

УДК 004.738.5

Модель функционирования распределенных информационных систем при использовании маскированных каналов связи

Иванов И. И.

Постановка задачи: Зная демаскирующие признаки информационных направлений и их информативность, злоумышленник может реконструировать структуру информационной системы (ИС) с высокой степенью подобия ее реальной структуре. Известны способы защиты структуры информационных систем от исследования путем маскирования (скрытия) реальной структуры и навязывания злоумышленнику ложной. Для этого в структуру информационных систем, осуществляющих информационное взаимодействие, вводят логическую избыточность на канальном и сетевом уровнях за счет динамического изменения IP- и MAC-адресов абонентов в передаваемых пакетах сообщений. Использование таких способов маскирования позволяет ввести злоумышленника в заблуждение относительно реальной структуры и алгоритмов функционирования информационных систем. **Целью работы** является разработка модели функционирования распределенных информационных систем при использовании маскированных вышеуказанным образом каналов связи в интересах формирования математического обеспечения протокола динамического управления множеством маскированных каналов связи. **Используемые методы:** решение задачи исследования процесса функционирования распределенных информационных систем в условиях компьютерной разведки при различных стратегиях взаимодействующих сторон, а также управления (установления и поддержания) маскированных соединений, заключается в представлении процесса их взаимодействия в виде марковского случайного процесса с дискретными состояниями и непрерывным временем. **Новизна:** элементами новизны представленной модели является применение математического аппарата теории марковских случайных процессов и решение уравнений Колмогорова для исследования задачи защиты распределенной ИС, использующей маскированные каналы связи, от дестабилизирующих воздействий как естественного (помехи в канале связи), так искусственного характера (атаки средств сетевой компьютерной разведки, ориентированные на вскрытие реальной структуры распределенной ИС). **Результат:** использование представленного решения позволяет повысить результативность защиты и эффективность функционирования наложенной виртуальной частной сети за счет формирования многоточечных маскированных каналов связи и динамического управления ими. **Практическая значимость** заключается в нахождении вероятностных и временных характеристик, описывающих состояния процесса функционирования информационных систем при использовании маскированных каналов связи при различных стратегиях информационного взаимодействия. Представленное решение предлагается реализовать в виде математического обеспечения протокола динамического управления множеством маскированных каналов связи для телекоммуникационного оборудования (маршрутизаторов), обеспечивающего маршрутизацию криптографически преобразованных пакетов сообщений.

Ключевые слова: распределенная информационная система, компьютерная разведка, маскированный канал, сетевой протокол.

Библиографическая ссылка на статью:

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.

Reference for citation:

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).

Актуальность

Процессы реформирования социально-экономической политики Российской Федерации связаны с необходимостью обеспечения национальной безопасности в информационной сфере. В связи с этим в Доктрине информационной безопасности отмечается, что основные информационные угрозы вызваны глобализацией и трансграничностью информационной инфраструктуры, а преодоление и предупреждение этих угроз предполагает [1]:

- совершенствование системы обеспечения информационной безопасности;
- инновационное развитие отрасли информационных технологий;
- ликвидацию зависимости отечественной промышленности от зарубежных информационных технологий;
- создание и внедрение информационных технологий, изначально устойчивых к различным видам воздействия.

Решение перечисленных задач позволит обеспечить устойчивое и бесперебойное функционирование информационной инфраструктуры России [2, 3] в условиях дестабилизирующих воздействий (ДВ).

Злоумышленник осуществляет некоторую совокупность дестабилизирующих воздействий с использованием всего арсенала доступных ему средств и стремится влиять на качество решений, принимаемых оппонентом (системой защиты) [4-9]. Для этого он реализует действия, которые можно условно расположить в диапазоне от перехвата управления информационной системой (ИС) до перевода ее в неисправное состояние (атаки типа «отказ в обслуживании»). Последняя фаза всегда очевидна для системы защиты и далеко не всегда выгодна для злоумышленника, так как он, во-первых, компрометирует свои действия, во-вторых, сам теряет связь с объектом воздействия. Поэтому обязательным условием для реализации планов злоумышленника является возможность непрерывного мониторинга объекта защиты [10-12].

Диапазон действий защищаемой стороны также потенциально велик. Известны следующие направления обеспечения защиты [2-4]: увеличение дистанции между системой защиты и злоумышленником до безопасных границ; управление каналами воздействия; управление информационными потоками.

Первое направление реализует принцип пространственного обеспечения безопасности. На первоначальном этапе своего развития ИС обособлялись как топологически (территориально), так и путем снижения электромагнитной доступности защищаемой системы [13]. Эволюция ИС привела к их глобализации и трансграничности, поэтому построение выделенных ИС не соответствует современным экономическим вызовам и стремлению к формированию информационного общества.

Второе направление заключается в установлении физических и логических препятствий, имеющих управляемые характеристики для противодействия злоумышленнику. Это направление не препятствует созданию глобальных и трансграничных инфраструктур, но накладывает на их реализацию ассортимент регламентов, определяющих порядок работы ИС. Однако в условиях глобализации технологий и инфраструктур идентификация источника ДВ зачастую за-

труднительна, невозможна или не доступна системе защиты. В этом случае происхождение источника ДВ определяется как несубъектное (естественный процесс техногенного характера), а всю ответственность за последствия не санкционированного воздействия возлагают либо на недостатки регламентов, либо на их невыполнение конкретным пользователем.

Третье направление имеет принципиальное отличие, заключающееся в том, что устраняет антагонизм в противостоянии системы защиты и злоумышленника. Применение этого направления дает возможность сделать их цели независимыми или совпадающими (например, эксплуатация неограниченных ресурсов). Для этого необходимо, чтобы система информационной безопасности не ограничивала разнообразие состояний ИС, но и конструктивно управляла этим разнообразием, увеличивая его по мере необходимости, исходя из оперативной обстановки. При этом злоумышленник предъявляет к объекту защиты требование информативности, а средства добывания информации представлены в ИС в виде виртуальных точек присутствия и (или) недеklarированных возможностей аппаратного и программного обеспечения [14]. В результате система защиты должна являться источником сообщений для системы принятия решений злоумышленника, формировать неверные эталоны с использованием всего многообразия возможных состояний. Причем чем масштабнее объект и разнообразнее его состояния, тем легче его защищать.

В рамках третьего направления защиты известна стратегия киберобмана или Moving Target Defense (MTD) [15], защитные механизмы которой направлены на замену статических параметров ИС (используемое ПО, форматы данных, сетевые параметры, среда и платформа выполнения) динамическими, в результате чего злоумышленник не может получить актуальную информацию и реализовать уязвимости аппаратного и программного обеспечения [16].

В настоящее время ведутся исследования по повышению защищенности ИС с использованием стратегии MTD, о чем свидетельствуют труды Стародубцева Ю.И., Крылова В.В., Максимова Р.В., Язова Ю.К. и других ученых.

В работе [17] представлена модель функционирования сети связи с неизвестным уровнем доверия, которая учитывает структурные и потоковые характеристики физической сети связи и развёрнутых на её основе логических сетей для решения задач по выявлению слабых мест в существующих физических и логических сетях.

Для решения задачи динамического управления ресурсными возможностями ИС за счет управления параметрами сетевых соединений в работе [18] использовался математический аппарат теории марковских случайных процессов. Разработанная авторами модель позволяет определять вероятностные и временные характеристики, описывающие состояния ИС при различных стратегиях управления параметрами соединений. Известные технические решения по динамическому управлению ресурсными возможностями ИС [19-22] позволяют повысить результативность ее защиты, за счет снижения вероятности обнаружения нарушителем факта использования средств защиты и идентификации их характеристик путем имитации канала связи с плохим качеством. Однако задача скрытия (маскирования) структуры, состава и алгоритмов функцио-

нирования ИС при использовании информационно-телекоммуникационных сетей общего пользования (ИТКС ОП) не исследовалась.

Авторами работ [23, 24] описан способ защиты IP-подсетей от DDoS-атак путем псевдослучайной смены сетевых адресов (IPv6-адресов). Заявленный результат достигается путем распределения трафика между легитимными пользователями и злоумышленником на отдельные потоки. Недостатком такого подхода является увеличение количества используемого телекоммуникационного оборудования и поддержка только протокола IPv6. Однако задача навязывания злоумышленнику ложной функционально-логической структуры ИС не исследовалась.

Авторами работ [16, 25] описывается ассортимент технических решений по маскированию информационных направлений между локальными сегментами ИС, интегрированными в ИТКС ОП путем навязывания злоумышленнику ложной функционально-логической структуры ИС, сформулированы основные цели маскирования. Разработанные технические решения [26-31] позволяют организовывать маскированные каналы связи не более чем для двух абонентов выделенного канала связи. Однако задача организации и управления маскированными каналами связи ИС (для двух и более абонентов) не исследовалась.

Анализ работ [17-31], опубликованных по направлению защиты ИС от исследования структуры в рассматриваемой предметной области, показал значительный интерес ученых к вопросу обеспечения защиты ИС, функционирующих в ИТКС ОП, с использованием стратегии МТД. Однако вопросы управления множеством маскированных каналов связи ИС, функционирующих в ИТКС ОП, все еще недостаточно раскрыты, что обуславливает актуальность проводимого исследования.

В статье представлены результаты исследования принципов маскирования информационных направлений ИС в информационном пространстве и модель функционирования распределенных ИС при использовании маскированных каналов связи, которые позволяют обеспечить скрывание структуры, состава и алгоритмов функционирования ИС.

Использование маскирования информационных направлений ИС позволит реализовать следующие меры защиты информации в соответствии с руководящими документами ФСТЭК России [32-34]:

- навязывание злоумышленнику ложного представления об истинных информационных технологиях и (или) структурно-функциональных характеристиках информационной системы [32, 33];
- сокрытие архитектуры и конфигурации информационной системы [34];
- обеспечение доверенного канала (маршрута) [34];
- создание (эмуляция) ложных информационных систем или их компонентов, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности информации [32-34];
- перевод информационной (автоматизированной) системы в безопасное состояние при возникновении отказов (сбоев) [34];

- обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны [33];
- защита периметра (физических, логических границ) информационной системы при ее взаимодействии с иными информационными системами [33].

Анализ объекта исследования

В архитектуре современных ИС для обеспечения информационного взаимодействия используется единый стек протоколов TCP/IP [35-38]. Упрощенная архитектура ИС (рис. 1) представляет собой совокупность территориально распределенных сетей (подсетей), объединенных каналами связи через ИТКС ОП с использованием телекоммуникационного оборудования (маршрутизаторов, коммутаторов, межсетевых экранов и др.). В структуре современных ИС могут быть как локальные вычислительные сети, так и отдельные оконечные устройства – удаленные рабочие места пользователей, осуществляющие доступ к информационным ресурсам ИС (серверам и сервисам).

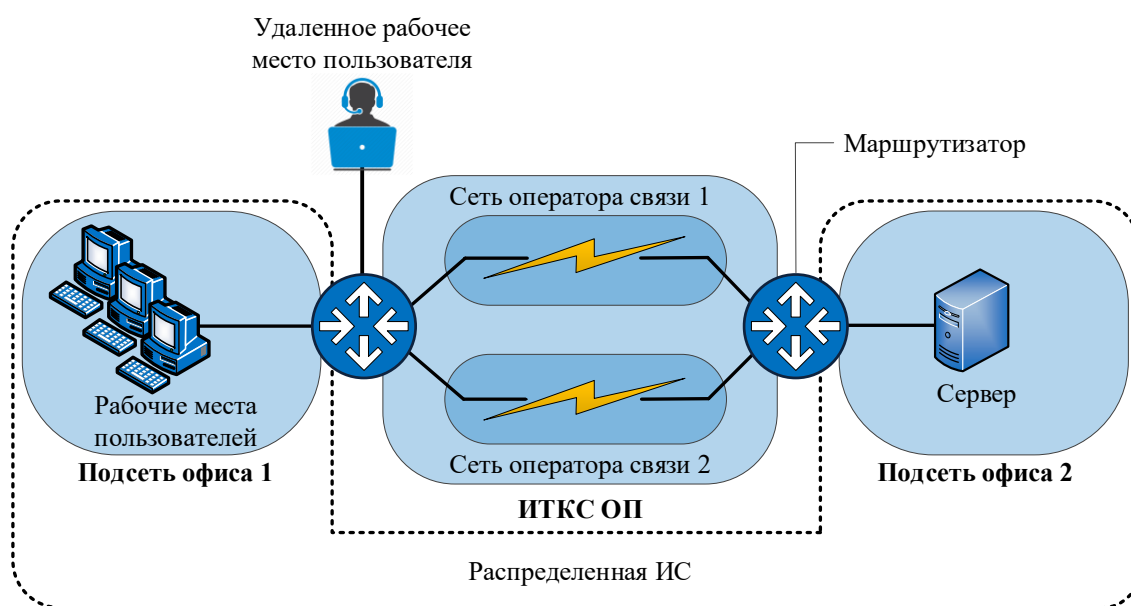


Рис.1. Упрощенная архитектура ИС

Учитывая представленную архитектуру, выделим следующие особенности функционирования ИС: распределенная структура; разделяемая среда передачи; повышенная отказоустойчивость, которая обеспечивается путем резервирования каналов связи в ИТКС ОП; постоянное совершенствование используемой технологической базы под воздействием растущих информационных потребностей пользователей.

В представленной архитектуре (рис. 2) расположение средств компьютерной разведки злоумышленника в разделяемой сетевой среде заранее неизвестно. Поэтому между защищаемыми сегментами ИС (подсети офисов 1 и 2 на рис. 2), следует рассматривать так называемые виртуальные точки присутствия – места

вероятного расположения средств компьютерной разведки злоумышленника за пределами контролируемой зоны. При этом большая протяженность каналов связи и интеграция ИС в ИТКС ОП увеличивает возможности злоумышленника по вскрытию информационных направлений ИС [39-41].

