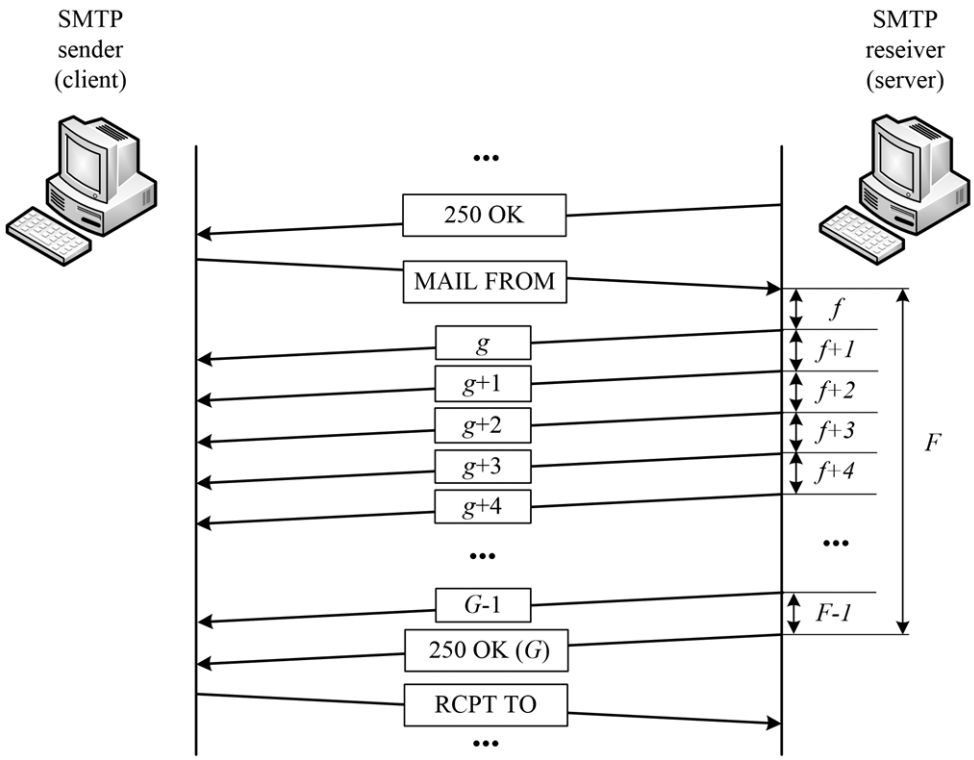

Рис. 4. Иллюстрация процесса почтовой транзакции в момент направления несанкционированному отправителю множества фрагментов ответного отклика через заданные значения времени задержки

ют состояние установленного соединения с активным (блок 13). В случае, если клиент (злоумышленник) после получения очередного фрагмента ответного отклика направил почтовому серверу команду на разрыв установленного соединения, то сетевое соединение с ним разрывают (блок 21), значение счетчика клиента обнуляют, а значение счетчика общего количества подключений уменьшают на единицу (блок 20). В ином случае, после направления всех фрагментов ответного отклика, если установленное соединения с клиентом по-прежнему активно (блок 13), переходят к следующему этапу почтовой транзакции.

На следующем этапе процесса почтовой транзакции принимают от отправителя сообщений очередную команду (команда RCTP), идентифицирующую получателя сообщений электронной почты (блок 14). После выделения в модуле анализа идентификаторов получателя сообщений (почтовый ящик получателя) сравнивают их с санкционированными получателями (блок 15) и в случае их совпадения переходят к следующему этапу процесса почтовой транзакции — передаче текста сообщения электронной почты (блок 19). После получения полного текста сообщения электронной почты сетевое соединение с санкционированным отправителем сообщений электронной почты завершают, для чего разрывают установленное сетевое соединение (блок 21), значение счетчика подключений клиента обнуляют, а значение счетчика общего количества подключений уменьшают на единицу (блок 20), после чего завершают почтовую транзакцию (блок 22). В ином случае, по команде с модуля проактивной защиты формируют (блок 16) U ложных ответных откликов на команды отправителя сообщений, содержащих коды ошибки в соответствии со спецификацией протокола SMTP, перечень которых представлен в [11]. Для каждого ложного ответного отклика несанкционированному отправителю сообщений электронной почты значение кода ошибки выбирают случайным образом из стандартных кодов ошибки протокола SMTP. После этого направляют несанкционированному отправителю сообщений электронной почты ложный ответный отклик, содержащий код ошибки (блок 17). Иллюстрация процесса направления несанкционированному отправителю ложного ответного отклика, содержащего код ошибки представлена на рис. 5.

