УДК 004.057.7

Модель функционирования и алгоритм конфигурирования адресации ложных сетевых информационных объектов в условиях сетевой разведки

Лебедкина Т. В., Хорев Г. А.

Постановка задачи: *расширение возможностей и повышение результативности сетевой разведки по вскрытию информационных систем актуализируют вопросы по обеспечению их информационной безопасности. Инерционные свойства применяемых средств защиты в полной мере не обеспечивают защищенность информационных систем от сетевой разведки и компьютерных атак. Технология ложных сетевых информационных объектов – ресурс безопасности, предназначение которого состоит в том, чтобы быть исследованным или подвергнутым кибератакам со стороны нарушителя информационной безопасности.* ***Целью работы*** *является разработка модели и алгоритма, позволяющих обеспечить защищенность информационной системы, обеспечить оперативное обслуживание санкционированных клиентов с одновременным снижением качества обслуживания запросов от средств злоумышленника посредством выбора оптимального режима функционирования ложных сетевых информационных объектов.* ***Используемые методы****: формализация процесса функционирования ложных сетевых информационных объектов при конфигурировании параметров адресации в условиях сетевой разведки путем представления процесса их взаимодействия в виде марковского случайного процесса с дискретными состояниями и непрерывным временем, а также решение задачи управления численными и аналитическими методами.* ***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 функционирования ложных сетевых информационных объектов. Элементами новизны разработанного алгоритма является применение представленной модели функционирования ложных сетевых информационных объектов, постановке и решении прямой задачи исследования операций для максимизации вероятности формирования и отправки актуальных ложных данных на запросы от средства сетевой разведки.* ***Результат****: проведенные расчеты свидетельствуют о повышении защиты информационных ресурсов за счет своевременной обработки запросов от средства сетевой разведки и отправки ему ответов за время, не превышающее среднее время отклика реального узла сети на TCP- и ARP-запросы. Представленный алгоритм позволяет повысить результативность защиты за счет снижения возможностей средств сетевой разведки по идентификации ложных сетевых информационных объектов, путем конфигурирования параметров адресации.* ***Практическая значимость****: заключается в нахождении вероятностно-временных характеристик, описывающих состояния процесса функционирования ложных сетевых информационных объектов в условиях сетевой разведки, а также в решении прямой задачи исследования операций для максимизации вероятности формирования и отправки актуальных ложных данных на запросы от средств сетевой разведки и снижение возможностей компрометации средств защиты.*

Ключевые слова: *сетевая разведка, ложные сетевые информационные объекты, компьютерная атака, протокол, устойчивость, случайный процесс.*

Библиографическая ссылка на статью:
Лебедкина Т. В., Хорев Г. А. Модель функционирования и алгоритм конфигурирования адресации ложных сетевых информационных объектов в условиях сетевой разведки // Системы управления, связи и безопасности. 2023. № 2. С. 23–62. DOI: 10.24412/2410-9916-2023-2-23-62

Reference for citation:
Lebedkina T. V., Horev G. A. Functioning model and algorithm for configuring the addressing of false network information objects in the conditions of network reconnaissance. *Systems of Control, Communication and Security*, 2023, no. 2, pp. 23–62 (in Russian). DOI: 10.24412/2410-9916-2023-2-23-62

Актуальность

Рост количества и сложности компьютерных атак на доступность информации, как одного из критериев информационной безопасности, остается основной тенденцией последних лет в сфере компьютерных преступлений. Это связано со стремительным ростом вычислительных мощностей, как серверного оборудования, так и персональных электронных вычислительных машин.

Наиболее важным из этапов подготовки компьютерных атак является сетевая разведка, которая проводится с целью добывания информации о составе, структуре, алгоритмах функционирования информационных систем (ИС), 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]. Прозрачность функционирования (определяется известными протоколами информационного взаимодействия – использованием стека протоколов TCP/IP) и общность архитектуры (определяется применением мировых практик при проектировании ИС) приводит к тому, что злоумышленник при анализе ИС обладает всей полнотой информации об их характеристиках [7–9].

Традиционные системы безопасности ИС, использующие такие средства сетевой защиты как межсетевые экраны, системы обнаружения вторжений и антивирусы являются пассивными и по своей природе могут обнаруживать только известные атаки.

Данный вопрос особенно актуален в настоящее время, когда, теоретически, злоумышленник располагает неограниченным запасом времени для изучения инфраструктуры и поиска в ней уязвимых мест – он имеет существенное преимущество перед защитой, возможности которой в общем случае ограничены созданием средств мониторинга и дополнительных барьеров, призванных блокировать проникновение вредоносных программ и попыток получения несанкционированного доступа.

Для современной защиты ИС от сетевой разведки (СР) и компьютерных атак применяются новые технические решения, реализующие механизмы введения в заблуждение нарушителей, представляющие собой специальный тип механизмов защиты, предназначенных для навязывания нарушителям ложной информации с целью уменьшения возможности реализации угроз (вторжения), облегчения обнаружения атак, замедления действий по реализации угроз и исследования намерений и стратегий нарушителей [2–6, 8–29].

Для выполнения этих подзадач могут быть использованы ложные сетевые информационные объекты (ложные информационные системы, или «обманные» системы, называемые также имитаторами ИС или «ловушками» [30, 31]). Основными функциями таких систем являются привлечение и удержание внимания злоумышленников на ложных информационных целях, введение злоумышленников в заблуждение, обнаружение и фиксация действий нарушителей, их контроль, а также сбор и агрегация данных о действиях нарушителей из различных источников. Эти системы защиты представляют собой программно-аппаратные средства обеспечения информационной безопасности, реализующие функции сокрытия и маскирования защищаемых информационных ресур-

сов, а также дезинформации нарушителей. С помощью фиксации и сбора данных, обнаружения вторжений и обмана нарушителей (на основе имитации ложных целей, уязвимых для нападения), а также других механизмов эти системы позволяют в реальном времени выявлять атаки, направлять их по ложному следу, ограничивать их распространение, идентифицировать нарушителей, исследовать их действия и определять намерения [32].

Следует отметить, что известные технические решения, реализующие механизмы введения в заблуждение нарушителей, еще недостаточно проработаны и обладают существенными недостатками, а задачи приведения в соответствие таких мер защиты ИС (централизованному) замыслу противодействия средствам СР только начинают формулироваться отдельными авторами и их кооперациями [2–6, 10–29,], что обуславливает актуальность проводимого исследования.

Анализ объекта исследования

Ложный сетевой информационный объект (ЛСИО) – это виртуальный объект реальной информационной системы (ИС), эмулирующий работу целевой системы, и воздействующий на средства сетевой разведки (СР) с целью введения их в заблуждение о структуре и топологии ИС, затруднения и препятствования атакам на целевую систему и навязывания специально подготовленной ложной информации.

Ложный сетевой информационный объект может имитировать отдельный протокол (SMTP, FTP, SOCKS, HTTP, SSH и т.д.), отдельную рабочую станцию или сервер под управлением операционной системы и целые ЛВС, их уязвимости и защищенность.

ЛСИО классифицируют по уровню взаимодействия со средством СР следующим образом:

- низкий – эмулируют сервисы (и соответствующие ОС), ограничивая количество действий, которые может выполнить средство СР с ЛСИО. Это взаимодействие ограничивается тем, насколько подробно эмулируются сервисы;
- средний – отличительной особенностью таких ЛСИО является создание виртуальных ОС вместо реализации эмуляции сервисов. Виртуальная ОС контролируется со стороны реальной ОС, но предоставляет функциональность реальной ОС, хотя и специально ограниченную для уменьшения риска компрометации системы;
- высокий – основаны на применении реальных информационных ресурсов, в том числе ОС и приложений. Вместо эмуляции сервисов используются реальные сервисы. ЛСИО с высоким уровнем взаимодействия является реальной ИС, отличающейся от целевой системы тем, что она не выполняет целевых задач (не содержит реальной информации).

Перечисленные ЛСИО эмулируют сервисы реальных целевых систем и отличаются лишь уровнем реализации ЛСИО (ПО, виртуальная ОС или реальный узел ИС), который не влияет на организацию процесса взаимодействия

ЛСИО со средством СР. Далее в работе будет рассмотрен ЛСИО без детализации уровня реализации, так как взаимодействие ЛСИО со средством СР реализуется протоколами семейства TCP/IP.

Благодаря системе управления ЛСИО способен:

- менять свою конфигурацию;
- производить истощение ресурсов средств СР, путем удержания безответного соединения;
- переводить запросы средств СР из реальной сети в ложную.

Это способствует повышению защищенности ИС, где развернут ЛСИО, и повышению идентичности ЛСИО эмитируемым целевым системам.

Во время сетевой разведки ИС злоумышленник предполагает наличие в ней ЛСИО, поэтому средства СР усовершенствуются, меняются подходы к исследованию ИС с целью выявления в ней ЛСИО. Но остается неизменным подход получения первоначальных данных о ИС с целью ее анализа и создания профиля атакуемой цели – сканирование.

Сканирование – это набор процедур, позволяющих идентифицировать узлы, порты и сервисы целевой системы, различаются следующие типы сканирования [7, 8]:

- сетевое сканирование – определение находящихся в ИС узлов;
- сканирование портов – выявление открытых портов и функционирующих сервисов;
- сканирование безопасности системы – выявление известных уязвимостей ОС.

Сетевое сканирование (ARP-сканирование) позволяет обнаружить все подключенные к сети устройства, в том числе и скрытые, по заданному IP-адресу. Ответом на ARP-запрос является подтверждение существования узла ИС с заданным IP-адресом и его аппаратный MAC-адрес, который необходим для коммуникации внутри сети.

ARP-сканирование основано на работе ARP-протокола:

1. Узел, которому нужно выполнить отображение адреса IP на аппаратный адрес (MAC-адрес), формирует запрос ARP с адресом IP получателя, вкладывает его в кадр протокола канального уровня и рассылает его широковещательно.
2. Все узлы сегмента локальной сети получают запрос ARP и сравнивают указанный там адрес IP с собственным.
3. В случае совпадения собственного адреса IP с полученным в запросе ARP, узел формирует ответ ARP, в котором указывает и свой адрес IP, и свой аппаратный адрес, и отправляет его уже адресно на аппаратный адрес отправителя запроса ARP.

Преобразование адресов выполняется путём поиска в таблице соответствия адресов IP и MAC. Эта таблица, называемая таблицей ARP, хранится в памяти операционной системы узла и содержит записи для каждого известного ей узла сети. В двух столбцах содержатся адреса IP и MAC. Если требуется преоб-

разовать адрес IP в MAC, то в таблице ARP ищется запись с соответствующим адресом IP.

Исходя из описания принципа работы ARP-протокола, получаем, что ARP-пакет может быть исходящим или входящим. Это определяется значением поля заголовка ARP-протокола «код операции» (рис. 1):

– если значение поля равно 1, то ARP-пакет является входящим для узла ИС и содержит запрос от другого узла ИС на проверку IP-адреса узла-получателя запроса;
– если значение поля равно 2, то ARP-пакет является исходящим от узла ИС с ответом на ARP-запрос от другого узла ИС и содержит MAC-адрес узла-отправителя и его IP-адрес (рис. 2).

Рис. 1. Структура ARP-пакета

Таким образом, средство СР, находясь в подсети ИС, с помощью легитимного алгоритма ARP-сканирования может узнать структуру и состав подсети ИС (рис. 2).

Сканирование портов (TCP-сканирование) основано на особенностях работы TCP-протокола транспортного уровня, а именно на схеме «трехэтапного» согласования, которое позволяет синхронизировать передающий и получающий узлы и установить сессию (рис. 3).