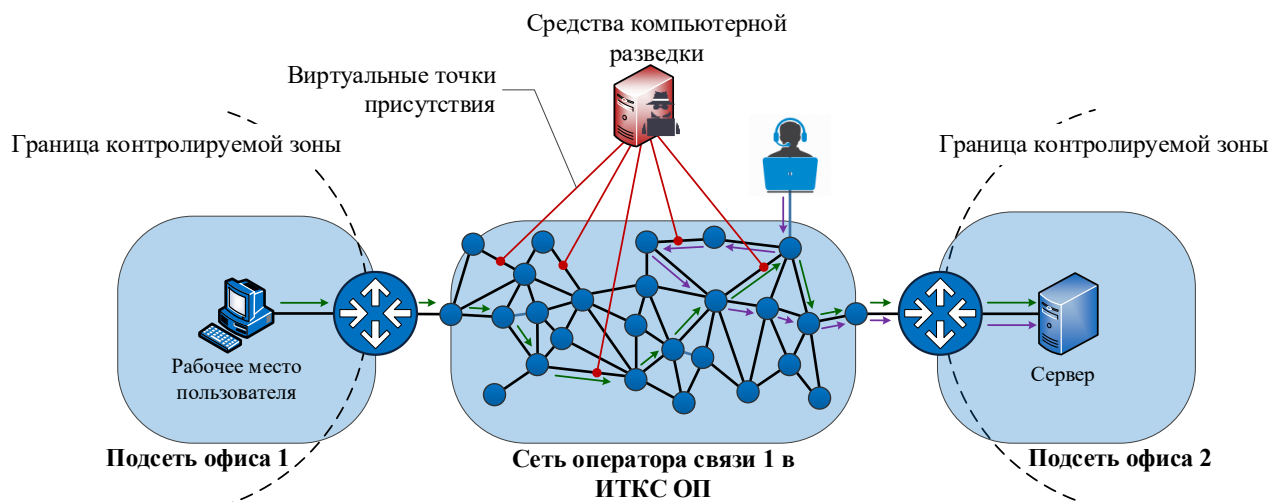


Рис.2. Расположение виртуальных точек присутствия в ИТКС ОП

Информационное направление – совокупность допустимых маршрутов в сети передачи данных между двумя территориально удаленными сегментами распределенной ИС, которые идентифицируются адресами отправителя и получателя пакетов сообщений.

Для вскрытия информационных направлений злоумышленник проводит анализ демаскирующих признаков в перехваченных через виртуальные точки присутствия пакетах сообщений. Телекоммуникационные узлы в ИС идентифицируются сетевыми адресами и логическими связями между ними по признаку наличия взаимного информационного обмена с указанием его интенсивности и направления.

Вскрытие информационных направлений ИС осуществляется посредством мониторинга трафика (анализа пакетов сообщений) с использованием известных технических средств [16, 25]. Вскрытие информационных направлений предоставляет исходные данные для реконструкции ИС и увеличивает вероятность осуществления преднамеренных ДВ на элементы ИС с использованием полученной в ходе анализа информации.

Под демаскирующим признаком средств связи и автоматизации принято понимать любую количественную или качественную характеристику физических полей, которые создаются, отражаются или искажаются средствами связи и автоматизации, если они раскрывают их наличие (отличие друг от друга) или свойства, подлежащие защите [42, 43].

Особенностью применения ИС является то, что их демаскирующие признаки могут быть использованы злоумышленником для получения защищаемых сведений не только о самих системах и режимах их функционирования, но и об информационных направлениях ИС и, как следствие, структуре системы управления организации, техническую основу которой составляют ИС.

Если при информационном взаимодействии демаскирующие признаки (идентификаторы отправителя и получателя) остаются неизменными в течение всего времени функционирования ИС, то такие демаскирующие признаки являются именными и их информативность максимальна. Зная демаскирующие признаки информационных направлений и их информативность, злоумышленник может реконструировать ИС с высокой степенью подобия ее реальной структуре.

Известен ряд способов [19-26] защиты сети связи, обеспечивающих маскирование структуры и алгоритмов функционирования ИС от компьютерной разведки. В указанных способах осуществляется защита информационного взаимодействия абонентов от реконструкции методом маскирования.

Маскирование – управление информативностью демаскирующих признаков информационных направлений без использования секретного ключа или с передачей (хранением) его вместе с сообщением [45].

Для защиты ИС от анализа и подавления в способах [26, 27] в ее структуру вводят логическую избыточность на канальном и сетевом уровнях, которая снижает информативность маскированного канала связи, за счет изменения IP- и MAC-адресов абонентов в передаваемых пакетах сообщений. Расширение адресного пространства демаскирующих признаков выполняется на внешних интерфейсах телекоммуникационного оборудования (маршрутизаторов), осуществляющих информационное взаимодействие.

Для повышения скрытности связи и затруднения идентификации абонентов сети в способах [28, 29] производится непрерывное изменение идентификаторов абонентов сети в передаваемых пакетах сообщений по всем доступным маршрутам. Для повышения результативности маскирования в способе [30] используются фиксированные значения приоритетов информационных направлений, определяющих интенсивность обмена маскирующими пакетами сообщений для каждой пары абонентов. Для расширения области применения маскирования структуры сети связи в способе [31] применяется передача пакетов сообщений между IP-адресами, формируемыми одним корреспондентом. Повышение результативности защиты в способах [19, 20] выполняется за счет учета максимального количества принятых от отправителя и необработанных пакетов сообщений, которые может обработать телекоммуникационное оборудование без перегрузки. При увеличении интенсивности несанкционированных информационных потоков в способах [21, 22] производится удержание в двустороннем порядке соединения и блокирование попыток отправителя пакетов сообщений разорвать соединение.

Использование рассмотренных способов устраняет единую точку отказа в сети за счет введения злоумышленника в заблуждение относительно структуры и алгоритмов функционирования ИС.

Несмотря на преимущества рассмотренных способов перед технологией трансляции сетевых адресов NAT (Network Address Translation), которая на сегодняшний день применяется для маскирования внутренней структуры сети и реализации мер защиты информации ФСТЭК России, они позволяют организовывать только двухточечные маскированные каналы связи. Каналы связи типа

«точка-точка» неэффективно используют преимущества технологии многопротокольной коммутации по меткам (MPLS) и виртуальных частных сетей (VPN) на ее основе (MPLS L2VPN). MPLS L2VPN позволяет использовать VPN канального уровня для организации территориально распределенной сети передачи данных наложенной на сеть оператора связи. В данной статье разработан прообраз сетевого протокола, который позволяет устранить указанный недостаток за счет формирования многоточечных маскированных каналов связи и динамического управления ими.

Разработка модели функционирования распределенных информационных систем при использовании маскированных каналов связи актуальна и необходима для описания существенных свойств информационного взаимодействия между распределенными сегментами ИС и дальнейшей разработки протокола динамического управления множеством маскированных каналов связи.

Постановка задачи

Для формальной постановки и решения задачи в работе введены обозначения, представленные в таблице 1.

Таблица 1 – Дискретные состояния распределенной ИС

Обозначение	Физический смысл обозначения
S	– распределенная ИС, использующая маскированный канал связи
C	– множество входных параметров модели (параметры маскирования)
M	– множество IPv4-адресов отправителей и получателей пакетов сообщений, выделяемых для маскирования абонентского трафика
M_S	– множество IPv4-адресов отправителей пакетов сообщений, выделяемых в соответствии с [44] для маскирования абонентского трафика
M_D	– множество IPv4-адресов получателей пакетов сообщений, выделяемых в соответствии с [44] для маскирования абонентского трафика
A	– множество IPv4-адресов отправителей и получателей пакетов сообщений, выделяемых для передачи и приема потоков маскирующего трафика
A_S	– множество IPv4-адресов отправителей пакетов сообщений, выделяемых в соответствии с [44] для передачи и приема потоков маскирующего трафика
A_D	– множество IPv4-адресов получателей пакетов сообщений, выделяемых в соответствии с [44] для передачи и приема потоков маскирующего трафика
X	– интенсивность вариации демаскирующими признаками (частота динамического изменения IPv4-адресов), устанавливаемая в пределах от 1 секунды до 24 часов на каждую пару IPv4-адресов
p_i	– множество выходных параметров модели, значения финальных вероятностей состояний системы S
Z	– множество внутренних параметров модели
Q	– показатель эффективности функционирования системы S
μ	– модель системы S

Пусть в распределенной информационной системе (рис. 3) имеется два телекоммуникационных узла (маршрутизатора) LR1-1 и DR1-1, обеспечивающих информационное взаимодействие (обмен абонентским трафиком) автоматизированных рабочих мест (APM) DU1-1 и LU1-1, а также серверного оборудования LS2-1 и DS2-1, расположенных в локальных сетях ЛВС-1 и ЛВС-2, по VPN-туннелю, организованному с использованием технологии многопротокольной коммутации по меткам (MPLS).

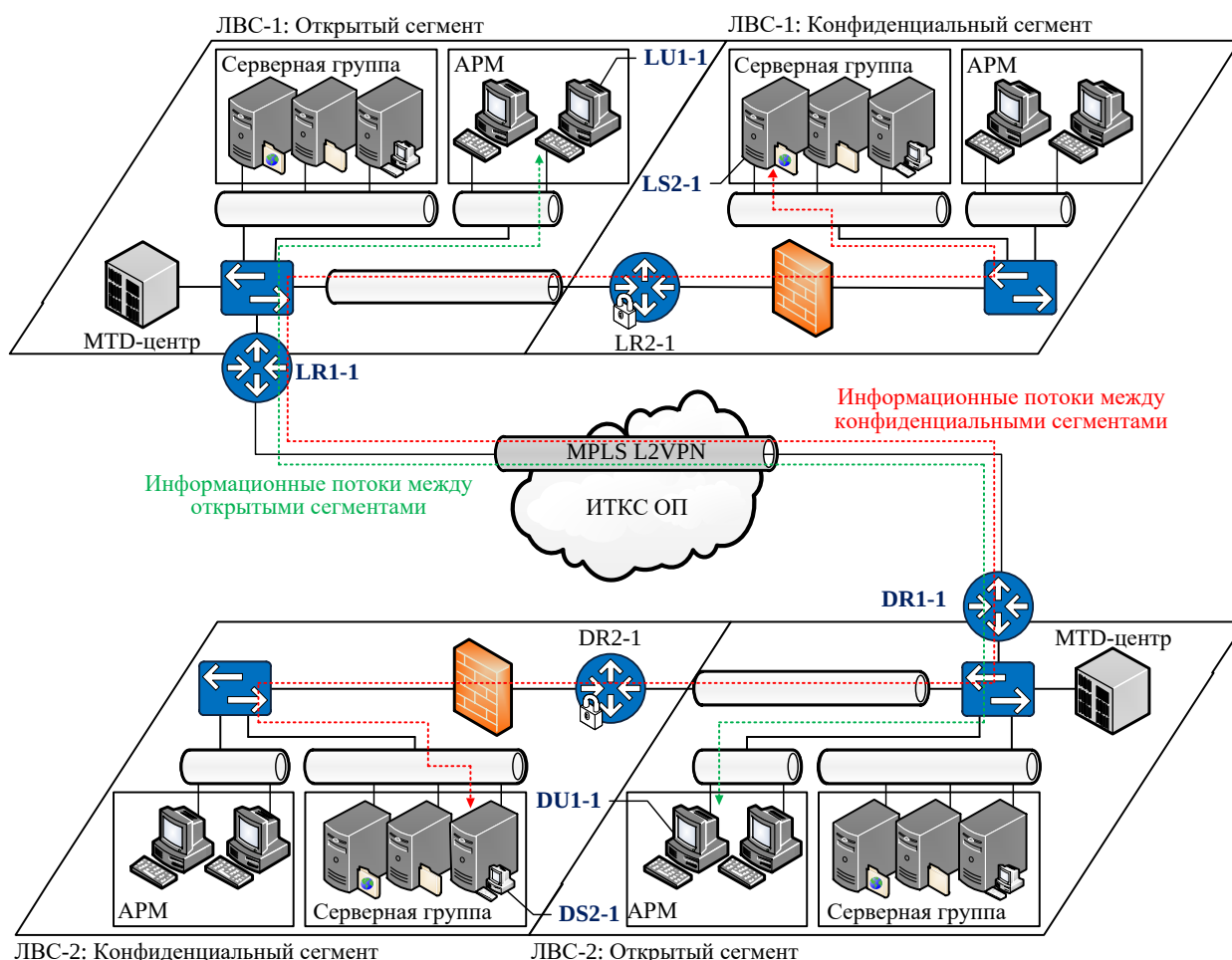


Рис.3. Схема информационного взаимодействия в распределенной ИС

Пусть для введения злоумышленника в заблуждение относительно структуры и алгоритмов функционирования ИС маршрутизаторы LR1-1 и DR1-1 используют маскированные каналы связи. Использование маскированных каналов связи обеспечивает скрывание структуры и алгоритмов функционирования ИС от средств компьютерной разведки.