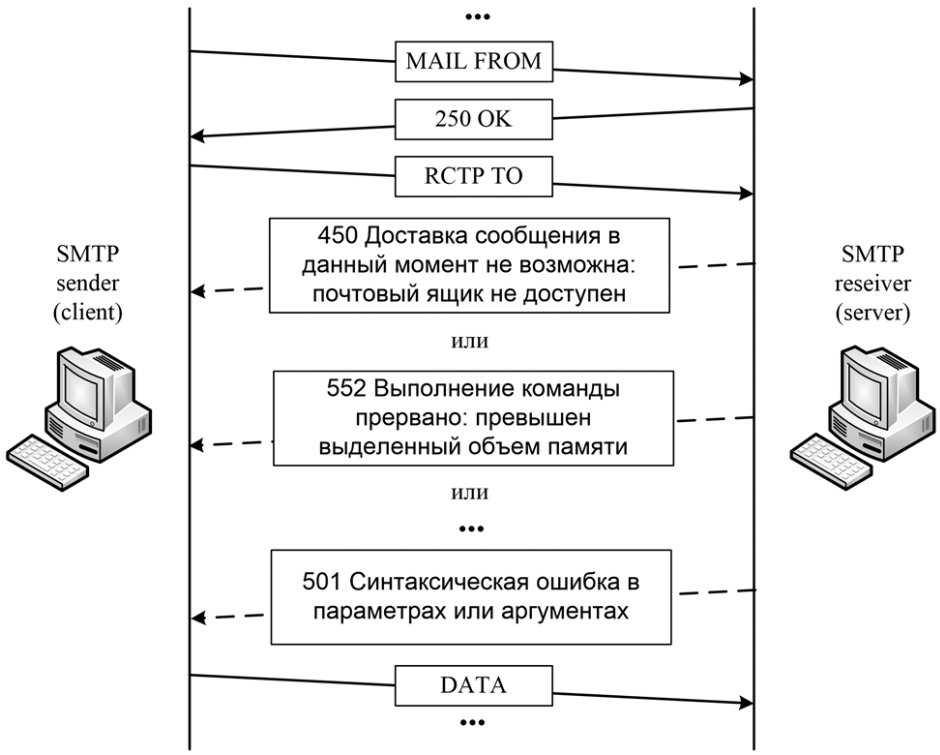

Рис. 5. Иллюстрация процесса почтовой транзакции в момент направления несанкционированному отправителю ложного ответного отклика, содержащего код ошибки

На рис. 5 блоками, направленными от клиента к серверу, обозначены команды, например, RCTP, а в обратном направлении блоки, изображающие ложные ответные отклики, содержащие код ошибки. В случае, если клиент (злоумышленник) после получения ложного ответного отклика, содержащего код ошибки, направил почтовому серверу команду на разрыв установленного соединения, то сетевое соединение с ним разрывают (блок 21), значение счетчика клиента обнуляют, а значение счетчика общего количества подключений уменьшают на единицу (блок 20). В ином случае, после получения от злоумышленника очередной команды, реагирующей на отклик с кодом ошибки, ему повторно направляют ложный ответный отклик (блок 17), содержащего код ошибки, и так до тех пор, пока несанкционированный клиент не разорвет соединение.

Выводы

Таким образом, в разработанном способе проактивной защиты почтовых серверов от нежелательных сообщений электронной почты обеспечивается повышение результативности защиты за счет снижения возможности обнаружения злоумышленником факта использования средств защиты, достигаемой имитацией канала связи с плохим качеством на различных этапах почтовой транзакции, за счет направления ответного отклика злоумышленнику после множества промежуточных откликов, направляемых через многочисленные малые интервалы времени задержки, разбиения ответного отклика злоумышленнику на фрагменты и направления этих фрагментов через многочисленные малые интервалы времени задержки, а также направления злоумышленнику заведомо ложных ответных откликов, содержащих код ошибки, соответствующий временной или постоянной невозможности продолжения почтовой транзакции.

Литература

1. Патент РФ № 2013125976/08, 2013.06.06. Смирнов Е.П., Бахмутов А.В., Лосева Д.В., Швырков Д.А. Система и способ определения рейтинга электронных сообщений для борьбы со спамом // Патент России № 2541123. 2015. Бюл. № 4.

2. Ковалев С.С., Шишаев М.Г. Современные методы защиты от нежелательных почтовых рассылок // Труды Кольского научного центра РАН. 2011. № 7. С. 100–111.

3. Сайты «Единой России» подверглись масштабной DDoS-атаке [Электронный ресурс] // Interfax: сайт. — URL: https://www.interfax.ru/russia/609414 (дата обращения 26.05.2020).

4. Соколовский С.П., Орехов Д.Н. Концептуализация проблемы проактивной защиты интегрированных информационных систем // Научные чтения имени профессора Н.Е. Жуковского: сб. научн. стат. VIII Междунар. науч. метод. конф. (Краснодар, 20–21 декабря 2017 г.). — Краснодар. 2018. С. 47–52.