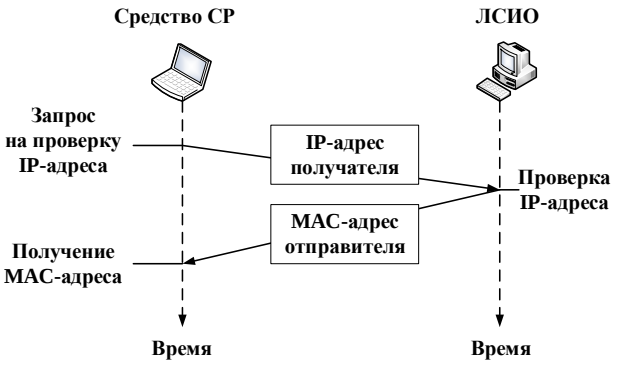

Рис. 2. Иллюстрация последовательности ARP-сканирования

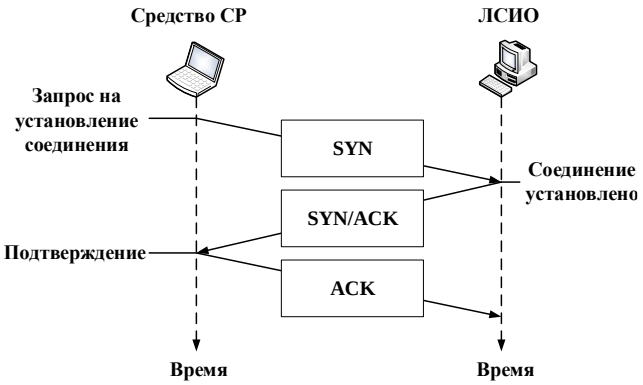

Рис. 3. Иллюстрация последовательности установки TCP-соединения

TCP-сканирование основано на работе TCP-протокола:

1. Узел ИС (средство СР) отправляет сегмент-запрос с установленным флагом SYN другому узлу ИС (ЛСИО). При этом сегменту присваивается произвольный порядковый номер в интервале от 1 до 232, относительно которого будет вестись дальнейший отсчет последовательности сегментов в соединении.
2. ЛСИО получает запрос с установленным флагом SYN и отправляет ответный сегмент с одновременно установленными флагами SYN+ACK, при этом записывает в поле «номер подтверждения», полученный порядковый номер, увеличенный на 1 (что подтверждает получение первого сегмента), а также устанавливает свой порядковый номер, который, как и в SYN-сегменте, выбирается произвольно.
3. После получения средством СР сегмента с флагами SYN+ACK соединение считается установленным, средство СР, в свою очередь, отправляет в ответ сегмент с флагом ACK, с обновленными номерами последовательности, и не содержащий полезной нагрузки.
4. Начинается передача данных.

Флаги SYN и ACK являются одними из возможных значений поля заголовка TCP-протокола «флаги» (рис. 4).

Рис. 4. Структура TCP-заголовка пакета сообщений

Используя этот легальный алгоритм, злоумышленник, представившись в ИС узлом, может выяснить, какие порты открыты на другом узле ИС, то есть понять, какие сервисы используются в системе, какая операционная система.

В процессе функционирования ЛСИО, также, как и средство СР, производит сканирование подсети ИС, в которой располагается, для сбора, обработки, формирования и поддержания в актуальном состоянии базы данных с ложными данными о структуре и составе подсети ИС, и обрабатывает поступающие к ЛСИО запросы от средства СР в условиях ограниченного вычислительного ресурса. Ограниченность вычислительного ресурса выражается в том, что ЛСИО способен обработать ограниченное количество запросов за единицу вре-

мени без переполнения буфера обмена ввиду выделения вычислительного ресурса на анализ поступивших ответов от легитимных узлов ИС и запросов от средства СР, а также на обработку транзакций в базах данных.

Задача ЛСИО – оперативно ответить на запрос средства СР ложной, заранее сформированной информацией, которая соответствует целевой подсети ИС, то есть является актуальной в настоящее время.

С целью поддержания идентичности реальным узлам ИС ЛСИО формирует базы данных ложных MAC-адресов и TCP-портов на основе сканирования действующей подсети ИС.

Время изменений структуры и состава подсети ИС заранее неизвестно (отключение или добавление новых узлов сети, замена сетевых карт на узлах, назначение новых TCP-портов для служб ОС), поэтому периодичность сканирования подсети ИС ЛСИО выбирается из соображения пропускной способности сети, но не реже периода «старения» ARP-таблиц узлов сети.

Единого стандарта тайм-аута обновления ARP-таблиц не существует и для каждой платформы устанавливается производителем:

Microsoft: 2 мин.
Cisco IOS: 4 ч.
Cisco NX-OS: 25 мин.
Cisco IOS 15M&T: 4 ч.
Juniper: 20 мин.
Linux: от 15 с до 2 мин.

Время проведения сетевой разведки средством СР также неизвестно и может совпасть с периодом сканирования ЛСИО подсети ИС. Во время обработки запросов от средства СР ЛСИО производит выборку из базы данных ложных MAC-адресов и TCP-портов в зависимости от типа запроса средства СР. Задача формирования и отправки ответа на запрос от средства СР является для ЛСИО приоритетной.

Таким образом, задача ЛСИО заключается в сокращении времени обработки запросов средства СР с учетом формирования баз данных с ложной информацией, чего можно достичь конфигурированием параметрами функционирования ЛСИО.

Постановка задачи

Приведенное описание процесса функционирования ЛСИО позволяет сформулировать постановку задачи на моделирование ЛСИО при конфигурировании параметров адресации в условиях СР.

Разработка модели функционирования ЛСИО необходима для описания существенных свойств процессов конфигурирования баз данных с ложными данными и режимов обработки запросов от средства СР, что необходимо для разработки алгоритма конфигурирования параметров и режимов функционирования ЛСИО в условиях СР. Математическая модель функционирования ЛСИО позволит произвести количественную оценку эффективности предлагаемых средств защиты. В настоящее время разработан обширный теоретико-

методологический аппарат формализованного представления функционирования информационных систем различного назначения [27–29, 33–42].

Потоки событий от средства СР и узлов ИС к ЛСИО и обратно представляют собой последовательность управления параметрами функционирования ЛСИО (содержание поля «флаги» TCP-пакета и поля «код операции» ARP-пакета), приводящими к изменению оперативности выдачи ЛСИО ответных пакетов средству СР.

В общем случае искомыми характеристиками исследуемого процесса являются:

- пространство состояний S_i системы (конечное множество событий, описывающих существенные свойства системы) и возможные траектории перехода системы из состояния в состояние (характеризуются ориентированным графом состояний моделируемой системы);
- распределение вероятностей пребывания системы в состояниях в начальный момент времени;
- функции распределения $\{F_{ij}(t)\}$ непрерывных случайных величин $\{T_{ij}\}$ времени ожидания перехода системы из соответствующих состояний, где $F_{ij}(t)=f(a_{ij},t)$, а в случае экспоненциального закона распределения параметры a_{ij} являются интенсивностями λ_{ij} функций распределения $F_{ij}(t)=1-e^{-\lambda t}$;
- множество управляемых параметров $X=\{a_{ij}^{c}\}$;
- множество неуправляемых параметров $A=\{a_{ij}^{nc}\}$;
- вероятности $p_i(t)$ пребывания системы в состоянии i в момент времени t, а также финальные вероятности p_i;
- функция распределения $G_{ij}(t)$ времени первого посещения системой состояния j, при условии, что в момент времени $t=0$, система находилась в состоянии i, позволяющая вычислить оперативность функционирования ЛСИО.

Функция распределения $G_{ij}(t)$ принята в исследовании показателем оперативности конфигурирования адресации ЛСИО в условиях СР.

С практической точки зрения наиболее целесообразно изменение оперативности оценивать по значению времени завершения конфигурирования адресации ЛСИО при фиксированном значении $G_{ij}(t)$.

Для оценки эффективности предполагается решение прямой задачи исследования операций: чему будет равен показатель эффективности $G_{ij}(t)$, если принять какое-то решение $a_{ij}^{c} \in X$ в условиях $a_{ij}^{nc} \in A$.

Модель функционирования ложных сетевых информационных объектов при конфигурировании параметров адресации в условиях сетевой разведки

Пусть имеется ЛСИО S, реализующая конфигурирование параметров адресации в условиях СР. Моделируемая система S с течением времени переходит из одного состояния в другое.

Моменты возможных переходов ЛСИО из состояния в состояние происходят под действием потоков событий, характеризующиеся их интенсивностью λ, переводящих ЛСИО в различные состояния функционирования. Характер выбранных значений интенсивностей определяется в соответствии с ситуациями взаимодействия ЛСИО и средства СР – сторон ресурсного конфликта.

Модель функционирования ЛСИО учитывает обмен запросами с ЛСИО санкционированных клиентов, а также несанкционированных клиентов (средств СР), осуществляющих сетевую разведку.

Использование модели предполагает поиск ситуаций взаимодействия ЛСИО и средства СР, и позволяет перейти к вероятностной оценке способности обеспечивать бескомпроматное диалоговое взаимодействие со средством СР. Учет в марковской модели времени формирования ЛСИО исходящих данных на запросы от средства СР в зависимости от ситуаций взаимодействующих сторон позволяет исследовать динамику функционирования ЛСИО.

Процесс функционирования ЛСИО можно представить, как марковский случайный процесс с дискретными состояниями и непрерывным временем. Необходимое условие применения математического аппарата однородных марковских случайных процессов с дискретными состояниями и непрерывным временем – потоки событий, инициирующих переходы системы из состояния в состояние, являются простейшими (обладают свойствами стационарности, ординарности и отсутствия последействия) [43, 44].

Исходными данными, при использовании аппарата цепей Маркова с непрерывным временем в ходе моделирования различных систем являются:

- пространство состояний системы (конечное множество несовместных (несовместимых) событий, описывающих существенные свойства системы и изменяющиеся «скачкообразно») (таблица 1) и возможные траектории перехода системы из состояния в состояние (характеризуются ориентированным графом состояний моделируемой системы, представленным на рис. 5);
- распределение вероятностей пребывания системы в состояниях в начальный момент времени;
- интенсивности потоков событий – (запросов, ответов), вызывающих переход системы из состояния в состояние (таблица 2).

Таблица 1 – Дискретные состояния ЛСИО

S_i	Интерпретация состояний в терминах объекта и предмета исследования
S_1	Состояние ожидания потока входных данных – ЛСИО находится в состоянии простоя, не принимает и не передает потоки данных
S_2	Состояние ожидания потока принятых данных – анализ поступивших данных от клиентов сети (легитимных и средств СР)
S_3	Состояние ожидания потока проанализированных ARP-запросов – обработка транзакций в базе данных ложных MAC-адресов
S_4	Состояние ожидания потока проанализированных TCP-запросов – обработка транзакций в базе данных ложных TCP портов

S_i	Интерпретация состояний в терминах объекта и предмета исследования
S_5	Состояние ожидания потока обработанных запросов – формирование исходящих данных от ЛСИО
S_6	Состояние ожидания потока сформированных данных – оценка значения доступности ЛСИО и отправка сформированных исходящих сообщений

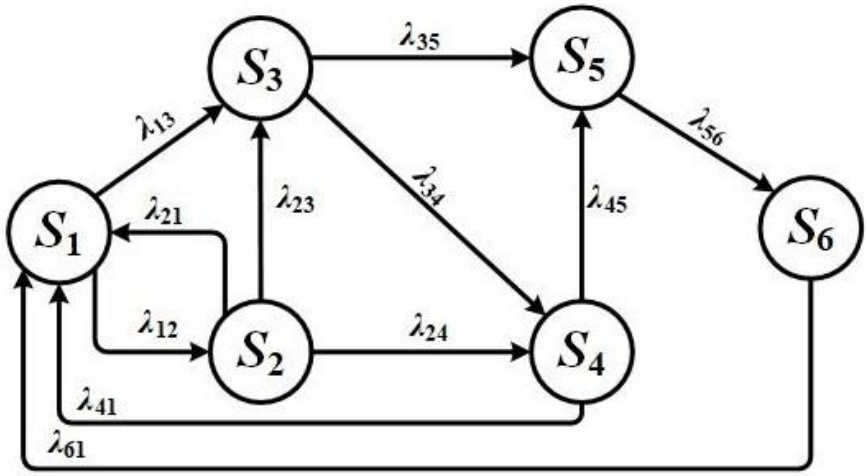

Рис. 5. Граф состояний функционирования ЛСИО при конфигурировании параметров адресации в условиях СР

Физический смысл интенсивности λ_{ij} – математическое ожидание количества случайных событий, вызывающих переход системы из состояния S_i в состояние S_j в единицу времени.

Таблица 2 – Интенсивности потоков событий

λ_{ij}	Интерпретация интенсивностей в терминах объекта и предмета исследования
λ_{13}	Интенсивность потока событий на выборку исходных данных из ARP-таблицы с ложными MAC-адресами для формирования запроса клиентам ИС
λ_{12}	Интенсивность потока событий на анализ поступивших запросов (ответов) ЛСИО от средств СР (клиентов ИС)
λ_{21}	Интенсивность потока событий на отказ в формировании ответного пакета данных (игнорирование запроса СР)
λ_{23}	Интенсивность потока событий на формирование актуальной ARP-таблицы с ложными MAC-адресами или выдачу исходных данных для формирования ответа на запрос СР
λ_{24}	Интенсивность потока событий на формирование актуальной таблицы с ложными TCP портами или выдачу исходных данных для формирования ответа на запрос СР
λ_{34}	Интенсивность потока событий на создание актуальной таблицы ложных TCP портов (актуальная ARP-таблица с ложными MAC-адресами создана)
λ_{35}	Интенсивность потока событий на формирование ARP-запроса клиентам ИС или ARP-ответа средству СР
λ_{41}	Интенсивность потока событий на перевод ЛСИО в исходное состояние (таблица ложных TCP портов создана)
λ_{45}	Интенсивность потока событий на формирование TCP-запроса (SYN) клиентам ИС или TCP-ответа (ACK) средству СР

λ_{ij}	Интерпретация интенсивностей в терминах объекта и предмета исследования
λ_{56}	Интенсивность потока событий на открытие канала передачи данных и отправку ответов средству СР или запросов клиентам ИС
λ_{61}	Интенсивность потока событий на изменение режима обработки входных данных и закрытие канала передачи данных

Содержательное описание перехода моделируемой системы из состояния S_i в состояние S_j под воздействием потоков событий с интенсивностями λ_{ij} может быть представлено следующим образом.