Дано:

S – распределенная ИС, использующая маскированный канал связи;

C – множество входных параметров модели, параметры маскирования, $C \subseteq \{M, A, X\}$:

M – множество IPv4-адресов отправителей и получателей пакетов сообщений, выделяемых для маскирования абонентского трафика, $M \subseteq \{M_S, M_D\}$;

A – множество IPv4-адресов отправителей и получателей пакетов сообщений, выделяемых для передачи и приема потоков маскирующего трафика, $A \subseteq \{A_S, A_D\}$;

X – интенсивность вариации демаскирующими признаками (частота динамического изменения IPv4-адресов), $X = [1, 2, \dots, 86400]$;

p_i – множество выходных параметров модели, значения финальных вероятностей состояний системы S , $p_i = \lim_{t \rightarrow \infty} p_i(t)$, где $i = 1, 2, \dots, h$, причем число состояний конечно и из каждого из них можно за конечное число шагов перейти в любое другое;

Z – множество внутренних параметров модели $Z \subseteq \{S_i, \Lambda_j\}$, где $S_i = \{S_1, S_2, \dots, S_h\}$, $\Lambda_j = \{\lambda_1, \lambda_2, \dots, \lambda_j\}$ перечень моделируемых состояний системы и интенсивностей потоков событий в ней (описаны ниже по тексту);

Q – показатель эффективности функционирования системы S , $Q = \lim_{t \rightarrow \infty} P_{BC}(t)$, определяемый вероятностью вскрытия маскированного канала связи злоумышленником $P_{BC} \rightarrow \min$.

Найти: закономерность изменения множества p_i выходных параметров модели функционирования распределенных ИС при использовании маскированных каналов связи и множества Q показателей эффективности функционирования системы S от множества C значений входных параметров и множества Z значений внутренних параметров. На значения параметров множеств C , p_i , Z наложены условия их допустимости.

Тогда формальная постановка задачи на моделирование системы S :

$$\mu: \langle S, C, Z \rangle \rightarrow p_i, Q \mid C \subseteq \{M, A, X\}, p_i = \lim_{t \rightarrow \infty} p_i(t),$$

а формальная постановка задачи на оптимизацию показателя эффективности системы S :

$$\langle S, C, Z \rangle \rightarrow \min P_{BC} \mid P_{BC} \in \{p_i\}, i = 1, 2, \dots, h,$$

для минимизации вероятности вскрытия маскированного канала связи злоумышленником.

Модель функционирования распределенной информационной системы при использовании маскированных каналов связи

Маршрутизаторы LR1-1 и DR1-1 (рис. 3) выполняют управление (установление, поддержание и разрыв соединения) маскированным каналом связи, по которому передается маскированный абонентский трафик с АРМ пользователей (трафик, сгенерированный по правилам маскирования и несущий ложную адресную информацию в пакетах, с целью навязать злоумышленнику ложное представление о структуре распределенной ИС, несущий полезную нагрузку, передаваемую пользователями) и маскирующий трафик (трафик, сгенерированный по правилам маскирования и несущий ложную адресную информацию в пакетах, с целью навязать злоумышленнику ложное представление о структуре распределенной ИС, не несущий полезной нагрузки, передаваемой пользователями). Распределенная ИС S с течением времени меняет свое состояние (пере-

ходит из одного состояния в другое). Необходимые для исследования состояния $S_1, S_2, \dots, S_n$ перечислены в таблице 2.

Оценка эффективности процессов функционирования ИС при использовании маскированных каналов связи связана с необходимостью моделирования процесса в реальном времени. Это обуславливает целесообразность использования математического аппарата марковских процессов, необходимое условие которого – потоки событий являются простейшими, иными словами обладают свойствами стационарности, ординарности и не имеют последствий.

Таким образом, процесс функционирования рассматриваемой ИС можно представить, как марковский случайный процесс с дискретными состояниями и непрерывным временем.

Таблица 2 – Дискретные состояния распределенной ИС

№ п/п	Номер состояния	Наименование состояния	Описание состояния
1	S_1	Ожидание соединения	Маскированный канал связи находится в состоянии простоя. Пакеты сообщений принимаются и передаются по открытому (немаскированному) VPN-туннелю
2	S_2	Установление соединения	Для инициализации и согласования параметров маскированного канала связи маршрутизаторы обмениваются служебными пакетами сообщений
3	S_3	Взаимная аутентификация абонентов	Для согласования параметров взаимной аутентификации маршрутизаторы обмениваются служебными пакетами сообщений
4	S_4	Передача абонентских пакетов сообщений	Маршрутизаторы выполняют формирование, передачу и прием потоков абонентского трафика по установленному маскированному каналу связи
5	S_5	Разрыв соединения	Для разрыва соединения маршрутизаторы обмениваются служебными пакетами сообщений. Разрыв соединения происходит под воздействием помех (дестабилизирующих воздействий), ошибок конфигурации или в случае вскрытия злоумышленником реальной структуры сети
6	S_6	Передача маскирующих пакетов сообщений	При отсутствии абонентского трафика маршрутизаторы выполняют формирование, передачу и прием потоков маскирующего трафика по установленному маскированному каналу связи

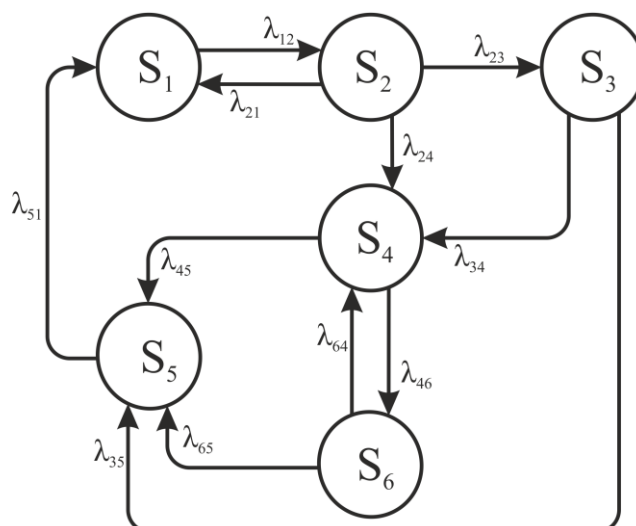


Рис.4. Граф состояний функционирования распределенной ИС

Моменты возможных переходов распределенной ИС из состояния в состояние при использовании маскированного канала связи неопределенны, случайны и происходят под действием потоков событий, которые характеризуются интенсивностями λ_{ij} (таблица 3). Интенсивности являются важной характеристикой потоков событий и представляют среднее число событий, приходящееся на единицу времени.

Таблица 3 – Интенсивности потоков событий распределенной ИС

№ п/п	Описание потока событий	Номер потока событий
1	Интенсивность потока заявок на инициализацию (нового) маскированного соединения	λ_{12}
2	Интенсивность потока заявок на переход в состояние простоя при инициализации маскированного соединения	λ_{21}
3	Интенсивность потока заявок на переход в состояние простоя при разрыве маскированного соединения	λ_{51}
4	Интенсивность потока заявок на взаимную аутентификацию абонентов	λ_{23}
5	Интенсивность потока заявок на передачу и прием потока абонентских пакетов сообщений после взаимной аутентификации абонентов	λ_{34}
6	Интенсивность потока заявок на передачу и прием потока абонентских пакетов сообщений после инициализации маскированного соединения	λ_{24}
7	Интенсивность потока заявок на инициализацию разрыва установленного соединения при согласовании параметров аутентификации маскированного канала связи	λ_{35}
8	Интенсивность потока событий при вскрытии злоумышленником реальной структуры сети	λ_{45}
9		λ_{65}
10	Интенсивность потока заявок на передачу и прием потока маскирующих пакетов сообщений	λ_{46}
11	Интенсивность потока заявок на передачу и прием потока абонентских пакетов сообщений	λ_{64}

Граф состояний функционирования распределенной ИС представлен на рис. 4.

Рассмотрим сценарий перехода моделируемой системы из состояния S_i в состояние S_j под воздействием потоков событий с интенсивностями λ_{ij} .

Пусть S_1 – начальное состояние моделируемой ИС, в котором она не принимает и не передает потоки пакетов сообщений по маскированному каналу связи, то есть состояние простоя маскированного канала связи.

В состоянии простоя маскированного канала связи маршрутизаторы передают абонентские пакеты сообщений между АРМ пользователей по открытому (немаскированному) VPN-туннелю. В состояние S_1 маршрутизаторы переводятся в следующих случаях:

- ошибка при согласовании параметров маскированного соединения под воздействием заявок на переход в состояние простоя λ_{21} ;
- успешный разрыв соединения под воздействием заявок на переход в состояние простоя λ_{51} .

Заявки на переход в состояние простоя при инициализации маскированного соединения λ_{21} возникают под воздействием помех (преднамеренных или непреднамеренных) в канале связи. Маршрутизаторы, которым длительное время не удалось согласовать параметры маскированного канала связи, переводятся в состояние S_1 .

Заявки на переход в состояние простоя λ_{51} при разрыве маскированного соединения возникают под воздействием помех в канале связи, в случае, когда отсутствует необходимость дальнейшего использования маскированного канала связи или в случае вскрытия злоумышленником реальной структуры сети и необходимости проведения повторного цикла маскирования (изменения параметров маскирования).

Обнаружение помех в канале связи выполняется с использованием механизма контроля соединения (keepalive), который описан в запросах на комментарии [46, 47]. Маршрутизаторы каждый установленный интервал времени (по умолчанию одна секунда) выполняют отправку служебных пакетов сообщений типа *Request-Echo* и ожидают ответ от удаленной стороны в виде служебного пакета типа *Ack-Echo*. Если за установленный интервал времени от удаленной стороны не получен служебный пакет типа *Ack-Echo*, то маршрутизатор переходит в состояние S_5 , полагая, что на удаленной стороне произошел сбой в канале связи.

Служебные пакеты сообщений протокола динамического управления множеством маскированных каналов связи инкапсулируются в Ethernet-кадр со специальным номером в поле EtherType и имеют формат заголовка, представленный на рис. 5.

В состояниях S_4 и S_6 выполняется вариация демаскирующими признаками информационных направлений ИС по маскированному каналу связи. Интенсивность вариации демаскирующими признаками (частота динамического изменения IP- и MAC-адресов) устанавливается в файле конфигурации и согласуется путем передачи пакетов типа *Request-Config* (рис. 6).

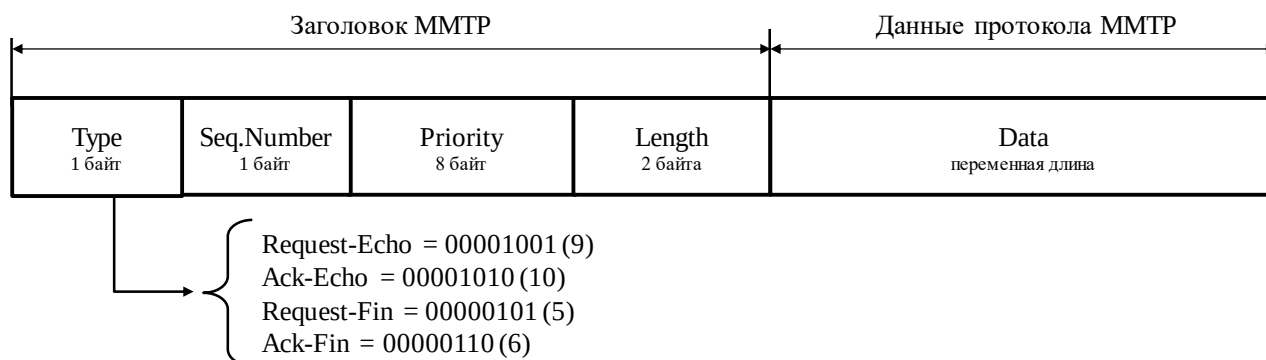


Рис.5. Формат служебных пакетов протокола динамического управления множеством маскированных каналов связи

В состоянии S_4 маршрутизаторы выполняют формирование, передачу и прием потоков абонентского трафика по установленному маскированному каналу связи. В это состояние маршрутизаторы переводятся в следующих случаях:

- успешная аутентификация под воздействием заявок на передачу и прием потока абонентских пакетов сообщений после взаимной аутентификации абонентов λ_{34} ;
- успешная инициализация (нового) маскированного соединения под воздействием заявок на передачу и прием потока абонентских пакетов сообщений λ_{24} ;
- необходимость передачи (приема) абонентских пакетов сообщений под воздействием заявок на передачу и прием потока абонентских пакетов сообщений λ_{64} .

Если отсутствует необходимость взаимной аутентификации абонентов, что определяется параметрами конфигурации маскированного канала связи, то осуществляется переход из состояния S_2 в S_4 .

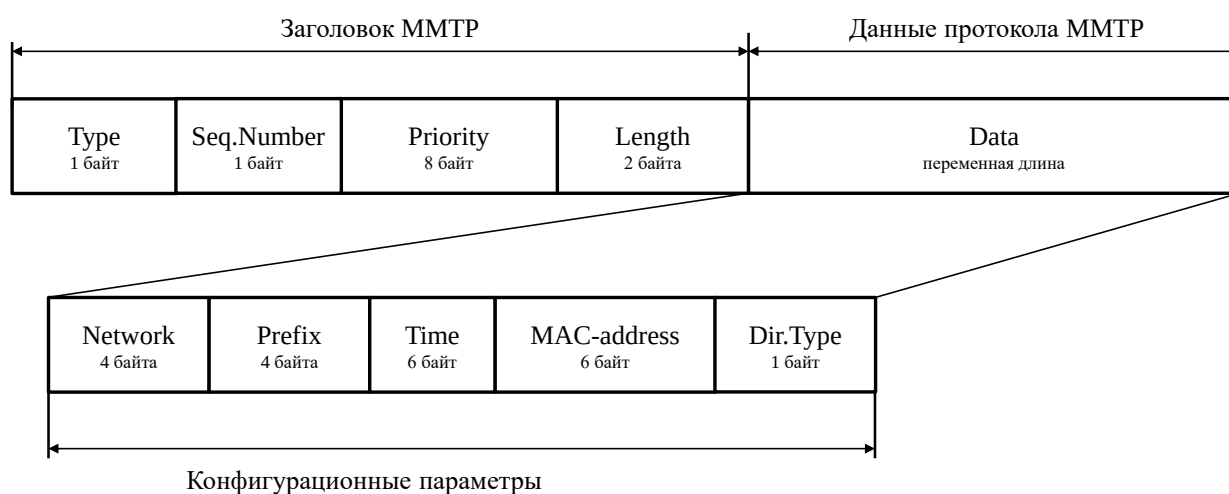


Рис.6. Формат заголовка служебных пакетов типа Request-Config

Состояния S_2 , S_3 и S_5 являются транзитными состояниями моделируемой ИС и используются для согласования параметров маскированного канала связи

перед переходом системы S в состояния использования маскированного канала связи S_4 и S_6 .

