УДК 004.738.5

Модель функционирования и алгоритм проактивной защиты сервиса электронной почты от сетевой разведки

Горбачев А. А., Соколовский С. П., Усатиков С. В.

Постановка задачи: *существующие угрозы информационной безопасности сервиса электронной почты обусловлены реактивностью применяемых средств защиты, анализирующих содержимое электронных сообщений, протокольными возможностями SMTP и особенностями воздействия средств сетевой разведки. Инерционные свойства применяемых средств защиты в полной мере не обеспечивают защищенность сервиса электронной почты от сетевой разведки и компьютерных атак.* ***Целью работы*** *является разработка модели и алгоритма, позволяющих обеспечить оперативное обслуживание максимального количества запросов санкционированных клиентов сервиса электронной почты с одновременным снижением качества обслуживания запросов от средств сетевой разведки посредством управления процессом передачи сообщений.* ***Используемые методы****: решение задачи управления процессом функционирования сервиса электронной почты в условиях сетевой разведки на различных этапах почтовой транзакции за счет управления ресурсными возможностями средств сетевой разведки на прикладном уровне, заключается в представлении процесса их взаимодействия в виде марковского случайного процесса с дискретными состояниями и непрерывным временем, использовании методов динамического программирования, а также численных методов.* ***Новизна:*** *элементами новизны представленной модели является применение математического аппарата однородных цепей Маркова с непрерывным временем с учетом свойств асимптотической устойчивости и робастности, для обоснования выбора оптимальных режимов передачи почтовых сообщений на различных этапах почтовой транзакции. Новизна представленного алгоритма проактивной защиты сервиса электронной почты от сетевой разведки заключается в применении модели функционирования сервиса электронной почты, основанной на использовании математического аппарата однородных цепей Маркова с непрерывным временем, для управления ресурсными возможностями средств разведки при передаче почтовых сообщений на различных этапах почтовой транзакции.* ***Результат****: проведенные расчеты свидетельствуют о повышении доступности информационных ресурсов сервиса электронной почты клиентам, за счет управления процессом передачи сообщений электронной почты. Представленный алгоритм позволяет повысить результативность защиты за счет снижения возможностей злоумышленника по обнаружению факта использования средств защиты и идентификации их характеристик, а также за счет управления ресурсными возможностями средств разведки на различных этапах почтовой транзакции путем имитации канала связи с плохим качеством.* ***Практическая значимость****: заключается в нахождении вероятностно-временных характеристик, описывающих процесс функционирования сервиса электронной почты на различных этапах почтовой транзакции. Практическая значимость представленного алгоритма заключается в решении задачи оптимального управления процессом передачи сообщений электронной почты, обеспечивающей управление вычислительным и временным ресурсом средств сетевой разведки, а также снижение возможностей компрометации средств защиты и идентификации их характеристик.*

Ключевые слова: *сетевая разведка, сервис электронной почты, проактивная защита, устойчивость, случайный процесс, отказ в обслуживании.*

Актуальность

Существование глобальных компьютерных сетей неразрывно связано с использованием сервиса электронной почты, посредством которого осуществля-

Библиографическая ссылка на статью:
Горбачев А. А., Соколовский С. П., Усатиков С. В. Модель функционирования и алгоритм проактивной защиты сервиса электронной почты от сетевой разведки // Системы управления, связи и безопасности. 2021. № 3. С. 60-109. DOI: 10.24412/2410-9916-2021-3-60-109

Reference for citation:
Gorbachev A. A., Sokolovsky S. P., Usatikov S. V. Functioning model and algorithm of email service proactive protection from network intelligence. *Systems of Control, Communication and Security*, 2021, no. 3, pp. 60-109 (in Russian). DOI: 10.24412/2410-9916-2021-3-60-109

ется передача значительной части важной информации между потребителями. В связи с возрастанием популярности сервиса электронной почты значительно активизировалась деятельность злоумышленников по проведению массовых и целевых атак, результатом которой является массовая рассылка почтовых сообщений рекламного характера, фишинг, внедрение вредоносного программного обеспечения, кража интеллектуальной собственности, мошенничество, нарушение доступности сервиса электронной почты. При этом наиболее важным из этапов подготовки компьютерных атак является сетевая разведка, которая проводится с целью добывания информации о составе, структуре, алгоритмах функционирования, местоположении, принадлежности элементов системы электронной почты, анализа хранимых, обрабатываемых данных и осуществляется для поиска потенциальных целей, их уязвимостей и направлений сосредоточения усилий при реализации компьютерных атак или иных злонамеренных воздействий [1-6].

Основными видами сетевой (компьютерной) разведки являются: добывающая, обрабатывающая, активная разведки [7]. Добывающая сетевая разведка может быть реализована в формах анализа сетевого трафика (перехват трафика), сетевого сканирования (сетевой анализ) и непосредственного взаимодействия (установление сетевого соединения, проникновение) с объектом разведки [8]. Анализ сетевого трафика осуществляется с целью определения активности и объемов передаваемой информации, извлечения передаваемых сведений, в частности, паролей, идентификаторов и другой ценной информации. Сетевое сканирование производится с целью определения потенциальных точек проникновения в целевую информационную систему, в частности, осуществляется оценка размерности целевой подсети, поиск активных портов, сбор метаданных, идентификация аппаратного и программного обеспечения средств вычислительной техники и т.д. Непосредственное взаимодействие при ведении сетевой разведки осуществляется с целью сбора информации о применяемом программном обеспечении, средствах защиты, поиске возможных уязвимостей, внедрении вредоносного программного обеспечения [1, 7-9].

Анализ публикаций в области противодействия сетевой разведки [2-6, 8-29] показал, что в настоящее время ведутся активные разработки как по наращиванию средств защиты информационных систем от реализации рассматриваемых угроз, так и средств реализации сетевой разведки и компьютерных атак.

Так, применительно к объекту исследования, противодействие анализу трафика с целью обеспечения конфиденциальности и целостности передаваемой информации между клиентами и серверами сервиса электронной почты осуществляется за счет использования средств криптографической защиты на основе стандартов Secure/Multipurpose Internet Mail Extensions (S/MIME), и Pretty Good Privacy (PGP). С другой стороны, злоумышленниками постоянно совершенствуются способы криптоанализа зашифрованного трафика [30].

Снижение эффективности сетевого сканирования осуществляется за счет использования средств маскирования структуры сети посредством динамического изменения структурно-функциональных характеристик защищаемой сети, использованием ложных информационных объектов, сетевых «приманок»

(honeypots). Тем не менее, развиваются методы и средства идентификации демаскирующих признаков применяемых средств защиты [3-6, 16, 19, 21, 24, 25].

Основной формой защиты от проведения непосредственной сетевой разведки сервиса электронной почты является проверка содержимого электронных сообщений на предмет спама и вредоносного программного обеспечения средствами фильтрации, антивирусной защиты, аутентификации [31-34]. Однако данные средства являются вычислительно интенсивными, требуют постоянной актуализации и технической поддержки. Перспективными средствами защиты от проведения непосредственной сетевой разведки и компьютерных атак, дополняющими вышеуказанные, являются так называемые сетевые «ловушки» (network tarpits). Сущность сетевых «ловушек» заключается в использовании различных механизмов замедления информационного обмена между злоумышленником и целевой системой, имитирующих загруженные каналы связи. К примеру, некоторые ловушки используют механизмы управления потоком данных транспортного уровня (варьирование размера окна «window») [2, 35-37].

Применительно к сервису электронной почты, использование сетевых «ловушек» позволит снизить эффективность проведения непосредственной сетевой разведки и компьютерных атак типа «отказ в обслуживании» за счет исчерпания временного и вычислительного ресурса злоумышленника посредством имитации канала связи низкого качества [39-41].

Математическая модель функционирования сервиса электронной почты позволяет произвести количественную оценку эффективности предлагаемых средств защиты. В настоящее время разработан обширный теоретико-методологический аппарат формализованного представления функционирования информационных систем различного назначения [42-51].

Математический аппарат случайных процессов, в частности, марковских процессов с дискретными состояниями и непрерывным временем, широко распространен при формализации информационно-телекоммуникационных систем. Например, указанный метод применялся для моделирования процесса мониторинга безопасности информации в информационно-телекоммуникационных системах [45], функционирования распределенных информационных систем при использовании маскированных каналов связи [47], средств защиты автоматизированных систем специального назначения [48], конфликта автоматизированных систем обработки информации и управления с системой деструктивных воздействий нарушителя [46], совместного применения средств радиоэлектронной борьбы и огневого поражения в интересах повышения эффективности борьбы за превосходство в управлении [49], узла доступа VPN как объекта сетевой и потоковой компьютерной разведок и DDOS-атак [50], процессов реализации сетевых атак типа «отказ в обслуживании» [51].

В рассмотренных работах при использовании математического аппарата марковских процессов не прорабатывались вопросы управления процессом информационного обмена в системах передачи электронной почты с использованием методов динамического программирования, не учитывалась оценка робастности и асимптотической устойчивости модели к погрешности исходных данных.

Существующие алгоритмы по реализации сетевых «ловушек» для защиты сервиса электронной почты [52-55] обладают рядом недостатков: относительно низкая результативность защиты, обусловленная отсутствием учета возможностей злоумышленника по блокированию и перенаправлению пересылаемых ему средств лечения программы, рассылающей спам; отсутствие учета возможности злоумышленника по спам-рассылке с поддельных адресов электронной почты, что повышает вероятность успешной реализации некоторых видов NDR-атак (Non Delivery Report), основанных на возврате отправителю почтовых сообщений, получателя которых не существует; возможность компрометации применяемых средств защиты, что вынуждает злоумышленника продолжать вредоносное воздействие и (или) изменять его стратегию.

Актуальность исследования обусловлена учетом указанных недостатков при разработке модели функционирования и алгоритма проактивной защиты сервиса электронной почты от сетевой разведки.

Анализ объекта исследования

Сервис электронной почты представляет собой инфокоммуникационную систему, включающую совокупность клиентов, серверов и коммуникационного оборудования, соединенного физическими линиями связи. Он имеет клиент-серверную архитектуру, обеспечивающую отложенную передачу электронных сообщений. Функционирование сервиса осуществляется в системе стека сетевых протоколов TCP/IP (Transmission Control Protocol/Internet Protocol).

Трансляция электронных почтовых сообщений между промежуточными серверами осуществляется с использованием простого протокола передачи почты Simple Mail Transfer Protocol (SMTP). После организации коммуникационного канала и согласования параметров клиент обычно инициирует почтовую транзакцию, состоящую из последовательности команд, задающих отправителя и получателя (получателей) сообщения электронной почты, а также передачу содержимого письма (включая все заголовки и прочие структуры) [56]. После обмена приветственными сообщениями сервера и клиента, а именно получения от клиента команды EHLO (HELO), содержащей полное доменное имя клиента SMTP, если такое имя доступно, происходит идентификация отправителей сообщений электронной почты. Далее начинается почтовая транзакция, включающая три этапа. Началом транзакции служит команда MAIL, содержащая идентификаторы отправителя (название почтового ящика отправителя, количество подключений). После этого следует одна или несколько команд RCPT, указывающих получателей сообщения. Последний этап транзакции начинается командой DATA, которая инициирует передачу почтовых данных и завершается индикатором end of mail, который также подтверждает транзакцию. Каждый объект электронной почты состоит из конверта (envelope) и содержимого. Конверт SMTP передается как серия протокольных элементов SMTP. Конверт содержит адрес отправителя (по которому должны возвращаться отчеты об ошибках) и один или более адресов получателей, а также дополнительную информацию для расширений протокола.

Команды SMTP и данные сообщений передаются от отправителя к получателю через коммуникационный канал в форме строк. Получатель отвечает откликом на каждую из полученных команд, который содержит трехзначный номер (передается как три числовых символа), за которым обычно следует строка текста и представляет собой подтверждение (или отказ, содержащий сообщение с кодом временной или постоянной ошибки), передаваемое в форме строк от получателя к отправителю через коммуникационный канал. Диалог между отправителем и получателем осуществляется поэтапно (команда – отклик – команда …), как представлено на рис. 1.

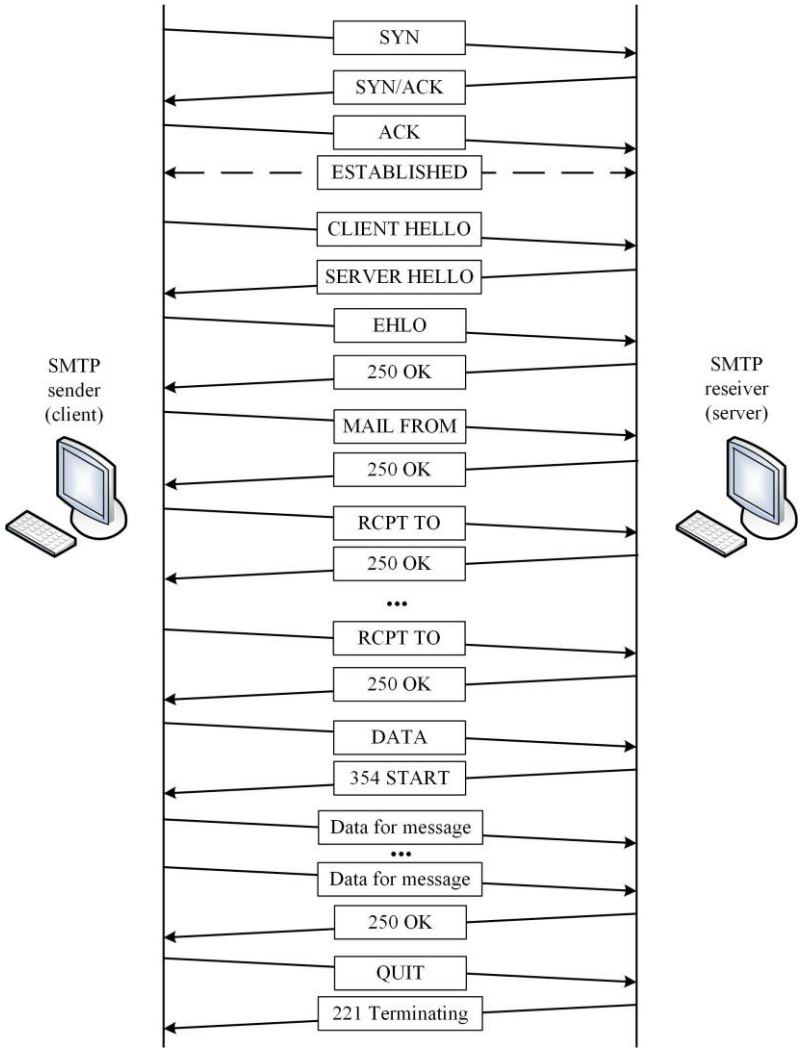


Рис. 1. Иллюстрация процесса установления сетевого соединения и почтовой транзакции SMTP

В связи с этим управление процессом передачи сообщений электронной почты может осуществляться с применением следующих механизмов:

– направлением сервером на поступившие от клиента команды многочисленных промежуточных ответных откликов через изменяемые интервалы времени;

– направлением сервером на поступившие от клиента команды фрагментированного ответного отклика, фрагменты которого также направляются через изменяемые интервалы времени;
– направлением сервером на поступившие от клиента команды откликов, содержащих код временной или постоянной ошибки.

В первом случае, многострочный ответный отклик может содержать несколько строк, количество которых не ограничено, но в таких случаях текст должен маркироваться так, чтобы отправитель мог узнать о завершении текста. Это требует использования для многострочных откликов специального формата, регламентирующего, чтобы каждая строка (кроме последней) начиналась кодом отклика, после которого следует дефис (–), а далее текст.

В последней строке вместо дефиса используется пробел, после которого может следовать текст. В многострочных откликах коды в каждой строке должны совпадать. В некоторых случаях важные для отправителя данные передаются в тексте отклика (рис. 2).

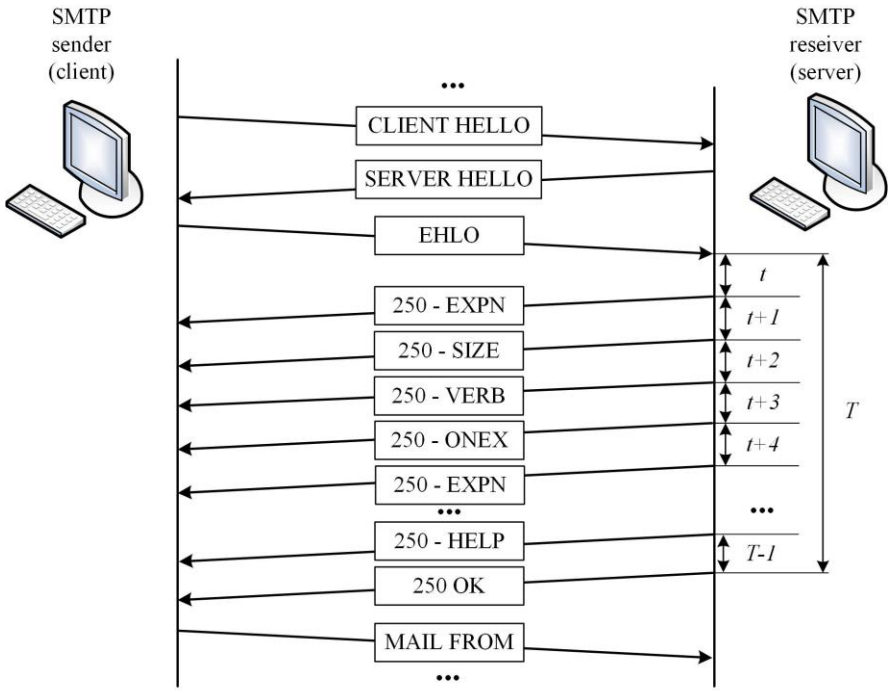


Рис. 2. Иллюстрация фрагмента почтовой транзакции в момент направления сервером на поступившие от клиента команды множества промежуточных откликов через заданные значения времени их задержки

Ниже приведен пример многострочного отклика:

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

После завершения передачи сообщения отправитель может запросить разрыв соединения или инициировать следующую почтовую транзакцию.

Во втором случае, ответный отклик на команду клиента разбивается на множество фрагментов, которые направляются клиенту через изменяемые интервалы времени задержки их отправления. Величину фрагментов, на которые разбивают ответный отклик несанкционированному отправителю сообщений электронной почты, выбирают в пределах нескольких байт, что определяется размером ответного отклика. Иллюстрация процесса направления множества фрагментов ответного отклика сервером на поступившие от клиента команды через заданные значения времени задержки представлена на рис. 3.

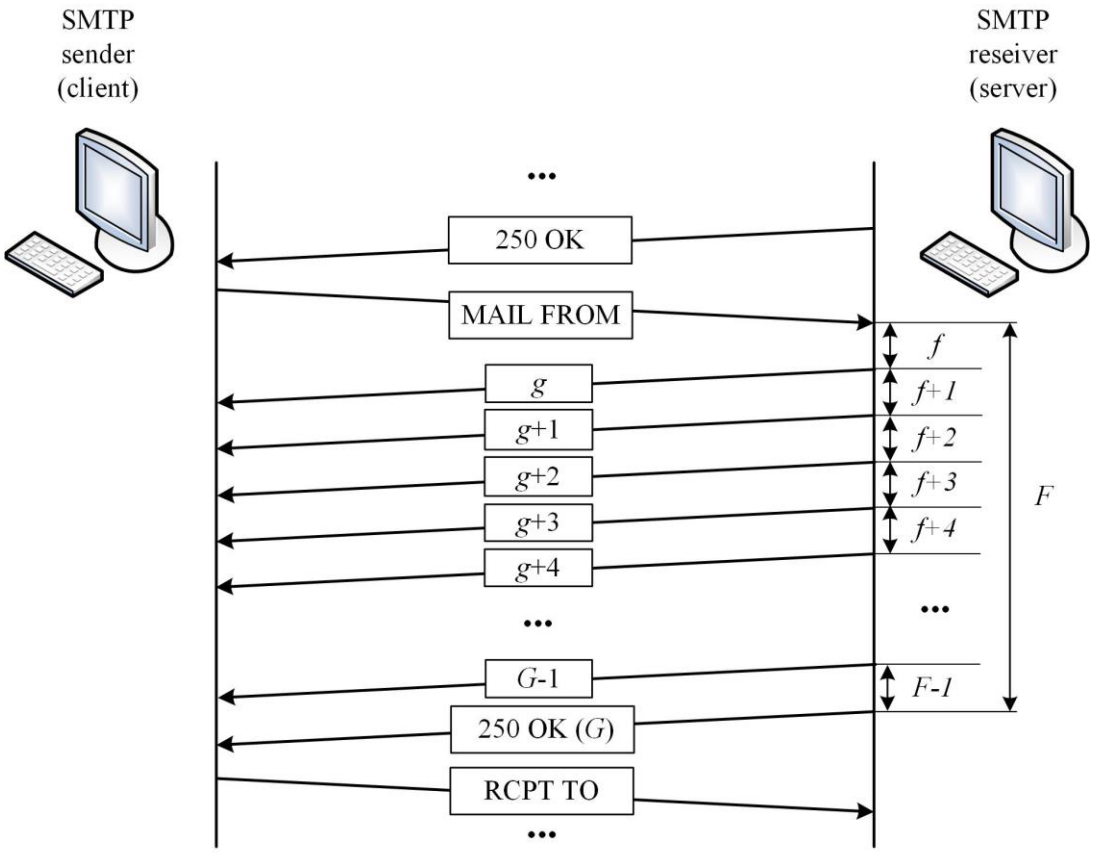


Рис. 3. Иллюстрация фрагмента почтовой транзакции в момент направления сервером на поступившие от клиента команды множества фрагментов ответного отклика через заданные значения времени их задержки

В третьем случае, формируется множество ложных ответных откликов на команды отправителя сообщений (рис. 4), содержащих коды ошибки в соответствии со спецификацией протокола SMTP.