Пусть S_1 – начальное состояние моделируемого ЛСИО, в котором он не принимает и не передает потоки данных, в этом случае средство СР, как и клиенты ИС не ведут информационный обмен с ЛСИО.

С периодичностью T = 300 с ЛСИО переходит в состояние S_3 потоком событий с интенсивностью λ_{13}, в котором осуществляется выборка из актуальной базы данных сгенерированных MAC-адресов (далее – БД$_{MAC}$) данные для формирования ARP-запросов легитимным клиентам ИС. Поток событий с интенсивностью λ_{35} переводит систему в состояние S_5, где обработчик событий формирует из полученных данных БД$_{MAC}$ ARP-запросы установленного образца и потоком событий с интенсивностью λ_{56} переводит систему в состояние S_6, в котором ЛСИО отправляет ARP-запросы через открытый канал связи легитимным узлам ИС. После чего ЛСИО переходит в состояние покоя (состояние S_1) потоком событий с интенсивностью λ_{61}. При завершении формирования актуальной БД$_{MAC}$ потоком событий с интенсивностью λ_{34} ЛСИО переходит в состояние S_4, в котором осуществляется выборка из актуальной базы данных сгенерированных ложных TCP-портов (далее – БД$_{TCP}$) данные для формирования TCP-запросов легитимным клиентам ИС. Поток событий с интенсивностью λ_{45} переводит систему в состояние S_5, где обработчик событий формирует из полученных данных БД$_{TCP}$ TCP-запросы установленного образца и потоком событий с интенсивностью λ_{56} переводит систему в состояние S_6, в котором ЛСИО отправляет TCP-запросы (SYN) через открытый канал связи легитимным узлам ИС. После чего ЛСИО переходит в состояние покоя (состояние S_1) потоком событий с интенсивностью λ_{61}.

После направления клиентами ИС или средством СР ложному сетевому информационному объекту потока ответов на запросы ЛСИО или запросов на инициализацию соединения, соответственно, с потоком событий с интенсивностью λ_{12} система переходит из состояния S_1 в состояние S_2, в котором производится первичная обработка и анализ входящих потоков данных для определения источника сообщений. Если это запросы на инициализацию соединения от узла ИС (легитимного или нелегитимного) в адрес несуществующего узла ИС (в базе данных ЛСИО нет такого IP или MAC-адреса для эмуляции), то ЛСИО игнорирует данный запрос и потоком событий с интенсивностью λ_{12} переходит в исходное состояние S_1. Если в базе данных ЛСИО есть такой IP или MAC-адрес для эмуляции, то в зависимости от источника сообщения (легитимный узел или средство СР) и типа поступивших пакетов (TCP или ARP-пакеты)

ЛСИО потоками событий с интенсивностями λ_{23} или λ_{24}, соответственно, переходит или в состояние S_3 или в состояние S_4.

Если источником сообщений являются легитимные узлы ИС, то ЛСИО в состоянии S_3 (поступил ARP-ответ) осуществляет проверку актуальности $БД_{MAC}$ и при наличии коллизий выполняет генерацию новых ложных MAC-адресов (формирует актуальную $БД_{MAC}$). При поступлении TCP-пакета (ACK) система переходит в состояние S_4 для проверки актуальности $БД_{TCP}$ и при наличии изменений производит генерацию новых ложных TCP-портов. Затем, в зависимости от текущего состояния, ЛСИО потоками событий с интенсивностями λ_{35} или λ_{45} переходит в состояние S_5, в котором формирует запросы легитимным узлам ИС для дальнейшего формирования баз данных. Потоком событий с интенсивностью λ_{56} переходит в состояние S_6, открывает канал передачи данных и отправляет сообщения легитимным узлам ИС. Потоком событий с интенсивностью λ_{61} ЛСИО переходит в состояние S_1 на прием входящих сообщений.

Если источником входящего сообщения является средство СР (ЛСИО находится в состоянии S_2), то производится проверка IP-адреса хоста-отправителя пакета на легитимность: если IP-адрес отсутствует в списке разрешенных IP-адресов, то есть средство СР должно находится в подсети с ЛСИО, то поступающий запрос игнорируется и ЛСИО потоком событий с интенсивностью λ_{21} переходит в начальное состояние S_1. Если IP-адрес входит в «белый» список, то ЛСИО производит дальнейший анализ на соответствие входящих данных одному из сетевых протоколов (ARP или TCP) и включается счетчик времени обработки поступивших запросов от средства СР.

При поступлении ARP-запроса от СР потоком событий с интенсивностью λ_{23} переводит систему в состояние S_3 для выборки из $БД_{MAC}$ необходимых данных для формирования ответа на запрос. Поток событий с интенсивностью λ_{35} система переходит в S_5, в котором формируется ARP-ответ и считывается показание счетчика времени на обработку запроса от средства СР. Если время обработки запроса от средства СР превышает допустимое значение, то ЛСИО переходит в режим обработки только запросов от средства СР. В ином случае ЛСИО продолжает обрабатывать также и входящие ответы от легитимных узлов ИС. Далее потоком событий с интенсивностью λ_{56} система переходит в состояние S_6 для открытия канала связи и отправки ARP-ответа средству СР. После чего ЛСИО переходит в исходное состояние покоя S_1 потоком событий с интенсивностью λ_{61}.

При поступлении TCP-запроса поток событий с интенсивностью λ_{24} переводит систему в состояние S_4 для выборки из $БД_{TCP}$ необходимых данных для формирования ответа на запрос. Поток событий с интенсивностью λ_{45} переводит систему в состояние S_5, в котором ЛСИО формирует TCP-ответ (ACK) и также считывается показание счетчика времени на обработку запроса от СР. Далее потоком событий с интенсивностью λ_{56} система переходит в состояние S_6 для открытия канала связи и отправки ARP-ответа средству СР. После чего ЛСИО переходит в исходное состояние покоя S_1 потоком событий с интенсивностью λ_{61}.

Моделируемая ЛСИО при конфигурировании параметров адресации в условиях СР может находиться в состояниях S_i с разной вероятностью $p_i(t)$. По размеченному графу состояний составлены уравнения Колмогорова – дифференциальные уравнения с неизвестными функциями $p_i(t)$:

$$\begin{cases} \frac{dp_1(t)}{dt} = \lambda_{21} p_2(t) + \lambda_{41} p_4(t) + \lambda_{61} p_6(t) - (\lambda_{12} + \lambda_{13}) p_1(t), \\ \frac{dp_2(t)}{dt} = \lambda_{12} p_1(t) - (\lambda_{21} + \lambda_{23} + \lambda_{24}) p_2(t), \\ \frac{dp_3(t)}{dt} = \lambda_{23} p_2(t) + \lambda_{13} p_1(t) - (\lambda_{35} + \lambda_{34}) p_3(t), \\ \frac{dp_4(t)}{dt} = \lambda_{34} p_3(t) + \lambda_{24} p_2(t) - (\lambda_{41} + \lambda_{45}) p_4(t), \\ \frac{dp_5(t)}{dt} = \lambda_{35} p_3(t) + \lambda_{45} p_4(t) - \lambda_{56} p_5(t), \\ \sum_{i=1}^{6} p_i(t) = 1. \end{cases} \quad (1)$$

Задавая численные значения интенсивностей λ_{ij} в соответствии с условиями функционирования ЛСИО (ситуациями *SIT*), вектор вероятностей начальных состояний, учитывая нормировочное условие и переходя к непрерывному времени $t \to \infty$, систему линейных дифференциальных уравнений (СЛДУ) (1) с постоянными коэффициентами 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 специальных численных методов нахождения собственных чисел. Поэтому, для решения систем линейных однородных дифференциальных уравнений большой размерности целесообразно использование численных методов дифференцирования функций [45].

Характер выбранных значений интенсивностей определяется в соответствии с условиями функционирования ЛСИО. Эти условия (ситуации *SIT*) определяются вариацией исходных данных (соотношением исходных данных) – семейством реализаций λ_{ij} по аналогии с понятием сечения случайного процесса [43]. Наибольшее практическое значение при функционировании ЛСИО имеют следующие ситуации SIT_1 – SIT_3. Ситуации SIT_1 и SIT_2, описывают работу ЛСИО в штатном режиме без режима оценки доступности. Ситуация SIT_3 – описывает стратегию функционирования ЛСИО при формировании баз данных ложных MAC-адресов и TCP-портов в условиях воздействия средства СР с режимом оценки доступности.

Ситуация SIT_1. ЛСИО формирует базы данных ложных TCP-портов и MAC-адресов, рассылая легитимным узлам ИС ARP и TCP-запросы. Ответы от

узлов ИС обрабатываются без задержки. Средства СР не воздействуют на ЛСИО, система работает в штатном режиме.

Поскольку в данном случае ЛСИО функционирует в штатном режиме, рассылает запросы легитимным узлам ИС для создания баз данных ложных TCP-портов и MAC-адресов, то рассматривается, как влияют интенсивности λ_{23} – на формирование актуальной ARP таблицы с ложными MAC-адресами и λ_{24} – на формирование актуальной таблицы с ложными TCP портами, тогда пусть $\lambda_{23}= x$, $\lambda_{24}= y$.

Составим матрицу интенсивностей потоков событий B, для системы дифференциальных уравнений Колмогорова (1) (с условием нормировки).

$$B_{SIT1} = \begin{pmatrix} -(\lambda_{12}+\lambda_{13}) & \lambda_{21} & \dots & \lambda_{61} \\ \lambda_{12} & -(\lambda_{21}+\lambda_{23}+\lambda_{24}) & \dots & \lambda_{62} \\ \lambda_{13} & \lambda_{23} & \dots & \lambda_{63} \\ \lambda_{14} & \lambda_{24} & \dots & \lambda_{64} \\ \lambda_{15} & \lambda_{25} & \dots & \lambda_{65} \\ 1 & 1 & \dots & 1 \end{pmatrix} \quad (2)$$

Для оценки устойчивости разработанной модели используется понятие робастной устойчивости модели к возмущению исходных данных. 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 ν [27, 45] матрицы интенсивностей потоков событий B (2).

Применительно к ситуации SIT_1 на рис. 6 представлена зависимость числа обусловленности матрицы B от варьируемых интенсивностей $\lambda_{23}=x$ и $\lambda_{24}=y, x \in [0,100]$, $y \in [0,100]$ потоков событий в форме спектральной нормы $||B||_2$.

Так как значение числа обусловленности ν не превышает 38 для вариации λ_{23} и λ_{24} в диапазоне (0; 100), то построенная математическая модель марковского процесса в ситуации SIT_1 является робастной.

Для получения оценки переходных процессов в ситуации SIT_1 перейдем к решению СЛДУ (1) численным методом. Исходные данные для расчета: СЛДУ, вектор вероятностей начальных состояний, нормировочное условие, значения интенсивностей потоков событий задаем постоянными в соответствии с выбранными условиями функционирования ЛСИО.

Производим расчет по методу Рунге–Кутты с средневзвешенной величиной поправок каждого этапа интегрирования.

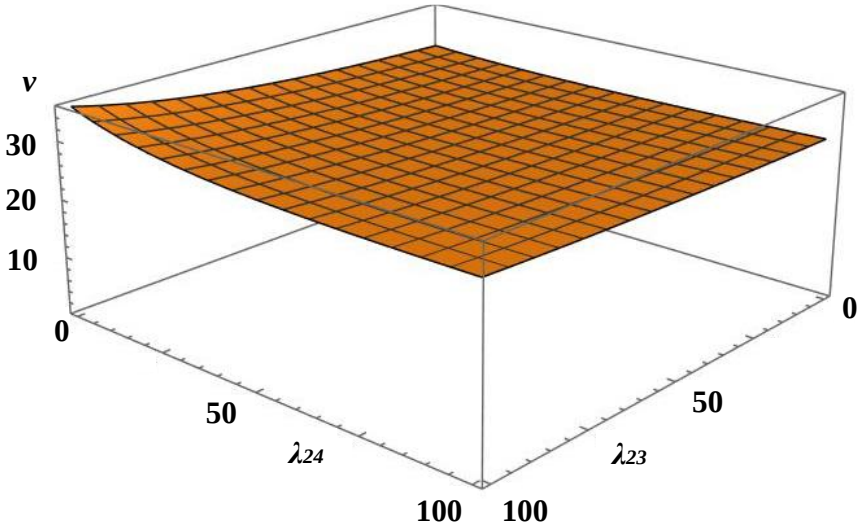

Рис. 6. Зависимость числа обусловленности матрицы B в форме спектральной нормы от варьируемых λ_{23} и λ_{24} применительно к SIT_1

Сплайн-интерполяция значений p_i на интервале $t \in [0;0,04]$ представлена на графиках зависимостей вероятностей состояний от времени (рис. 7).