В состоянии S_2 маршрутизаторы обмениваются служебными пакетами сообщений для инициализации и согласования параметров маскированного канала связи. В это состояние маршрутизаторы переводятся под воздействием заявок на инициализацию (нового) маскированного соединения λ_{12} .

При установлении соединения параметры маскирования локального маршрутизатора (интенсивность вариации демаскирующими признаками, используемые при маскировании диапазоны IP- и MAC-адресов и другие) сравниваются с полученными в пакетах типа Request-Config (формат пакета представлен на рис. 6) параметрами удаленного маршрутизатора. Если параметры отличаются, маршрутизаторы выбирают роль в информационном взаимодействии – Master (ведущий) или Slave (ведомый). Если топологии совпадают, удаленному маршрутизатору отправляются служебные пакеты типа Ack-Config и Request-Config для подтверждения.

Роль маршрутизатора выбирается на основе сравнения поля *Priority* (приоритет): маршрутизатор с большим значением в поле *Priority* становится ведущим. Затем в зависимости от роли либо изменяются локальные параметры маршрутизатора, в случае если роль удаленного маршрутизатора Master, в противном случае удаленному маршрутизатору отправляются служебные пакеты типа Nak-Config и Request-Config.

В состоянии S_3 маршрутизаторы обмениваются служебными пакетами сообщений для согласования параметров аутентификации. В это состояние маршрутизаторы переводятся под воздействием заявок на взаимную аутентификацию абонентов λ_{23} .

При взаимной аутентификации абонентов сравниваются локальные параметры аутентификации с полученными в пакетах типа Request-Auth (формат пакета представлен на рис. 7) параметрами аутентификации удаленного маршрутизатора. В пакетах типа Request-Auth сравнивается следующая информация: длина имени пользователя; значение имени пользователя; длина парольной фразы; значение парольной фразы.

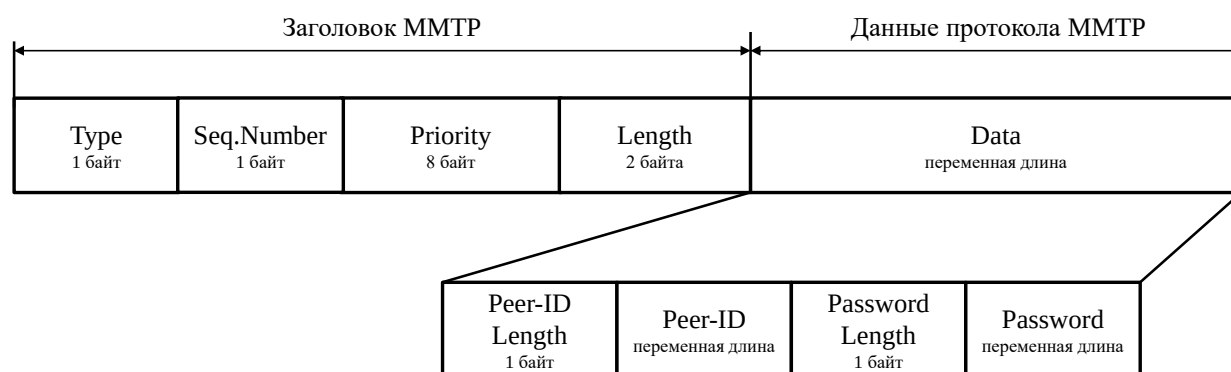


Рис.7. Формат заголовка служебных пакетов типа Request-Auth

Если параметры аутентификации на маршрутизаторах не совпадают, то отправляются пакеты типа $Nak-Auth$ и осуществляется переход в стадию разрыва соединения S_5 под воздействием заявок на инициализацию разрыва установленного соединения λ_{35} .

Если за установленный интервал времени от удаленной стороны не получен служебный пакет типа $Ack-Auth$ или $Nak-Auth$, то маршрутизатор переходит в состояние S_5 , полагая, что на удаленной стороне произошел сбой в канале связи.

В состоянии S_5 маршрутизаторы обмениваются служебными пакетами сообщений для разрыва соединения. Разрыв соединения происходит в следующих случаях:

- получены заявки на инициализацию разрыва установленного (маскированного) соединения под воздействием потоков событий при вскрытии злоумышленником реальной структуры сети λ_{45} и λ_{65} ;
- получены заявки на инициализацию разрыва установленного (маскированного) соединения при согласовании параметров аутентификации маскированного канала связи λ_{35} .

При разрыве соединения инициатором разрыва соединения отправляются пакеты типа $Request-Fin$ и ожидается получение пакетов типа $Ack-Fin$ и $Request-Fin$ (формат FIN -пакетов соответствует пакетам типа $Request-Config$, исключая поле данных и представлен на рис. 6) от удаленного маршрутизатора.

Если за установленный интервал времени от удаленной стороны не получен служебный пакет типа $Ack-Fin$, то маршрутизатор переходит в состояние S_1 , полагая, что на удаленной стороне произошел сбой в канале связи.

Моделируемая система, находясь в состояниях S_4 и S_6 , под воздействием потоков событий при вскрытии злоумышленником реальной структуры сети λ_{45} и λ_{65} переходит в транзитное состояние S_5 и приступает к разрыву соединения.

Переход между состояниями S_4 и S_6 происходит под воздействием заявок на передачу и прием потока маскирующих и абонентских пакетов сообщений λ_{46} и λ_{64} соответственно.

При отсутствии абонентских пакетов сообщений в системе S возникают заявки λ_{46} , переводящие систему S в состояние S_6 , в котором производится обмен маскирующими пакетами сообщений между абонентами. Если в системе S появляются абонентские пакеты сообщений, то возникают заявки λ_{64} , переводящие систему S в состояние S_4 , в котором производится обмен абонентскими и пакетами сообщений между абонентами по маскированному каналу связи. Заявки λ_{46} и λ_{64} позволяют динамически изменять режимы работы маскированного канала связи в системе S .

Заявки λ_{21} , λ_{35} , λ_{45} и λ_{65} могут быть вызваны как помехами канала связи, так и дестабилизирующими воздействиями злоумышленника на процесс информационного взаимодействия маршрутизаторов.

По размеченному графу состояний распределенной ИС (рис. 4), строится математическая модель ее функционирования.

Моделируемая ИС может находиться в состояниях $S_1, S_2, \dots, S_6$. Вероятность $p_i(t)$ того, что в момент времени t система будет находиться в состоянии S_i называется вероятностью i -го состояния. По размеченному графу состояний составляются согласно правилам [48] уравнения Колмогорова – дифференциальные уравнения с неизвестными функциями $p_i(t)$:

$$\begin{cases} \frac{dp_1(t)}{dt} = \lambda_{21}p_2(t) + \lambda_{51}p_5(t) - \lambda_{12}p_1(t), \\ \frac{dp_2(t)}{dt} = \lambda_{12}p_1(t) - (\lambda_{21} + \lambda_{23} + \lambda_{24})p_2(t), \\ \frac{dp_3(t)}{dt} = \lambda_{23}p_2(t) - (\lambda_{34} + \lambda_{35})p_3(t), \\ \frac{dp_4(t)}{dt} = \lambda_{24}p_2(t) + \lambda_{64}p_6(t) + \lambda_{34}p_3(t) - (\lambda_{45} + \lambda_{46})p_4(t), \\ \frac{dp_5(t)}{dt} = \lambda_{45}p_4(t) + \lambda_{65}p_6(t) + \lambda_{35}p_3(t) - \lambda_{51}p_5(t), \\ \frac{dp_6(t)}{dt} = \lambda_{46}p_4(t) - (\lambda_{65} + \lambda_{64})p_6(t), \\ \sum_{i=1}^6 p_i(t) = 1. \end{cases} \quad (1)$$

Для решения уравнения (1) задаются начальные условия. Вектор вероятностей начальных состояний марковской цепи с учетом отсутствия воздействий на ИС в начальный момент времени имеет вид:

$$p_i(0) = [1 \ 0 \ 0 \ 0 \ 0 \ 0]. \quad (2)$$

Задавая численные значения интенсивностей λ (таблица 3) и переходя к непрерывному времени $t \rightarrow \infty$, решается система линейных дифференциальных уравнений (1) с постоянными коэффициентами (однородный марковский процесс). Для любого момента времени t сумма всех вероятностей состояний равна единице:

$$\sum_{i=1}^n p_i(t) = 1. \quad (3)$$

Характер выбранных значений интенсивностей определяется в соответствии со стратегиями участников информационного взаимодействия.

Модель функционирования ИС при использовании маскированного канала связи учитывает взаимные воздействия участников информационного обмена, с различными приоритетами запросов и количеством заявок. Использование модели предполагает поиск стратегий взаимодействия маршрутизаторов, использующих маскированные каналы связи для защиты информации о структуре и алгоритмах функционирования ИС, и позволит перейти к вероятностной оценке вскрытия маскированного канала связи $P_{BC} \rightarrow \min$.

Учет в марковской модели времени пребывания ИС в каждом из состояний в зависимости от стратегий взаимодействующих сторон позволяет исследовать временную динамику функционирования ИС при использовании маскированного канала связи.

В качестве исходных данных для моделирования выступают:

- система линейных дифференциальных уравнений (1);
- вектор вероятностей начальных состояний (2);
- значения интенсивностей потоков событий (таблица 9);
- нормировочное условие (3).

Системой линейных дифференциальных уравнений (ЛДУ) называется система уравнений $S_i(t, p_1(t), p_2(t), \dots, p'_1(t), p'_2(t), \dots) = 0$, где $i = 1, 2, \dots$, которая связывает независимую переменную t , искомые функции $p_1 = p_1(t)$, $p_2 = p_2(t)$, ... и их производные.

Решения задач для системы ЛДУ можно разделить на три группы [49]:

- приближенно-аналитические методы;
- графические или машинно-графические методы;
- численные методы.

Применение цифровой вычислительной техники позволяет применить численные методы решения системы ЛДУ, предполагающие получение числовой таблицы приближенных значений p_i искомых решений $p(t)$ на некотором интервале $t \in [t_0; t_1]$. Применение к полученной числовой таблице значений p_i способа аппроксимации, например, сплайн-интерполяции, позволяет иметь приближенное решение $p(t)$ на заданном интервале времени, что по сравнению с другими методами решения, позволяет решать поставленную прикладную задачу и оценивать ее возможности.

Недостатки методов Эйлера и других численных методов решения более высоких порядков [49], заключающиеся в необходимости вычисления на каждом шаге частных производных функции $S(t, p)$, что приводит к большой вычислительной сложности, предопределили выбор в качестве метода решения системы ЛДУ классический метод – метод Рунге-Кутты четвертого порядка с фиксированным шагом интегрирования, имеющий вид (4), где h – приращение, соответствующее шаговой поправке Эйлера, Δp_i – средневзвешенная величина поправок $h\eta_1^i, h\eta_2^i, h\eta_3^i, h\eta_4^i$ каждого этапа интегрирования (с весовыми коэффициентами $\frac{1}{6}, \frac{2}{6}, \frac{2}{6}, \frac{1}{6}$ соответственно), то есть результат усреднения с указанными коэффициентами четырехэтапных поправок.

Первый этап соответствует применению явного метода Эйлера, четвертый – неявного, а второй и третий – уточненных методов Эйлера. Геометрическое толкование метода известно и описано, например, в работе [49].

Дополнительное обоснование необходимости использования метода Рунге-Кутты заключается в том, что для решения приведенной системы уравнений (1) методов исключения или Эйлера недостаточно, поскольку в ней присутствует уравнение, связывающее функции $p_i(t)$ вместе.

$$\begin{cases} \eta_1^i = S(t_i, p_i), \\ \eta_2^i = S(t_i + \frac{h}{2}, p_i + \frac{h}{2} \eta_1^i), \\ \eta_3^i = S(t_i + \frac{h}{2}, p_i + \frac{h}{2} \eta_2^i), \\ \eta_4^i = S(t_i + h, p_i + h \eta_3^i), \\ \Delta p_i = \frac{h}{6} (\eta_1^i + 2\eta_2^i + 2\eta_3^i + \eta_4^i), \\ p_{i+1} = p_i + \Delta p_i. \end{cases} \quad (4)$$

Приведем систему (1) к векторному представлению – столбец D , где каждый элемент соответствует правой части определенного дифференциального уравнения в системе:

$$D(t, p) = \begin{pmatrix} \lambda_{21}p_2(t) + \lambda_{51}p_5(t) - \lambda_{12}p_1(t) \\ \lambda_{12}p_1(t) - (\lambda_{21} + \lambda_{23} + \lambda_{24})p_2(t) \\ \lambda_{23}p_2(t) - (\lambda_{34} + \lambda_{35})p_3(t) \\ \lambda_{24}p_2(t) + \lambda_{64}p_6(t) + \lambda_{34}p_3(t) - (\lambda_{45} + \lambda_{46})p_4(t) \\ \lambda_{45}p_4(t) + \lambda_{65}p_6(t) + \lambda_{35}p_3(t) - \lambda_{51}p_5(t) \\ \lambda_{46}p_4(t) - (\lambda_{65} + \lambda_{64})p_6(t) \end{pmatrix} \quad (5)$$

Используя известный [49] порядок решения системы ЛДУ методом Рунге-Кутты, учитывая вектор вероятностей начальных состояний $p_i(0)$, интервал интегрирования $[t_0; t_1]$ и число этапов интегрирования n , производится расчет для заданных значений интенсивностей событий $\lambda_{ij} = \text{const}$ (марковский однородный процесс) (таблица 4), что позволяет получить числовую таблицу приближенных значений p_i искомых решений $p(t)$ на некотором интервале $t \in [t_0; t_1]$ (таблица 4).