Таким образом, в процессе функционирования сервиса электронной почты на каждом из этапов почтовой транзакции инициатор соединения (клиент) формирует команды, которые направляет серверу, обрабатывающему их в условиях ограниченного вычислительного ресурса. Ограниченность вычислительного ресурса выражается в том, что сервер способен обработать ограниченное количество команд за единицу времени без переполнения буфера обмена или же снижения качества обслуживания заявок.

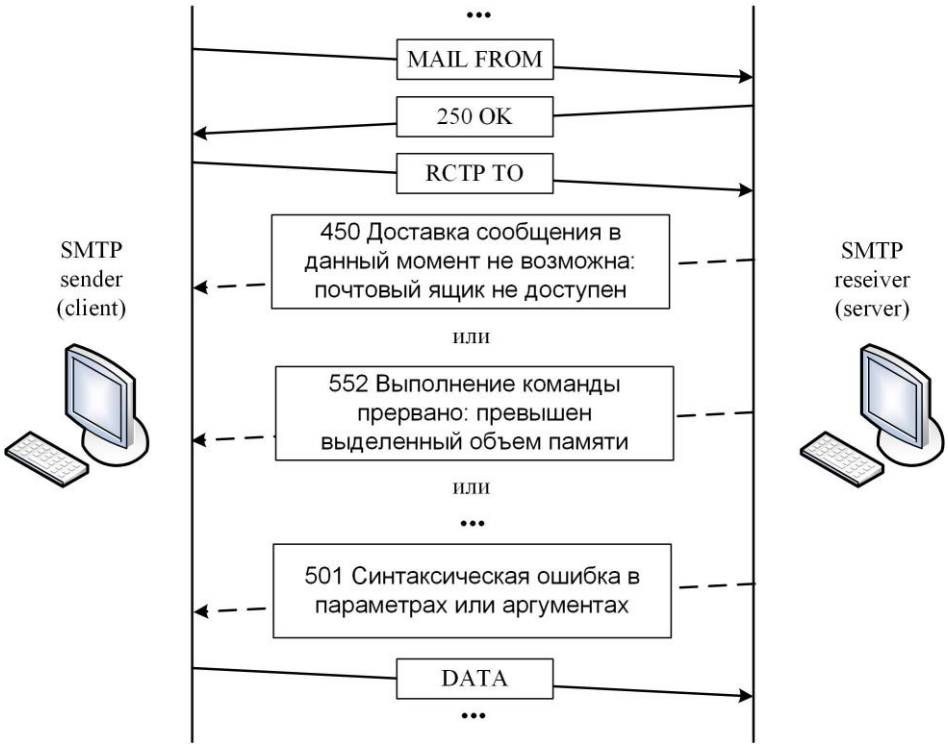


Рис. 4. Иллюстрация фрагмента почтовой транзакции в момент направления сервером на поступившие от клиента команды ложного ответного отклика, содержащего код ошибки

Задачей сервера является своевременное обслуживание максимального количества команд и передача сообщений электронной почты от клиентов, что достигается исключением разрыва соединений или блокирования команд от клиентов после превышения допустимого количества соединений клиентов и сервера электронной почты за счет применения вышеприведенных механизмов управления процессом передачи сообщений электронной почты.

Модель функционирования сервиса электронной почты

Рассмотрим сервис электронной почты, имеющий клиент-серверную архитектуру, в котором взаимодействие клиента и сервера на прикладном уровне осуществляется посредством протокола SMTP или его расширения.

При функционировании сервиса электронной почты возникают объективные ограничения на производительность сервиса в целом, так и его элементов. При возникновении клиентов, с потребностями в больших количествах параллельных подключений ситуация усугубляется. В этой связи в таких сервисах электронной почты используют диспетчеризацию запросов клиентов к серверу. В случае необходимости обработку запросов клиентов, превышающих установленные ограничения по количеству подключений, приостанавливают, не разрывая с ними соединения. Это рационально, так как повторное установление соединения вызывает повтор технологических операций, связанных с ним, что это отрицательно влияет на производительность сервиса электронной почты.

В данной работе оценка эффективности функционирования сервиса электронной почты осуществляется посредством расчета количественных вероятностно-временных характеристик.

Исходя из предположений, что команды (заявки) клиентов, направляемые почтовому серверу, имеют случайный характер, являются взаимно независимыми, и каждая команда клиента в некотором смысле имеет малое влияние на суммарный поток команд, в соответствии с теоремой Гнеденко о сходимости сумм независимых и бесконечно малых случайных процессов к процессу Пуассона [57], авторами вводятся допущения об однородности, стационарности и отсутствии последействия потоков событий, представляющих собой моменты времени принятия команд от клиентов и отправки откликов почтовым сервером.

Вместе с тем, моделируемая система в ходе функционирования может находиться в одном из состояний, характеризующимся этапом почтовой транзакции, смена которого осуществляется через некоторое случайное время мгновенно, в связи с появлением события (команды клиента или отклика сервера), инициирующего переход системы в другое состояние.

Вводимые допущения обусловливает целесообразность использования математического аппарата случайных процессов. В рамках данной работы используются однородные цепи Маркова с непрерывным временем (марковские процессы с дискретными состояниями и непрерывным временем). Однородность марковского процесса обусловлена стационарностью случайного процесса в широком смысле слова, характеризующаяся независимостью математического ожидания (интенсивностей простейших потоков событий), дисперсии случайного процесса от параметра (времени) и зависимостью корреляционной функции процесса только от величины промежутка времени [58].

Исходными данными, при определении цепей Маркова с непрерывным временем являются:

- пространство фазовых состояний системы L (конечное множество несовместных событий, описывающих существенные свойства системы и изменяющиеся скачкообразно) и возможные траектории перехода системы из состояния в состояние (характеризуются ориентированным графом состояний моделируемой системы). Рассматриваемая система L может принимать конечное число состояний $\{S_1, S_2, \ldots, S_9\}$ (таблица 1);
- распределение вероятностей пребывания системы в состояниях в начальный момент времени $\{p_1(0), p_2(0), \ldots, p_9(0)\}$;
- интенсивности потоков событий $\{\lambda_{11}, \lambda_{12}, \ldots, \lambda_{ij}\}$ – факторов, вызывающих переход системы из состояния в состояние (таблица 2).

Таблица 1 – Пространство фазовых состояний сервиса электронной почты в процессе почтовой транзакции

Переменная	Состояния
S_1	Состояние, в котором клиент находится в состоянии простоя, не принимает и не передает сообщения электронной почты
S_2	Состояние инициализации сетевого соединения клиента с почтовым серве-

Переменная	Состояния
	ром на транспортном уровне, проверка счетчика общего количества подключений клиентов к серверу
S_3	Состояние инициализации почтовой транзакции, получение почтовым сервером от клиента команды EHLO проверка идентификаторов отправителя сообщений электронной почты (доменное имя)
S_4	Состояние, в котором клиент (при превышении допустимого значения общего количества подключений клиентов к серверу) перед ответным откликом от почтового сервера, принимает от сервера множество промежуточных откликов, направляемых через изменяемые интервалы времени их задержки
S_5	Состояние очередного этапа процесса почтовой транзакции, получение почтовым сервером от клиента команды MAIL, проверка идентификаторов отправителя сообщений электронной почты (название почтового ящика отправителя и количество получателей сообщений электронной почты)
S_6	Состояние, в котором клиент после отправления команды MAIL (при превышении допустимого количества указанных получателей сообщений электронной почты или превышения количества попыток отправки сообщений на несуществующие адреса электронной почты) перед ответным откликом, принимает от почтового сервера ответные отклики, содержащие код ошибки
S_7	Состояние соответствующее очередному этапу почтовой транзакции, получение почтовым сервером от клиента команды RCPT, проверка идентификаторов получателей электронной почты (имя почтового ящика и домена, а также количество получателей сообщений электронной почты)
S_8	Состояние, в котором клиент (при превышении допустимого количества получателей сообщений электронной почты) принимает содержащий код ошибки о невозможности дальнейшей передачи ответный отклик, разделенный на фрагменты, направляемые через интервалы времени их задержки
S_9	Состояние, соответствующее заключительному этапу почтовой транзакции, получение почтовым сервером от клиента команды DATA и передача текста сообщения электронной почты

Переход системы L из состояния S_i в состояние S_j происходит под воздействием простейшего потока событий (заявок) λ_{ij}, обладающего соответствующими свойствами. В связи с чем, функции распределения случайных величин времени ожидания смены состояний S_i системы, подчиняются экспоненциальному закону распределения с параметрами, численно равными интенсивностям выхода λ_i из соответствующих состояний. Интенсивность потока событий численно равна математическому ожиданию числа событий в единицу времени. Эволюция процесса функционирования сервиса электронной почты происходит под воздействием потоков случайных событий, приведенных в таблице 2.

Таблица 2 – Интенсивности потоков событий

Переменная	Описание потока событий
λ_{12}	Интенсивность потока событий по установлению сетевого соединения между клиентом и почтовым сервером (среднее количество поступивших на порт 25 почтового сервера пакетов в единицу времени), [шт/с]
λ_{21}	Интенсивность потока событий по разрыву установленного сетевого соединения клиента и сервера, в случае превышения допустимого количества подключений клиентов к серверу (среднее количество отправленных сервером откликов с кодом 450 «Requested mail action not taken: mailbox unavailable» в единицу времени), [шт/с]
λ_{24}	Интенсивность потока событий по отправке клиентам множества промежуточных ответных откликов через настраиваемое время задержки в связи с превышением значения счетчика общего количества подключений к серверу (среднее количество отправленных сервером промежуточных ответных откликов «250-example.ru» в единицу времени), [шт/с]
λ_{23}	Интенсивность потока событий по поступлению от клиентов команд EHLO на начало почтовой транзакции (среднее количество команд EHLO в единицу времени), [шт/с]
λ_{34}	Интенсивность потока событий по отправке клиентам множества промежуточных ответных откликов, в связи с ошибками представления клиентов почтовому серверу командной EHLO (среднее количество ошибок представления в командах EHLO в единицу времени), [шт/с]
λ_{35}	Интенсивность потока событий по успешному представлению клиентов серверу командой EHLO (среднее количество откликов сервера «250 HELP» в единицу времени), [шт/с]
λ_{41}	Интенсивность потока событий по сбросу установленного соединения по инициативе клиента в связи с истечением RTO (Retransmission Timeouts) тайм-аута повторной передачи протокола TCP при получении множества ответных откликов от сервера (среднее количество сбросов соединений по истечение RTO в единицу времени), [шт/с]
λ_{43}	Интенсивность потока событий по поступлению от клиентов команд EHLO на начало почтовой транзакции после приема промежуточных ответных откликов (среднее количество команд EHLO, полученных сервером после отправки промежуточных откликов «250-VRFY», в единицу времени), [шт/с]
λ_{45}	Интенсивность потока событий по поступлению от клиентов команд MAIL после корректировки ошибок представления клиентов (среднее количество команд MAIL, полученных сервером после отправки промежуточных откликов «250-VRFY», в единицу), [шт/с]
λ_{56}	Интенсивность потока событий по отправке сервером ответных откликов с кодом временной ошибки о невозможности передачи сообщений электронной почты (среднее количество ответных откликов сервера с кодом ошибки 552 «Requested mail action aborted: exceeded storage allocation», 501 «Syntax error in parameters or arguments» и т.д., в единицу времени), [шт/с]
λ_{57}	Интенсивность потока событий по поступлению от клиентов команд RCTP (среднее количество команд RCTP в единицу времени), [шт/с]
λ_{61}	Интенсивность потока событий по разрыву соединения клиентом после получения ответного отклика, содержащего код ошибки (среднее количество сбросов соединений клиентами после получения отклика сервера с кодом ошибки 552 «Requested mail action aborted: exceeded storage allocation», 501 «Syntax error in parameters or arguments», в единицу времени), [шт/с]

Переменная	Описание потока событий
λ_{67}	Интенсивность потока событий по направлению клиентом почтовому серверу команды RCPT после корректировки количества или адресов почтовых ящиков получателей сообщений электронной почты (среднее количество команд RCTP после корректировки параметров сообщения, в единицу времени), [шт/с]
λ_{78}	Интенсивность потока событий по отправке клиентам фрагментов ответного отклика с кодом постоянной ошибки о невозможности передачи сообщений электронной почты (среднее количество отправленных сервером фрагментов ответного отклика с кодом постоянной ошибки 450 «Requested mail action not taken: mailbox unavailable» о невозможности передачи сообщений электронной почты, в единицу времени), [шт/с]
λ_{79}	Интенсивность потока событий по направлению клиентом почтовому серверу команды DATA (среднее количество команд DATA в единицу времени), [шт/с]
λ_{81}	Интенсивность потока событий по сбросу установленного соединения по инициативе клиента в связи с истечением RTO (Retransmission Timeouts) тайм-аута повторной передачи протокола TCP при получении множества фрагментов с кодом постоянной ошибки о невозможности передачи сообщений электронной почты (среднее количество сбросов соединений по истечение RTO при получении фрагментов с кодом ошибки ошибки 450 «Requested mail action not taken: mailbox unavailable», в единицу времени), [шт/с]
λ_{89}	Интенсивность потока событий по направлению клиентом почтовому серверу команды DATA, после изменения им количества получателей сообщений электронной почты на допустимое значение (среднее количество команд DATA после корректировки сообщения, в единицу времени), [шт/с]
λ_{91}	Интенсивность потока событий по разрыву соединения после успешной передачи сообщения (среднее количество откликов сервера с кодом 221 «Mail.company.STMP.closing connection», в единицу времени), [шт/с]
λ_{97}	Интенсивность потока событий по получению сервером команды DATA после передачи сообщения (среднее количество команд DATA после передачи сообщения электронной почты в единицу времени), [шт/с]

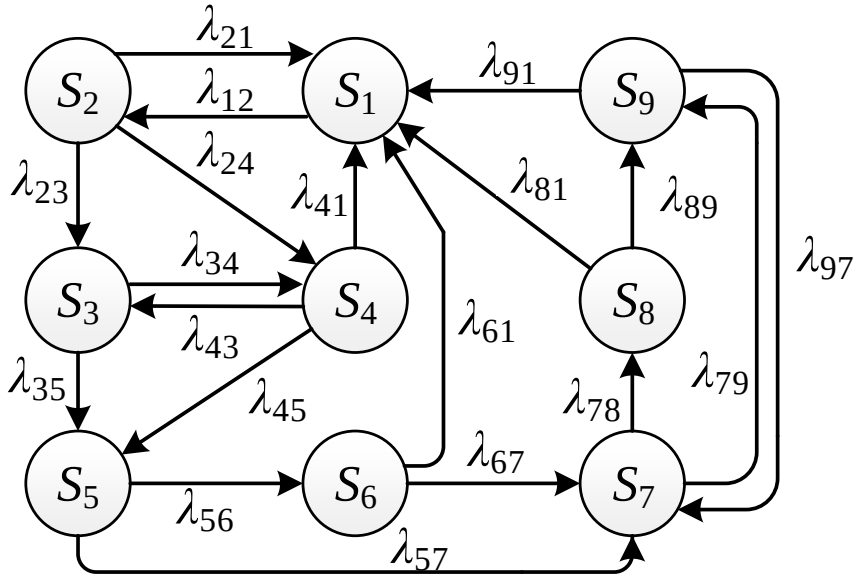


Рис. 5. Ориентированный граф состояний функционирования сервиса электронной почты

Полученная модель представляет собой цепь Маркова с непрерывным временем, которая может быть представлена с помощью ориентированного графа (рис. 5).

Содержательное описание эволюции разработанной модели может быть представлено следующим образом.

Пусть S_1 – начальное состояние моделируемой системы, в котором сервис электронной почты не принимает и не передает сообщения электронной почты и находится в состоянии покоя. При нахождении сервиса электронной почты этом состоянии клиент также находится в состоянии простоя.

После направления клиентами почтовому серверу заявок с интенсивностью λ_{12} система переходит из состояния S_1 в состояние S_2, в котором осуществляется инициализация сетевого соединения между клиентом и сервером на транспортном уровне, проверка счетчика общего количества подключений клиентов к серверу.

В случае, когда общее количество подключений клиентов к серверу больше их максимально допустимого значения I_{cmax} возникает поток событий по отправке клиентам множества промежуточных ответных откликов с интенсивностью λ_{24} для увеличения времени получения клиентом ответного отклика от сервера. Этот поток событий переводит моделируемую систему из состояния S_2 в состояние S_4, в котором клиент принимает от сервера ответный отклик через множество промежуточных откликов, направляемых через интервалы времени их задержки. Это обеспечивает замедление обработки очередных заявок от клиентов сервером и выстраивание их в очередь на обработку без разрыва установленных соединений между клиентами и сервером ввиду превышения значения I_{smax}. Обработка заявок осуществляется по принципу «первый зашел, первый вышел».

В противном случае, когда общее количество подключений клиентов меньше значения параметра I_{smax}, возникает поток событий интенсивностью λ_{23} по поступлению от клиентов команд EHLO на начало почтовой транзакции, переводящий моделируемую систему из состояния S_2 в состояние S_3. В этом состоянии осуществляется инициализация процесса почтовой транзакции посредством направления клиентом серверу электронной почты команды EHLO. Данная команда содержит идентификаторы отправителя сообщений электронной почты и данные, необходимые для представления клиента почтовому серверу. При наличии ошибок представления клиента почтовому серверу возникает поток событий интенсивностью λ_{34} по отправке клиентам множества промежуточных ответных откликов для увеличения времени получения клиентами ответных откликов от сервера, переводящий систему состояния из S_3 в состояние S_4. В случае корректировки ошибок представления идентификаторов клиентов почтовому серверу, клиенты направляют поток заявок с командой MAIL почтовому серверу с интенсивностью λ_{45} и система переходит из состояния S_4 в состояние S_5. На этом этапе процесса почтовой транзакции осуществляется получение почтовым сервером от клиентов команды MAIL, содержащей идентификаторы отправителей сообщений электронной почты (название почтового ящика отправителя и количество получателей). При отсутствии ошибок представления

клиентов почтовому серверу возникает поток заявок с командами MAIL с интенсивностью λ_{35} без отправки клиентам множества промежуточных ответных откликов.

При превышении максимально допустимого количества получателей сообщений электронной почты I_{cmax}, указанных в полученной командах MAIL или превышении количества попыток отправки сообщений на несуществующие адреса электронной почты возникает поток событий интенсивностью λ_{56}, переводящий систему в состояние S_6. В этом состоянии клиент принимает ответные отклики, содержащие код ошибки. В случае истечения тайм-аута ожидания повторной передачи сообщения или по инициативе клиента соединение разрывается и система переходит в состояние S_1 с интенсивностью λ_{61}. Либо после корректировки количества или названий адресов почтовых ящиков получателей сообщений электронной почты, система переходит в состояние S_7 с интенсивностью потока событий λ_{67}. В случае успешной проверки идентификаторов команды MAIL возникает поток событий по направлению клиентами почтовому серверу команд RCPT с интенсивностью λ_{57}, переводящей систему в состояние S_7.