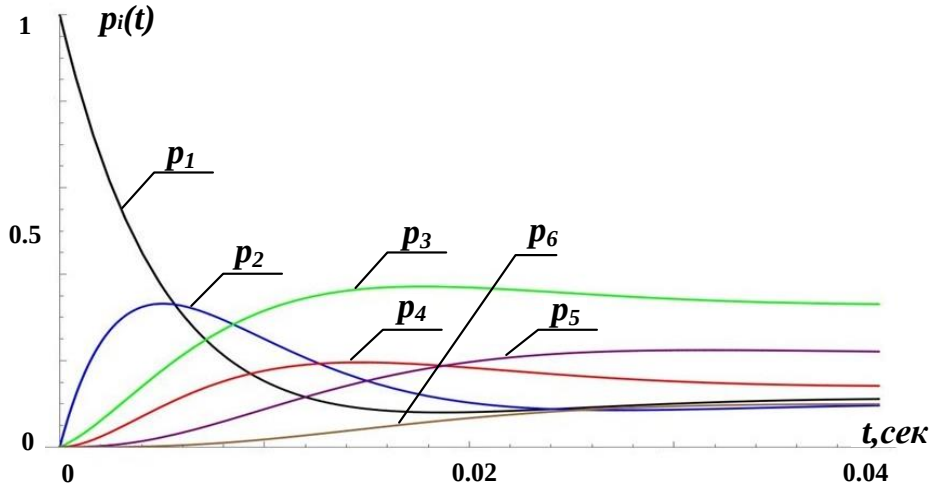

Рис. 7. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий соответствующие ситуации SIT_1

На интервале времени [0; 0,04] ЛСИО находится в переходном режиме функционирования, где наблюдается всплеск значения вероятности $p_3(t)$, что соответствует нахождению ЛСИО в состоянии обработки транзакций в базе данных ложных MAC-адресов и TCP портов, а также увеличение значения вероятности $p_5(t)$ которое соответствует нахождению ЛСИО в состоянии, формирования запросов легитимным узлам ИС и начале передачи данных.

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 $\{p_i\}$.

№2. 2023
ISSN 2410-9916

$$p_{41} = \frac{\lambda_{41}}{\lambda_{41} + \lambda_{45}} \quad (3)$$

Вероятность p_{41} означает вероятность перехода ЛСИО в исходное состояние (таблица ложных TCP-портов создана). Нахождение значения вероятности p_{41} позволяет определить вероятностно-временную характеристику состояния ЛСИО, когда его вычислительные ресурсы не потребляются, то есть находятся на максимуме, и он готов оперативно обработать запросы от средства СР при их поступлении. Графики зависимости финальных вероятностей от переходной вероятности p_{41} представлены на рис. 8. Графики зависимости финальных вероятностей от времени и от переходной вероятности p_{41} представлены на рис. 9.

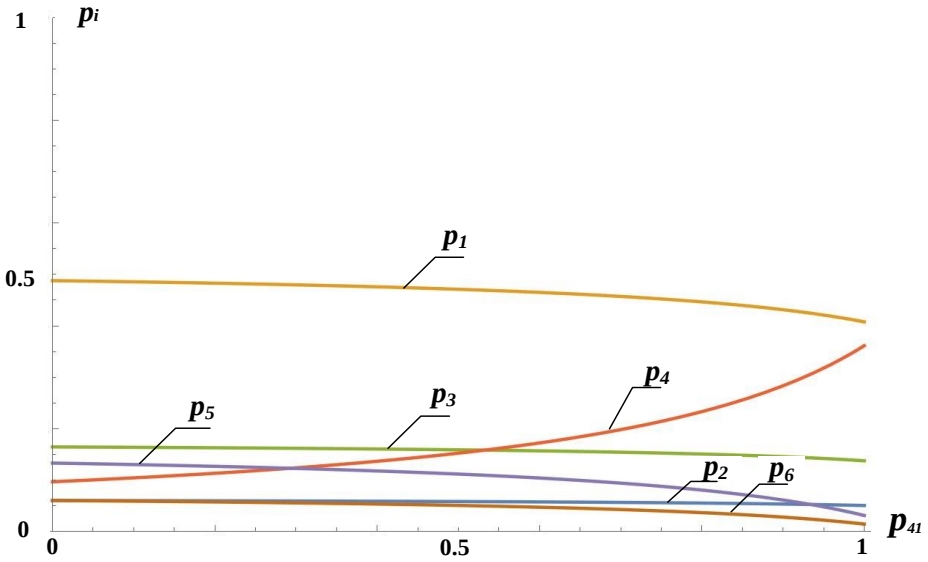

Рис. 8. Результаты расчета зависимости вероятностей состояний от переходной вероятности p_{41} для значений интенсивностей событий, соответствующих ситуации SIT_1

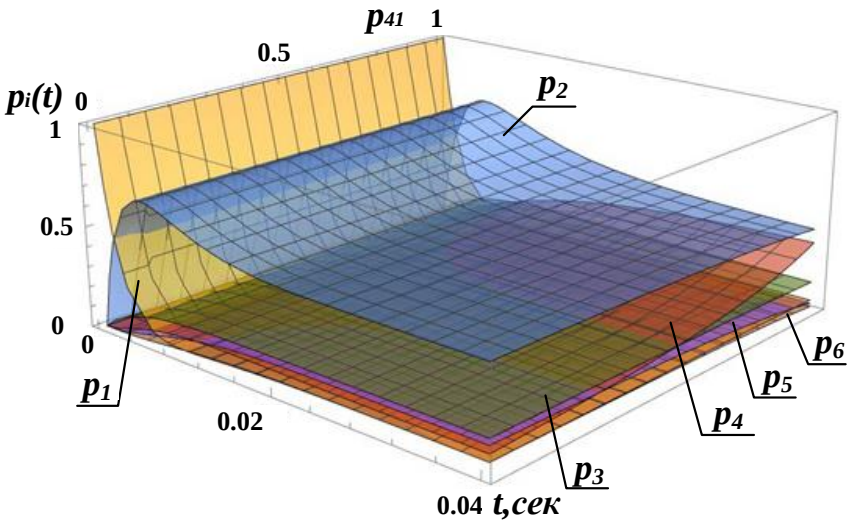

Рис. 9. Результаты расчета зависимости вероятностей состояний от времени и от переходной вероятности p_{41} для значений интенсивностей событий, соответствующих ситуации SIT_1

Ситуация SIT_2. ЛСИО формирует базы данных ложных TCP-портов и MAC-адресов, рассылает легитимным узлам ИС ARP и TCP- запросы. Средство СР воздействует на ЛСИО, ведет разведку структуры и состава ИС. ЛСИО обрабатывает запросы от средства СР и все ответы от узлов ИС.

Поскольку в данном случае ЛСИО формирует и запросы узлам ИС и ответы на запросы от средства СР, то рассмотрим, как влияют интенсивности λ_{12} – на анализ поступивших запросов от средства СР и ответов от узлов ИС и λ_{61} – на изменение режима обработки входящих данных и закрытие канала передачи данных, тогда пусть $\lambda_{12}= x$, $\lambda_{61}= y$.

Применительно к ситуации SIT_1 на рис. 10 представлена зависимость числа обусловленности матрицы B от варьируемых интенсивностей $\lambda_{23}=x$ и $\lambda_{24}=y$, $x \in [0, 100]$, $y \in [0, 100]$ потоков событий в форме спектральной нормы $||B||_2$.

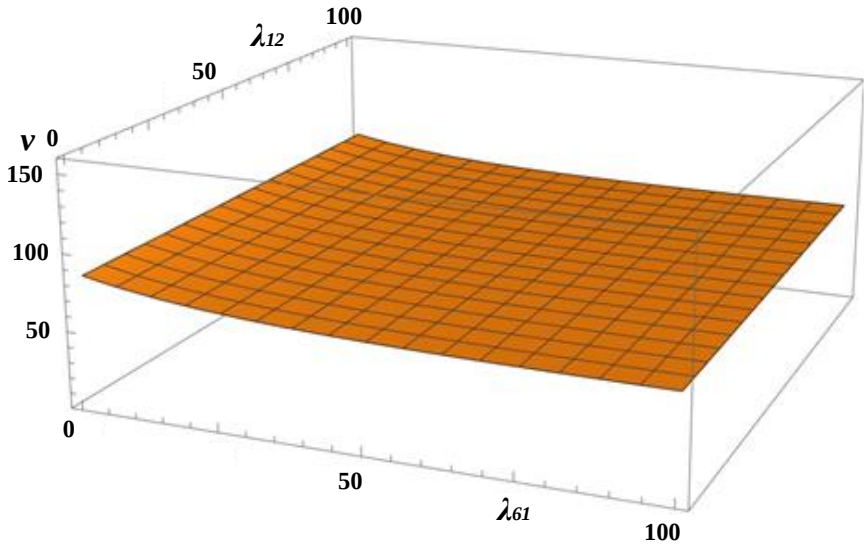

Рис. 10. Зависимость числа обусловленности матрицы B в форме спектральной нормы от варьируемых λ_{12} и λ_{61} применительно к SIT_2

Так как значение числа обусловленности ν не превышает 90 для вариации λ_{12} и λ_{61} в диапазоне (0; 100), то построенная математическая модель марковского процесса в ситуации SIT_2 является робастной в этом диапазоне.

Для получения оценки переходных процессов в ситуации SIT_2 перейдем к решению СЛДУ численным методом. Сплайн-интерполяция значений p_i на интервале $t \in [0; 0,03]$ представлена на графиках зависимостей вероятностей состояний от времени (рис. 11).

На интервале времени [0; 0,02] ЛСИО находится в переходном режиме функционирования, где наблюдается всплеск значения вероятности состояния $p_2(t)$, что соответствует нахождению ЛСИО в состоянии анализа поступивших запросов от средства СР.

Вероятность p_{41} определяет вероятность перехода системы из состояния S_4 (таблица ложных TCP-портов создана) в состояние S_1 (ЛСИО находится в состоянии простоя, не принимает и не передает потоки данных), за конечное число переходов. При интервале значений p_{41} вероятности $P_1(t)$ – $P_6(t)$ не равны 0.

№2. 2023
ISSN 2410-9916

Это означает, что ЛСИО за конечное число обработки ответов на свои запросы от легитимных узлов ИС сформирует таблицу ложных TCP-портов и перейдет в состояние простоя.

Графики зависимости финальных вероятностей от переходной вероятности p_{41} (3) представлены на рис. 12.

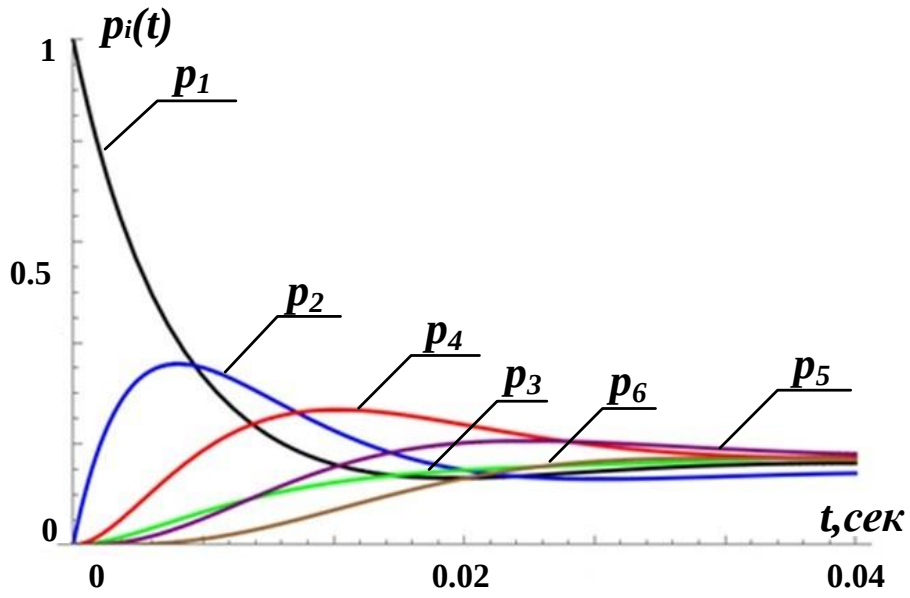

Рис. 11. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий соответствующие ситуации SIT_2