Применяя интерполяцию, имеем приближенное решение $p(t)$ на заданном интервале времени.

Таблица 4 – Приближенные решения $p(t)$ на заданных интервалах времени

Этапы интегрирования, n	Точка интервала интегрирования, $[t_0, t_1]$	$p(t)$					
		$p_1(t)$	$p_2(t)$	$p_3(t)$	$p_4(t)$	$p_5(t)$	$p_6(t)$
1	t_0	$p_1(t_0)$	$p_2(t_0)$	$p_3(t_0)$	$p_4(t_0)$	$p_5(t_0)$	$p_6(t_0)$
...	...	...	...	...	...	...	...
n	t_1	$p_1(t_1)$	$p_2(t_1)$	$p_3(t_1)$	$p_4(t_1)$	$p_5(t_1)$	$p_6(t_1)$

Таким образом, получены вероятностные и временные характеристики, описывающие состояния процесса функционирования ИС при использовании маскированного канала связи, которые в свою очередь составляют основу для исследования данного процесса при различных стратегиях взаимодействующих сторон (таблица 5), что позволяет оценивать состояние ИС.

Учитывая формальное описание протокола динамического управления множеством маскированных каналов связи, вероятность защиты от компьютерной разведки $P_3 = p_4(t) + p_6(t)$, а вероятность вскрытия маскированного канала связи $P_{BC} = p_5(t)$.

Таблица 5 – Значения интенсивностей событий в зависимости от стратегии функционирования распределенной ИС

Признаки	Стратегии			
	C_1	C_2	C_3	C_4
Наличие заявок, λ_{51}	max	max	min	min
Наличие заявок, λ_{45}	max	min	max	min

Пример расчета

Оценим устойчивость модели к вариациям исходных данных, задавая граничные значения в стратегиях взаимодействующих сторон, в случае, когда маскированные каналы связи устанавливаются без взаимной аутентификации абонентов $\lambda_{23} = \lambda_{34} = \lambda_{35} = 0$ и выполняется только передача абонентских пакетов сообщений без передачи маскирующих пакетов сообщений $\lambda_{65} = \lambda_{46} = \lambda_{64} = 0$. ДВ злоумышленника вызывают увеличение потока событий λ_{45} , поэтому для защиты ИС необходимо проведение повторного цикла маскирования (изменения параметров маскирования), что вызывает увеличение интенсивности потока заявок на переход в состояние простоя при разрыве маскированного соединения λ_{51} . Рассмотрим следующие варианты стратегий.

C_1 – прием и передача потоков абонентского трафика по маскированному каналу связи без процедуры аутентификации с высоким уровнем ДВ злоумышленника. В этой стратегии высокий уровень ДВ злоумышленника порождает увеличение интенсивности потока событий при вскрытии злоумышленником реальной структуры сети λ_{45} . Поэтому для защиты ИС и проведения повторного цикла маскирования (изменения параметров маскирования) происходит увеличение интенсивности потока заявок на переход в состояние простоя при разрыве маскированного соединения λ_{51} .

C_2 – прием и передача потоков абонентского трафика по маскированному каналу связи без процедуры аутентификации с низким уровнем ДВ злоумышленника. В этой стратегии низкий уровень ДВ злоумышленника порождает уменьшение интенсивности потока событий при вскрытии злоумышленником реальной структуры сети λ_{45} , однако для обеспечения защиты ИС интенсивность потока заявок на переход в состояние простоя при разрыве маскированного соединения λ_{51} остается высокой;

C_3 – прием и передача потоков абонентского трафика преимущественно по открытому (немаскированному) VPN-туннелю с высоким уровнем ДВ. В этой стратегии высокий уровень ДВ злоумышленника порождает увеличение интенсивности потока событий при вскрытии злоумышленником реальной структуры сети λ_{45} , а использование немаскированного VPN-туннеля ведет к

уменьшению интенсивности потока заявок на переход в состояние простоя при разрыве маскированного соединения λ_{51} .

C_4 – прием и передача потоков абонентского трафика преимущественно по открытому (немаскированному) VPN-туннелю с низким уровнем ДВ злоумышленника. В этой стратегии низкий уровень ДВ злоумышленника порождает уменьшение интенсивности потока событий при вскрытии злоумышленником реальной структуры сети λ_{45} , а использование немаскированного VPN-туннеля ведет к уменьшению интенсивности потока заявок на переход в состояние простоя при разрыве маскированного соединения λ_{51} .

Исходные данные для расчета: система ЛДУ (1), вектор вероятностей начальных состояний (2), нормировочное условие (3), значения интенсивностей потоков событий задаем постоянными (таблица 6) в соответствии с выбранной стратегией взаимодействия клиентов и сервера, например, стратегией C_1 .

Таблица 6 – Интенсивности потоков событий для каждой из стратегий информационного взаимодействия

№ п/п	Интенсивность	λ	Значения интенсивности потоков событий			
			C_1	C_2	C_3	C_4
1	Заявки на инициализацию (нового) маскированного соединения	λ_{12}	100	100	100	100
2	Заявки на переход в состояние простоя при инициализации маскированного соединения	λ_{21}	10	10	10	10
3	Заявки на переход в состояние простоя при разрыве маскированного соединения	λ_{51}	100	100	10	10
4	Заявки на передачу и прием потока абонентских пакетов сообщений после инициализации маскированного соединения	λ_{24}	100	100	100	100
5	События при вскрытии злоумышленником реальной структуры сети	λ_{45}	100	10	100	10

Определяем интервал интегрирования, например, $t_0 = 0$, $t_1 = 10$ и число этапов интегрирования, например, $n = 10000$. Приводим систему (1) к векторному представлению, где каждый элемент соответствует правой части определенного ДУ в системе с заданными значениями интенсивностей событий.

Производим расчет по методу Рунге-Кутты со средневзвешенной величиной поправок каждого этапа интегрирования (4) и получаем числовую таблицу приближенных значений p_i на интервале $t \in [0; 10]$ с фиксированным шагом интегрирования 10^3 (таблица 7). Расчет произведен с помощью пакета математического программирования «MathCAD 15». Проверим условие (3), что для любого момента времени t сумма всех вероятностей состояний равна единице, например для $t = 10$:

$$\sum_{i=1}^6 p_i(10) = 0,434 + 0,357 + 0 + 0,161 + 0,049 + 0 = 1. \quad (6)$$

Применяем к полученной числовой таблице значений p_i способ аппроксимации (сплайн-интерполяцию), имеем приближенное решение $p(t)$ на заданном интервале времени. Графики зависимостей вероятностей состояний процесса функционирования ИС при использовании маскированного канала связи от времени $p_1(t), p_2(t), \dots, p_6(t)$ для значений интенсивностей событий соответствующие стратегии C_1 (таблица 7), представлены на рис. 8.

На интервале времени $[0; 0,07]$ ИС находится в переходном режиме функционирования, где наблюдается всплеск значений вероятности состояния $p_2(t)$ и $p_5(t)$ что соответствует нахождению ИС в состоянии инициализации и разрыва соединения участниками информационного взаимодействия.

При $t \rightarrow \infty$ в ИС устанавливается стационарный режим, когда ИС случайным образом меняет свои состояния и ее вероятности $p_1(t), p_2(t), \dots, p_6(t)$ уже не зависят от времени и равны финальным (предельным) вероятностям.

Таблица 7 – Числовая таблица приближенных значений $p_i(t)$ для λ в стратегии C_1

Этапы интегрирования, n	Точка интервала интегрирования, $[t_0, t_1]$	$p(t)$					
		$p_1(t)$	$p_2(t)$	$p_3(t)$	$p_4(t)$	$p_5(t)$	$p_6(t)$
1	0	1	0	0	0	0	0
2	$1 \cdot 10^{-3}$	0,905	0,09	0	$4,51 \cdot 10^{-3}$	$1,496 \cdot 10^{-4}$	0
3	$2 \cdot 10^{-3}$	0,82	0,162	0	0,016	$1,085 \cdot 10^{-3}$	0
...	...	...	...	...	...	...	...
10^3	10	0,268	0,244	0	0,244	0,244	0

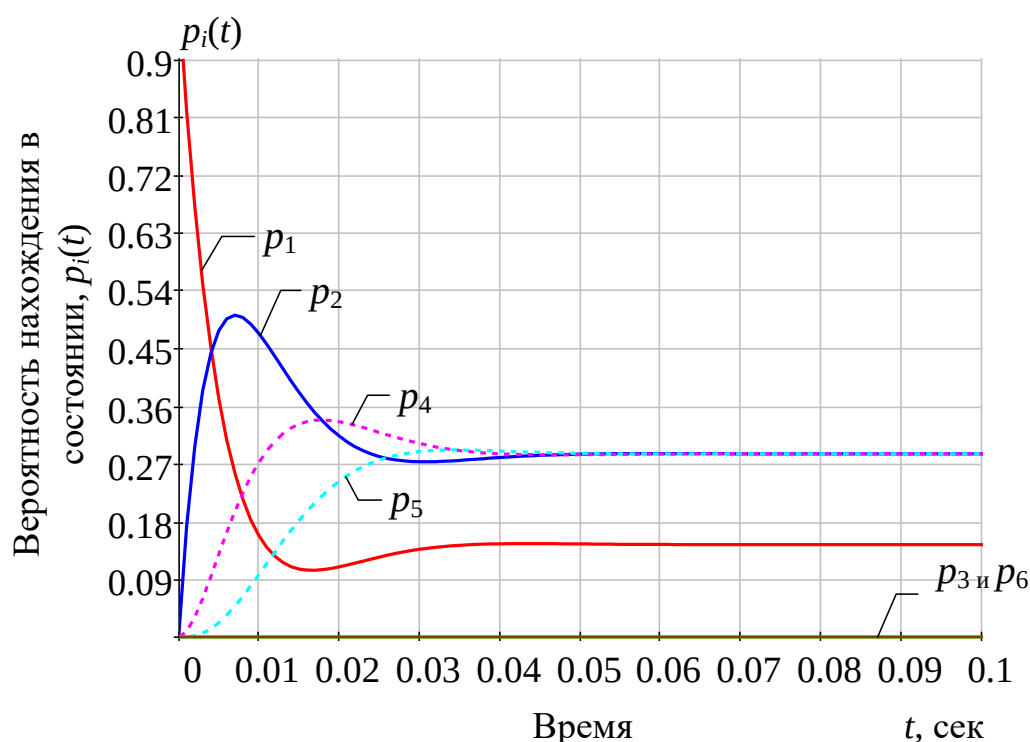


Рис.8. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий соответствующие стратегии C_1

Полученные значения финальных вероятностей $p_1 = 0,268$, $p_2 = 0,244$, $p_3 = 0$, $p_4 = 0,244$, $p_5 = 0,244$, $p_6 = 0$ показывают, сколько времени ИС в среднем находится в соответствующих состояниях. Учитывая значения финальных вероятностей, вероятность вскрытия маскированного канала связи для стратегии C_1 составляет $P_{BC} = 0,244$.

Для исследования процесса функционирования и защиты ИС при перечисленных стратегиях функционирования ИС (таблица 6) и соответствующих им значений интенсивностей событий производится расчет вероятностных и временных характеристик согласно вышеизложенному примеру.

Графики зависимостей вероятностей состояний процесса функционирования ИС при использовании маскированного канала связи от времени $p_1(t), p_2(t), \dots, p_6(t)$ для значений интенсивностей событий соответствующие стратегии C_2 (таблица 8), представлены на рис. 9.

Таблица 8 – Числовая таблица приближенных значений $p_i(t)$
для λ в стратегии C_2

Этапы интегрирования, n	Точка интервала интегрирования, $[t_0, t_1]$	$p(t)$					
		$p_1(t)$	$p_2(t)$	$p_3(t)$	$p_4(t)$	$p_5(t)$	$p_6(t)$
1	0	1	0	0	0	0	0
2	$1 \cdot 10^{-3}$	0,819	0,172	0	$9,025 \cdot 10^{-3}$	$2,991 \cdot 10^{-5}$	0
3	$2 \cdot 10^{-3}$	0,671	0,297	0	0,033	$2,172 \cdot 10^{-4}$	0
...	...	...	...	...	...	...	...
10^3	10	0,04	0,08	0	0,8	0,08	0

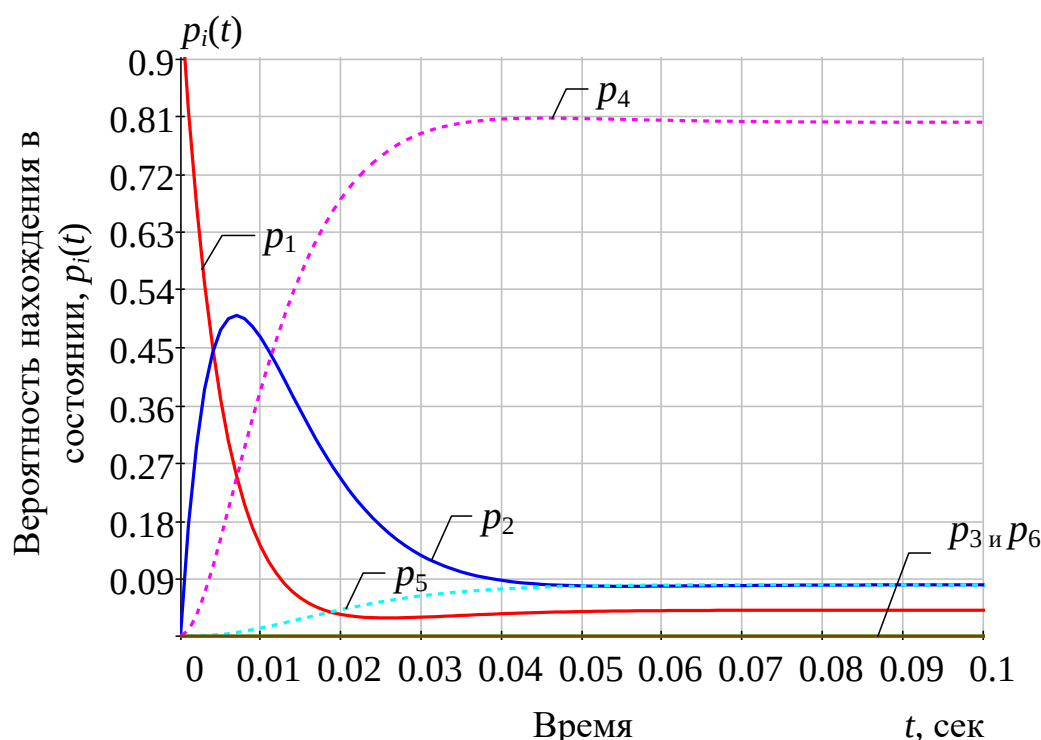


Рис.9. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий соответствующие стратегии C_2

Учитывая значения финальных вероятностей, вероятность вскрытия маскированного канала связи для стратегии C_2 составляет $P_{BC} = 0,076$.