При превышении максимально допустимого количества получателей сообщений электронной почты, заданного для каждого из клиентов, возникает поток событий по отправке клиентам фрагментов ответного отклика с кодом постоянной ошибки о невозможности передачи сообщений электронной почты с интенсивностью λ_{78}, переводящий систему в состояние S_8. Далее, при истечении тайм-аута ожидания повторной передачи сообщения или по инициативе клиента, возникает поток событий интенсивностью λ_{81}, вызывающий переход системы в состояние S_1. В случае успешной проверки идентификаторов команды RCPT возникает поток событий с интенсивностью λ_{79} по отправке клиентами почтовому серверу команд DATA, переводящий систему в состояние S_9. Этому состоянию соответствует заключительный этап почтовой транзакции, получение почтовым сервером от клиента команды DATA и передача текста сообщения электронной почты. В случае повторной отправки клиентами сообщения электронной почты без разрыва соединения, клиентами направляются команды DATA с интенсивностью λ_{97}, в результате чего система из состояния S_9 переходит в состояние S_7. В ином случае, после полного завершения почтовой транзакции между клиентом и сервером, система с интенсивностью λ_{91} переходит в состояние S_1 в связи с завершением соединения.

Искомыми характеристиками модели являются вероятностно-временные характеристики случайного процесса: вектор функций безусловных вероятностей нахождения системы в состояниях S_i в любой момент времени $p_i(t)$, вектор финальных (стационарных) вероятностей p_i (в случае, если случайный процесс обладает свойством эргодичности). Искомый вектор функций $\{p_i(t)\}$ являются решением системы обыкновенных (линейных с постоянными коэффициентами) дифференциальных уравнений (СДУ) Колмогорова с начальным условием, характеризующим распределение вероятностей пребывания системы S в каждом из состояний в начальный момент времени {1, 0, 0, 0, 0, 0, 0, 0, 0}. Это означает, что в момент времени t=0 система достоверно находится в состоянии S_1.

Для нахождения вектора финальных вероятностей $\{p_i\}$ в СДУ левую часть приравнивают к нулю и исключают одно из уравнений на условие нормировки ($\sum p_i=1$), получая при этом систему линейных алгебраических уравнений.

$$\begin{cases} \frac{dp_1}{dt} = p_2\lambda_{21} + p_4\lambda_{41} + p_6\lambda_{61} + p_8\lambda_{81} + p_9\lambda_{91} - p_1\lambda_{12}, \\ \frac{dp_2}{dt} = p_1\lambda_{12} - p_2(\lambda_{21} + \lambda_{23} + \lambda_{24}), \\ \frac{dp_3}{dt} = p_2\lambda_{23} + p_4\lambda_{43} - p_3(\lambda_{34} + \lambda_{35}), \\ \frac{dp_4}{dt} = p_2\lambda_{24} + p_3\lambda_{34} - p_4(\lambda_{41} + \lambda_{43} + \lambda_{45}), \\ \frac{dp_5}{dt} = p_3\lambda_{35} + p_4\lambda_{45} - p_5(\lambda_{56} + \lambda_{57}), \\ \frac{dp_6}{dt} = p_5\lambda_{56} - p_6(\lambda_{61} + \lambda_{67}), \\ \frac{dp_7}{dt} = p_5\lambda_{57} + p_6\lambda_{67} + p_9\lambda_{97} - p_7(\lambda_{78} + \lambda_{79}), \\ \frac{dp_8}{dt} = p_7\lambda_{78} - p_8(\lambda_{81} + \lambda_{89}), \\ \frac{dp_9}{dt} = p_7\lambda_{79} + p_8\lambda_{89} - p_9(\lambda_{91} + \lambda_{97}). \end{cases} \quad (1)$$

В матричной форме система линейных алгебраических уравнений (СЛАУ) Колмогорова представляет собой:

$$B \cdot p = b, \quad (2)$$

$$B = \begin{vmatrix} -(\lambda_{12} + \lambda_{13} + \ldots + \lambda_{19}) - \lambda_{91} & \ldots & \lambda_{81} - \lambda_{91} \\ \lambda_{12} - \lambda_{92} & \ldots & \lambda_{82} - \lambda_{92} \\ \ldots & \ldots & \ldots \\ \lambda_{18} - \lambda_{98} & \ldots & -(\lambda_{81} + \lambda_{82} + \ldots + \lambda_{89}) - \lambda_{98} \end{vmatrix}, \quad (3)$$

$$b = \begin{vmatrix} -\lambda_{91} \\ -\lambda_{92} \\ \ldots \\ -\lambda_{98} \end{vmatrix}, \quad (4)$$

где: B – матрица интенсивностей с учетом условия нормировки (полученное исключением из СЛАУ уравнения, определяющего финальную вероятность p_9); b – вектор свободных членов с учетом условия нормировки; p – вектор искомых финальных вероятностей.

СДУ (1) решают численными или аналитическими методами. Аналитическая форма общего решения СДУ Колмогорова с учетом условия нормировки сводится к решению алгебраической задачи на собственные значения (числа). Особенностью нахождения собственных чисел является ее высокая вычислительная сложность, связанная с размерностью матрицы коэффициентов, в частности, размерность матрицы более четырех вынуждает применение специаль-

ных численных методов нахождения собственных чисел. Поэтому, для решения систем линейных однородных дифференциальных уравнений большой размерности целесообразно использование численных методов дифференцирования функций [59]. Численные методы позволяют решать двухпараметрические СДУ Колмогорова с учетом варьирования дополнительного параметра случайного процесса (рис. 7).

Постановка задачи

Формализованную постановку задачи на управление процессом передачи сообщений электронной почты в терминах динамического программирования можно сформулировать следующим образом: при заданном уравнении объекта управления, ограничениях на вектор фазовых переменных и вектор управлений, краевых (начальных) условиях требуется найти такой вектор управлений и фазовую траекторию, при которых функционал качества управлений (целевая функция) принимает минимальные значения.

1. Вектор $x(t)$ фазовых переменных системы L – распределение вероятностей пребывания системы в состояниях $\{S_1, S_2, ..., S_9\}$ в момент времени t:

$$x(t) = \{p_1(t), p_2(t), \cdots, p_9(t)\}. \quad (5)$$

2. Вектор управлений $u(t)$ представляет собой интенсивности потоков событий, посредством которых осуществляются управляющие воздействия на вектор фазовых переменных системы L:

$$u(t) = \{u_1(t), u_2(t), u_3(t), u_4(t)\}, \quad (6)$$

$$u_1(t) = \lambda_{43}(t) = 1/(d \cdot T), \quad (7)$$

$$u_2(t) = \lambda_{45}(t) = 1/(d \cdot T), \quad (8)$$

$$u_3(t) = \lambda_{67}(t) = 1/(n \cdot m \cdot F), \quad (9)$$

$$u_4(t) = \lambda_{89}(t) = 1/(m \cdot F), \quad (10)$$

где: $T = [1, 2, ..., 10]$ – значение времени задержки между промежуточных откликов от сервера электронной почты на команды клиента, [с]; $d = [1, \ldots, 1000]$ – общее количество ответных промежуточных откликов, которые будут направлены клиенту от сервера электронной почты, [шт]; $n = [1, \ldots, 100]$ – общее количество ответных откликов, от сервера электронной почты на команды клиента, содержащих сообщения об ошибках, [шт]; $m = [1, \ldots, 1000]$ – общее количество фрагментов, на которые разбиваются ответные отклики от сервера электронной почты, направляемые клиенту, [шт]; $F = [1, 2, \ldots, 15]$ – значение времени задержки между отправкой фрагментов отклика клиенту сервиса электронной почты, [с].

3. Начальное условие: распределение вероятностей пребывания системы в состояниях в начальный момент времени:

$$x(0) = \{p_1(0), p_2(0), \cdots, p_9(0)\} = \{1,0,0,0,0,0,0,0,0\}. \quad (11)$$

4. Допустимые значения вектора фазовых переменных:

$$0 \le p_i(t) \le 1. \quad (12)$$

5. Допустимые значения вектора управления, вычисленные исходя из численных значений параметров (см. выражение (6-10)):

$$10^{-4} \le u_1(t) \le 1, \quad (13)$$

$$10^{-4} \le u_2(t) \le 1, \quad (14)$$

$$0{,}67 \cdot 10^{-6} \le u_3(t) \le 1, \quad (15)$$

$$0{,}67 \cdot 10^{-4} \le u_4(t) \le 1. \quad (16)$$

6. Уравнение объекта управления (системы L) представляет собой систему обыкновенных дифференциальных уравнений Колмогорова, в матричной форме:

$$\frac{dx}{dt} = A \cdot x, \quad (17)$$

$$A = \begin{vmatrix} -(\lambda_{12}(t) + \ldots + \lambda_{19}(t)) & \lambda_{21}(t) & \ldots & \lambda_{19}(t) \\ \lambda_{21}(t) & \ldots & \ldots & \lambda_{29}(t) \\ \ldots & \ldots & \ldots & \ldots \\ \lambda_{19}(t) & \lambda_{29}(t) & \ldots & -(\lambda_{91}(t) + \ldots + \lambda_{98}(t)) \end{vmatrix}. \quad (18)$$

7. Функционал качества управления (целевая функция):

$$J(t) = J[x(t), u(t)] = p_1(t) \to \min. \quad (19)$$

Для оценки эффективности управления процессом передачи сообщений электронной почты, в целях обеспечения доступности информационных ресурсов сервиса электронной почты клиентам, рассмотрим следующие ситуации:

C_1 – без замедления передачи сообщения электронной почты от клиента серверу, в этом случае, при превышении максимально допустимого значения общего количества устанавливаемых соединений клиентов с сервером, а также при превышении максимально допустимого значения количества устанавливаемых соединений одного клиента с сервером, сервер в одностороннем порядке разрывает устанавливаемые соединения, для исключения своей перегрузки и возникновения ситуации отказа в обслуживании;

C_2 – с замедлением передачи сообщения электронной почты от клиента серверу, в этом случае, при превышении максимально допустимого значения общего количества устанавливаемых соединений клиентов с сервером, а также при превышении максимально допустимого значения количества устанавливаемых соединений одного клиента с сервером, сервер получив множество заявок на соединение от клиентов выстраивает их в очередь и далее последовательно обрабатывает.

Рассмотрим ситуацию C_1 без замедления передачи сообщения электронной почты от клиента серверу (λ_{24}, λ_{56}, λ_{78}=0). В данных условиях на начальном этапе почтовой транзакции, при угрозе возникновения перегрузки почтового сервера, обусловленной получением сервером такого количества запросов на обработку от клиентов, которое он не в состоянии обработать в настоящий момент, осуществляется разрыв очередных устанавливаемых соединений, то есть переход клиентов в состояние простоя S_1 (λ_{21}>0).

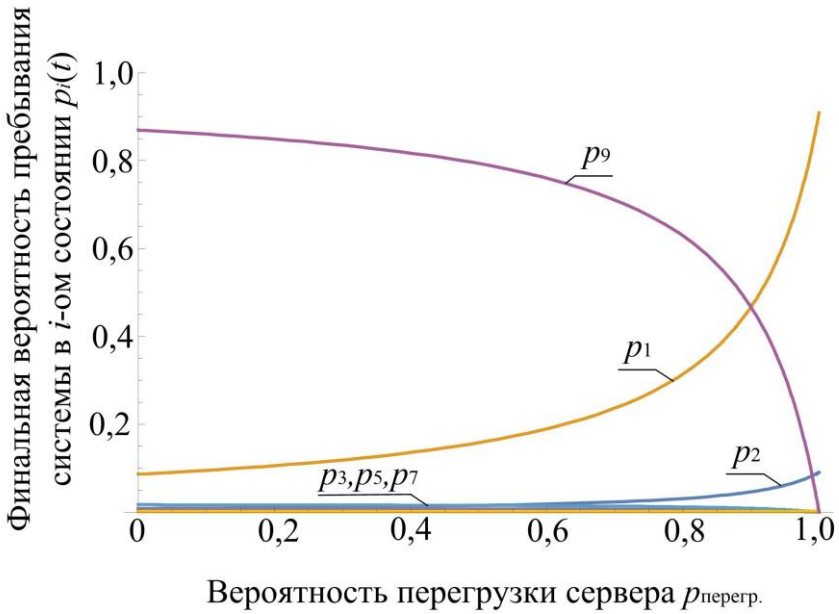


Рис.6. Зависимость финальных вероятностей состояний моделируемой системы от вероятности перегрузки сервера $p_{перегр.}$ заявками от клиентов, соответствующие ситуации C_1

На начальном этапе проверки условий для исключения перегрузки почтового сервера S_2, вероятность разрыва устанавливаемого соединения между клиентом и сервером, ведущего к перегрузке запросами последнего, можно выразить через интенсивности потоков событий, переводящие систему из состояний S_2 в состояния S_1 и S_3:

$$p_{21} = p_{перегр.} = \frac{\lambda_{21}}{\lambda_{21} + \lambda_{23}}. \quad (20)$$

Варьируя значениями интенсивности потока событий по разрыву сетевого соединения λ_{21}, и фиксируя значение интенсивности потока событий по переходу к первому этапу почтовой транзакции λ_{23} с учетом высокой интенсивности подключений клиентов λ_{12} можно оценить зависимость финальных вероятностей p_i пребывания системы в состояниях от вероятности перегрузки сервера $p_{перегр.}$

Как видно из рис. 6 при значительном увеличении интенсивности потока заявок λ_{21}, приводящего к увеличению вероятности перегрузки сервера $p_{перегр.}$ значение финальной вероятности пребывания клиента в состоянии простоя S_1, после достижения количества полученных сервером заявок от клиентов значения I_{smax}, также увеличивается и в пределе составляет величину 0,71, а значение финальной вероятности пребывания системы в состоянии S_2 составляет 0,29.

Разработанная математическая модель позволяет определить вероятностно-временные характеристики переходного процесса. Переходный процесс представляет собой промежуток времени, в течение которого вероятности пребывания системы в состояниях $\{p_i(t)\}$ изменяются от начальных значений $\{p_i(0)\}$ до финальных (стационарных) значений $\{p_i\}$. Применяя для решения СДУ численный метод Рунге-Кутты четвертого порядка с фиксированным шагом интегрирования и сплайн-интерполяцию точечных результатов, можно по-

лучить графическую зависимость вероятностей пребывания системы от времени и от вероятности перегрузки сервера (рис. 7).

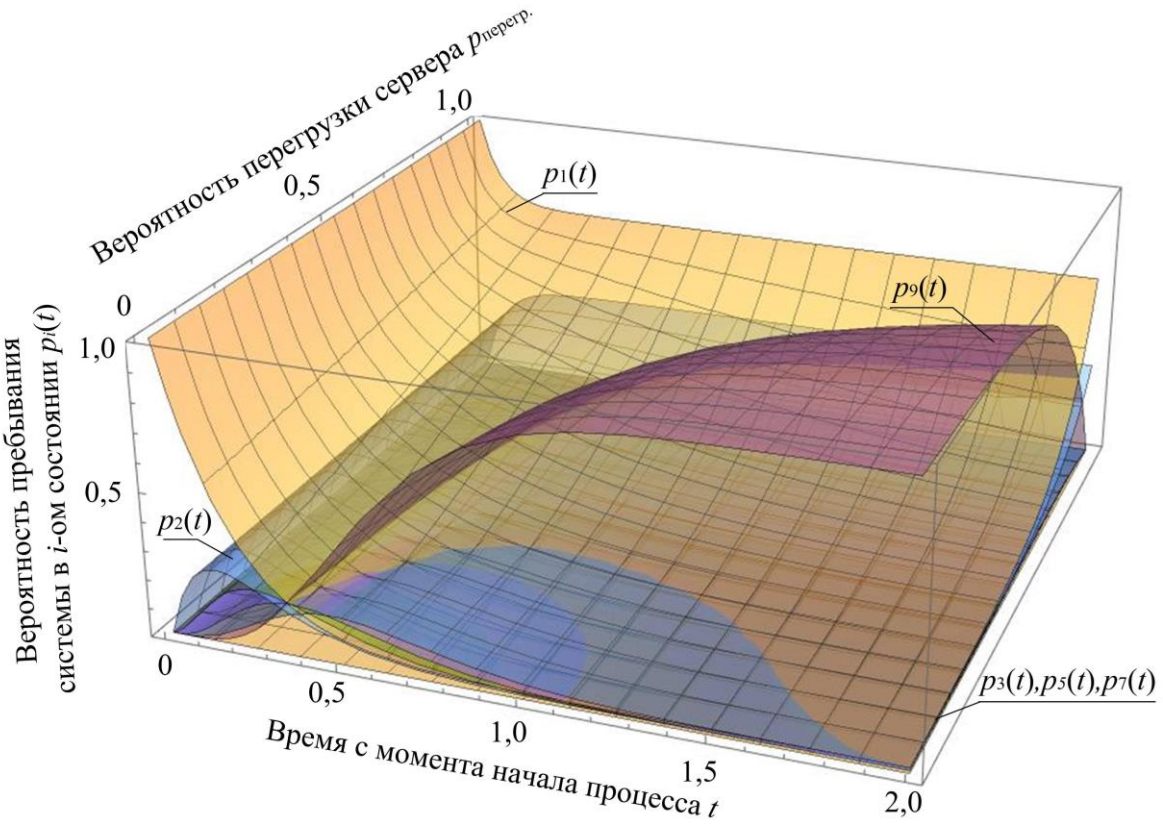


Рис. 7. Результаты расчетов зависимостей вероятностей $p_i(t)$ системы L от вероятности перегрузки сервера $p_{перегр.}$ в ситуации C_1

Как видно из рис. 7 длительность переходного процесса эволюции моделируемой системы L составляет около 2 с, за которые вероятности пребывания системы в состояниях $\{p_i(t)\}$ достигают стационарных (финальных) значений $\{p_i\}$. На интервале времени [0, 0,5] наблюдается всплеск значений вероятностей пребывания системы в состояниях $p_2(t)$, $p_3(t)$, соответствующих инициализации сетевого соединения, проверке счетчика общего количества подключений к серверу и переходу к начальному этапу почтовой транзакции. При малых значениях вероятности перегрузки сервера $p_{перегр.}$ [0, 0,3], на интервале времени [0,5, 2,0], наблюдается монотонный рост вероятности пребывания системы в состоянии $p_9(t)$, соответствующем передаче сервером сообщения электронной почты.

Рассмотрим ситуацию C_2 в которой, с целью повышения доступности информационных ресурсов сервера электронной почты клиентам, осуществляется замедление передачи сообщений электронной почты (λ_{24}, λ_{56}, $\lambda_{78}>0$), количество которых превышает возможности по немедленной обработке их сервером, без разрыва соединений по инициативе сервера ($\lambda_{21}=0$). В данном случае, вероятность перегрузки сервера определяется интенсивностью заявок на замедление передачи сообщения электронной почты на различных этапах почтовой транзакции, то есть:

$$p_{24} = p_{перегр.1} = \frac{\lambda_{24}}{\lambda_{24} + \lambda_{23}}, \quad (21)$$

$$p_{56} = p_{перегр.2} = \frac{\lambda_{56}}{\lambda_{56} + \lambda_{57}}, \quad (22)$$

$$p_{78} = p_{перегр.3} = \frac{\lambda_{78}}{\lambda_{78} + \lambda_{79}}, \quad (23)$$

Пусть значения вероятностей перегрузки почтового сервера на различных этапах почтовой транзакции равны между собой $p_{\text{перегр.1}}=p_{\text{перегр.2}}=p_{\text{перегр.3}}=p_{\text{перегр}}$. Тогда с учетом высокой интенсивности подключений клиентов λ_{12}, можно оценить зависимость финальных вероятностей p_i пребывания системы в различных состояниях от вероятности $p_{\text{перегр.}}$ перегрузки сервера в условиях управления процессом передачи сообщений электронной почты (рис. 8).