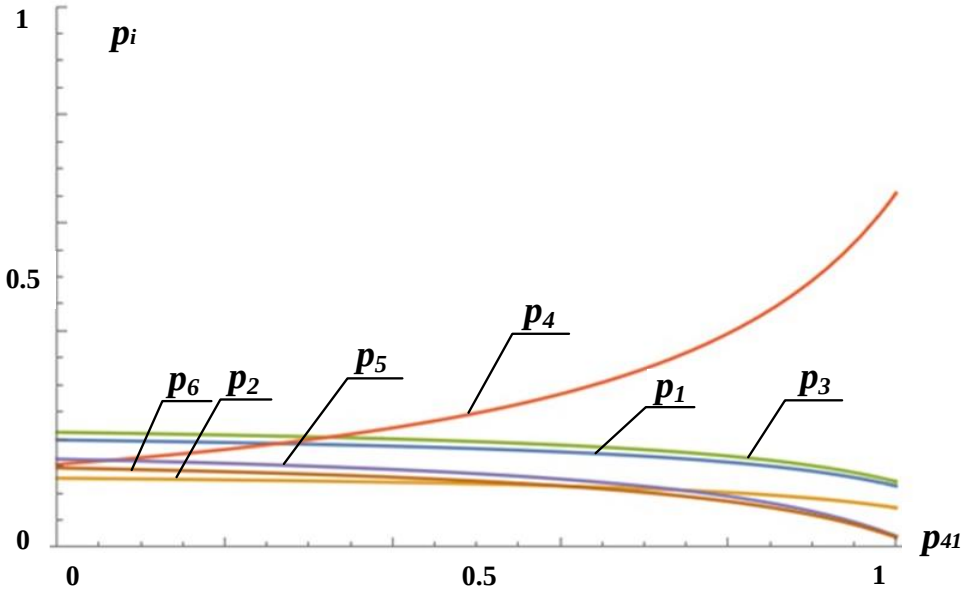

Рис. 12. Результаты расчета зависимости вероятностей состояний от переходной вероятности p_{41} для значений интенсивностей событий, соответствующих ситуации SIT_2

Графики зависимости финальных вероятностей от времени и от переходной вероятности p_{41} представлены на рис. 13.

DOI: 10.24412/2410-9916-2023-2-23-62
URL: https://sccs.intelgr.com/archive/2023-02/02-Lebedkina.pdf

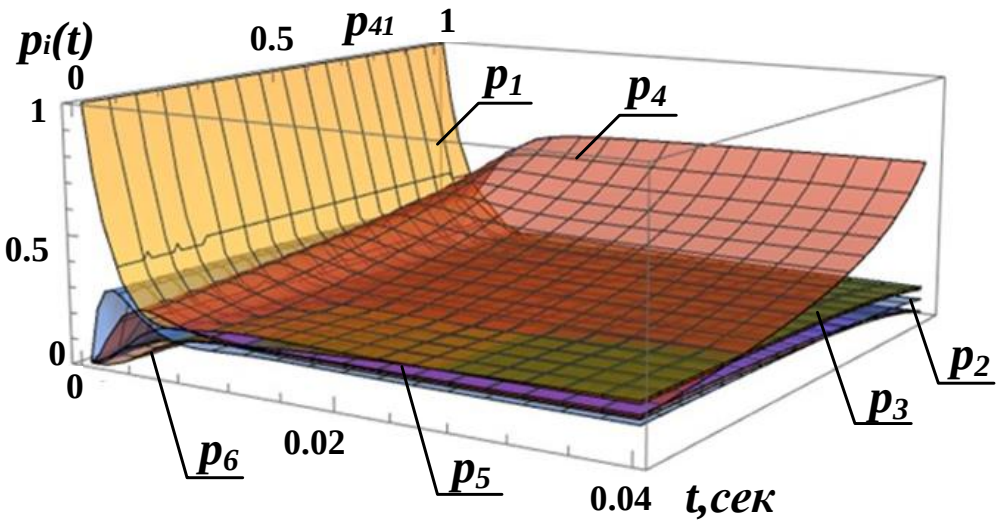

Рис. 13. Результаты расчета зависимости вероятностей состояний от времени и от переходной вероятности p_{41} для значений интенсивностей событий, соответствующих ситуации SIT_2

С увеличением времени и вероятности p_{41} увеличивается вероятность нахождения системы в состоянии S_4. Тем самым подтверждается, что ЛСИО за определенное конечное время сформирует таблицу ложных TCP-портов и перейдет в состояние простоя.

Снизить нагрузку на данное состояние ЛСИО возможно путем увеличения его ресурса за счет отклонения части входящих пакетов данных на обработку от легитимных узлов ИС посредством изменения режима обработки ЛСИО.

Научная новизна модели заключается в применении математического аппарата теории марковских случайных процессов для исследования возможностей функционирования ложных сетевых информационных объектов при конфигурировании параметров адресации в различных условиях информационного обмена и получения оценок устойчивости решений к изменению (вариации и погрешности) исходных данных.

Практическая значимость заключается в нахождении вероятностно-временных характеристик, описывающих состояния процесса функционирования ложных сетевых информационных объектов в условиях сетевой разведки.

Алгоритм конфигурирования адресации ложных сетевых информационных объектов в условиях сетевой разведки

Алгоритм относится к области информационной безопасности ИС и может быть использован в системах обнаружения и предупреждения атак с целью противодействия несанкционированным воздействиям в ИС, основанных на семействе коммуникационных протоколов TCP/IP.

Недостатками известных алгоритмов является относительно низкая бескомпроматность функционирования ЛСИО, заключающаяся в возможности идентификации ЛСИО средствами СР, что приводит к снижению результативности защиты ИС.

Низкая бескомпроматность функционирования ЛСИО обусловлена низкой оперативностью конфигурирования адресации ЛСИО в условиях СР, вызванной декларативным заданием параметров конфигурации и отсутствием обоснования доли выделяемых для ЛСИО вычислительных ресурсов ИС.

Назначением разработанного алгоритма является конфигурирование адресации ложных сетевых информационных объектов в условиях СР, обеспечивающая повышение оперативности защиты ИС для снижения возможностей СР по идентификации ЛСИО (компрометации средств защиты), и, как следствие, вскрытия структуры и состава ИС.

Информационный обмен между клиентами ИС и ЛСИО детализирован в модели функционирования ЛСИО. В процессе функционирования ЛСИО, средство СР инициирует запросы к ЛСИО, блокирование запросов средства СР приводит к компрометации ЛСИО, в результате средство СР может менять стратегию воздействия. Бескомпроматное функционирование ЛСИО, обеспечиваемое оперативной конфигурацией параметров обработки запросов в ЛСИО при воздействии средства СР, приведет к введению в заблуждение средства СР об истинном составе и структуре ИС.

Для оценки эффективности осуществляется решение прямой задачи исследования операций: чему будет равен показатель эффективности $G_{16}(t)$, если принять решение о значении интенсивности потока событий λ_{35} на формирование ARP-запроса клиентам ИС или ARP-ответа средству СР. Длительность цикла широковещательного запроса (и получения ответов) по протоколу ARP для ИС, состоящей из 254 сетевых устройств соответствует $t = t_{crit} = 0{,}1$.

Показателем оперативности конфигурирования адресации ЛСИО в условиях СР является функция распределения $G_{16}(t)$ времени первого посещения системой состояния S_6, при условии, что в момент времени t=0, система находилась в состоянии S_1. С практической точки зрения наиболее целесообразно выигрыш оперативности оценивать по значению времени завершения конфигурирования адресации ЛСИО при фиксированной вероятности (при фиксированном значении) $G_{16}(t) = 0{,}98$.

Физическая постановка задачи. В качестве основных исходных данных в алгоритме выступают:

IP – IP-адрес отправителя пакета;

TCP – TCP-пакет протокола передачи данных, стека TCP/IP;

ARP – ARP-пакет протокола разрешения адресов, стека TCP/IP;

Ts – счетчик времени начала опроса ЛСИО узлов ИС для актуализации своих баз данных (исходных данных);

TR – счетчик времени обработки ЛСИО запроса от средства СР;

TD – значение допустимого времени на обработку ЛСИО запроса от средства СР, которое задается администратором безопасности информации;

U – режим обработки запросов ложным сетевым информационным объектом, $U = \{0,1\}$, где 0 – обработка ЛСИО всех входящих пакетов, 1 – обработка только запросов от средства СР;

M – множество санкционированных IP-адресов ИС;

множество входных и внутренних параметров математической модели функционирования ЛСИО при конфигурировании параметров адресации в условиях СР $Z \subseteq \{S, X, A\}$, где $S = \{S_1, \ldots, S_6\}$, $X = \{\lambda_{35}\}$, $A = \{\lambda_{21}, \lambda_{23}, \lambda_{24}, \lambda_{34}, \lambda_{41}, \lambda_{45}, \lambda_{56}, \lambda_{61}\}$ перечень моделируемых состояний системы и интенсивностей потоков событий в ней описаны ниже по тексту.

На рис. 14 и рис. 15 представлена блок-схема последовательности действий, реализующая алгоритм конфигурации ложного сетевого объекта при одновременном взаимодействии с узлами ИС и средством СР.

На начальном этапе задают исходные данные (блок 1 на рис. 14). В качестве исходных данных выступают интенсивности потоков неконтролируемых (неуправляемых) событий (таблица 2). Затем, используя модель функционирования ЛСИО при конфигурировании параметров адресации в условиях СР, вычисляют ВВХ, описывающие состояния процесса функционирования ЛСИО при конфигурировании параметров адресации в условиях СР.

Рассматриваемый алгоритмом процесс соответствует ситуации SIT_3: средством СР ведется сетевая разведка ИС. ЛСИО формирует базу данных ложных MAC-адресов и TCP-портов. Время обработки поступивших данных в ЛСИО возрастает в виду ограниченных вычислительных возможностей.

Главным приоритетом ЛСИО является формирование и отправка ответов на запросы средства СР. При возрастании времени обработки запросов от средства СР ЛСИО меняет режим обработки входящих сообщений. Сообщения от санкционированных узлов ИС игнорируются, базы данных ложных MAC-адресов и TCP-портов не обновляются до уменьшения времени обработки ЛСИО запросов от средства СР до допустимого значения.

На следующем этапе (блок 3 на рис. 14), включают счетчик *Ts*. После включения счетчика проверяют поступление пакета данных (блок 4 на рис. 14). Если пакеты данных не поступили, то считывают значение счетчика *Ts* (блоки 4, 5 на рис. 14). Если значение *Ts* не достигло 300, то цикл начинают сначала с проверки поступления пакета данных.

При достижении *Ts* значения 300 формируют ARP-запросы узлам ИС, отправляют их и выключают счетчик *Ts* (блоки 8–10 на рис. 14). После отправки запросов проверяют поступление пакета данных (блок 4 на рис. 14).

При получении пакета данных проверяю IP-адрес отправителя пакета на принадлежность его множеству легитимных IP-адресов ИС (блоки 11, 12 на рис. 14). Если IP-адрес отправителя пакета не принадлежит множеству легитимных IP-адресов ИС, то запрос игнорируют и проверяют поступления новых пакетов данных. Если IP-адрес отправителя пакета принадлежит множеству легитимных IP-адресов ИС, то проверяют класс поступившего пакета (ARP-пакет или TCP-пакет) (блоки 13–15 на рис. 14).