Графики зависимостей вероятностей состояний процесса функционирования ИС при использовании маскированного канала связи от времени $p_1(t), p_2(t), \dots, p_6(t)$ для значений интенсивностей событий соответствующие стратегии C_3 (таблица 9), представлены на рис. 10.

Таблица 9 – Числовая таблица приближенных значений $p_i(t)$ для λ в стратегии C_3

Этапы интегрирования, n	Точка интервала интегрирования, $[t_0, t_1]$	$p(t)$					
		$p_1(t)$	$p_2(t)$	$p_3(t)$	$p_4(t)$	$p_5(t)$	$p_6(t)$
1	0	1	0	0	0	0	0
2	$1 \cdot 10^{-3}$	0,819	0,172	0	$8,756 \cdot 10^{-3}$	$2,991 \cdot 10^{-4}$	0
3	$2 \cdot 10^{-3}$	0,671	0,297	0	0,031	$2,172 \cdot 10^{-3}$	0
...	...	...	...	...	...	...	...
10^3	10	0,04	0,08	0	0,08	0,8	0

Учитывая значения финальных вероятностей, вероятность вскрытия маскированного канала связи для стратегии C_3 составляет $P_{BC} = 0,763$.

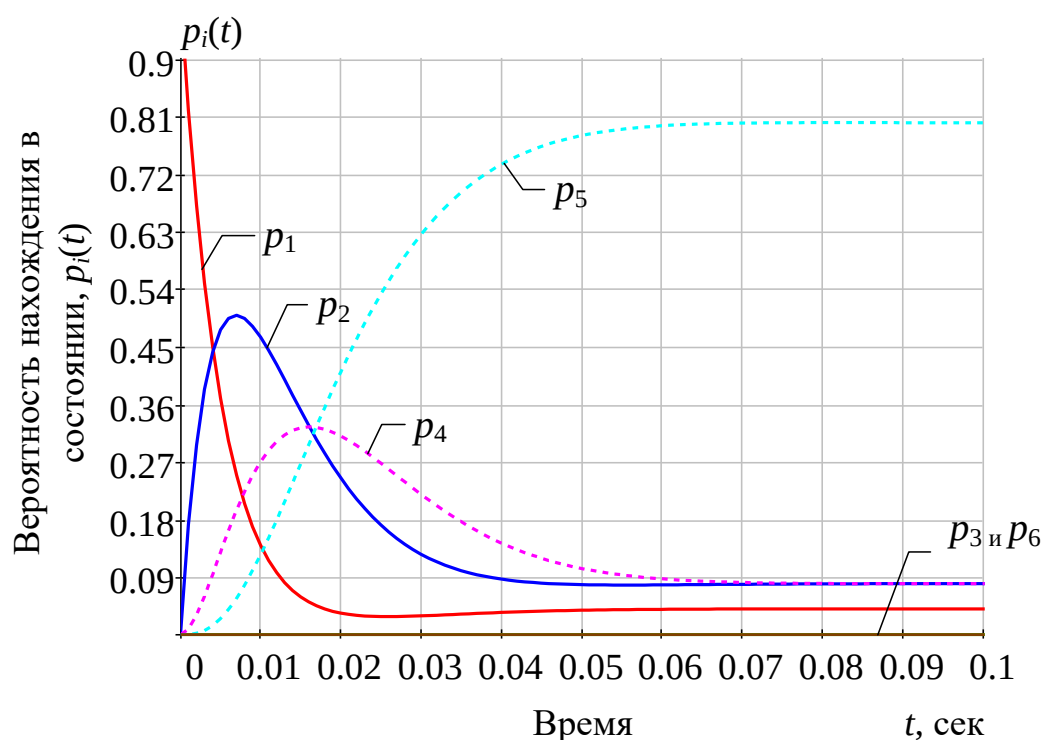


Рис.10. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий соответствующие стратегии C_3

Графики зависимостей вероятностей состояний процесса функционирования ИС при использовании маскированного канала связи от времени

$p_1(t), p_2(t), \dots, p_6(t)$ для значений интенсивностей событий соответствующие стратегии C_4 (таблица 10), представлены на рис. 11.

Таблица 10 – Числовая таблица приближенных значений $p_i(t)$ для λ в стратегии C_4

Этапы интегрирования, n	Точка интервала интегрирования, $[t_0, t_1]$	$p(t)$					
		$p_1(t)$	$p_2(t)$	$p_3(t)$	$p_4(t)$	$p_5(t)$	$p_6(t)$
1	0	1	0	0	0	0	0
2	$1 \cdot 10^{-3}$	0,819	0,172	0	$9,025 \cdot 10^{-3}$	$3,066 \cdot 10^{-5}$	0
3	$2 \cdot 10^{-3}$	0,671	0,297	0	0,033	$2,275 \cdot 10^{-4}$	0
...	...	...	...	...	...	...	...
10^3	10	0,023	0,047	0	0,465	0,465	0

Учитывая значения финальных вероятностей, вероятность вскрытия маскированного канала связи для стратегии C_4 составляет $P_{BC} = 0,452$.

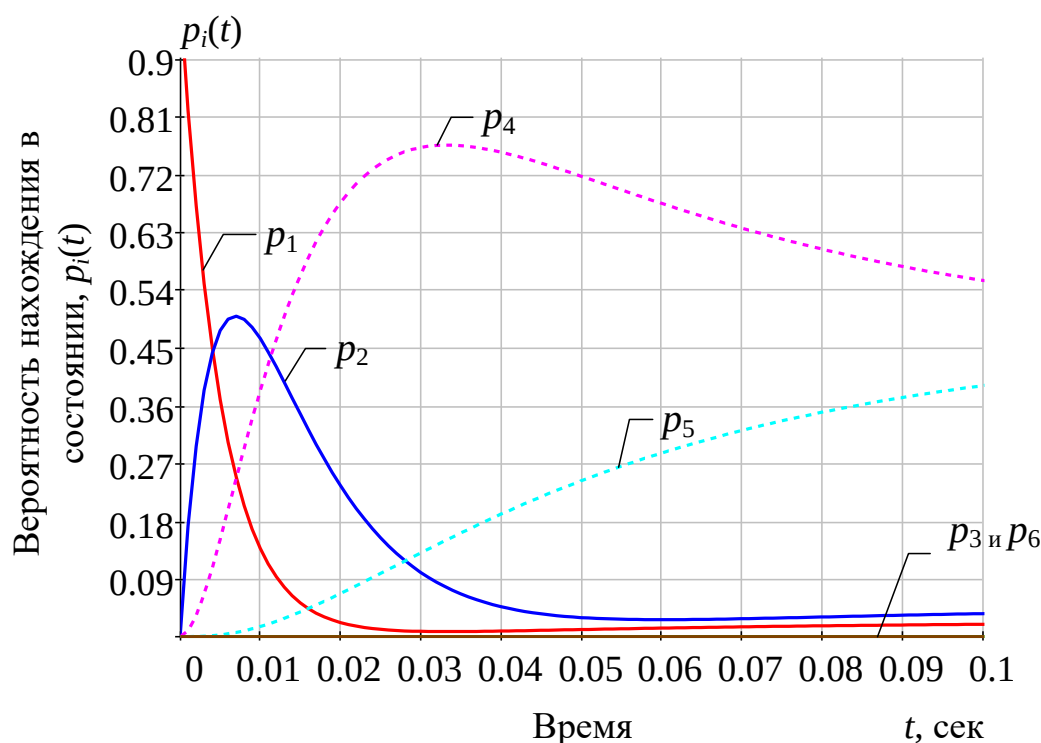


Рис.11. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий соответствующие стратегии C_4

Гистограмма зависимости вероятности вскрытия маскированного канала связи P_{BC} от стратегии функционирования распределенной ИС представлена на рис. 12.

Разработанная модель функционирования ИС при использовании маскированных каналов связи учитывает влияние и характер воздействия на ИС потоков событий при вскрытии злоумышленником реальной структуры сети. Процесс защиты взаимодействующих маршрутизаторов от вскрытия в соответствии

с данной моделью сводится к минимизации вероятности вскрытия злоумышленником реальной структуры сети $P_{BC} \rightarrow \min$. Модель позволяет: вскрыть зависимости процесса функционирования ИС при использовании маскированных каналов связи от потоков ДВ; оценивать эффективность защиты ИС от ДВ, обоснованно выбирать алгоритмы защиты от ДВ.

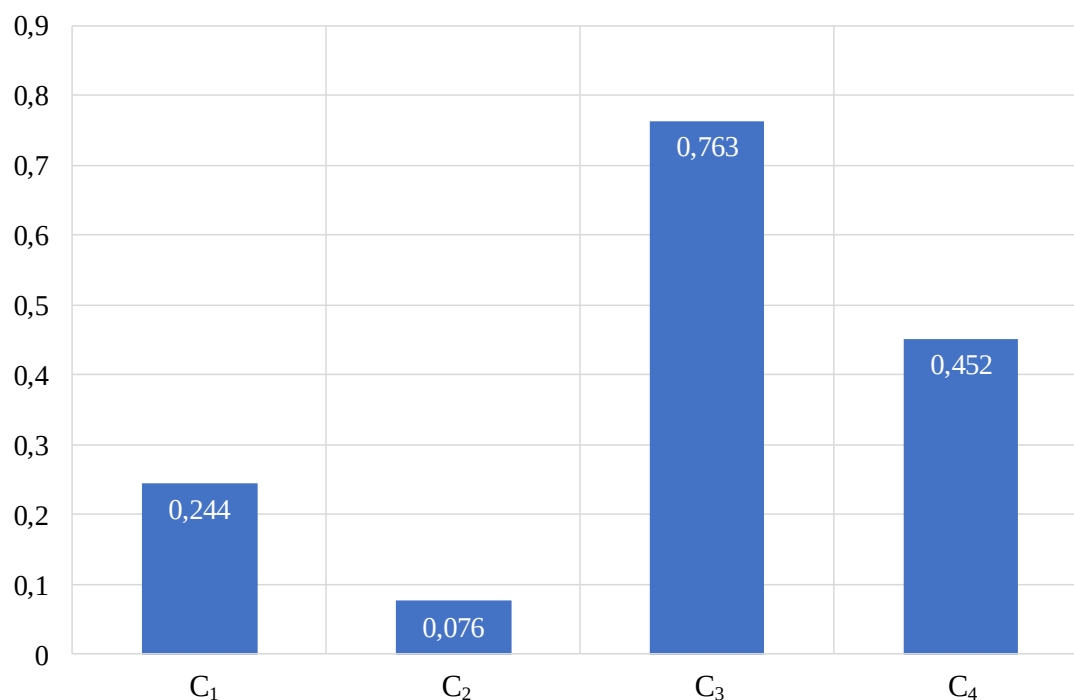


Рис.12. Гистограмма зависимости вероятности вскрытия маскированного канала связи P_{BC} от стратегии функционирования распределенной ИС

Увеличение интенсивностей заявок соответствует изменению стратегий взаимодействующих сторон. Рассмотрим стратегию C_1 при которой по маскированному каналу связи без процедуры аутентификации с высоким уровнем ДВ злоумышленника выполняется прием и передача потоков абонентского трафика.

При увеличении интенсивности потока заявок на переход в состояние простоя при разрыве маскированного соединения λ_{51} до предельного значения $\lambda_{51} = 2785$, которая соответствует состоянию системы с наибольшей частотой изменения параметров маскирования, вероятности вскрытия злоумышленником реальной структуры сети минимальна и равна $P_{BC} = 0,011$. При превышении указанного порогового значения маршрутизаторы будут постоянно находиться в состоянии использования маскированного канала, а негативное влияние ДВ злоумышленника будет минимизировано.

Научная новизна модели заключается в применении математического аппарата теории марковских случайных процессов и решении уравнений Колмогорова для исследования и решения задачи защиты распределенной ИС, использующей маскированные каналы связи, от ДВ как естественного (помехи в канале связи), так искусственного характера (атаки средств сетевой компьютерной

разведки, ориентированные на вскрытие реальной структуры распределённой ИС).

Практическая значимость заключается в нахождении вероятностных и временных характеристик, описывающих состояния процесса функционирования ИС при использовании маскированного канала связи при различных стратегиях установления и поддержания параметров соединений взаимодействующими сторонами.

Выводы

Разработанная модель функционирования распределённых информационных систем при использовании маскированных каналов связи позволяет определять вероятностные и временные характеристики, описывающие состояния процесса функционирования ИС, использующих такие каналы, при различных стратегиях информационного обмена, что позволяет оценивать состояние ИС и ее системы защиты.