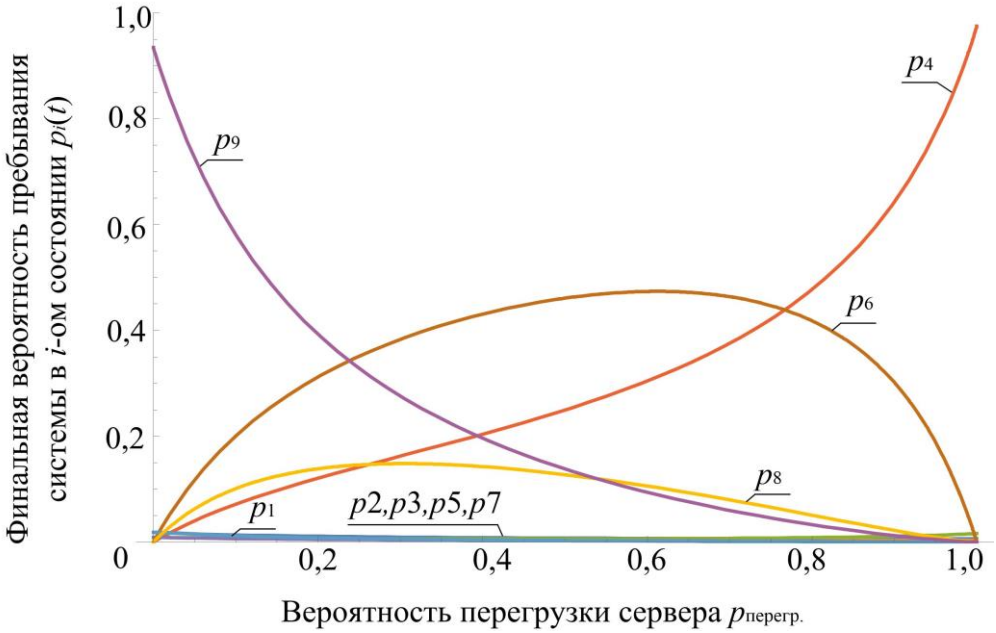


Рис. 8. Результаты расчетов зависимостей финальных вероятностей p_i системы L от вероятности $p_{\text{перегр.}}$ перегрузки сервера, соответствующие ситуации C_2

При значительном увеличении интенсивностей потоков заявок λ_{24}, λ_{56}, λ_{78} в случае увеличения вероятности перегрузки сервера, финальная вероятность простоя клиента S_1, заявки от которого уже поступили к серверу, снижается и в пределе составляет величину 0,03. По мере роста вероятности перегрузки сервера, финальная вероятность p_9 пребывания системы в состоянии передачи сообщения снижается, вероятность p_4 пребывания системы в состоянии, соответствующем замедлению передачи сообщения электронной почты на начальном этапе почтовой транзакции увеличивается. Финальные вероятности удержания клиентов p_6 и p_8 на последующих этапах почтовой транзакции сначала растут, а затем снижаются до 0, в связи с тем, что основные усилия сервера будут затра-

чены на замедление передачи поступивших сообщений электронной почты от клиента, переводящие систему в состояние S_4.

В соответствии с формализованной постановкой задачи показателем эффективности функционирования сервиса электронной почты является минимизация вероятности простоя клиента p_1.

Графическая интерпретация (рис. 9) зависимостей финальных вероятностей p'_1 и p'_9 в состояниях для ситуации C_1 и вероятностей p''_1 и p''_9 для ситуации C_2 от вероятности перегрузки сервера $p_{\text{перегр}}$. позволяет сравнить эффективность функционирования сервиса электронной почты в ситуациях C_1 и C_2. При использовании механизмов замедления передачи клиентами серверу очередных сообщений электронной почты, в условиях любой степени перегруженности почтового сервера, вероятность простоя клиента p''_1, заявки от которого выстроены в очередь для обработки, практически равна нулю. При увеличении интенсивности замедления передачи клиентами очередных сообщений электронной почты в связи с возрастающей перегрузкой сервера происходит стремительное снижение вероятности пребывания системы в состоянии передачи электронного сообщения p''_9 и рост вероятности пребывания системы в состоянии удержания S_4. Причем, чем выше среднее значение суммарного времени замедления передачи клиентами серверу сообщений электронной почты клиента в состояниях S_4, S_6, S_8, тем быстрее снижается вероятность пребывания системы в состоянии передачи сообщений p''_9.

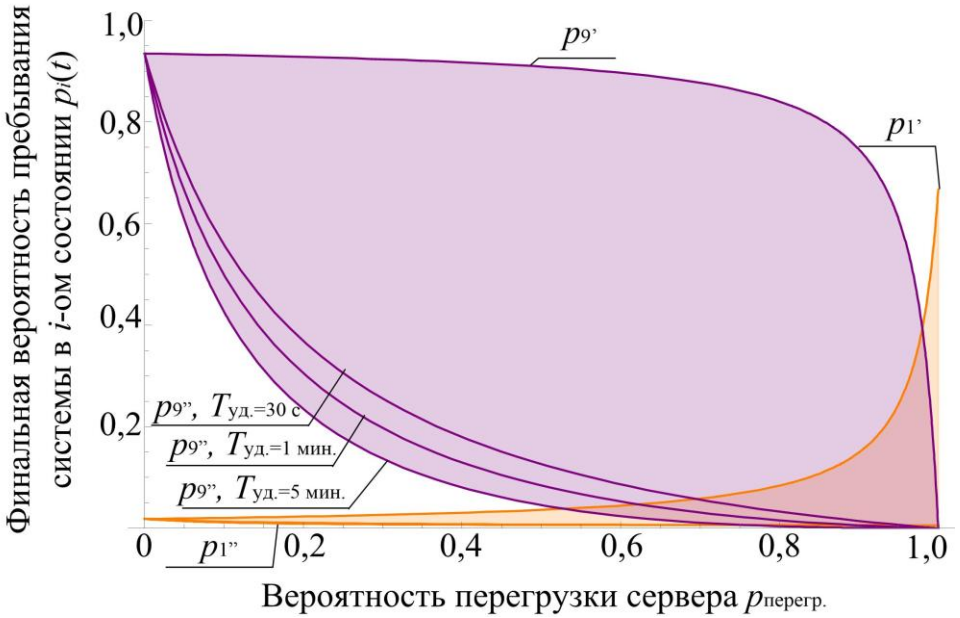


Рис. 9. Зависимости финальных вероятностей p_1 и p_9 для ситуаций C_1 и C_2 от вероятности перегрузки сервера $p_{\text{перегр}}$.

Определение вероятностно-временных характеристик случайного процесса позволяет определить характер и длительность переходного процесса эволюции системы L (рис. 10).

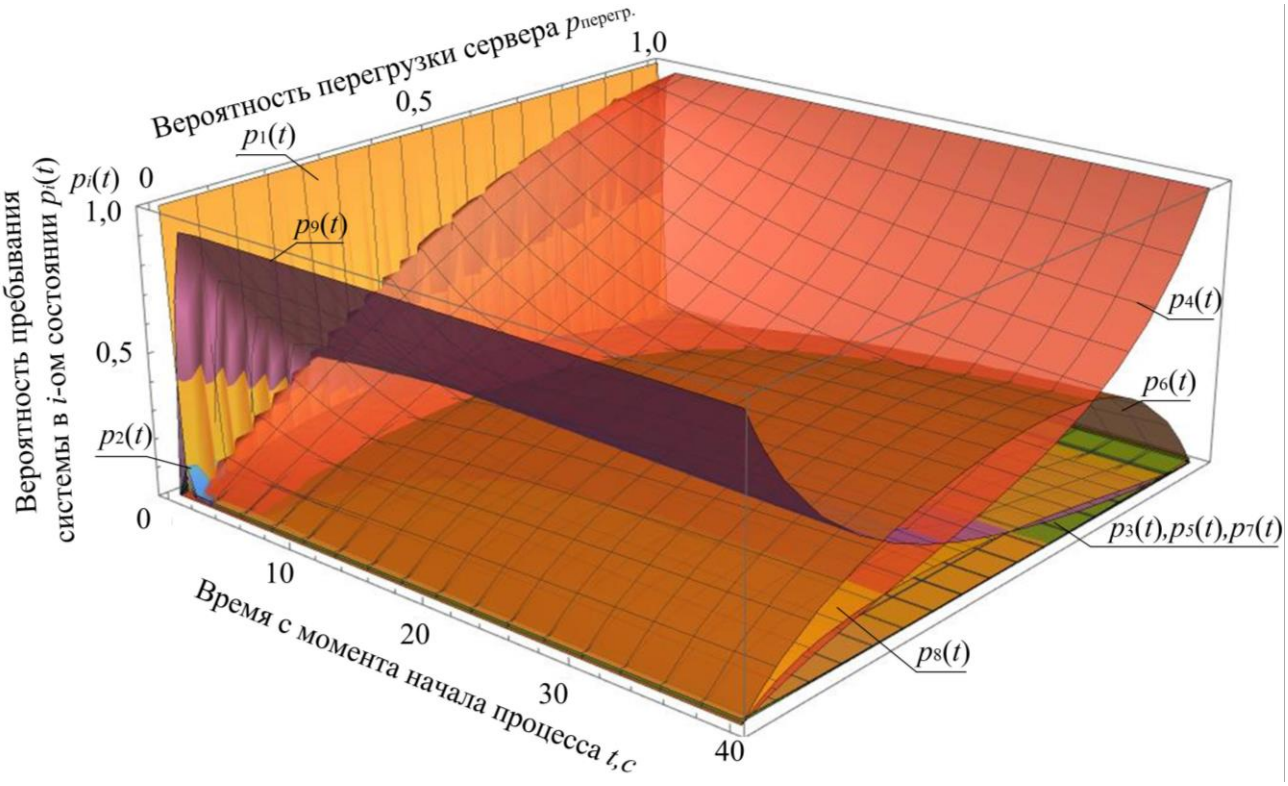


Рис. 10. Результаты расчетов зависимостей вероятностей $p_i(t)$ системы L от вероятности перегрузки сервера $p_{\text{перегр.}}$ в ситуации C_2

Как видно из результатов расчетов (рис. 10), длительность переходного процесса составляет величину около 40 с, за которые вероятности пребывания системы $\{p_i(t)\}$ достигают стационарных (финальных) значений $\{p_i\}$ при соответствующих значениях вероятности перегрузки сервера $p_{\text{перегр.}}$. Наименьшее время (около 0,15 с) от начала отсчета требуется для достижения стационарных значений вероятностей p_1, p_2, p_3, p_5, p_7, p_9. Длительность установления стационарного распределения вероятностей $\{p_i\}$ определяется временем достижения своих финальных значений вероятностями замедления передачи клиентами серверу очередных сообщений электронной почты p_4, p_6, p_8 на различных этапах почтовой транзакции в связи с более низкими интенсивностями выхода λ_4, λ_6, λ_8 из данных состояний. В связи с чем, средняя длительность замедления передачи клиентами серверу очередных сообщений электронной почты через соответствующие интенсивности потоков событий по выходу системы L из состояний замедления передачи клиентами серверу очередных сообщений электронной почты S_4, S_6, S_8 характеризуют инерционность системы.

Представленные на рис. 11 результаты расчетов показывают, что по истечении 0,1 с наблюдается всплеск значений вероятностей пребывания системы во всем пространстве состояний $\{S_i\}$, причем, чем выше значение интенсивности подключения клиента λ_{12}, тем выше величина всплеска вероятностей.

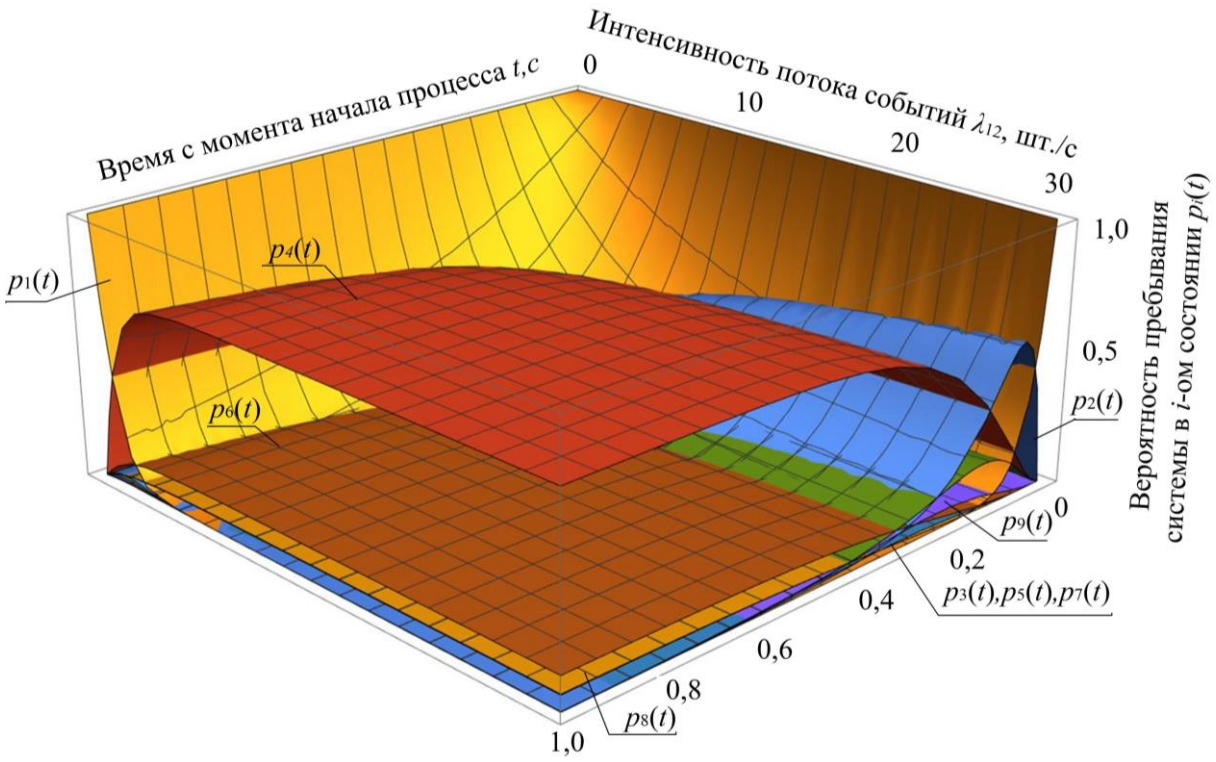


Рис. 11. Результаты расчета зависимостей вероятностей $p_i(t)$ системы L от интенсивности подключения клиента λ_{12} в ситуации C_2

По истечении 1 с наступает стационарный режим, в котором система значительную часть времени пребывает в состоянии замедления передачи клиентами серверу очередных сообщений электронной почты, причем финальные вероятности нахождения системы в состояниях замедления передачи сообщения электронной почты от клиента серверу достигают своих максимальных значений уже при λ_{12}=5.

Ограничения и устойчивость математической модели

Разработанная модель позволяет оценить вероятностно-временные характеристики функционирования сервиса электронной почты в различных ситуациях управления процессом передачи сообщений электронной почты. Однако, возникает вопрос устойчивости формируемых параметров передачи сообщений электронной почты по отношению к возмущениям (погрешностям) исходных данных (интенсивностей потоков событий). Во-первых, строго говоря, система обладает инерционностью, а интенсивности потоков событий изменяются с течением времени, во-вторых, интенсивности определяются с некоторой погрешностью. В данном случае используется понятие робастной и асимптотической устойчивости модели к возмущению исходных данных.

Под робастной устойчивостью модели понимается свойство обеспечения устойчивости системы при всех допустимых отклонениях реального объекта или процесса от формализованной модели. Соответственно по отношению к объекту исследования устойчивость есть способность сервиса электронной по-

чты выполнять свои функции в результате воздействия дестабилизирующих факторов, возмущающих элементы матрицы интенсивностей потоков событий.

Определение робастной устойчивости модели посредством оценки влияния возмущения исходных данных относительно получаемых вероятностно-временных характеристик позволяет определить требования к точности формируемых исходных данных с целью повышения адекватности математической модели.

Робастность (устойчивость к возмущениям) решения (вектора финальных вероятностей $\{p_i\}$) к изменению входных параметров (интенсивностей потоков событий), как погрешность решения системы линейных алгебраических уравнений (СЛАУ) Колмогорова при соответствующей погрешности исходных данных, позволяет оценить число обусловленности μ матрицы интенсивностей потоков событий B (см. выражение (3)). Число (мера) обусловленности является коэффициентом связи относительной погрешности решения СЛАУ и погрешности в определении матрицы коэффициентов.

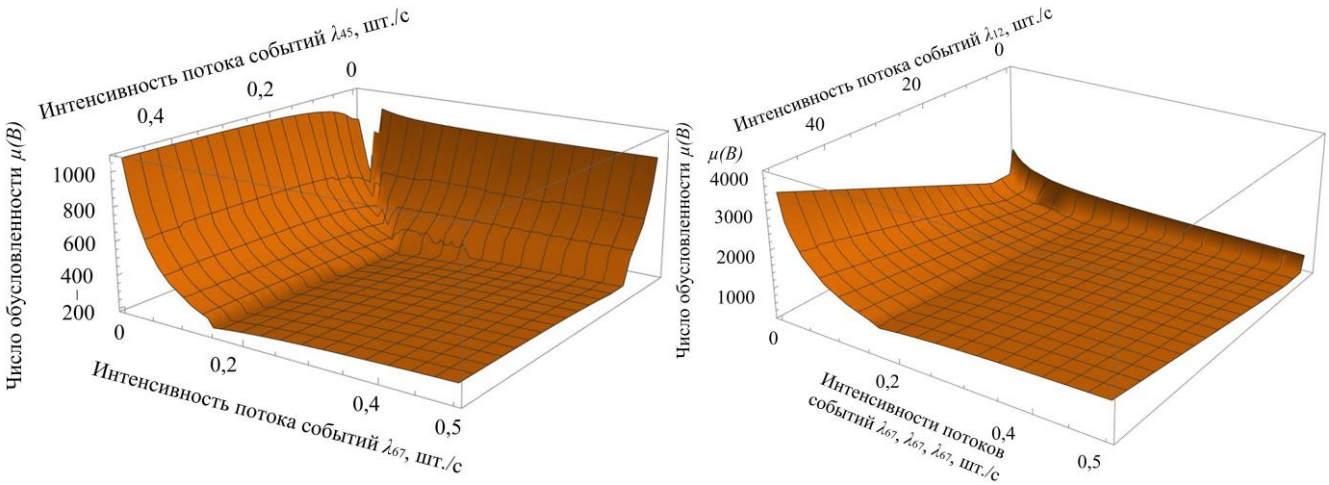
$$\left\| \frac{\Delta p}{p} \right\| \le \mu \cdot \left(\left\| \frac{\Delta b}{b} \right\| + \left\| \frac{\Delta B}{B} \right\| \right). \qquad (24)$$

Где $\|\Delta p/p\|$ – относительная погрешность вектора решения СЛАУ (вектора финальных вероятностей) в форме векторной нормы; $\|\Delta b/b\|$ - относительная погрешность вектора свободных членов в векторной нормы; $\|\Delta B/B\|$ - относительная погрешность матрицы интенсивностей с учетом условия нормировки; Δp – возмущения вектора решения СЛАУ, вызванное возмущением матрицы ΔB и возмущением вектора Δb.

Для оценки числа обусловленности используются следующие нормы: евклидова норма, норма-максимум, норма сумма матрицы. Система называется «плохо обусловленной» если число обусловленности матрицы велико. В качестве интерпретации значений числа обусловленности используют следующее соотношение: если $\mu=10^p$ и исходные данные имеют погрешность в l-м знаке после запятой, то независимо от способа решения СЛАУ в результате можно гарантировать не более l-p знаков после запятой [61]. Исходя из данных предположений, для рассматриваемой СЛАУ можно определить интервалы значения числа обусловленности матрицы, характеризующей интенсивности потоков событий марковского процесса с учетом условия нормировки, следующим образом: $1 \le \mu(B) \le 10$ – робастная (устойчивая); от $10 \le \mu(B) \le 1000$ – слабо робастная (слабоустойчивая); $\mu(B) \ge 1000$ – неробастная (неустойчивая) система.

Высокие значения числа обусловленности $\mu(B)$ в зависимости от изменения значений интенсивностей потоков событий по замедлению клиентов на первом и втором этапе реализации (λ_{45}, λ_{67}) почтовой транзакции характеризуют слабую робастность (слабую устойчивость) к возмущениям исходных данных (рис. 12). Наименьшая устойчивость модели наблюдается при низких значениях интенсивностей $\lambda_{45} \in [0; 0{,}05]$, $\lambda_{67} \in [0; 0{,}05]$ и при высоких значениях интенсивностей входящих запросов на установление соединения $\lambda_{12} \in [0; 10]$. Полученные результаты предъявляет повышенные требования к точности определения исходных данных при снижении робастности модели либо снижает надежность

полученных с помощью модели результатов при использовании исходных данных из указанных диапазонов.