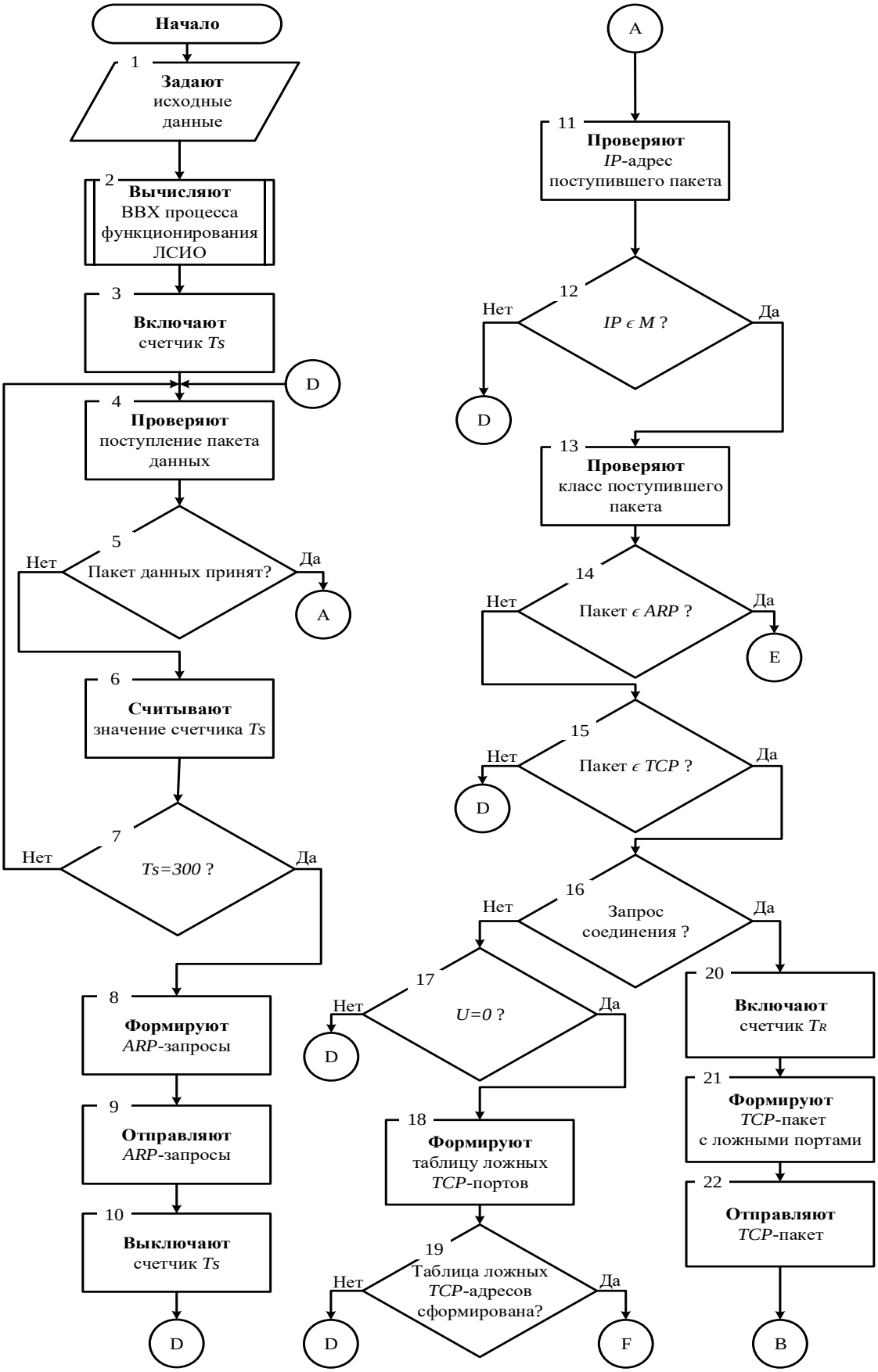

Рис. 14. Блок-схема последовательности действий, реализующая алгоритм конфигурации ложного сетевого объекта при одновременном взаимодействии с узлами ИС и средствами СР

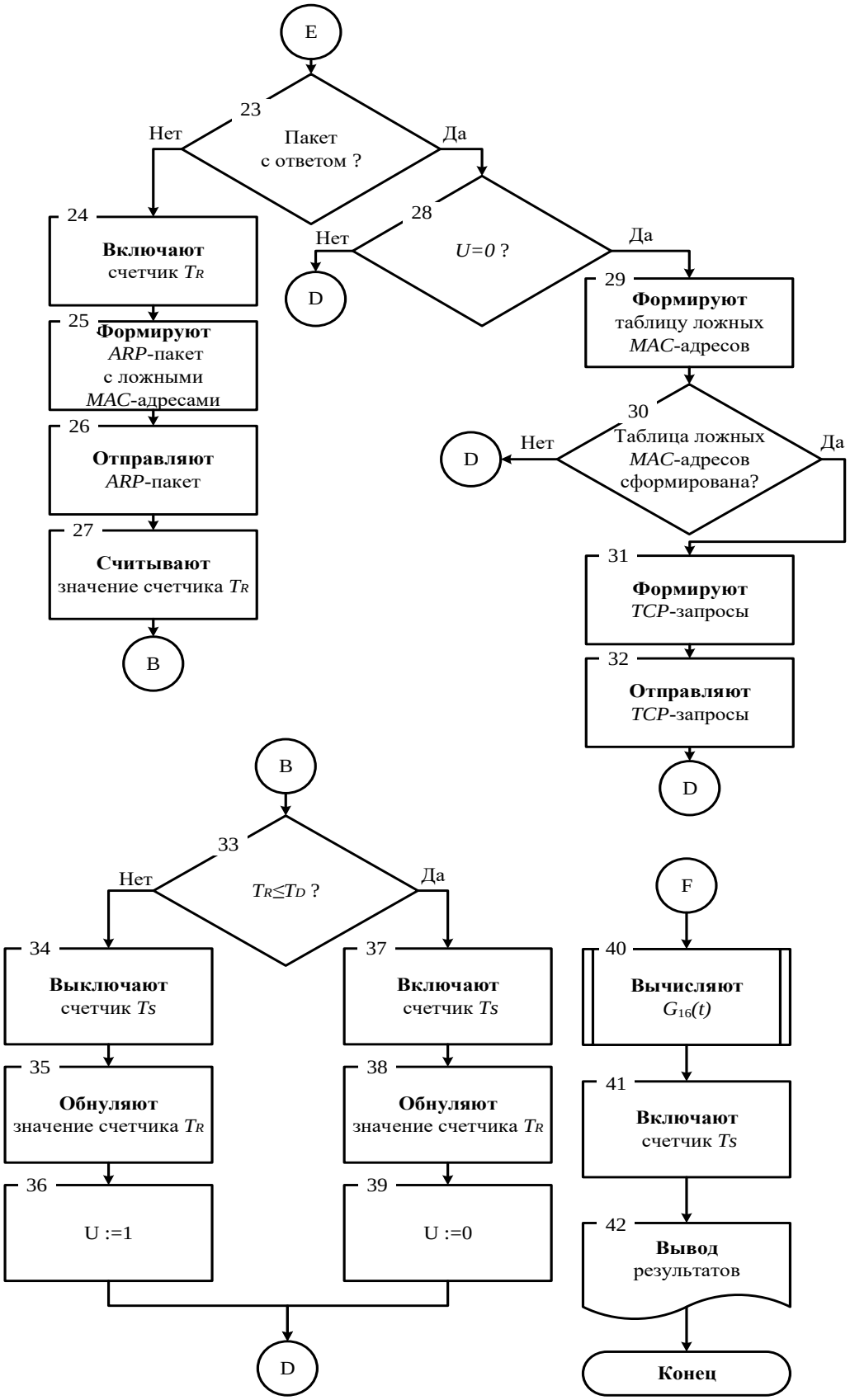

Рис. 15. Блок-схема последовательности действий, реализующая алгоритм конфигурации ложного сетевого объекта при одновременном взаимодействии с узлами ИС и средствами СР (продолжение)

Если поступивший пакет является ARP-пакетом, то проверяют его содержимое. Если пакет данных является ответом на ARP-запрос от ЛСИО (блок 23 на рис. 15), то проверяют режим обработки входящих пакетов ложным сетевым информационным пакетом (блок 28 на рис. 15). В исходном состоянии ЛСИО $U = 0$. Если равенство $U = 0$ выполняется, то формируют таблицу ложных MAC-адресов, проверяют окончание формирования таблицы ложных MAC-адресов (блоки 29, 30 на рис. 15). Если формирование таблицы ложных MAC-адресов не закончено, то проверяют поступление в ЛСИО пакета данных (блок 4 на рис. 14). В ином случае формируют TCP-запросы, отправляют их (блоки 31, 32 на рис. 15) и переходят к проверке поступления пакетов данных (блок 4 на рис. 14). Если поступивший пакет является TCP-пакетом (блок 15 на рис. 14), то проверяют его содержимое (блок 16 на рис. 14). Если TCP-пакет не является запросом на соединение и выполняется равенство $U = 0$ (блок 17 на рис. 14), то формируют таблицу ложных TCP-портов, проверяют окончание формирования таблицы ложных TCP-портов (блоки 18, 19 на рис. 14). Если таблица не сформирована, то проверяют поступление входящих пакетов данных (блок 4 на рис. 14). если таблица сформирована, то включают счетчик *Ts*.

Если поступивший пакет является ARP-пакетом и не является ответом на ARP-запрос от ЛСИО (блок 23 на рис. 15), то включают счетчик *TR*, формируют ARP-пакет с ложными MAC-адресами и отправляют этот пакет средству СР (блоки 24–26 на рис. 15). Затем считывают значение счетчика *TR* и проверяют равенство $TR \le TD$ (блоки 27, 33 на рис. 15). Если равенство $TR \le TD$ верно, то включают счетчик *Ts*, обнуляют значение счетчика *TR*, режиму обработки запросов *U* присваивают значение 0 (блоки 37–39 на рис. 15). Переходят к проверке поступления нового пакета данных (блок 4 на рис. 14). Если равенство $TR \le TD$ неверно, то выключают счетчик *Ts*, обнуляют значение счетчика *TR*, режиму обработки запросов *U* присваивают значение 1 (блоки 34–36 на рис. 15). Переходят к проверке поступления нового пакета данных (блок 4 на рис. 14). Если поступивший пакет является TCP-пакетом и является запросом на соединение с ЛСИО (блок 16 на рис. 14), то включают счетчик *TR*, формируют TCP-пакет с ложными портами и отправляют TCP-пакет средству СР (блоки 20–22 на рис. 14). Затем считывают значение счетчика *TR* и проверяют равенство $TR \le TD$ (блоки 27, 33 на рис. 15).

Когда поступивший в ЛСИО пакет данных является ответом от легитимного узла ИС (ARP-пакет (блок 23 на рис. 15) или TCP-пакет (блок 16 на рис. 14)), а режим обработки запросов ЛСИО $U = 1$ (блок 17 на рис. 14 или блок 28 на рис. 15), то запросы игнорируют и переходят к проверке поступления пакета данных (блок 4 на рис. 14).

Для оценивания ВВХ в разработанном алгоритме принимается следующая интерпретация дискретных состояний *S* и интенсивностей потоков событий в ЛСИО при взаимодействии с узлами ИС в условиях СР, приведенная в таблицах 3, 4.

Таблица 3 – Дискретные состояния ЛСИО при взаимодействии с узлами ИС в условиях СР

S_i	Состояния
S_1	Состояние, в котором ЛСИО находится в состоянии простоя, не принимает и не передает потоки данных
S_2	Состояние ожидания потока принятых данных (блоки 2–6, 10–12 на рис. 14)
S_3	Состояние ожидания потока проанализированных ARP-запросов (блок 13 на рис. 14, и блоки 22, 27–29 на рис. 15)
S_4	Состояние ожидания потока проанализированных TCP-запросов (блок 14–18 на рис. 14)
S_5	Состояние ожидания потока обработанных запросов (блок 7, 20 на рис. 14, и блоки 24, 30 на рис. 15)
S_6	Состояние ожидания потока сформированных данных (блоки 8, 21 на рис. 14, и блоки 25, 31, 32–38 на рис. 15)

Таблица 4 – Интенсивности потоков событий в ЛСИО при взаимодействии с узлами ИС в условиях СР

λ_{ij}	Описание потока событий
λ_{13}	Интенсивность потока событий на выборку исходных данных из ARP-таблицы с ложными MAC-адресами для формирования запроса клиентам ИС (блок 7 на рис. 14)
λ_{12}	Интенсивность потока на анализ поступивших запросов (ответов) ЛСИО от средств СР (клиентов ИС) (блоки 3, 4 на рис. 14)
λ_{21}	Интенсивность потока на отказ в формировании ответного пакета данных (игнорирование запроса СР) (блоки 11, 14 на рис. 14)
λ_{23}	Интенсивность потока на формирование актуальной ARP-таблицы с ложными MAC-адресами или выдачу исходных данных для формирования ответа на запрос СР (блок 13 на рис. 14 и блоки 22, 24, 27, 28 на рис. 15)
λ_{24}	Интенсивность потока на формирование актуальной таблицы с ложными TCP портами или выдачу исходных данных для формирования ответа на запрос СР (блоки 14–18 на рис. 14)
λ_{34}	Интенсивность потока на создание актуальной таблицы ложных TCP портов (актуальная ARP-таблица с ложными MAC-адресами создана) (блок 29 на рис. 15)
λ_{35}	Интенсивность потока на формирование ARP-запроса клиентам ИС или ARP-ответа средству СР (блоки 24, 30 на рис. 15)
λ_{41}	Интенсивность потока на перевод ЛСИО в исходное состояние (таблица ложных TCP портов создана) (блок 29 на рис. 15)
λ_{45}	Интенсивность потока на формирование TCP-запроса (SYN) клиентам ИС или TCP-ответа (ACK) средству СР (блок 20 на рис. 14 и блок 30 на рис. 15)
λ_{56}	Интенсивность потока на открытие канала передачи данных и отправку ответов средству СР или запросов клиентам ИС (блоки 8, 21 на рис. 14 и блоки 25, 31 на рис. 15)
λ_{61}	Интенсивность потока на изменение режима обработки входных данных и закрытие канала передачи данных (блоки 35, 38 на рис. 15)

Ситуация SIT_3 – стратегия взаимодействия ЛСИО со средством СР в процессе формирования баз данных ЛСИО. Поскольку в данном случае главной

задачей ЛСИО является быстрый анализ поступивших пакетов и оперативное уменьшение вычислительной нагрузки путем изменения режима обработки входящих сообщений, то рассмотрим, как влияют поступившие запросы от СР и ответы от легитимных узлов ИС λ_{12} – на анализ ЛСИО поступивших данных и поток событий на изменение режима обработки входных данных λ_{61} – на своевременную обработку ложным сетевым информационным объектом запросов от средства СР в процессе формирования баз данных ложных MAC-адресов и TCP-портов, тогда пусть $\lambda_{12}= x$, $\lambda_{61}= y$.