Наиболее близкими аналогами представленной модели являются: по своей технической сущности – способы защиты структуры сети связи [22-26], которые обеспечивают маскирование структуры и алгоритмов функционирования ИС от компьютерной разведки и технология NAT, которая применяется в IP-сетях для маскирования внутренней структуры; по используемому теоретическому подходу к формализации решаемой задачи – работа [18], в которой решалась задача динамического управления ресурсными возможностями ИС за счет управления параметрами сетевых соединений, для решения указанной задачи использовался математический аппарат теории марковских случайных процессов.

Недостатком способов [22-26] является низкая масштабируемость маскированных каналов связи, так как организовываются только двухточечные маскированные каналы связи. Недостатком технологии NAT является низкая скорость изменения транслируемого адресного пространства в случае необходимости его динамического изменения, а также разрыв сетевых соединений абонентов при таких изменениях.

Использование представленного в работе решения позволяет повысить результативность защиты и эффективность функционирования наложенной виртуальной частной сети за счет формирования многоточечных маскированных каналов связи и динамического управления ими

Литература

1. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646 // Российская газета [Электронный ресурс]. 2016. – URL: <https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html> (дата обращения: 28.02.2020).

2. 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.

3. Maximov R. V., Krupenin A. V., Sharifullin S. R., Sokolovsky S. P. Innovative development of tools and technologies to ensure the Russian information security and core protective guidelines // Вопросы кибербезопасности. 2019. № 1 (29). С. 10-17. doi: 10.21681/2311-3456-2019-1-10-17.

4. Выговский Л. С., Максимов Р. В. Модель преднамеренных деструктивных воздействий на информационную инфраструктуру интегрированных систем связи // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2009. № 1 (73). С. 181-187.

5. Михайлов Р. Л., Макаренко С. И. Оценка устойчивости сети связи в условиях воздействия на неё дестабилизирующих факторов // Радиотехнические и телекоммуникационные системы. 2013. № 4 (12). С. 69-79.

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

7. 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.

8. Макаренко С. И. Динамическая модель системы связи в условиях функционально-разнородного информационного конфликта наблюдения и подавления // Системы управления, связи и безопасности. 2015. № 3. С. 122-185. – URL: <http://sccs.intelgr.com/archive/2015-03/07-Makarenko.pdf> (дата обращения 28.02.2020).

9. Макаренко С. И. Информационное оружие в технической сфере: терминология, классификация, примеры // Системы управления, связи и безопасности. 2016. № 3. С. 292-376. – URL: <http://sccs.intelgr.com/archive/2016-03/11-Makarenko.pdf> (дата обращения: 28.02.2020).

10. 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.

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

12. 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.

13. Максимов Р. В., Выговский Л. С. Модель преднамеренных деструктивных воздействий на информационную инфраструктуру интегрированных систем связи // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2008. № 3 (60). С. 166-173.

14. Руководящий документ «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей // Государственная техническая комиссия при Президенте Российской Федерации от 04.06.1999 г. [Электронный ресурс]. 1999. – URL: <https://fstec.ru/component/attachments/download/294> (дата обращения 28.02.2020).

15. Jajodia S., Ghosh A. K., Swarup V., Wang C., Wang X. S. Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats. – Springer, 2011. – 184 p. doi: 10.1007/978-1-4614-0977-9.

16. 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. doi: 10.21681/2311-3456-2019-6-92-101.

17. Анисимов В. В., Бегаев А. Н., Стародубцев Ю. И. Модель функционирования сети связи с неизвестным уровнем доверия и оценки её возможностей по предоставлению услуги VPN с заданным качеством // Вопросы кибербезопасности. 2017. № 1 (19). С. 6-15. doi: 10.21581/2311-3456-2017-1-6-15.

18. 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. doi: 10.24411/2410-9916-2019-10403.

19. 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. – URL: <https://www.elibrary.ru/item.asp?id=37356739> (дата обращения 28.02.2020).

20. Гаврилов А. Л., Катунцев С. Л., Максимов Р. В., Орехов Д. Н., Крупенин А. В., Медведев А. Н., Соколовский С. П. Способ защиты вычислительных сетей // Патент на изобретение RU 2682432, опубл. 19.03.2019, бюл. № 8. – URL: <https://www.elibrary.ru/item.asp?id=37358354> (дата обращения 28.02.2020).

21. Гаврилов А. Л., Катунцев С. Л., Максимов Р. В., Орехов Д. Н., Прокопенко А. В., Проскуряков И. С., Соколовский С. П. Способ защиты вычислительных сетей // Патент на изобретение RU 2680038, опубл. 14.02.2019, бюл. № 5. – URL: <https://www.elibrary.ru/item.asp?id=37356739> (дата обращения 28.02.2020).

22. Гаврилов А. Л., Катунцев С. Л., Максимов Р. В., Орехов Д. Н., Маленков Е. С., Платов Н. Е., Соколовский С. П., Шаманов А. И. Способ защиты вычислительных сетей // Патент на изобретение RU 2690749, опубл. 05.06.2019, бюл. № 16. – URL: <https://www.elibrary.ru/item.asp?id=39389503> (дата обращения 28.02.2020).

23. Крылов В. В., Кравцов К. Н. Защита IP-подсетей от DDoS-атак и несанкционированного доступа методом псевдослучайной смены сетевых адресов // Вопросы защиты информации. 2014. № 3. С. 24-31.

24. Крылов В. В., Пономарев Д. М. Способ взаимодействия терминального устройства клиента с сервером по сети интернет с повышенным уровнем защиты от DDoS-атак и система для реализации способа // Патент на изобретение RU 2496136 C1, опубл. 20.10.2013, бюл. № 29. – URL: <https://www.elibrary.ru/item.asp?id=37517935> (дата обращения 28.02.2020).

25. 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. – URL: <http://sccs.intelgr.com/archive/2018-04/08-Sherstobitov.pdf> (дата обращения 28.02.2020).

26. Кожевников Д. А., Максимов Р. В., Павловский А. В. Способ защиты вычислительной сети (варианты) // Патент на изобретение RU 2325694 C1, опубл. 27.05.2008, бюл. № 15. – URL: <https://www.elibrary.ru/item.asp?id=37654434> (дата обращения 28.02.2020).

27. Ветошкин И. С., Дрозд Ю. А., Ефимов А. А., Зорин К. М., Игнатенко А. В., Кожевников Д. А., Краснов В. А., Кузнецов В. Е., Максимов Р. В. Способ защиты вычислительной сети с выделенным сервером // Патент на изобретение RU 2449361 C2, опубл. 27.04.2012, бюл. № 12. – URL: <https://www.elibrary.ru/item.asp?id=37763810> (дата обращения 28.02.2020).

28. Голуб Б. В., Горячая А. В., Кожевников Д. А., Лыков Н. Ю., Максимов Р. В., Тихонов С. С. Способ маскирования структуры сети связи // Патент на изобретение RU 2622842, опубл. 20.06.2017, бюл. № 17. – URL: <https://www.elibrary.ru/item.asp?id=38266148> (дата обращения 28.02.2020).

29. Выговский Л. С., Заргаров И. А., Кожевников Д. А., Максимов Р. В., Павловский А. В., Стародубцев Ю. И., Худайназаров Ю. К., Юров И. А. Способ (варианты) защиты вычислительных сетей // Патент на изобретение RU 2307392, опубл. 27.09.2007, бюл. № 27. – URL: <https://www.elibrary.ru/item.asp?id=37586213> (дата обращения 28.02.2020).

30. Голуб Б. В., Краснов В. А., Лыков Н. Ю., Максимов Р. В. Способ маскирования структуры сети связи // Патент на изобретение RU 2645292, опубл. 19.02.2018, бюл. № 5. – URL: <https://www.elibrary.ru/item.asp?id=39268862> (дата обращения 28.02.2020).

31. Дыбко Л. К., Иванов И. И., Лыков Н. Ю., Максимов Р. В., Проскуряков И. С., Хорев Г. А., Шарифуллин С. Р. Способ маскирования структуры сети связи // Патент на изобретение RU 2656839, опубл. 06.06.2018, бюл. № 16. – URL: <https://www.elibrary.ru/item.asp?id=37372704> (дата обращения 28.02.2020).

32. Методический документ «Меры защиты информации в государственных информационных системах» // ФСТЭК России от 11.02.2014 г. [Электронный ресурс]. 2014. – URL: <https://fstec.ru/component/attachments/download/675> (дата обращения 28.02.2020).

33. Приказ ФСТЭК «О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 февраля

2013 г. № 17» // ФСТЭК России от 15.02.2017 г. №27 [Электронный ресурс]. 2017. – URL: <https://fstec.ru/component/attachments/download/1499> (дата обращения 28.02.2020).

34. Приказ ФСТЭК «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» // ФСТЭК России от 25.12.2017 г. №239 [Электронный ресурс]. 2017. – URL: <https://fstec.ru/en/component/attachments/download/1879> (дата обращения 28.02.2020).

35. Максимов Р. В., Соколовский С. П., Орехов Д. Н. Особенности детектирования и способы маскирования демаскирующих признаков средств проактивной защиты вычислительных сетей // Радиолокация, навигация, связь: Сборник трудов XXIV Международной научно-технической конференции. Том 2. – Воронеж: ООО «Вэлборн», 2018. – С. 169-179.

36. Iskolnyy B. B., Maximov R. V., Sharifullin S. R. Survivability Assessment of Distributed Information and Telecommunication Networks // Secure Information Technologies 2017 (BIT 2017): CEUR Workshop Proceedings conference (Moscow, Russia, December 6-7, 2017). – Moscow, Bauman Moscow Technical University, 2017. P. 59-65.

37. 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. – Воронеж: Издательство «Научно-исследовательские публикации» (ООО «Вэлборн»), 2019. – С. 639-643.

38. Maximov R. V., Ivanov I. I., Sharifullin S. R. Network Topology Masking in Distributed Information Systems // Secure Information Technologies 2017 (BIT 2017): CEUR Workshop Proceedings conference (Moscow, Russia, December 6-7, 2017). – Moscow, Bauman Moscow Technical University, 2017. P. 83-87.

39. Filkins B. IT Security Spending Trends // SANS Institute. 2016, P. 1-23.

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

41. Andres S., Kenyon B., Birkolz E. P. Security Sage's Guide to Hardening the Network Infrastructure. – Sungress Publ., 2004. – 608 p.

42. Барабаш Ю. Л., Варский Б. В., Зиновьев В. Т. Вопросы статистической теории распознавания / под. ред. Б. В. Варского. – М.: Сов. радио, 1967. – 400 с.

43. Загоруйко Н. Г. Методы распознавания и их применение – М.: Сов. радио, 1972. – 208 с.

44. RFC 1918. Address Allocation for Private Internets. 1996. – URL: <https://tools.ietf.org/html/rfc1918> (дата обращения 16.12.2019).

45. Максимов Р. В., Иванов И. И. Этюды технологии маскирования функционально-логической структуры информационных систем // Инновационная деятельность в Вооруженных Силах Российской Федерации: Труды всеармейской научно-практической конференции (Санкт-Петербург, 11-12 октября 2017 г.) – СПб.: ВАС, 2017 – 147-154 с.

46. RFC 7828. The edns-tcp-keepalive EDNS0 option. 2016. – URL: <https://tools.ietf.org/html/rfc7828> (дата обращения 28.02.20).

47. RFC 6223. Indication of support for Keep-Alive. 2011. – URL: <https://tools.ietf.org/html/rfc6223> (дата обращения 16.12.2019).

48. Заусаев А. Ф. Разностные методы решения обыкновенных дифференциальных уравнений: учебное пособие. – Самара: Самарский государственный технический университет, 2010. – 100 с.

49. Вержбицкий В. М. Основы численных методов: учебник для вузов. – М.: Высшая. Школа, 2002. – 840 с.

References

1. Information Security Doctrine of the Russian Federation of December 5, 2016 no. 646. *Rossiiskaia hazeta* [Russian Newspaper]. Available at: <https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html> (accessed 28 February 2020) (in Russian).

2. Maximov R. V., Sokolovsky S. P., Sharifullin S. R., Chernoles V. P. Innovative Information Technologies in the Context of National Security. *Innovations*, 2018, no. 3 (233), pp. 28-35 (in Russian).

3. Maximov R. V., Krupenin A. V., Sharifullin S. R., Sokolovsky S. P. Innovative Development of Tools and Technologies to Ensure the Russian Information Security and Core Protective Guidelines. *Voprosy kiberbezopasnosti*, 2019, vol. 1, no. 29, pp. 10-17. doi: 10.21681/2311-3456-2019-1-10-17 (in Russian).

4. Vygovskij L. S., Maximov R. V. Model' prednamerennykh destruktivnykh vozdествii na informatsionnuiu infrastrukturu integrirovannykh sistem svyazi [Model of Intentional Destructive Impacts on the Information Infrastructure of Integrated Communication Systems]. *St. Petersburg State Polytechnical University Journal. Computer Science. Telecommunication and Control Systems*, 2009, vol. 1, no. 73, pp. 181-187 (in Russian).

5. Mikhailov R. L., Makarenko S. I. Estimating Communication Network Stability Under the Conditions of Destabilizing Factors Affecting it. *Radio and telecommunication systems*, 2013, no. 4, pp. 69-79 (in Russian).

6. Grecihnikov E. V., Belov A. S., Shumilin V. S., Sposob upravleniia zashchishchennost'iu setei svyazi v usloviiakh destruktivnykh programmnykh vozdествii [A Method of Controlling the Security of Communication Networks in Terms of Destructive Program Influences]. *Telecommunications*, 2014, no. 3, pp. 18-22 (in Russian).

7. Pakhomova A. S., Pakhomov A. P., Razinkin K. A. To the Problem of the Development of a Structural Model of Computer Intelligence. *Information and security*, 2013, vol. 16, no. 1, pp. 115-118 (in Russian).