а) б)

Рис. 12. Результаты расчетов зависимости числа обусловленности матрицы B (линейного оператора) СЛАУ Колмогорова от значения варьируемых значений интенсивностей: а) от λ_{45}, λ_{67} б) от λ_{12}, λ_{43}, λ_{45}, λ_{67}

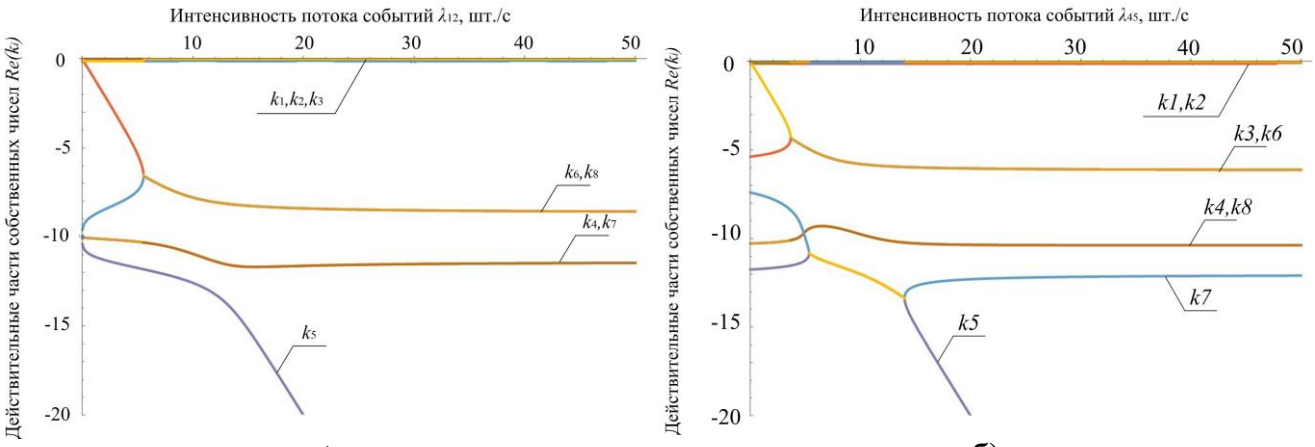
Асимптотическая устойчивость модели, основанной на математическом аппарате цепей Маркова, характеризуется свойством эргодичности, то есть существованием финальных (стационарных) вероятностей состояний, не зависящих от распределения вероятностей в начальный момент времени. Цепь Маркова, включающая замкнутый класс (конечное множество) сообщающихся состояний, является эргодической. [60].

Рассматриваемая математическая модель представляет собой замкнутый класс сообщающихся (транзитивных) состояний, поэтому разработанная модель является эргодической (асимптотически устойчивой).

Аналитически условием эргодичности цепи Маркова является отрицательность действительной части собственных чисел $Re(k_i)$ матрицы B, характеризующей СЛАУ. Величина действительной части собственных чисел определяет длительность переходного процесса, чем меньше значение, тем быстрее протекает переходный процесс.

К примеру, при варьировании значениями интенсивностей потоков событий λ_{12}, λ_{45} действительная часть собственных чисел $Re(k_i)$ всегда отрицательна (рис. 13), следовательно, процесс асимптотически устойчив (эргодический). Наибольшие значения имеют действительные части собственных чисел k_1, k_2, k_3, определяющие длительность переходного процесса при соответствующих значениях интенсивностей потоков событий.

Вследствие чего, математическая модель обладает асимптотической устойчивостью при любых значениях исходных данных, а ограничения корректности модели связаны со слабой робастностью модели относительно изменения исходных данных в указанном диапазоне значений.



а) б)

Рис. 13. Результаты расчетов зависимости действительной части собственных чисел $Re(k_i)$ матрицы (линейного оператора) СЛАУ Колмогорова от значений варьируемых интенсивностей потоков событий: а) от λ_{45}, б) от λ_{12}

Алгоритм проактивной защиты сервиса электронной почты от сетевой разведки

Одним из сценариев реализации компьютерных атак на сервис электронной почты является нарушение доступности клиентам информационных ресурсов сервера электронной почты. Под доступностью информации в статье понимается состояние ресурсов сервиса электронной почты, при котором клиенты, имеющие права доступа, могут реализовывать их беспрепятственно. Как правило, компьютерной атаке предшествует сбор сведений о структурно-функциональных характеристиках объекта атаки и выявление уязвимостей. Под структурно-функциональными характеристиками (СФХ) в соответствии с приказом ФСТЭК России № 17 от 11.02.2013 г. понимаются структура, состав, физические, логические, функциональные и технологические взаимосвязи между элементами системы электронной почты.

В частности, для сервиса электронной почты этими характеристиками являются тип применяемого оборудования, операционная система, применяемые средства защиты, и т.д. С некоторой полнотой данную информацию злоумышленник может получить посредством активного взаимодействия с объектом атаки, то есть сервером (агентом) передачи электронной почты. Это обусловлено наличием применяемых в настоящее время традиционных средств анализа содержимого электронных сообщений, криптографической защиты информации и аутентификации, которые не позволяют в полной мере обеспечить защиту от массовых и целевых атак, основанных на методах: подмены IP-адресов отправителей (spoofing), DDOS и DOS-атаках, фишинге, распространения спама и вредоносного программного обеспечения, NDR-атаках (Non Delivery Report attack), петлях системы электронной почты (mail loops) [31-36].

Данные обстоятельства позволяют злоумышленникам:

– использовать достаточный временной ресурс для проведения сетевой разведки и реализации компьютерных атак на компоненты сервиса электронной почты;

– сосредоточивать значительный вычислительный ресурс для осуществления вредоносных воздействий, обусловленный использованием распределенных средств вычислительной техники, зараженных вредоносным программным обеспечением, без использования собственных вычислительных мощностей.

К информационным системам критически важных, потенциально опасных объектов, а также объектов, представляющих повышенную опасность для жизни и здоровья людей и окружающей среды, предъявляются жесткие требования по обеспечению защиты от сетевой разведки и проведению компьютерных атак. В частности, должны быть реализованы: управление сетевыми соединениями (ЗИС.35), электронный почтовый обмен с внешними сетями через ограниченное количество контролируемых точек (ЗИС.15), защита от спама (ЗИС.16), сокрытие архитектуры и конфигурации информационной (автоматизированной) системы (ЗИС.8), разработка политики предотвращения вторжений (компьютерных атак) (СОВ.0), обнаружение и предотвращение вторжений (компьютерных атак) (СОВ.1), защита от угроз отказа в обслуживании (DOS, DDOS) ЗИС.34 (приказ ФСТЭК России № 138 от 09.08.2018 г., приказ ФСТЭК России № 239 от 25.12.2017 г.).

В настоящее время, выполнение перечисленных требований в полном объеме не представляется возможным в связи с отсутствием соответствующих технологий, а вследствие чего и невозможности предъявления требований по разработке, изготовлению и эксплуатации перспективных средств защиты сервиса электронной почты.

В связи с этим особую актуальность набирает необходимость разработки технологий проактивной защиты, обеспечивающих нивелирование преимуществ злоумышленника, в использовании им временного и вычислительного ресурса для ведения сетевой разведки и реализации компьютерных атак на компоненты сервиса электронной почты. Известные на текущий момент технические реализации средств проактивной защиты носят единичный характер и основаны на контроле сетевых соединений за счет использования механизмов транспортного уровня (управлении значениями параметров «размер окна» служебного заголовка TCP-пакетов сообщений, дубликатами подтверждений ACK) либо использовании отсроченной отправки служебной команды RCPT [2, 36-38]. Однако, данные решения должным образом не учитывают весь спектр особенностей функционирования сервиса электронной почты на прикладном уровне, а также имеют демаскирующие признаки, позволяющие использовать методы автоматического предотвращения замедления сетевого соединения со стороны злоумышленников и идентификации средств защиты (использование малых значений тайм-аутов ожидания ответа в рамках TCP-соединения, контроль значений скользящего окна).

Назначением разработанного алгоритма является управление процессом передачи сообщений электронной почты, обеспечивающее повышение результативности защиты за счет снижения вероятности обнаружения злоумышленником факта использования средств защиты, достигаемой имитацией канала связи с плохим качеством на различных этапах почтовой транзакции, за счет

разбиения ответного отклика злоумышленнику на фрагменты и направления этих фрагментов через многочисленные малые интервалы времени задержки, направления ответного отклика злоумышленнику после множества промежуточных откликов, отправленных через многочисленные малые интервалы времени задержки, а также направления злоумышленнику заведомо ложных сообщений о временной или постоянной невозможности продолжения почтовой транзакции.

Аналогами по своей технической сущности к представленному научно-методическому аппарату являются решения [54, 55], где обеспечивают более высокую результативность защиты по сравнению с аналогами за счет задержки на заданное время ответных откликов на команды злоумышленника в процессе передачи сообщений электронной почты, что позволяет уменьшить количество передаваемых им нежелательных сообщений и, тем самым, снизить и (или) прекратить вредоносное воздействие злоумышленника. Однако задержку по времени при отправке ответных откликов на команды злоумышленника, после его идентификации в процессе передачи сообщений электронной почты по протоколу SMTP, осуществляют через достаточно продолжительное время задержки, значение которого увеличивают в случае его повторных попыток передачи сообщений электронной почты. Это может привести к компрометации применяемых средств защиты, что вынуждает злоумышленника далее воздействовать на вычислительные сети и (или) менять применяемую стратегию воздействия, а также обходу применяемых средств защиты при установке злоумышленником достаточно коротких значений тайм-аутов ожидания ответных откликов от получателя сообщений на различных этапах процесса передачи сообщений электронной почты по протоколу SMTP.

Физическая (содержательная) постановка задачи. Обмен сообщениями электронной почты между абонентами (клиентами) и почтовым сервером детализирован в модели функционирования сервиса электронной почты. В процессе функционирования сервиса электронной почты, злоумышленник, применяя средства сетевой разведки, инициирует запросы об отправке сообщений электронной почты несуществующему адресату к серверу, подменяя при этом адрес отправителя. Специфика функционирования сервера SMTP вынуждает направлять ответные отклики клиенту о невозможности доставки сообщений. Тем самым злоумышленник способен реализовать два вида сетевых атак: используя SMTP-сервер в качестве прокси сервера осуществляя атаки типа «bounce message» или «backscatter-attack», а также осуществлять поиск валидных (активно используемых) адресов клиентов, атаки типа «trial-n-error attack». Кроме того, сервер обрабатывает запросы от клиента в условиях ограниченного вычислительного ресурса. Ограниченность вычислительного ресурса выражается в том, что сервер способен обработать ограниченное количество запросов за единицу времени без переполнения буфера обмена или же снижения качества обслуживания заявок. Блокирование запросов средств сетевой разведки приводит к компрометации системы защиты, в результате злоумышленник может менять стратегию воздействия. Бескомпроматное функционирование системы защиты, заключающееся в управлении процессом передачи сообщений электрон-

ной почты от средств сетевой разведки, может привести к истощению ресурса средств сетевой разведки.

Управление процессом передачи сообщений электронной почты в разработанном алгоритме основано на управлении потоком данных, реализуемом протоколом SMTP, путем снижения скорости передачи данных между средством сетевой разведки и сервером сообщений электронной почты в течение определенного сеанса. Такая дискриминация трафика осуществляется: путем направления злоумышленнику множества промежуточных откликов через время задержки перед ответным откликом; ограничения количества сегментов данных, передаваемых за один раз (разбиением ответных откликов на фрагменты и передачей их через время задержки); передачей ложных откликов, содержащих код ошибки о постоянной или временной недоступности сервера электронной почты.

Перечисленные параметры передачи сообщений электронной почты позволяют повысить результативность защиты за счет снижения вероятности обнаружения злоумышленником факта использования средств защиты, достигаемой имитацией канала связи с плохим качеством на различных этапах почтовой транзакции, вызывают «истощение» ресурсов у средства сетевой разведки для поддержания состояния соединения, замедляет процесс автоматического сканирования компонентов атакуемого сервиса электронной почты и, как результат, накладывает ограничение на используемый средствами сетевой разведки вычислительный ресурс, что приводит к невозможности средств сетевой разведки осуществлять сетевой информационный обмен.

Таким образом, возникает ряд противоречий:

- между результативностью защиты сервиса электронной почты от сетевой разведки и возможностями средств сетевой разведки по определению структуры сервиса электронной почты, идентификации характеристик средств защиты, имеющих демаскирующие признаки, и их компрометации;
- между наличием необходимости по управлению конфигурацией сервиса электронной почты и отсутствием алгоритмов управления процессом передачи сообщений электронной почты в условиях сетевой разведки.

На устранение указанных противоречий и направлен разработанный алгоритм.

Ограничения и допущения. Информация о легитимности и не легитимности клиентов сервиса электронной почты, устанавливающих соединения, считается достоверной за счет применения комплекса средств защиты. Исходя из определения понятия легитимный, т.е. соответствующий закону, под легитимностью клиента понимается его законное право использовать информационные ресурсы сервиса электронной почты, установленное политиками безопасности, требованиями и рекомендациями по обеспечению безопасности информации. Проверка на легитимность клиента должна производиться перед установлением сетевых соединений с сервером, а также на каждом из этапов почтовой транзакции. Для получения численных оценок процесса защиты от средств сетевой

разведки используется разработанная модель функционирования сервиса электронной почты. Управление процессом передачи сообщений электронной почты заключается в направлении средствам сетевой разведки множества промежуточных откликов через время их задержки перед ответным откликом; ограничения количества сегментов данных, передаваемых за один раз (разбиением ответных откликов на фрагменты и передачей их через время задержки); передачей ложных откликов, содержащих код ошибки о постоянной или временной недоступности сервера электронной почты.

Формализованная постановка задачи соответствует постановке задачи, приведенной выше. Исходные данные, применяемые в алгоритме, приведены в таблице 3.

Таблица 3 – Обозначение и описание основных исходных данных

Переменная	Описание
I_c	счетчик подключений клиента к серверу
I_{cmax}	максимально возможное количество подключений одного клиента к серверу
I_s	счетчик общего количества подключений всех клиентов к серверу
I_{smax}	максимально возможное количество подключений всех клиентов к серверу
R	общее количество промежуточных откликов, на который разделяется ответный отклик несанкционированному клиенту
T	общее количество сформированных значений времени задержки направления промежуточных откликов несанкционированному клиенту
G	общее количество сформированных фрагментов, на которые разделяют ответный отклик несанкционированному клиенту
F	общее количество сформированных значений времени задержки направления фрагментов ответного отклика несанкционированному клиенту
U	общее количество ответных откликов от сервера, на команды несанкционированного клиента, содержащих коды ошибки
N	массив опорных идентификаторов санкционированных отправителей и получателей сообщений электронной почты, к ним относятся доменное имя отправителя, *IP*-адрес отправителя, адреса почтовых ящиков отправителя и получателей (SMTP-receiver) и др.

Теоретической основой алгоритма являются теории систем управления, вероятности, массового обслуживания, исследования операций.

Последовательность действий, реализующих алгоритм проактивной защиты сервиса электронной почты, включает следующие основные этапы (рис. 14).

1. Задают основные исходные данные, обозначение и описание которых приведены в таблице 3.
2. Устанавливают сетевое соединение сервера с клиентом.
3. Увеличивают значение счетчиков I_c и I_s на единицу.
4. Сравнивают значение счетчика I_s с I_{smax} и в случае $I_s \geq I_{smax}$ уменьшают значения I_c и I_s на единицу и завершают соединение.
5. В ином случае принимают команду EHLO.

6. Выделяют идентификаторы клиента *n* (полное доменное имя, дословный адрес (Literal address) клиента).
7. Сравнивают выделенные идентификаторы клиента *n* с идентификаторами из массива опорных идентификаторов *N* и в случае соответствия идентификаторов направляют клиенту ответный отклик и принимают команду MAIL.
8. В ином случае формируют *R* промежуточных откликов и *T* значений времени задержки.
9. Направляют *R* промежуточных откликов через *T* значений времени задержки.
10. В случае получения после отправки промежуточного отклика команды на завершение сетевого соединения от клиента значения I_c и I_s уменьшают на единицу, а сетевое соединение клиента и сервера завершают.
11. В ином случае направляют клиенту ответный отклик.
12. Принимают от клиента команду MAIL.
13. Выделяют идентификаторы *n* клиента (почтовый ящик отправителя).
14. Сравнивают выделенные идентификаторы клиента *n* с идентификаторами из массива опорных идентификаторов *N* и в случае соответствия идентификаторов направляют клиенту ответный отклик и принимают команду RCPT.
15. В ином случае формируют *G* фрагментов ответного отклика и *F* значений времени задержки.
16. Направляют *G* фрагментов ответного отклика через *F* времени задержки.
17. В случае получения после отправки ответного отклика команды на завершение сетевого соединения от клиента значения I_c и I_s уменьшают на единицу, а сетевое соединение клиента и сервера завершают.
18. В ином случае принимают от клиента команду RCPT.
19. Выделяют идентификаторы получателя (почтовый ящик получателя, количество получателей).
20. Сравнивают выделенные идентификаторы получателя *n* с идентификаторами из массива опорных идентификаторов *N* и в случае соответствия идентификаторов принимают от клиента команду, инициирующую передачу почтовых данных.
21. В ином случае формируют *U* откликов с кодом ошибки.
22. Направляют отправителю ответный отклик с кодом ошибки.
23. В случае получения после отправки ответного отклика с кодом ошибки команды на завершение сетевого соединения от клиента значения I_c и I_s уменьшают на единицу, а сетевое соединение клиента и сервера завершают, в ином случае вновь формируют и направляют клиенту *U* откликов с кодом ошибки.
24. Принимают команду, инициирующую передачу почтовых данных.
25. Направляют отправителю ответный отклик.
26. Принимают текст сообщения электронной почты.

27. Завершают почтовую транзакцию.
28. Уменьшают значения I_c и I_s на единицу.
29. Завершают соединение.
30. Формируют отчет.

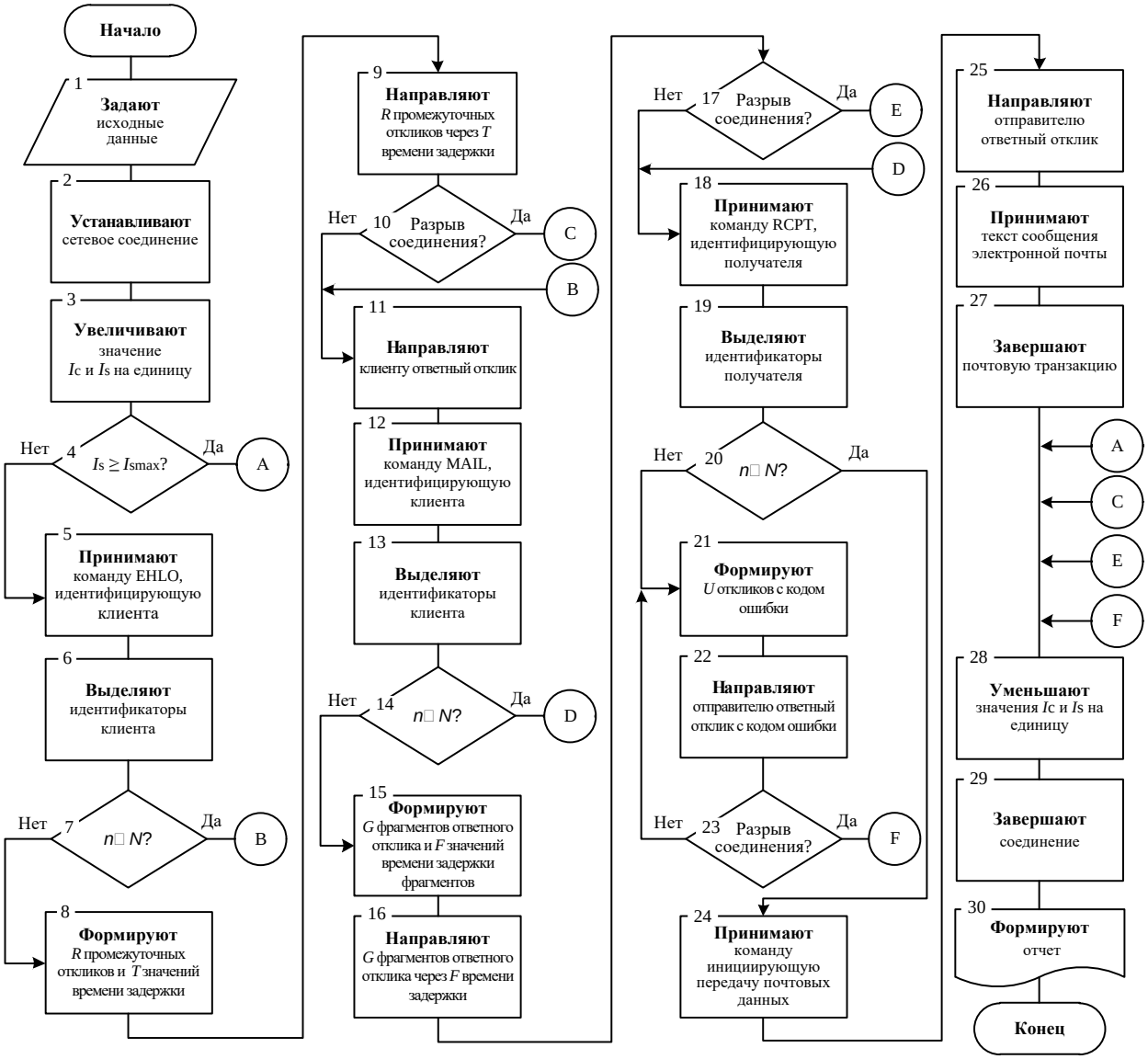


Рис. 14. Блок-схема последовательности действий, реализующих алгоритм проактивной защиты сервиса электронной почты от сетевой разведки

Для исключения компрометации средств защиты по постоянному значению времени задержки промежуточных откликов, значения времени задержки для каждого из промежуточных откликов несанкционированному клиенту, перед отправкой ответного отклика сервером, выбирают в пределах от 1 до 10 с. Количество промежуточных откликов, направляемых несанкционированному клиенту, перед отправкой ответного отклика сервером, выбирают в пределах от 1000 до 20000. Значение времени задержки для каждого из фрагментов ответного отклика, направляемого несанкционированному клиенту, выбирают в пределах от 1 до 15 с. Величину фрагментов, на которые разбивают ответный от-

клик несанкционированному клиенту, выбирают в пределах от 1 до 3 байт. Для каждого ложного ответного отклика несанкционированному клиенту значение кода ошибки выбирают случайным образом из стандартных кодов ошибки протокола SMTP.