Применительно к ситуации SIT_3 на рис. 16 представлена зависимость числа обусловленности матрицы B от варьируемых интенсивностей $\lambda_{12}=x$ и $\lambda_{61}=y$, $x \in [0, 100]$, $y \in [0, 100]$ потоков событий в форме спектральной нормы $||B||_2$.

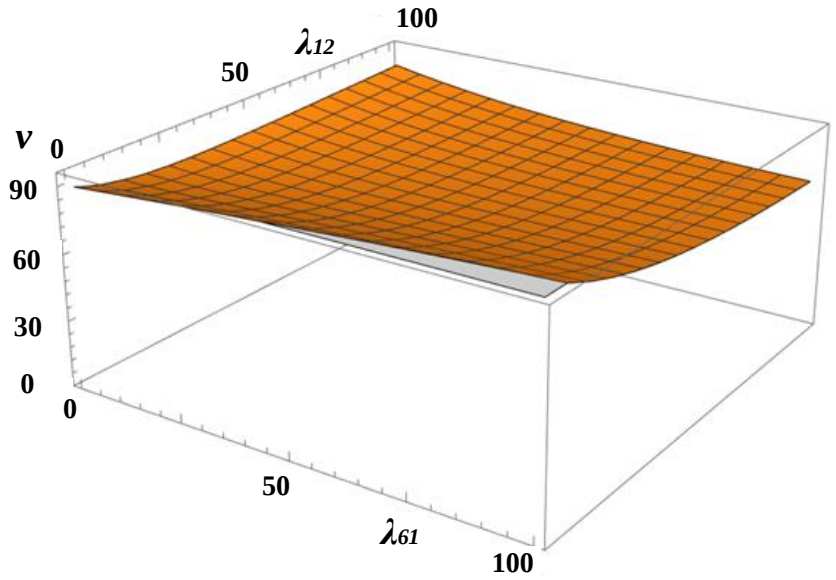

Рис. 16. Зависимость числа обусловленности матрицы B от варьируемых интенсивностей $\lambda_{12}=x$ и $\lambda_{61}=y$

Так как значение числа обусловленности v не превышает 100 для вариации λ_{12} и λ_{61} в диапазоне (0; 100), то построенная математическая модель марковского процесса в ситуации SIT_3 является робастной в этом диапазоне.

Сплайн-интерполяция значений p_i на интервале $t \in [0;0,04]$ представлена на графиках зависимостей вероятностей состояний от времени (рис. 17).

На интервале времени [0; 0,04] ЛСИО находится в переходном режиме функционирования, где наблюдается всплеск значения вероятности состояния $p_5(t)$, что соответствует нахождению ЛСИО в состоянии формирования запросов легитимным узлам ИС и начале передачи данных. Графики зависимости финальных вероятностей от переходной вероятности p_{41} представлены на рис. 18. Графики зависимости финальных вероятностей от времени и от переходной вероятности p_{41} представлены на рис. 19.

№2. 2023
ISSN 2410-9916

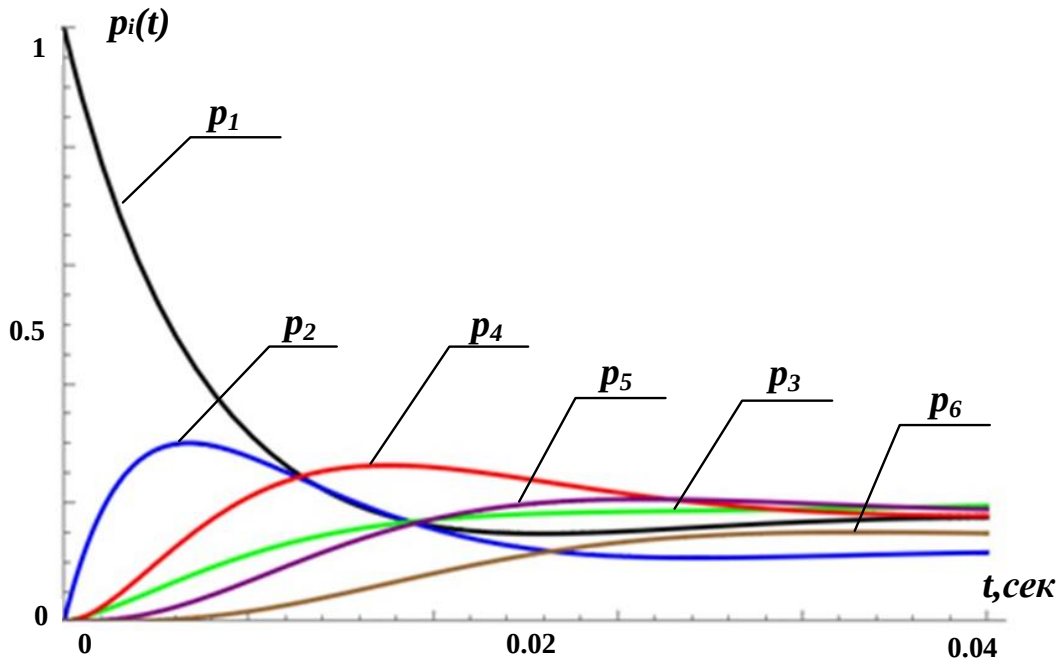

Рис. 17. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий соответствующие ситуации SIT_3

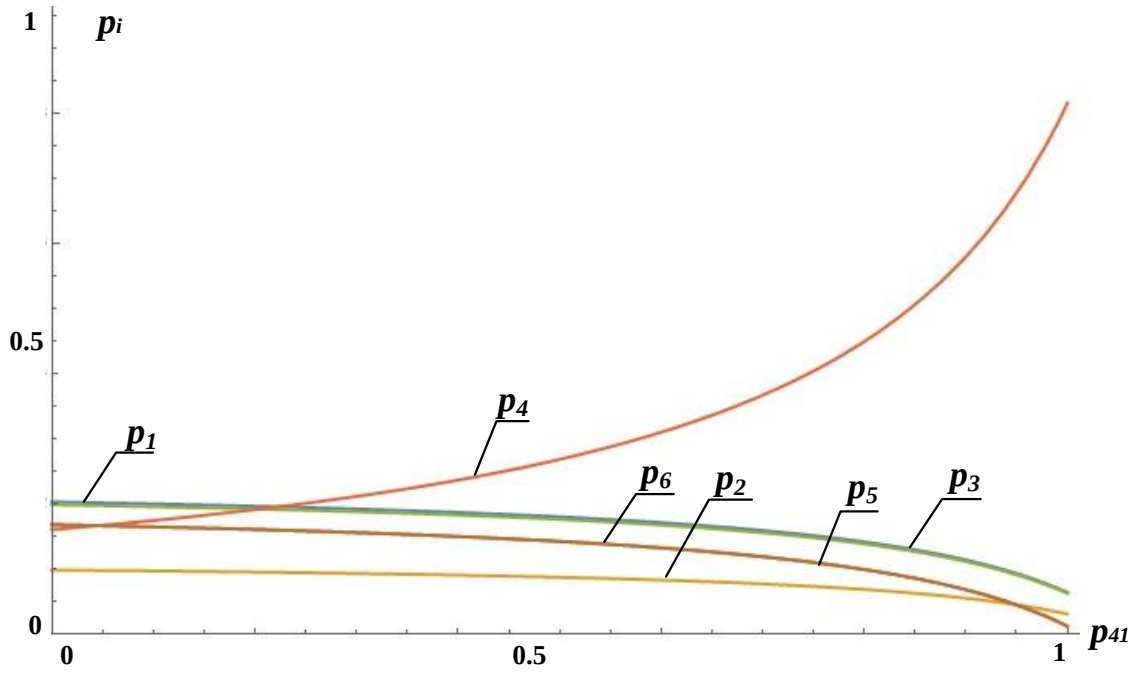

Рис. 18. Результаты расчета зависимости вероятностей состояний от переходной вероятности p_{41} для значений интенсивностей событий, соответствующих ситуации SIT_3

DOI: 10.24412/2410-9916-2023-2-23-62
URL: https://sccs.intelgr.com/archive/2023-02/02-Lebedkina.pdf

№2. 2023
ISSN 2410-9916

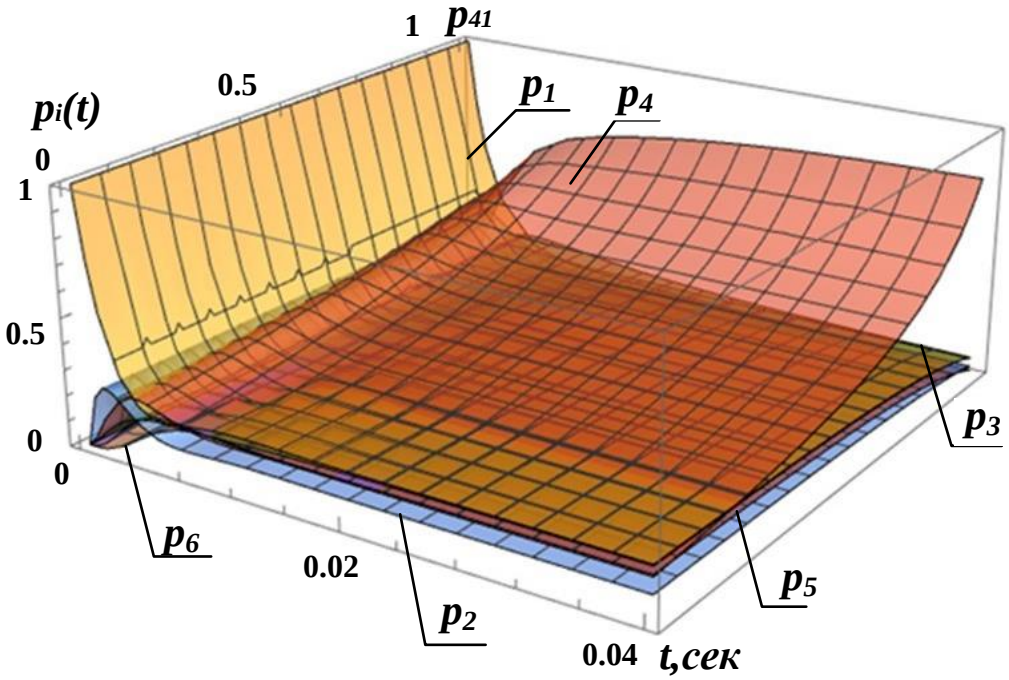

Рис. 19. Результаты расчета зависимости вероятностей состояний от времени и от переходной вероятности p_{41} для значений интенсивностей событий, соответствующих ситуации SIT_3

В качестве показателя эффективности в исследовании принята оперативность конфигурирования адресации ЛСИО в условиях СР как функция распределения $G_{16}(t)$ времени первого посещения системой состояния S_6, при условии, что в момент времени t=0, система находилась в состоянии S_1. В работах [29, 46] изложен порядок вычисления функции $G_{ij}(t)$. Функция $G_{ij}(t)$ представляет собой вероятность первого перехода из состояния i в состояние j к моменту времени (строго меньше) t. Оценка функций распределения $G_{ij}(t)$ производится из следующего выражения в матричной форме:

$$G(t)=\int_0^{\infty} L^{-1}\left\{p\cdot f(s)\cdot\left(I-p\cdot f(s)\right)^{-1}\cdot\left[I\times\left(I-p\cdot f(s)\right)^{-1}\right]^{-1}\right\}dt \qquad (4)$$

где L^{-1} – обратное преобразование Лапласа, «×» – произведение Адамара (поэлементное умножение матриц), p – матрица переходных вероятностей марковского процесса, $f(s)$ – матрица плотностей распределения времени ожидания наступления событий, I – единичная матрица.

Функция $G_{ij}(t)$ позволяет оценить вероятности достижения соответствующих состояний впервые к конкретному моменту времени (рис. 20). Регулируемым параметром является значение интенсивности потока событий λ_{35} на формирование ARP-запроса клиентам ИС или ARP-ответа средству СР, нерегулируемым параметром – значение интенсивности потока событий λ_{12} на анализ ЛСИО поступивших запросов (ответов) от средств СР.