5. Патент РФ № 2006133671/09, 2006.09.20. Борисов М.А., Кожевников Д.А., Максимов Р.В., Осадчий А.И., Павловский А.В., Стародубцев Г.Ю., Худайназаров Ю.К. Способ защиты локальной вычислительной сети при передаче сообщений электронной почты посредством глобальной информационной сети // Патент России № 2318296. 2008. Бюл. № 6.

6. Патент РФ № 2010130872/08, 23.07.2010. Рыбалко Р.В. Система анализа протоколов передачи данных с целью нейтрализации программ, рассылающих спам // Патент России № 101234. 2011.

7. Патент РФ № 2011120197/08, 19.05.2011. Небольсин В.А. Предотвращение несанкционированной массовой рассылки электронной почты // Патент России № 2472308. 2011. Бюл. № 1.

8. Максимов Р.В., Орехов Д.Н., Соколовский С.П. Модель и алгоритм функционирования клиент-серверной информационной системы в условиях сетевой разведки // Системы управления, связи и безопасности. 2019. № 4. С. 50–99.

9. Maximov R.V. Hiding computer network proactive security tools unmasking features. R.V. Maximov, S.P. Sokolovsky, L.A. Gavrilov // Selected Papers of the VIII All-Russian Conference with International Participation «Secure Information Technologies». — Moscow: Bauman Moscow Technical University. 2017. P. 88–92.

10. Патент РФ № 2018128075, 31.07.2018. Максимов Р.В., Орехов Д.Н., Соколовский С.П., Барабанов В.В., Ефремов А.А., Ворончихин И.С. Способ защиты вычислительных сетей // Патент России № 2696330. 2019. Бюл. № 22.

11. Request for comments 5321 [Электронный ресурс]. Режим доступа: https://tools.ietf.org/html/rfc5321 (дата обращения 03.12.2020).

12. Patent USA № 11/276,932. Wilbert de Graaf, Chandresh K.Jein. Response delay management using connection information // Патент США № 2007/0220600. 2007.

References

1. Patent RF № 2013125976/08, 2013.06.06. Smornov E.P., Bahmutov A.V., Loseva D.V., Shvyrkov D.A. System and method for determining the rating of electronic messages to combat spam. № 4. 2015.

2. Kovalev S.S., Shishaev M.G. Modern methods of protection against unwanted mailings. Proceedings of the Kola Scientific Center of the Russian Academy of Sciences. № 7. 2011. P. 100–111.

3. United Russia websites were subjected to a large-scale DDoS attack: URL: https://www.interfax.ru/russia/609414 (date of access 26.05.2020).

4. Sokolovsky S.P., Orehov D.N. Conceptualization of the problem of proactive protection of integrated information systems Scientific readings named after Professor N.E. Zhukovsky: sat. stat. VIII International Scientific Journal. method. conf. 2018. P. 47–52.

5. Patent RF № 2006133671/09, 2006.09.20. Borisov M.A., Kozhevnikov D.A., Maximov D.A., Osadchiy A.I., Pavlovskiy A.V., Starodubtsev G.Yu., Hudaynazarov Yu.K. Method for protecting a local area network when transmitting e-mail messages via a global information network // Russian Patent № 2318296. № 6. 2008.

6. Patent RF № 2010130872/08, 23.07.2010. Rybalko R.V. System for analyzing data transmission protocols in order to neutralize programs that send spam // Russian Patent № 101234. 2011.

7. Patent RF № 2011120197/08, 19.05.2011. Nebol'sin V.A. Preventing unauthorized mass email distribution // Russian Patent № 2472308. № 1. 2011.

8. Maximov R.V., Orehov D.N., Sokolovsky S.P., Model and algorithm of functioning of the client-server information system in the conditions of network intelligence. Control, communication and security systems. № 4. 2019. P. 50–99.

9. Maximov R.V. Hiding computer network proactive security tools unmasking features. R.V. Maximov, S.P. Sokolovsky, L.A. Gavrilov // Selected Papers of the VIII All-Russian Conference with International Participation «Secure Information Technologies». — Moscow: Bauman Moscow Technical University. 2017. P. 88–92.

10. Patent RF № 2018128075, 31.07.2018. Maxumov R.V., Orehov D.N., Sokolovsky S.P., Barabanov V.V., Efremov A.A.,Voronchihin I.S. Method for protecting computer networks // Russian Patent № 2696330. № 22. 2019.

11. Request for comments 5321: https://tools.ietf.org/html/rfc5321.

12. Patent USA № 11/276,932. Wilbert de Graaf, Chandresh K.Jein. Response delay management using connection information // Patent USA № 2007/0220600. 2007.