Для оценки вероятности простоя средств сетевой разведки и вероятности передачи вредоносного сообщения электронной почты злоумышленником в разработанном алгоритме используется модель функционирования сервиса электронной почты. При этом интенсивность потоков события λ_{12} интерпретируется как интенсивность потока событий на установление сетевого соединения между злоумышленником и почтовым сервером, λ_{34}, λ_{56}, λ_{78} как интенсивности потоков событий по удержанию соединения со злоумышленником после проверки опорных идентификаторов клиентов на соответствующем этапе почтовой транзакции (поступление команд EHLO, MAIL, RCPT).

Рассмотрены следующие ситуации:

C_3 – без замедления передачи сообщений электронной почты от злоумышленника, в этом случае, при идентификации злоумышленника средствами сетевой защиты, сервер в одностороннем порядке разрывает устанавливаемые злоумышленником соединения, для исключения возникновения ситуации отказа в обслуживании и получения вредоносных сообщений электронной почты;

C_4 – с замедлением передачи сообщений электронной почты от злоумышленника на соответствующих этапах почтовой транзакции, в этом случае, при идентификации злоумышленника средствами сетевой защиты, сервер, получая команды от злоумышленника, направляет ему ответные отклики через изменяемые значения времени их замедления или отклики, содержащие код ошибки.

Ситуация C_3, по сути, идентична ситуации C_1, рассмотренной ранее, за исключением того, что в ней отсутствует элемент проверки количества подключений, устанавливаемых злоумышленником. То есть, в случае идентификации злоумышленника как такового, не важно, какое количество подключений он пытается установить, соединение с ним сразу разрывается сервером в одностороннем порядке для исключения ситуации отказа в обслуживании клиентов ввиду перегрузки сервера массовой рассылкой вредоносных сообщений электронной почты. Вследствие чего, в настоящей статье, ситуация C_3 далее детально не рассматривается.

Рассматривая ситуацию C_4, в рамках данной статьи, будут исследованы ситуации:

C_{41} – зависимость равного изменения каждой из интенсивностей потоков событий λ_{34}, λ_{56}, λ_{78} по замедлению передачи злоумышленником сообщений электронной почты на соответствующих этапах почтовой транзакции с целью оценки их влияния на вероятности $p_4(t)$, $p_6(t)$, $p_8(t)$ пребывания системы в состояниях S_4, S_6, S_8 замедления передачи сообщений электронной почты злоумышленником и на вероятность $p_9(t)$ пребывания системы в состоянии S_9 передачи вредоносного сообщения электронной почты;

C_{42} – влияние изменения интенсивностей потоков событий λ_{34}, λ_{56}, λ_{78} по замедлению передачи сообщений электронной почты злоумышленником и одновременное увеличение интенсивностей потоков событий λ_{35}, λ_{57}, λ_{79} по пере-

ходу злоумышленника к очередным этапам почтовой транзакции на вероятностно-временные характеристики пребывания сервиса электронной почты $p_i(t)$ в различных состояниях;

C_{43} – влияние изменения интенсивностей потоков событий по одностороннему разрыву соединений злоумышленником λ_{41}, λ_{61}, λ_{81} в случае компрометации им средств защиты на вероятностно-временные характеристики пребывания сервиса электронной почты $p_i(t)$ в различных состояниях.

Результаты расчетов, представленные на рис. 15, показывают, что интенсивность потока событий λ_{34} по отправке клиентам множества промежуточных ответных откликов, в связи с ошибками представления клиентов почтовому серверу, выявленными при проверке команд EHLO, оказывает значительное влияние на вероятности $p_4(t)$, $p_6(t)$, $p_8(t)$ состояний принудительного удержания злоумышленника в «сетевой ловушке».

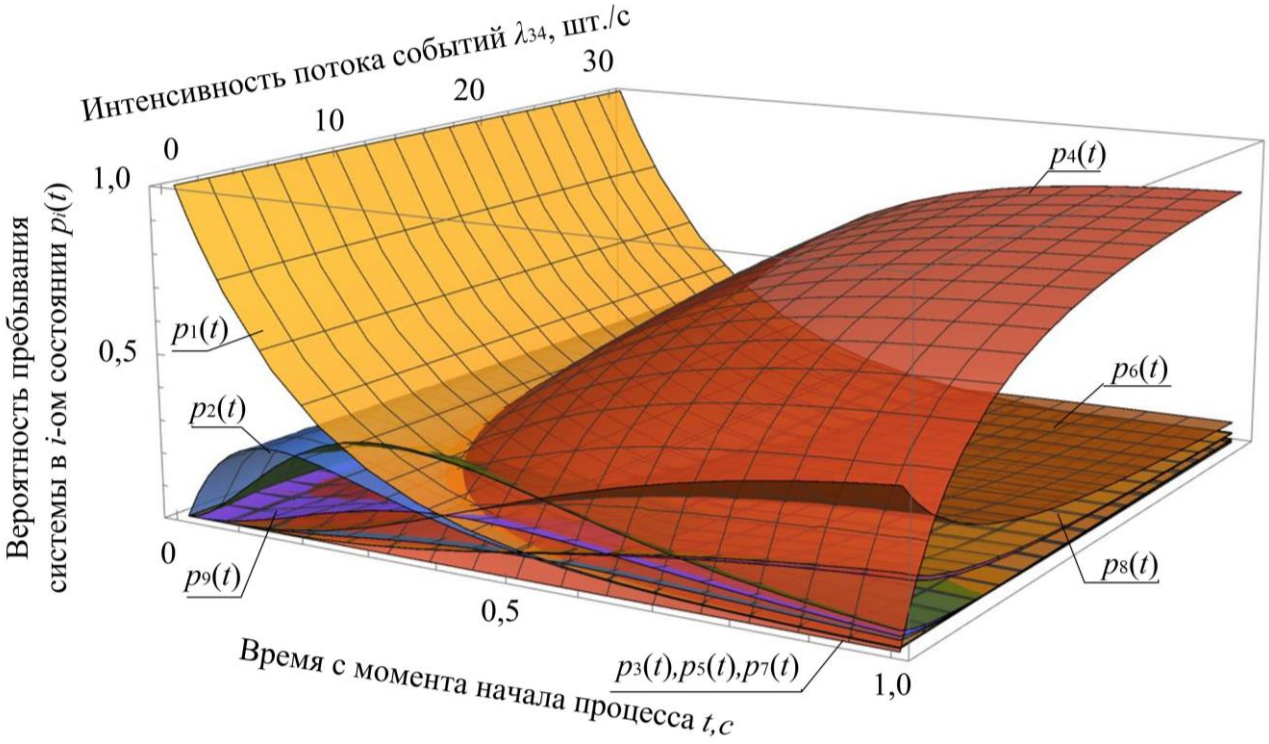


Рис. 15. Результаты расчетов зависимостей вероятностей $p_i(t)$ системы L от интенсивности замедления передачи злоумышленником сообщений электронной почты λ_{34} в ситуации C_{41}

Так, при увеличении значения λ_{34} до 20, система S значительную часть времени находится в состоянии S_4 замедления передачи злоумышленником сообщений электронной почты с финальной вероятностью p_4= 0,786, в то время, как финальная вероятность $p_9(t)$, нахождения системы в состоянии S_9 передачи сообщения злоумышленником, стремится к нулю.

Результаты расчетов (рис.16) показывают, что на величину вероятности $p_6(t)$ замедления передачи злоумышленником сообщений электронной почты посредством отправки множества фрагментов ответного отклика сервера, после

проверки идентификаторов, выделенных из команды MAIL, значительно влияет интенсивность потока событий λ_{56}. Однако, при увеличении значения λ_{56} до 20, система S также находится в состоянии удержания злоумышленника S_6, но значение финальной вероятности $p_6(t)$ составляет величину 0,246, а значение вероятности $p_9(t)$ пребывания системы в состоянии S_9 передачи вредоносного сообщения электронной почты злоумышленником, стремится к нулю.

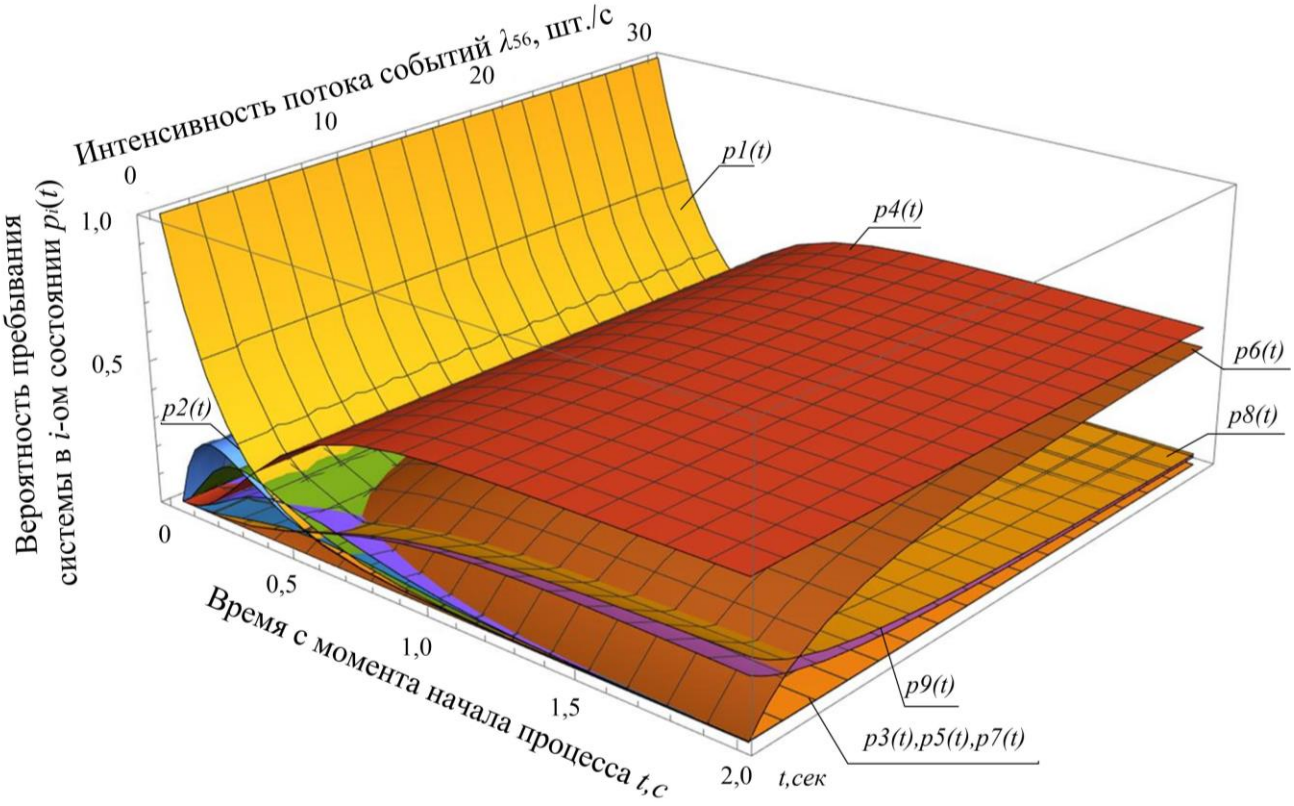


Рис. 16. Результаты расчетов зависимостей вероятностей $p_i(t)$ системы L от интенсивности замедления передачи злоумышленником сообщений электронной почты λ_{56} в ситуации C_{41}

Графическая интерпретация результатов расчета показывает (рис. 17), что интенсивность потока событий по замедлению передачи злоумышленником сообщений электронной почты λ_{78} на третьем этапе проверки легитимности пользователей (после получения команды RCPT) оказывает меньшее влияние как на изменение величины вероятности $p_8(t)$ замедления передачи злоумышленником сообщений электронной почты, так и на величину вероятности успешной реализации почтовой транзакции злоумышленником $p_9(t)$.

Так увеличение значения λ_{56} до 20, приводит к менее интенсивному снижению значения вероятности передачи электронного сообщения злоумышленником $p_9(t)$ до финального значения p_9=0,07, что свидетельствует о большей эффективности применения конкретных механизмов замедления передачи злоумышленником сообщений электронной почты непосредственно на начальных этапах его идентификации в процессе почтовой транзакции.

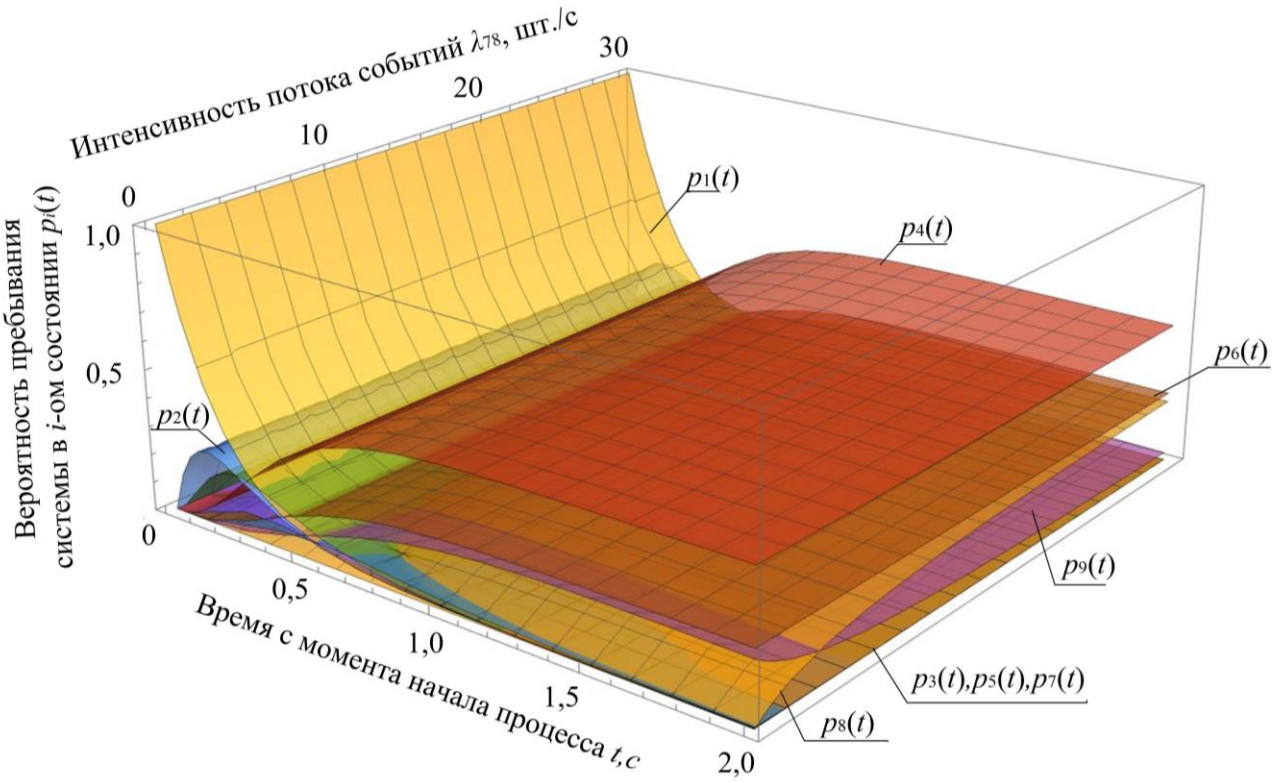


Рис. 17. Результаты расчетов зависимостей вероятностей $p_i(t)$ системы L от интенсивности замедления передачи злоумышленником сообщений электронной почты λ_{78} в ситуации C_{41}

Приведенные на (рис. 18) результаты расчетов, соответствующие ситуации C_{42}, позволяют произвести оценку влияния усилий злоумышленника по преодолению средств сетевой защиты на каждом из этапов почтовой транзакции.

Рассмотрены зависимости вероятностно-временных характеристик от соотношения интенсивностей потоков событий по замедлению передачи злоумышленником сообщений электронной почты λ_{34}, λ_{56}, λ_{78} и интенсивностей потоков событий по переходу к следующим этапам почтовой транзакции λ_{35}, λ_{57}, λ_{79}. Для этого введен относительный показатель q, физически интерпретируемый, как соотношение интенсивности обнаружения злоумышленника системой защиты к интенсивности усилий злоумышленника по обходу средств защиты на каждом из этапов почтовой транзакции (проверка идентификаторов команд EHLO, MAIL, RCPT). Показатель принимает численные значения $q_1 = \lambda_{34}/\lambda_{35}$, $q_2 = \lambda_{56}/\lambda_{57}$, $q_3 = \lambda_{78}/\lambda_{79}$.

Рассмотрим случай, когда относительные показатели на всех этапах почтовой транзакции численно равны между собой, то есть $q = q_1 = \lambda_{34}/\lambda_{35} = q_2 = \lambda_{56}/\lambda_{57} = q_3 = \lambda_{78}/\lambda_{79}$. С ростом значения величины q, то есть с ростом интенсивности обнаружения злоумышленника средствами защиты на каждом этапе почтовой транзакции, значения вероятностей замедления передачи злоумышленником сообщений электронной почты $p_4(t)$, $p_6(t)$, $p_8(t)$ на каждом из этапов почтовой транзакции монотонно растут и достигают максимальных финальных значений (т.к. $p_4+p_6+p_8=1$) при $q=3$, когда система находится лишь в состоянии замедления передачи злоумышленником сообщений электронной почты. При

дальнейшем увеличении соотношения по компрометации злоумышленника (q>3) финальные значения вероятностей состояний по замедлению злоумышленника не изменяются и принимают значения $p_4(t)$=0,713; $p_6(t)$=0,201; $p_8(t)$=0,086.

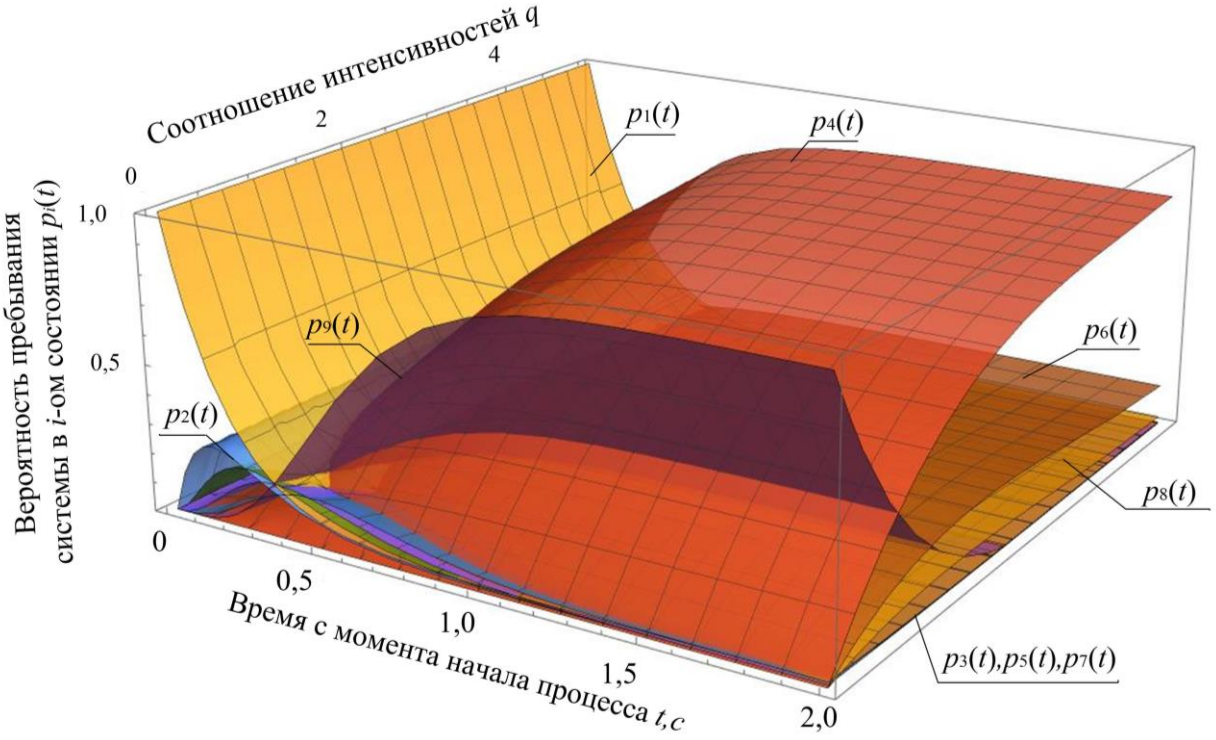


Рис. 18. Результаты расчетов зависимостей вероятностей $p_i(t)$ системы L от соотношения интенсивностей q_1=q_2=q_3=q в ситуации C_{42}

Вероятность успешной передачи сообщения злоумышленником $p_9(t)$ принимает высокие значения [0,2; 0,89] после прохождения переходного процесса (t > 1 с) при значениях относительного показателя q входящего в интервал [0; 1,4].