8. Makarenko S. I. Dynamic Model of Communication System in Conditions the Functional Multilevel Information Conflict of Monitoring and Suppression. *Systems of Control, Communication and Security*, 2015, no. 3, pp. 122-185. Available at: <http://sccs.intelgr.com/archive/2015-03/07-Makarenko.pdf> (accessed 28 February 2020) (in Russian).

9. Makarenko S. I. Information Weapons in the Technical Sphere: Terminology, Classification, Examples. *Systems of Control, Communication and Security*, 2016. no. 3, pp. 292-376. Available at: <http://sccs.intelgr.com/archive/2016-03/11-Makarenko.pdf> (accessed 28 February 2020) (in Russian).

10. Maximov R. V., Pavlovskiy A. V., Starodubcev Yu. I. *Zashchita informatsii ot tekhnicheskikh sredstv razvedki v sistemakh sviazi i avtomatizatsii* [Information Security from Technical Means of Investigation in Communication Systems and Automation]. Saint-Petersburg, Military Academy of the Signal Corps, 2007. 88 p. (in Russian).

11. Serdechnyy A. L., Sharov I. A., Sigitov V. N. Approach to Modeling Process of Cyberespionage in Information System with Changing Composition and Structure. *REDS: Radio-Electronic Devices and Systems*, 2015, vol. 5, no. 4, pp. 439-443 (in Russian).

12. Evgrlevskaya N. V., Privalov A. A., Skudneva E. V. Markovskaia model' konflikta avtomatizirovannykh sistem obrabotki informatsii i upravleniia s sistemoi destruktivnykh vozdviistvii narushitel'ia [Markov Model of Conflict of Automated Information Processing and Management Systems with the System of Destructive Effects of an Offender]. *Proceedings of Petersburg Transport University*, 2015, vol. 1, no. 42, pp. 78-84 (in Russian).

13. Maximov R. V., Vygovskij L. S. Model' prednamerennykh destruktivnykh vozdviistvii na informatsionnuu infrastrukturu integrirovannykh sistem sviazi [The Model of the Intentional Destructive Impact on the Integrated Communication Systems Infrastructure]. *St. Petersburg State Polytechnical University Journal. Computer Science. Telecommunication and Control Systems*, 2008, vol. 3, no. 60, pp. 166-173 (in Russian).

14. Guidance document. Protection against unauthorized access to information. Part 1. Software for information security. Classification by level of control of the absence of undeclared opportunities of June 4, 1999 no. 114 Available at: <https://fstec.ru/component/attachments/download/294> (accessed 28 February 2020) (in Russian).

15. Jajodia S., Ghosh A. K., Swarup V., Wang C., Wang X. S. *Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats*. Springer, 2011. 184 p. doi: 10.1007/978-1-4614-0977-9.

16. Voronchikhin I. S., Ivanov I. I., Maximov R. V., Sokolovsky S. P. Masking of Distributed Information Systems Structure in Cyber Space. *Voprosy kiberbezopasnosti*, 2019, no. 6 (34), pp. 92-101. doi: 10.21681/2311-3456-2019-6-92-101 (in Russian).

17. Anisimov V. V., Begaev A. N., Starodubtsev YU. I. Functional Model for Communication Network with Unknown Assurance Level and Evaluation of its Capabilities of Rendering VPN Service of the Set Quality. *Voprosy kiberbezopasnosti*, 2017, no. 1 (19). pp. 6-15. doi: 10.21581/2311-3456-2017-1-6-15 (in Russian).

18. 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).

19. Maximov R. V., Orekhov D. N., Proskuryakov I. S., Sokolovsky S. P. *Sposob zashchity vychislitel'nyh setej* [Method of Protection of Computer Networks]. Patent Russia, no. 2649789, 2018.

20. Gavrilov A. L., Katuncev S. L., Maximov R. V., Orekhov D. N., Krupenin A. V., Medvedev A. N., Sokolovsky S. P. *Sposob zashchity vychislitel'nyh setej* [Method of Protection of Computer Networks]. Patent Russia, no. 2682432, 2019.

21. Gavrilov A. L., Katuncev S. L., Maximov R. V., Orekhov D. N., Prokopenko A. V., Proskuryakov I. S., Sokolovsky S. P. *Sposob zashchity vychislitel'nyh setej* [Method of Protection of Computer Networks]. Patent Russia, no. 2680038, 2019.

22. Gavrilov A. L., Katuncev S. L., Maximov R. V., Orekhov D. N., Malenkov E. S., Platov N. E., Sokolovsky S. P., Shamanov A. I. *Sposob zashchity vychislitel'nyh setej* [Method of Protection of Computer Networks]. Patent Russia, no. 2690749, 2019.

23. Krylov V. V., Kravtsov K. N. IP-networks Security Against DDoS-attacks and Traffic Interception Based on IP Fast Hopping Method. *Voprosy zashchity informatsii*, 2014, no. 3, pp. 24-31 (in Russian).

24. Krylov V. V., Ponomarev D. M. *Sposob vzaimodejstviya terminal'nogo ustrojstva klienta s serverom po seti internet s povyshennym urovnem zashchity ot DDoS-atak i sistema dlya realizatsii sposoba* [The Way the Client Terminal Device Interacts with the Server over the Internet with a High Level of Protection Against DDoS Attacks and a System for Implementing the Method]. Patent Russia, no. 2496136, 2013.

25. Sherstobitov R. S., Sharifullin S. R., Maximov R. V. Masking of Departmental-Purpose Integrated Communication Networks. *Systems of Control, Communication and Security*, 2018, no. 4, pp. 136-175. Available at: <http://sccs.intelgr.com/archive/2018-04/08-Sherstobitov.pdf> (accessed 28 February 2020) (in Russian).

26. Kozhevnikov D. A., Maximov R. V., Pavlovskij A. V. *Sposob zashchity vychislitel'noj seti (varianty)* [Method of Computer Network Protection (Options)]. Patent Russia, no. 2325694, 2008.

27. Vetoshkin I. S., Drozd YU. A., Efimov A. A., Zorin K. M., Ignatenko A. V., Kozhevnikov D. A., Krasnov V. A., Kuznecov V. E., Maximov R. V. *Sposob zashchity vychislitel'noj seti s vydelennym serverom* [Method of Protection of a Computer Network with a Dedicated Server]. Patent Russia, no. 2449361, 2011.

28. Golub B. V., Goryachaya A. V., Kozhevnikov D. A., Lykov N. U., Maximov R. V., Tihonov S. S. *Sposob maskirovaniya struktury seti syazi* [A Method of Masking a Structure of a Communication Network]. Patent Russia, no. 2622842, 2017.

29. Vygovskij L. S., Zargarov I. A., Kozhevnikov D. A., Maximov R. V., Pavlovskij A. V., Starodubcev Yu. I., Hudajazarov Yu. K., Yurov I. A. *Sposob*

(varianty) zashchity vychislitel'nyh setej [Method (Options) of Protection of Computer Networks]. Patent Russia, no. 2307392, 2007.

30. Golub B. V., Krasnov V. A., Lykov N. U., Maximov R. V. *Sposob maskirovaniya struktury seti svyazi* [The Method of Masking the Structure of the Communication Network]. Patent Russia, no. 2645292, 2017.

31. Dybko L.K., Ivanov I.I., Lykov N.U., Maximov R.V., Proskuryakov I.S., Horev G.A., SHarifullin S.R. *Sposob maskirovaniya struktury seti svyazi* [The Method of Masking the Structure of the Communication Network]. Patent Russia, no. 2656839, 2018.

32. Methodical document. Information security measures in state information systems of February 11, 2014. Available at: <https://fstec.ru/component/attachments/download/675> (accessed 28 February 2020) (in Russian).

33. Order of FSTEC of February 15, 2017 no. 27 «On amendments to the Requirements for the protection of information not constituting state secrets contained in state information systems, approved by order of the Federal Service for Technical and Export Control of February 11, 2013 no. 17». Available at: <https://fstec.ru/component/attachments/download/1499> (accessed 28 February 2020) (in Russian).

34. Order of FSTEC of December 25, 2017 no. 239 «On approval of requirements for ensuring the security of significant objects of critical information infrastructure of the Russian Federation». Available at: <https://fstec.ru/en/component/attachments/download/1879> (accessed 28 February 2020) (in Russian).

35. Maximov R. V., Sokolovsky S. P., Orekhov D. N. Ways of Detecting and Hiding Computer Network Proactive Security Tools Unmasking Features. *Sbornik trudov 24 Mezhdunarodnoj nauchno-tekhnicheskoy konferencii RLNC* [Proceedings of the 24 International Scientific and Technical Conference RLNC]. Voronezh, 2018, pp. 169-179 (in Russian).

36. Iskolnyy B. B., Maximov R. V., Sharifullin S. R. Survivability Assessment of Distributed Information and Telecommunication Networks. *Selected Papers of the VIII All-Russian Conference with International Participation «Secure Information Technologies» (BIT 2017)*. Moscow, Bauman Moscow Technical University, 2017, pp. 59-65.

37. Sokolovsky S. P., Telenga A. P., Voronchikhin I. S. Moving Target Defense for Securing Distributed Information Systems. *Sbornik materialov 19 mezhdunarodnoi nauchno-metodicheskoi konferentsii Informatika. Problemy, metodologiya, tekhnologii* [Proceedings of the 19 International Scientific and Methodological Conference Informatics. Problems, methodology, technology]. Voronezh, 2019, pp. 639-643.

38. Maximov R. V., Ivanov I. I., Sharifullin S. R. Network Topology Masking in Distributed Information Systems. *Selected Papers of the VIII all-Russian Conference with International Participation «Secure Information Technologies»*. Moscow, Bauman Moscow Technical University, 2017, pp. 83-87 (in Russian).

39. Filkins B. IT Security Spending Trends. *SANS Institute*. 2016, pp. 1-23.

40. Davydov A. E., Maximov R. V., Savickij O. K. *Zashchita i bezopasnost' vedomstvennyh integrirovannyh infokommunikacionnyh sistem* [The Protection and Security of Departmental Integrated Information and Communication Systems]. Moscow, Voentelekom Publ, 2015. 520 p. (in Russian).
41. Andres S., Kenyon B., Birkolz E. P. Security Sage's Guide to Hardening the Network Infrastructure. *Sungress Publ.*, 2004. 608 p.
42. Barabash U. L., Varskij B. V., Zinov'ev V. T. *Voprosy statisticheskoy teorii raspoznavaniya* [Questions of Statistical Recognition Theory]. Moscow, 1967. 400 p. (in Russian).
43. Zagorujko N. G. *Metody raspoznavaniya i ih primenenie* [Recognition Methods and Their Application]. Moscow, 1972. 208 p. (in Russian).
44. RFC 1918. Address Allocation for Private Internets. 1996. Available at: <https://tools.ietf.org/html/rfc1918> (accessed 4 December 2019).
45. Maximov R. V., Ivanov I. I. *Etyudy tekhnologii maskirovaniya funkcional'no-logicheskoy struktury informacionnyh system* [Studies of Technology Masking the Functional and Logical structure of Information Systems]. *Trudy vsearmejskoj nauchno-prakticheskoy konferencii Innovacionnaya deyatel'nost' v Vooruzhennyh Silah Rossijskoj Federacii* [Proceedings of the All-Army Scientific and Practical Conference Innovative activity in the Armed Forces of the Russian Federation]. St. Petersburg, 2017, pp. 147-154.
46. RFC 7828. The edns-tcp-keepalive EDNS0 option. 2016. Available at: <https://tools.ietf.org/html/rfc7828> (accessed 4 December 2019).
47. RFC 6223. Indication of support for Keep-Alive. 2011. Available at: <https://tools.ietf.org/html/rfc6223> (accessed 4 December 2019).
48. Zausaev A. F. *Raznostnye metody resheniia obyknovennykh differentsial'nykh uravnenii. Uchebnoe posobie* [Difference Methods for Solving Ordinary Differential Equations]. Samara, Samara State Technical University, 2010. 100 p (in Russian).
49. Verzhbitskii V. M. *Osnovy chislennykh metodov* [Fundamentals of Numerical Methods]. Moscow, Vysshaya Shkola Publ, 2002. 840 p (in Russian).

Статья поступила 19 декабря 2019 г.

Информация об авторе

Иванов Илья Игоревич – соискатель ученой степени кандидата технических наук. Старший научный сотрудник. Краснодарское высшее военное училище. 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: 7570745@mail.ru

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

Distributed Information Systems Functioning Model with Masked Communication Links

I. I. Ivanov

Relevance: Knowing information system unmasking attributes allows an attacker to reconstruct an information system structure with a high degree of accuracy. To protect against information system structure (topology) analysis by network gathering tools, masking methods are used that counter network intelligence. For this, the logical redundancy is introduced into the information system structure, IP and MAC addresses in transmitted messages are continuously changing. Using masking methods eliminates a single point of failure in the network and misleads an attacker regarding the information system structure and functioning algorithms. **The aim of the work** is to develop distributed information systems functioning model with masked communication links for mathematical support of the multi-link masked topology protocol. **Methods:** In this work Markovian processes with discrete states and continuous time are used for solve the problem of information system functioning with different interconnection strategies and controlling network intelligence resources. **The novelty of the paper** is the use of the Markovian processes and the Kolmogorov equations for control an information system resource by network connection parameters. **Results:** The developed technical solution allows to increase the protection and efficiency of using an overlay virtual private network. Finding probability and time characteristics, which describe information system functioning process, is the **practical relevance of the work**.

Key words: distributed information system, network intelligence, masked link, network protocol.

Information about Author

Ilya Igorevich Ivanov – applicant for academic degree of candidate of technical sciences. Senior Researcher. Krasnodar Higher Military School. 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: 7570745@mail.ru

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