Таким образом, высокая эффективность функционирования средств проактивной защиты обеспечивается при значениях величины q>1,4.

Длительность пребывания системы L в состояниях S_4, S_6, S_8 зависит от значений интенсивностей λ_{41}, λ_{61}, λ_{81} потоков событий по разрыву соединения злоумышленником в одностороннем порядке на различных этапах почтовой транзакции в случае их компрометации средствами защиты.

Рассмотрим ситуацию C_{43} (рис. 19), в которой интенсивности разрыва соединения злоумышленником на каждом из этапов равны между собой λ_{41}=λ_{61}=λ_{81}.

Результаты расчетов показывают, что по мере роста значений интенсивностей разрыва соединения злоумышленником λ_{41}, λ_{61}, λ_{81} на каждом из этапов до 5 происходит монотонное убывание вероятностей замедления передачи злоумышленником сообщений электронной почты, которые принимают следующие финальные значения: $p_4(t)$=0,122; $p_6(t)$=0,163; $p_8(t)$=0,085, и рост вероятно-

сти $p_9(t)$ успешной передачи сообщения злоумышленником до величины 0,556. Компрометация средств защиты приводит к увеличению интенсивности усилий злоумышленника по разрыву соединений и преодолению средств защиты сервиса электронной почты, функционирующего в условиях сетевой разведки.

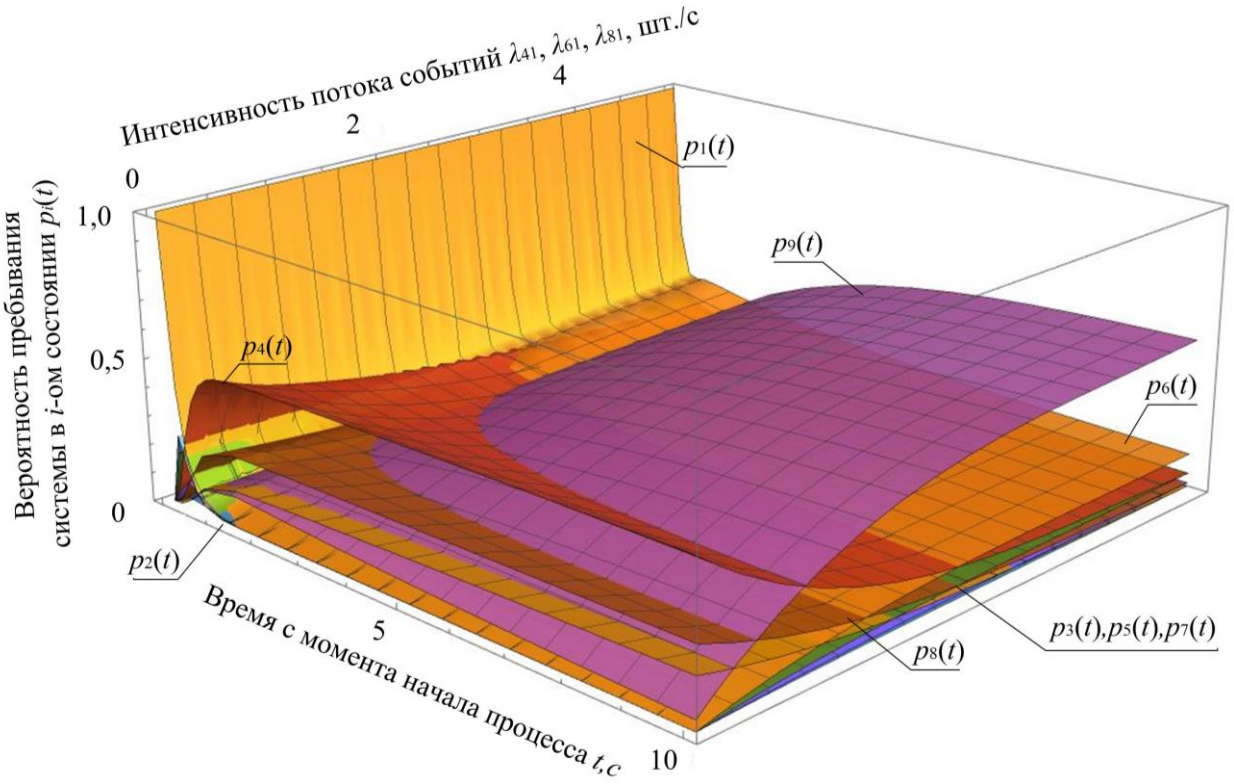


Рис. 19. Результаты расчетов зависимостей вероятностей $p_i(t)$ системы L от интенсивностей $\lambda_{41}=\lambda_{61}=\lambda_{81}$ в ситуации C_{42}

Заключение

Разработанная модель позволяет определять вероятностно-временные характеристики, описывающие функционирование сервиса электронной почты при различных ситуациях управления процессом передачи сообщений электронной почты. Новизна математической модели, по отношению к известным работам [2, 43-51], заключается в следующем:

- во-первых, в формализации функционирования сервиса электронной почты, как случайного процесса посредством применения математического аппарата однородных марковских процессов с дискретными состояниями и непрерывным временем;
- во-вторых, в применении методов динамического программирования для управления процессом передачи сообщений электронной почты с целью обоснования оптимального режима работы сервиса электронной почты;
- в третьих, в оценке асимптотической устойчивости и робастности модели относительно возмущений значений исходных параметров с це-

лью повышения адекватности модели при выборе режимов программного управления процессом передачи сообщений электронной почты.

Разработанный алгоритм позволяет повысить результативность защиты сервиса электронной почты за счет снижения возможностей злоумышленника по компрометации средств защиты, а также перерасхода временного и вычислительного ресурса злоумышленника, достигаемого имитацией канала связи с плохим качеством на различных этапах почтовой транзакции. Новизна разработанного алгоритма по отношению к известным [52-55] состоит в следующем:

- во-первых, в применении модели функционирования сервиса электронной почты, разработанной с использованием методов динамического программирования, математического аппарата однородных марковских процессов с дискретными состояниями и непрерывным временем, методов оценки свойств робастной и асимптотической устойчивости модели;
- во-вторых, в управлении процессом передачи сообщений электронной почты за счет разбиения ответного отклика злоумышленнику на фрагменты и направления этих фрагментов через многочисленные малые интервалы времени задержки, направления ответного отклика злоумышленнику после множества промежуточных откликов, отправленных через многочисленные малые интервалы времени задержки, а также направления злоумышленнику заведомо ложных сообщений о временной или постоянной невозможности продолжения почтовой транзакции.

Литература

1. Давыдов А. Е., Максимов Р. В., Савицкий О. К. Защита и безопасность ведомственных и интегрированных инфокоммуникационных систем. – М.: Воентелеком, 2015. – 520 с.

2. 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.

3. Шерстобитов Р. С., Шарифуллин С. Р., Максимов Р. В. Маскирование интегрированных сетей связи ведомственного назначения // Системы управления, связи и безопасности. 2018. № 4. С. 136–175.

4. Ворончихин И. С., Иванов И. И., Максимов Р. В., Соколовский С. П. Маскирование структуры распределенных информационных систем в киберпространстве // Вопросы кибербезопасности. 2019. № 6(34). С. 92–101.

5. Максимов Р. В., Соколовский С. П., Шарифуллин С. Р., Чернолес В. П. Инновационные информационные технологии в контексте обеспечения национальной безопасности государства // Инновации. 2018. № 3(233). С. 28–35.

6. Sokolovsky S. P., Telenga A. P., Voronchikhin I. S. Moving target defense for securing Distributed Information Systems // Информатика: проблемы, методология, технологии: Сборник материалов XIX международной научно-

методической конференции / под. ред. Д.Н. Борисова. – Воронеж: ВГУ, 2019. С. 639–643.

7. Меньшаков Ю. К. Теоретические основы технических разведок. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2008. – 536 с.

8. Пахомова А. С., Пахомов А. П., Разинкин К. А. К вопросу о разработке структурной модели угрозы компьютерной разведки // Информация и безопасность. 2013. Том 16. № 1. С. 115-118.

9. Вандич А. П., Яичкин М. А., Карганов В. В., Привалов А. А., Скуднева Е. В. К вопросу об организации информационного обмена для повышения защищенности сети передачи данных от технической компьютерной разведки // Труды ЦНИИС. Санкт-Петербургский филиал. 2017. Т. 1. № 4. С. 72-78.

10. Гречишников Е. В., Горелик С. П., Белов А. С. Способ управления защищенностью сетей связи в условиях деструктивных программных воздействий // Телекоммуникации. 2014. № 3. С. 18-22.

11. Язов Ю. К., Сердечный А. Л., Шаров И. А. Методический подход к оцениванию эффективности ложных информационных систем // Вопросы кибербезопасности. 2014. № 1 (2). С. 55-60.

12. Максимов Р. В., Павловский А. В., Стародубцев Ю. И. Защита информации от технических средств разведки в системах связи и автоматизации. – СПб.: ВАС, 2007. – 88 с.

13. Привалов А. А., Скуднева Е. В., Вандич А. П., Яичкин М. А. Метод повышения структурной скрытности сетей передачи данных оперативно технологического назначения ОАО «РЖД» // ТРУДЫ ЦНИИС. Санкт-Петербургский филиал. 2016. № 2 (3). С. 65-74.

14. Бухарин В. В., Кирьянов А. В., Стародубцев Ю. И. Способ защиты вычислительных сетей // Информационные системы и технологии. 2012. № 4 (72). С. 116-121.

15. Сердечный А. Л., Шаров И. А., Сигитов В. Н. Подход к моделированию процесса компьютерной разведки в информационных системах с изменяющимися составом и структурой // REDS: Телекоммуникационные устройства и системы. 2015. Т. 5. № 4. С. 439-443.

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

17. Максимов Р. В., Орехов Д. Н., Соколовский С. П., Барабанов В. В., Ефремов А. А., Ворончихин И. С. Способ защиты вычислительных сетей // Патент на изобретение RU 2696330, опубл. 01.08.19, бюл. № 22. 30 с.

18. Максимов Р. В., Орехов Д. Н., Проскуряков И. С., Соколовский С. П. Способ защиты вычислительных сетей // Патент на изобретение RU 2649789, опубл. 04.04.2018, бюл. № 10. 25 с.

19. Максимов Р. В., Соколовский С. П., Ворончихин И. С. Алгоритм и технические решения динамического конфигурирования клиент-серверных вычислительных сетей // Информатика и автоматизация. 2020. № 5. С. 1018-1049.

20. Максимов Р. В., Соколовский С. П., Ворончихин И. С. Способ защиты вычислительных сетей // Патент на изобретение RU 2716220, опубл. 06.03.20, бюл. № 7. 33 с.

21. Крупенин А. В., Соколовский С. П., Хорев Г. А., Калач А. В. Маскирование идентификаторов канального уровня средств проактивной защиты интегрированных сетей связи специального назначения // Вестник Воронежского института ФСИН России. 2018. № 3. С. 81–89.

22. Кожевников Д. А., Максимов Р. В., Павловский А. В., Юрьев Д. Ю. Способ выбора безопасного маршрута в сети связи (маршруты) // Патент на изобретение RU 2331158, опубл. 10.08.2008, бюл. № 22. 34 с.

23. Максимов Р. В. Модель случайных помех интегрированным системам ведомственной связи // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2008. № 3 (60). С. 151-155.

24. Иванов И. И., Максимов Р. В. Этюды технологии маскирования функционально-логической структуры информационных систем // Инновационная деятельность в Вооруженных Силах Российской Федерации. Труды всеармейской научно-практической конференции. – СПб: ВАС, 2017. С. 147-154.

25. Иванов И. И., Максимов Р. В. Спецификация функциональной модели для расширения пространства демаскирующих признаков в виртуальных частных сетях // Инновационная деятельность в Вооруженных Силах Российской Федерации. Труды всеармейской научно-практической конференции. – СПб: ВАС, 2017. С. 138-147.

26. Берест П. А., Богачев К. Г., Выговский Л. С., Зорин К. М., Игнатенко А. В., Кожевников Д. А., Краснов В. А., Кузнецов В. Е., Максимов Р. В. Способ сравнительной оценки структур информационно-вычислительной сети // Патент RU 2408928, опубл. 10.01.2011, бюл. № 1. 16 с.

27. Андриенко А. А., Кожевников Д. А., Колбасова Г. А., Максимов Р. В., Павловский А. В., Стародубцев Ю. И. Способ (варианты) и устройство (варианты) защиты канала связи вычислительной сети // Патент RU 2306599, опубл. 20.09.2007, бюл. № 26. 56 с.

28. Евстигнеев А. С., Зорин К. М., Карпов М. А., Костырев А. Л., Максимов Р. В., Орлов Е. В., Павловский А. В. Способ мониторинга безопасности автоматизированных систем // Патент RU 2355024, опубл. 10.05.2009, бюл. № 13. 15 с.

29. Андриенко А. А., Куликов О. Е., Костырев А. Л., Максимов Р. В., Павловский А. В., Лебедев А. Ю., Колбасова Г. С. Способ контроля информационных потоков в цифровых сетях связи // Патент RU 2267154, опубл. 27.12.2005, бюл. № 36. 16 с.

30. Singh A., Gahlawat M. Electronic Mail Security // International Journal of Advanced Recearch in Computer Engineering and Technology (IJARCET). 2013. pp. 71-76.

31. Горбачев А. А., Казьмин Г. Ю. Обоснование задачи динамического управления сетевыми соединениями для предотвращения массовой рассылки

спама // Информатика: проблемы, методология, технологии: Сборник материалов XX международной научно-методической конференции / под. ред. Д.Н. Борисова. – Воронеж: ВГУ, 2020. С. 946-955.

32. Горбачев А. А., Лавренов Д. В. Алгоритм защиты информационных систем от массовой рассылки спама на основе управления сетевыми соединениями // Информатика: проблемы, методология, технологии: Сборник материалов XX международной научно-методической конференции / под. ред. Д.Н. Борисова. – Воронеж: ВГУ, 2020. С. 956-963.

33. Kumari A., Agrawal N., Umesh L. Attack over Email System: Review // International Journal of Scientific Research and Engineering Trends. 2017. pp. 200-206.

34. Bencsath B., Ronai M. A. Empirical Analysis of Denial of Service Attack Against SMTP Servers // Proceedings of The 2007 International Symposium on Collaborative Technologies and Systems. 2007. pp. 72-79.

35. Walla S., Rossow C. MALPITY: Automatic identification and Exploitation of Tarpit Vulnerabilities in Malware // 2019 IEEE European Symposium on Security and Privacy (EuroS&P). 2019. pp. 590-605.

36. Hunger T., Terry P., Judge A. Distributed Tarpitting: Impeding Spam Across Multiple Servers // Proceedings of the 17th Large Installation Systems Administration Conference. 2003. pp. 223-236.

37. Соколовский С. П., Орехов Д. Н. Концептуализация проблемы проактивной защиты интегрированных информационных систем // Научные чтения имени профессора Н.Е. Жуковского: сборник научных статей VIII Международной научно-практической конференции. – Краснодар: КВВУ, 2018. С. 47–52.

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

39. Eggendorger T., Keller J. Combining SMTP and HTTP tar pits to proactively reduce spam // Proceedings of the 2006 International Conference on Security & Management. 2006. pp. 1-7.

40. Соколовский С. П., Горбачев А. А. Способ проактивной защиты почтового сервера от нежелательных сообщений электронной почты // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2021. № 3-4 (153-154). С. 31-40.

41. Максимов Р. В., Соколовский С. П., Починок В. В., Горбачев А. А., Теленьга А. П., Шерстобитов Р. С. Способ защиты вычислительных сетей // Патент на изобретение RU 2745004, опубл. 18.03.21, бюл. № 8. 27 с.

42. Макаренко С. И., Михайлов Р. Л. Информационные конфликты – анализ работ и методологии исследования // Системы управления, связи и безопасности. 2016. № 3. С. 95–178.

43. Выговский Л. С., Максимов Р. В. Модель преднамеренных деструктивных воздействий на информационную инфраструктуру интегрированных систем связи // Информатика, телекоммуникации и управление. 2009. № 1 (73). С. 181-187.

44. Выговский Л. С., Максимов Р. В. Модель преднамеренных деструктивных воздействий на информационную инфраструктуру интегрированных систем связи // Информатика, телекоммуникации и управление. 2008. № 3 (60). С. 166-173.

45. Стародубцев Ю. И., Ерышов В. Г., Корсунский А. С. Модель процесса мониторинга безопасности информации в информационно-телекоммуникационных системах // Автоматизация процессов управления. 2011. № 1 (23). С. 58-61.

46. Евглевская Н. В., Привалов А. А., Скуднева Е. В. Марковская модель конфликта автоматизированных систем обработки информации и управления с системой деструктивных воздействий нарушителя // Известия Петербургского университета путей сообщения. 2015. № 1 (42). С. 78-84.

47. Иванов И. И. Модель функционирования распределенных информационных систем при использовании маскированных каналов связи // Системы управления, связи и безопасности. 2020. № 1. С. 198-234. DOI: 10.24411/2410-9916-2020-10107.

48. Иванов К. В. Марковские модели средств защиты автоматизированных систем специального назначения // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. 2007. № 39. С. 10-19.

49. Козлитин С. Н., Козирацкий Ю. Л., Будников С. А. Моделирование совместного применения средств радиоэлектронной борьбы и огневого поражения в интересах повышения эффективности борьбы за превосходство в управлении // Системы управления, связи и безопасности. 2020. № 1. С. 49-73. DOI: 10.24411/2410-9916-2020-00001.

50. Гречишников Е. В., Добрышин М. М., Закалкин П. В. Модель узла доступа VPN как объекта сетевой и потоковой компьютерных разведок и DDOS-атак // Вопросы кибербезопасности. 2016. № 3 (16). С. 4-12.

51. Язов Ю. К., Бурушкин А. А., Панфилов А. П. Марковские модели процессов реализации сетевых атак типа «отказ в обслуживании» // Информационная безопасность. 2008. № 1. С. 79-84.

52. 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 на изобретение RU 2318296, опубл. 27.02.08, бюл. № 6. 5 с.

53. Рыбалко Р. В. Система анализа протоколов передачи данных с целью нейтрализации программ, рассылающих спам // Патент на полезную модель RU 101234, опубл. 10.01.2011. 23 с.

54. Небольсин В. А. Предотвращение несанкционированной массовой рассылки электронной почты // Патент на изобретение RU 2472308, опубл. 10.01.13, бюл. № 1. 1 с.

55. Wilbert de Graaf, Chandresh K. Jein. Response delay management using connection information. Patent US, no. 2007/0220600, Publish. 20.09.2007.

56. RFC 5321. Simple Mail Transport Protocol. 2008. [Электронный ресурс]. 21.04.2021. – URL: https://tools.ietf.org/html/rfc5321 (дата обращения 21.04.2021).

57. Гнеденко Б. В., Коваленко И. Н. Введение в теорию массового обслуживания. – М.: Наука, 1966. – 431 с.

58. Розанов Ю. А. Случайные процессы. – М.: Наука, 1971. – 286 с.

59. Вержбицкий В. М. Основы численных методов. – М.: Высшая школа, 2002. – 840 с.

References

1. Davydov A. E., Maksimov R. V., Savitsky O. K. *Zashchita i bezopasnost' vedomstvennyh i integrirovannyh infokommunikacionnyh sistem* [Protection and security of departmental and integrated information and communication systems]. Moscow, Voentelekom Publ., 2015. 520 p. (In Russian).

2. Maximov R. V., Orekhov D. N., Sokolovsky S. P. Model and Algorithm of Client-Server Information System Functioning in Network Intelligence Conditions. *Systems of Control, Communication and Security*, 2019, no. 4, pp. 50-99. DOI: 10.24411/2410-9916-2019-10403 (in Russian).

3. Sherstobitov R. S., Sharifullin S. R., Maksimov R. V. Masking of integrated communication networks for institutional purposes. *Systems of Control, Communication and Security*, 2019, no. 4, pp. 136–175 (in Russian).

4. Voronchihin I. S., Ivanov I. I., Maksimov R. V., Sokolovskij S. P. Masking the structure of distributed information systems in cyberspace. *Voprosy kiberbezopasnosti*, 2019, vol. 6, no. 34, pp. 92–101 (in Russian).

5. Maximov R. V., Sokolovsky S. P., Sharifullin S. R., Chernoles V. P. Innovative information technologies in the context of ensuring national security of the state. *Innovations*, 2018, vol. 3, no. 233, pp. 28–35 (in Russian).

6. Sokolovsky S. P., Telenga A. P., Voronchikhin I. S. Moving target defense for securing Distributed Information Systems. *Informatika: problemy, metodologiia, tekhnologii. Sbornik materialov XIX mezhdunarodnoi nauchno-metodicheskoi konferentsii* [Informatics: problems, methodology, technologies: collection of materials of the XIX international scientific and methodological conference]. Voronezh, Voronezh State University, 2019, pp. 639–643.

7. Menshakov Yu. K. *Teoreticheskie osnovy tekhnicheskih razvedok* [Theoretical foundations of technical intelligence]. Moscow, Bauman Moscow State Technical University Publ., 2008. 536 p. (In Russian).

8. Pakhomova A. S., Pakhomov A. P., Razinkin K. A. On the development of a structural model of the threat of computer intelligence. *Information and security*, 2013, vol. 16, no. 1, pp. 115-118 (in Russian).

9. Vandich A. P., Yaichkin M. A., Karganov V. V., Privalov A. A., Skudneva E. V. On the issue of the organization of information exchange for improving the security of the data transmission network from technical computer intelligence. *Trudy CNIIS. Sankt-Peterburgskij filial*, 2017, vol. 1, no. 4, pp. 72-78 (in Russian).

10. Grechishnikov E. V., Gorelik S. P., Belov A. S. A method for managing the security of communication networks in the conditions of destructive software impacts. *Telekommunikatsii*, 2014, no. 3, pp. 18-22 (in Russian).

11. Yazov Yu. K., Serdny A. L., Sharov I. A. Methodological approach to evaluating the effectiveness of false information systems. *Voprosy kiberbezopasnosti*, 2014, vol. 1, no. 2, pp. 55-60 (in Russian).

12. Maksimov R. V., Pavlovsky A. V., Starodubtsev Yu. I. *Zashchita informacii ot tekhnicheskih sredstv razvedki v sistemah svyazi i avtomatizacii* [Protection of information from technical means of intelligence in communication and automation systems]. St. Petersburg, Military Telecommunications Academy Publ., 2007. 88 p. (In Russian).

13. Privalov A. A., Skudneva E. V., Vandich A. P., Yaichkin M. A. Method of increasing the structural secrecy of data transmission networks for operational and technological purposes of JSC "Russian Railways". *TRUDY CNIIS. Sankt-Peterburgskij filial*, 2016, no 2 (3), pp. 65-74 (in Russian).

14. Bukharin V. V., Kiryanov A. V., Starodubtsev Yu. I. A method for protecting computer networks. *Information Systems and Technologies*, 2012, no. 4 (72), pp. 116-121 (in Russian).

15. Serdechnyj A. L., SHarov I. A., Sigitov V. N. Approach to modeling the process of computer intelligence in information systems with changing composition and structure. *REDS: Telekommunikacionnye ustrojstva i sistemy*, 2015, vol. 5, no. 4, pp. 439-443 (in Russian).

16. Maximov R. V., Sokolovsky S. P., Gavrilov L. A. Hiding computer network proactive security tools unmasking features. *Selected Papers of the VIII All-Russian Conference with International Participation «Secure Information Technologies»*, Moscow, Bauman Moscow State Technical University, 2017. pp. 88-92 (in Russian).

17. Maksimov R. V., Orekhov D. N., Sokolovskij S. P., Barabanov V. V., Efremov A. A., Voronchihin I. S. Method of Protection of Computer Networks. Patent Russia, no. RU 2696330. Publish. 01.08.2019, bul. no. 22 (in Russian).

18. Maksimov R. V., Orekhov D. N., Proskuryakov I. S., Sokolovskij S. P. Method for protecting computer networks. Patent Russia, no. RU 2649789. Publish. 04.04.2018, bul. no. 10 (in Russian).

19. Maksimov R. V., Sokolovskij S. P., Voronchihin I. S. Algorithm and technical solutions for dynamic configuration of client-server computer networks. *Informatics and Automation*, 2020, no. 5, pp. 1018-1049 (in Russian).

20. Maksimov R. V., Sokolovskij S. P., Voronchihin I. S. Method for protecting computer networks. Patent Russia, no. RU 2716220. Publish. 06.03.2020, bul. no. 7 (in Russian).

21. Krupenin A. V., Sokolovskij S. P., Horev G. A., Kalach A. V. Masking of channel-level identifiers for proactive protection of integrated special-purpose communication networks. *Vestnik Voronezhskogo instituta FSIN Rossii*, 2018, no. 3, pp. 81–89 (in Russian).

22. Kozhevnikov D. A., Maksimov R. V., Pavlovskij A. V., Yur'ev D. Yu. The method of choosing a safe route in the communication network (routes). Patent Russia, no. RU 2331158. Publish. 10.08.2008, bul. no. 22 (in Russian).

23. Maksimov R. V. Random interference model for integrated departmental communication systems. *Computing, Telecommunications and Control*, 2008, vol. 3, no. 60, pp. 151-155 (in Russian).

24. Ivanov I. I., Maksimov R. V. Etyudy tekhnologii maskirovaniya funkcional'no-logicheskoj struktury informacionnyh sistem [Etudes of the technology of masking the functional and logical structure of information systems]. *Innovacionnaya deyatel'nost' v Vooruzhennyh Silah Rossijskoj Federacii. Trudy vsearmejskoj nauchno-prakticheskoj konferencii*, 2017, Saint Peterburg, Mititary Telecommunications Academy, 2017, pp. 147-154 (in Russian).

25. Ivanov I. I., Maksimov R. V. Specifikaciya funkcional'noj modeli dlya rasshireniya prostranstva demaskiruyushchih priznakov v virtual'nyh chastnyh setyah [Specification of a functional model for expanding the space of unmasking features in virtual private networks]. *Innovacionnaya deyatel'nost' v Vooruzhennyh Silah Rossijskoj Federacii. Trudy vsearmejskoj nauchno-prakticheskoj konferencii*, 2017, Saint Peterburg, Mititary Telecommunications Academy, 2017, pp. 138-147 (in Russian).

26. Berest P. A., Bogachev K. G., Vygovskij L. S., Zorin K. M., Ignatenko A. V., Kozhevnikov D. A., Krasnov V. A., Kuznecov V. E., Maksimov R. V. Method of comparative evaluation of information and computer network structures. Patent Russia, no. RU 2408928. Publish. 10.01.2011, bul. no. 1 (in Russian).

27. Andrienko A. A., Kozhevnikov D. A., Kolbasova G. A., Maksimov R. V., Pavlovskij A. V., Method (options) and device (options) for protecting the communication channel of a computer network. Patent Russia, no. RU 2306599. Publish. 20.09.2007, bul. no. 26 (in Russian).

28. Evstigneev A. S., Zorin K. M., Karpov M. A., Kostyrev A. L., Maksimov R. V., Orlov E. V., Pavlovskij A. V. Method for monitoring the security of automated systems. Patent Russia, no. RU 2355024. Publish. 10.05.2009, bul. no. 13 (in Russian).

29. Andrienko A. A., Kulikov O. E., Kostyrev A. L., Maksimov R. V., Pavlovskij A. V., Lebedev A. Yu., Kolbasova G. S. A method for controlling information flows in digital communication networks. Patent Russia, no. RU 2267154. Publish. 27.12.2005, bul. no. 36 (in Russian).

30. Singh A., Gahlawat M. Electronic Mail Security. *International Journal of Advanced Recearch in Computer Engineering and Technology (IJARCET)*, 2013, pp. 71-76.

31. Gorbachev A. A., Kaz'min G. Yu. Obosnovanie zadachi dinamicheskogo upravleniya setevymi soedineniyami dlya predotvrashcheniya massovoj rassylki spama [Justification of the task of dynamic network connection control to prevent mass spam distribution]. *Informatika: problemy, metodologiia, tekhnologii. Sbornik materialov XIX mezhdunarodnoi nauchno-metodicheskoi konferentsii* [Informatics: problems, methodology, technologies: collection of materials of the XIX international

scientific and methodological conference]. Voronezh, Voronezh State University, 2020, pp. 946-955 (in Russian).

32. Gorbachev A. A., Lavrenov D. V. Algoritm zashchity informacionnyh sistem ot massovoj rassylki spama na osnove upravleniya setevymi soedineniyami [Algorithm for protecting information systems from mass spam distribution based on network connection management]. *Informatika: problemy, metodologiia, tekhnologii. Sbornik materialov XIX mezhdunarodnoi nauchno-metodicheskoi konferentsii* [Informatics: problems, methodology, technologies: collection of materials of the XIX international scientific and methodological conference]. Voronezh, Voronezh State University, 2020, pp. 956-963 (in Russian).

33. Kumari A., Agrawal N., Umesh L. Attack over Email System: Review. *International Journal of Scientific Research and Engineering Trends*, 2017, pp. 200-206.

34. Bencsath B., Ronai M. A. Empirical Analysis of Denial of Service Attack Against SMTP Servers. *Proceedings of The 2007 International Symposium on Collaborative Technologies and Systems,* 2007, pp. 72-79.

35. Walla S., Rossow C. MALPITY: Automatic identification and Exploitation of Tarpit Vulnerabilities in Malware. *2019 IEEE European Symposium on Security and Privacy (EuroS&P),* 2019, pp. 590-605.

36. Hunger T., Terry P., Judge A. Distributed Tarpitting: Impeding Spam Across Multiple Servers. *Proceedings of the 17th Large Installation Systems Administration Conference*, 2003, pp. 223-236.

37. Sokolovskij S. P., Orekhov D. N. Konceptualizaciya problemy proaktivnoj zashchity integrirovannyh informacionnyh sistem [Conceptualization of the problem of proactive protection of integrated information systems]. *Nauchnye chteniya imeni professora N.E. Zhukovskogo* [scientific readings named after Professor N. E. Zhukovsky]. Krasnodar, Krasnodar Higher Military School named after General of the Army S.M. Shtemenko, 2018, pp. 47–52 (in Russian).

38. Kovalev S. S., Shishaev M. G. Modern methods of protection against unwanted mailings. *Trudy Kol'skogo nauchnogo centra RAN*, 2011, vol. 7, pp. 100-111 (in Russian).

39. Eggendorger T., Keller J. Combining SMTP and HTTP tar pits to proactively reduce spam. *Proceedings of the 2006 International Conference on Security & Management*, 2006, pp. 1-7.

40. Sokolovskij S. P., Gorbachev A. A. Sposob proaktivnoj zashchity pochtovogo servera ot nezhelatel'nyh soobshchenij elektronnoj pochty [A way to proactively protect the mail server from unsolicited email messages]. *Enginery Problems. Series 16. Anti-Terrorist Engineering Means*, 2021, vol. 3-4, no. 153-154, pp. 31-40 (in Russian).

41. Maksimov R. V., Sokolovskij S. P., Pochinok V. V., Gorbachev A. A., Telen'ga A. P., Sherstobitov R. S. Method for protecting computer networks. Patent Russia. no. RU 2745004, Publish. 18.03.21, bul. no. 8 (in Russian).

42. Makarenko S. I., Mikhailov R. L. Information conflicts - analysis of works and research methodology. *Systems of Control, Communication and Security*, 2016, no. 3, pp. 95-178 (in Russian).

43. Vygovskij L. S., Maksimov R. V. Model of deliberate destructive impacts on the information infrastructure of integrated communication systems. *Computing, Telecommunications and Control*, 2009, vol. 1, no. 73, pp. 181-187 (in Russian).

44. Vygovskij L. S., Maksimov R. V. Model of deliberate destructive impacts on the information infrastructure of integrated communication systems. *Computing, Telecommunications and Control*, 2008, vol. 3, no. 60, pp. 166-173 (in Russian).

45. Starodubtsev Yu. I., Eryshov V. G., Korsunsky A. S. Model of the process of monitoring information security in information and telecommunications systems. *Automation of Control Processes*, 2011, no. 1 (23), pp. 58-61 (in Russian).

46. Yevglevskaya N. V., Privalov A. A., Skudneva E. V. Markov model of conflict of automated information processing and management systems with the system of destructive influences of the violator. *Izvestiya Peterburgskogo universiteta putej soobshcheniya*, 2015, no. 1 (42), pp. 78-84 (in Russian).

47. Ivanov I. I. Distributed Information Systems Functioning Model with Masked Communication Links. *Systems of Control, Communication and Security*, 2020, no. 1, pp. 198-234. DOI: 10.24411/2410-9916-2020-10107 (in Russian).

48. Ivanov K. V. Markov models of means of protection of automated systems of special purpose. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2007, no. 39, pp. 10-19 (in Russian).

49. Kozlitin S. N., Koziratsky Yu. L., Budnikov S. A. Electronic warfare and fire damage means joint use modeling for improving a superiority of control struggle efficiency. *Systems of Control, Communication and Security*, 2020, no. 1, pp. 49-73. DOI: 10.24411/2410-9916-2020-00001 (in Russian).

50. Grechishnikov E. V., Dobryshin M. M., Zakalkin P. V. Model of a VPN access node as an object of network and streaming computer intelligence and DDOS attacks. *Voprosy kiberbezopasnosti*, 2016, no. 3 (16), pp. 4-12 (in Russian).

51. Yazov Yu. K., Burushkin A. A., Panfilov A. P. Markov models of processes for implementing network attacks of the "denial of service" type. *Informacionnaya bezopasnost'*, 2008, no. 1, pp. 79-84 (in Russian).

52. Borisov M. A., Kozhevnikov D. A., Maksimov R. V., Osadchij A. I., Pavlovskij A. V., Starodubcev G. Yu., Hudajnazarov Yu. K. A method for protecting a local computer network when transmitting e-mail messages via a global information network. Patent Russia, no. RU 2318296. Publish. 27.02.2008, bul. no. 6 (in Russian).

53. Rybalko R. V. A system for analyzing data transmission protocols in order to neutralize programs that send spam. Patent Russia, no. RU 101234. Publish. 10.01.2011. (In Russian).

54. Nebol'sin V. A. Preventing unauthorized mass email distribution. Patent Russia, no. RU 2472308. Publish. 10.01.2013, bul. no. 1 (in Russian).

55. Wilbert de Graaf, Chandresh K. Jein. Response delay management using connection information. Patent US no. 2007/0220600. Publish. 20.09.2007.

56. RFC 5321. Simple Mail Transport Protocol. *Tools*, 21 April 2021. Available at: https://tools.ietf.org/html/rfc5321 (accessed 21 April 2021).

57. Gnedenko B. V., Kovalenko I. N. *Vvedenie v teoriyu massovogo obsluzhivaniya* [Introduction to Queuing Theory]. Moscow, Nauka Publ., 1966. 431 p. (In Russian).

58. Rozanov Yu. A. *Sluchajnye processy* [Random processes]. Moscow, Nauka Publ., 1971. 286 p. (In Russian).

59. Verzhbickij V. M. *Osnovy chislennyh metodov* [Fundamentals of numerical methods]. Moscow, Vysshaya shkola Publ., 2002. 840 p. (In Russian).

Статья поступила 11 мая 2021 г.

Информация об авторах

Горбачев Александр Александрович – соискатель ученой степени кандидата технических наук. Адъюнкт. Краснодарское высшее военное училище им. генерала армии С.М. Штеменко. Область научных интересов: обеспечение информационной безопасности; синтез и системный анализ систем защиты информации критически важных объектов; маскирование информационных ресурсов интегрированных ведомственных сетей связи. E–mail: infosec23.00@mail.ru

Соколовский Сергей Петрович – кандидат технических наук, доцент, докторант. Краснодарское высшее военное училище им. генерала армии С.М. Штеменко. Область научных интересов: обеспечение информационной безопасности; синтез и системный анализ систем защиты информации критически важных объектов; маскирование информационных ресурсов интегрированных ведомственных сетей связи. E–mail: mtd.krd@mail.ru

Усатиков Сергей Васильевич – доктор физико-математических наук, доцент. Профессор кафедры. Краснодарское высшее военное училище им. генерала армии С.М. Штеменко. Область научных интересов: математическое моделирование. E–mail: sv@usatikov.com

Адрес: 350063, Россия, г. Краснодар, улица Красина, д. 4.

Functioning model and algorithm of email service proactive protection from network intelligence

A. A. Gorbachev, S. P. Sokolovsky, S. V. Usatikov

***Purpose**: Existing threats to the information security of the e-mail service are caused by the reactivity of the applied security tools that analyze the content of electronic messages, SMTP protocol capabilities and the peculiarities of the impact of network intelligence tools. The inertia properties of the applied security tools do not fully ensure the email service's protection against network intelligence and computer attacks. The aim of the work is to develop a model and an algorithm that allows you to quickly serve the maximum number of requests from authorized clients of e-mail service while reducing the quality of service requests from network intelligence tools by controlling the process of messaging. **Methods** used: the solution to the problem of managing thee-mail service operation process in conditions of network intelligence at various stages of a mail transaction by managing the resource capabilities of network intelligence facilities at the application level, which consists in representing the process of their interaction as a Markov random process with discrete states and continuous time, using dynamic programming methods, as well as numerical*

methods. The elements of novelty of the presented model are the application of the mathematical apparatus of homogeneous Markov chains with continuous time, taking into account the asymptotic stability and robustness properties, to justify the choice of optimal modes of e-mail messages transmission at various stages of the e-mail transaction. The ***novelty*** *of the presented algorithm of e-mail service proactive protection from network intelligence consists in the application of the model of e-mail service functioning, based on the use of the mathematical apparatus of homogeneous Markov chains with continuous time, to control the resource possibilities of intelligence means during the e-mail messages transfer at various stages of the mail transaction.* ***Result****: The calculations show an increase in the availability of e-mail service information resources to clients, due to the management of the process of transferring e-mail messages. The presented algorithm makes it possible to improve the efficiency of protection by reducing the ability of the attacker to detect the fact of the use of security features and identification of their characteristics, as well as by managing the resource capabilities of intelligence tools at various stages of the e-mail transaction by simulating a communication channel with poor quality.* ***Practical significance****: consists in finding the probabilistic and temporal characteristics describing the process of e-mail service operation at various stages of the mail transaction. The practical significance of the presented algorithm consists in solving the problem of optimal management of the e-mail transmission process, which provides management of computing and temporal resources of network intelligence tools, as well as reducing the possibility of compromising the security tools and identification of their characteristics.*

Key words: *network intelligence, email service, proactive protection, resilience, random process, denial of service.*

Information about Authors

Alexander Alexandrovich Gorbachev – post graduate student. Krasnodar Higher Military School named after General of the Army S.M. Shtemenko. Research interests: information security; synthesis and system analysis of information security systems of critical objects; masking and simulation of information resources of integrated departmental communication networks. E–mail: infosec23.00@mail.ru

Sergey Petrovich Sokolovsky – Ph.D. of Engineering Sciences, Associate Professor. Doctoral Candidate. Krasnodar Higher Military School named after General of the Army S.M. Shtemenko. Research interests: information security; synthesis and system analysis of information security systems of critical objects; masking and simulation of information resources of integrated departmental communication networks. E–mail: mtd.krd@mail.ru

Sergey Vasilyevich Usatikov – Dr. habil. of Physical and Mathematical Sciences, Associate Professor. Professor a Department. Krasnodar Higher Military School named after General of the Army S.M. Shtemenko. Field of research: mathematical modeling. E–mail: sv@usatikov.com

Address: Russia, 350063, Krasnodar, Krasina Street, 4.