DOI: 10.24412/2410-9916-2023-2-23-62
URL: https://sccs.intelgr.com/archive/2023-02/02-Lebedkina.pdf

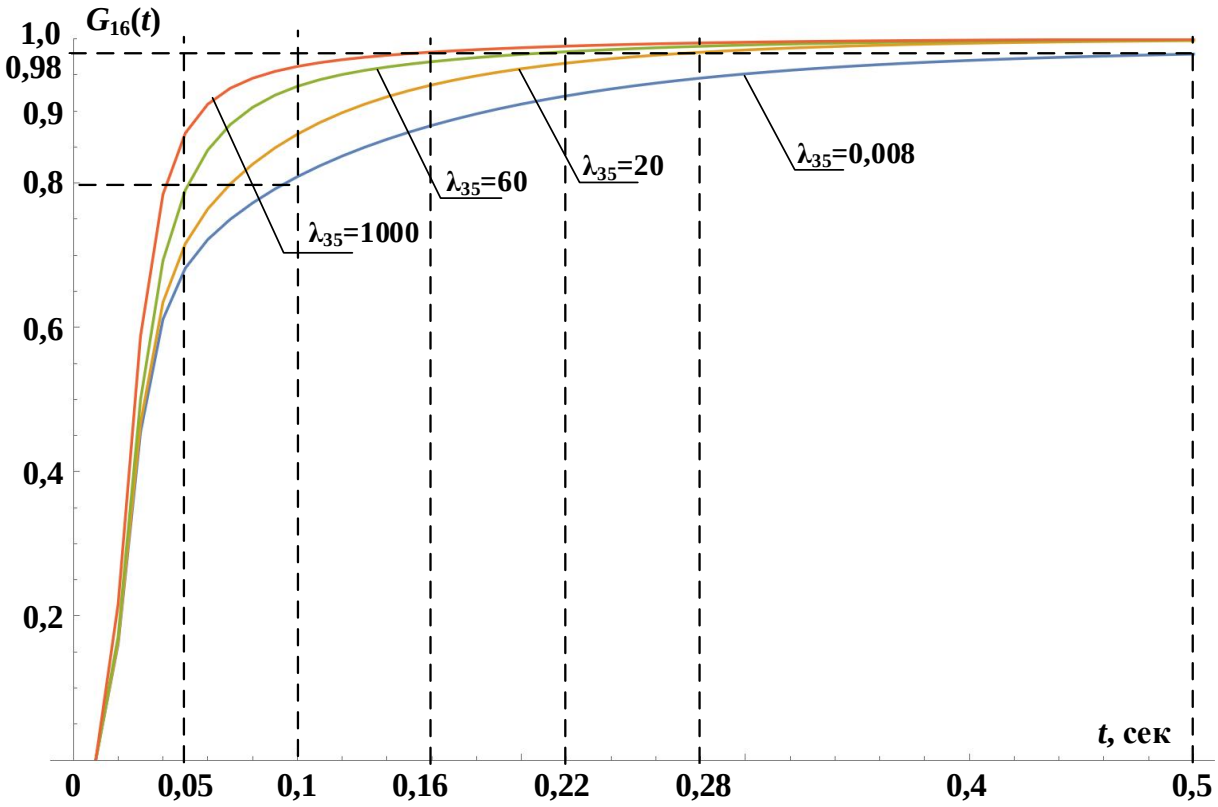

Рис. 20. Функции распределения $G_{16}(t)$ времени первого посещения системой состояния S_6 без использования (λ_{35}=0,08) и с использованием конфигурирования адресации ЛСИО

Окончанию переходных процессов соответствует $t = 0{,}05$ с; $t = t_{crit} = 0{,}1$ с соответствует длительности цикла широковещательного запроса (и получения ответов) по протоколу ARP для ИС, состоящей из 254 сетевых устройств (допущение), и актуализацию информации у средства СР. Из опыта эксплуатации ЛСИО выявлено, что t_{crit} находится в диапазоне [0,05; 0,4] в зависимости от количества сетевых устройств и настроек их операционных систем.

С практической точки зрения наиболее целесообразно выигрыш оперативности оценивать по значению времени завершения конфигурирования адресации ЛСИО при фиксированной вероятности. Тогда завершению конфигурирования адресации с вероятностью $G_{16}(t) = 0{,}98$ соответствует значение времени 0,5 с без изменения режима обработки входящих сообщений ($t > t_{crit}$).

С использованием разработанного алгоритма оперативность возрастает: $t = 0{,}16$ с – при λ_{35}=1000, $t = 0{,}22$ с – при λ_{35}=60, $t = 0{,}28$ с – при λ_{35}=20. То есть при заданных исходных данных оперативность увеличивается в 3,125 раза ($t < t_{crit}$).

Детерминированность алгоритма. Алгоритм имеет постоянство структуры вычислительного процесса, выдает уникальный и предопределенный результат для заданных входных данных λ_{ij}. Каждое предписание алгоритма имеет однозначную (недвусмысленную) трактовку.

Устойчивость алгоритма. Свойство алгоритма не увеличивать или увеличивать в незначительной степени погрешности, допущенной в начальных дан-

ных или допускаемой при вычислениях. Устойчивость алгоритма определяется устойчивостью математической модели и соответствует степени обусловленности (робастности) исследуемого процесса.

Точность алгоритма. Ошибка алгоритма при оценке параметров конфигурирования адресации ЛСИО в условиях СР главным образом зависит от точности оценок статистических параметров, закона распределения и от точности численных алгоритмов обратного преобразования Лапласа (относительная погрешность менее $10–^4$).

Сложность алгоритма. Верхняя оценка асимптотической сложности алгоритма конфигурирования адресации ЛСИО в условиях СР имеет линейный вид, общая оценка сложности алгоритма – O(n).

Конечность алгоритма. Алгоритм сходится к решению (окончанию конфигурирования адресации ЛСИО в условиях СР) за конечное число шагов.

Дискретность алгоритма. Алгоритм представляет собой конечную последовательность операций, каждая операция выполняется за конечное (ограниченное) время.

Результативность алгоритма. Результативность алгоритма оценивается вычислением функции распределения $G_{16}(t)$ времени первого посещения системой состояния S_6 исходя из конкретных значений исходных данных.

Научная новизна алгоритма заключается в применении модели функционирования ложных сетевых информационных объектов при конфигурировании параметров адресации, основанной на математическом аппарате теории марковских случайных процессов, для оценивания оперативности конфигурирования адресации ложных сетевых информационных объектов в условиях сетевой разведки.

Практическая значимость заключается в повышении оперативности конфигурирования адресации ложных сетевых информационных объектов и снижении возможностей сетевой разведки по идентификации средств защиты ИС.

Заключение

Разработанная модель позволяет определять вероятностно-временные характеристики, описывающие процесс функционирования ЛСИО при различных стратегиях взаимодействующих сторон, при этом выбор ситуаций обусловлен особенностями процессов ЛСИО, реализованными в протоколе передачи данных TCP и протоколе разрешения адресов ARP. Модель позволяет показать зависимости процесса конфигурирования адресации ЛСИО в условиях СР от потоков воздействий, оценивать оперативность обработки ЛСИО поступающих входных данных, обоснованно выбирать режимы функционирования ЛСИО для оптимального использования его вычислительных ресурсов. Новизна модели заключается в применении математического аппарата теории марковских случайных процессов для исследования возможностей функционирования ЛСИО при конфигурировании параметров адресации в различных условиях информационного обмена и получения оценок устойчивости решений к изменению (вариации и погрешности) исходных данных.

Разработанный алгоритм позволяет повысить результативность защиты ИС за счет снижения возможностей средств СР по идентификации ЛСИО, путем конфигурирования параметров адресации ЛСИО. Обеспечение снижения возможностей средств СР по идентификации ЛСИО в сети и его обходу, достигается за счет своевременной обработки запросов от средства СР и отправки ему ответов за время, не превышающее среднее время отклика реального узла сети на TCP и ARP-запросы, а сокрытие факта применения ЛСИО – достигается выбором оптимального режима функционирования ЛСИО. Новизна разработанного алгоритма заключается в применении модели функционирования ЛСИО, основанной на математическом аппарате теории марковских случайных процессов, постановке и решении прямой задачи исследования операций для максимизации вероятности формирования и отправки ЛСИО актуальных ложных данных на запросы от средств СР путем конфигурирования адресации ЛСИО.

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.: 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., Соколовский С. П., Лебедкина Т. В. Способ защиты вычислительных сетей // Патент на изобретение RU 2754101, опубл. 26.08.21, бюл. № 24. 22 с.

13. Искольный Б. Б., Максимов Р. В., Шарифуллин С. Р. Оценка живучести распределенных информационно-телекоммуникационных сетей // Вопросы кибербезопасности. 2017. № 5 (24). С. 72–82. DOI 10.21681/2311-3456-2017-5-72-82.

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. Макаренко С. И. Информационное оружие в технической сфере: терминология, классификация, примеры // Системы связи, управления и безопасности. 2016. № 3. С. 292–376.

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. 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.

28. Лебедкина Т. В., Соколовский С. П. Модель функционирования защищенной технологии файлового обмена // Вопросы кибербезопасности. 2021. № 5 (45). С. 52–62. DOI: 10.21681/2311-3456-2021-5-52-62.

29. Горбачев А. А., Модель и параметрическая оптимизация проактивной защиты сервиса электронной почты от сетевой разведки // Вопросы кибербезопасности. 2022. № 3 (49). С. 69–81. DOI: 10.21681/2311-3456-2022-2-69-81.

30. Котенко И. В., Степашкин М. В. Обманные системы для защиты информационных ресурсов в компьютерных сетях // Труды СПИИРАН. 2004. № 2 (1). С. 211–230

31. Котенко И. В., Степашкин М. В. Системы-имитаторы: назначение, функции, архитектура и подход к реализации // Труды СПИИРАН. 2006. № 3. С. 3–9.

32. Лукьянов Н. М., Дергачев А. М. Ложные вычислительные системы для исследования и отвлечения атак // Сети ЭВМ и информационные технологии. 2007. Т. 7. № 11 (45). С. 32–38.

33. Лебедкина Т. В. Алгоритм проактивной защиты информационных систем файлового обмена от сетевой разведки // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2021. № 11–12 (161–162). С. 93–101.

34. 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.

35. 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.

36. 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.

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

38. 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.

39. 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.

40. 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.

41. 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.

42. 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.

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

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

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

46. Warr R. L., Collins D. H. An Introduction to Solving for Quantities of Interest in Finite-State Semi-Markov Processes. 2012. pp. 1–18.

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., Sokolovsky S. P., Lebedkina T. V. Method of Protection of Computer Networks. Patent Russia, no. RU 2754101. Publish. 26.08.2021, bul. no. 24 (in Russian).

13. Iskolnyy B. B., Maximov R. V., Sharifullin S. R. Evaluation of the Survivability of Integrated Information-Telecommunication Networks. *Voprosy kiberbezopasnosti*, 2017, no. 5 (24), pp. 72–82. DOI: 10.21681/2311-3456-2017-5-72–82 (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. Makarenko S. I. Information Weapons in the Technical Sphere: Terminology, Classification, Examples. *Systems of Control, Communication and Security*, 2016, no. 3, pp. 292–376 (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. 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

28. Lebedkina T. V., Sokolovsky S. P. Model of secure file exchange information technology operation. *Voprosy kiberbezopasnosti*, 2021, no 5 (45), pp. 52–62 (in Russian).

29. Gorbachev A. A., Model and parametric optimization of proactive protection of an email service from network reconnaissance. *Voprosy kiberbezopasnosti*, 2022, no. 3 (49), pp. 69–81 (in Russian).

30. Kotenko I. V., Stepashkin M. V. Deception systems for protection of information resources in computer networks. *SPIIRAS Proceeding*, 2004, no. 2 (1), pp. 211–230 (in Russian).

31. Kotenko I. V., Stepashkin M. V. Systems-simulators: assignment, functioning, architecture and approach to implementation. *SPIIRAS Proceeding*, 2006, no. 3, pp. 3–9 (in Russian).

32. Lukyanov N. M., Dergachev A. M. Lozhnye vychislitel'nye sistemy dlja issledovanija i otvlechenija atak [False computing systems for research and

distraction of attacks]. *Seti JeVM i informacionnye tehnologii* [Computer networks and information technologies], 2007, vol. 7, no. 11 (45), pp. 32–38 (in Russian).

33. Lebedkina T. V. Algoritm proaktivnoj zashhity informacionnyh sistem fajlovogo obmena ot setevoj razvedki [Algorithm for proactive protection of file exchange information systems from network reconnaissance]. *Enginery Problems. Series 16. Anti-Terrorist Engineering Means*, 2021, vol. 11–12, no. 161–162, pp. 93–101 (in Russian).

34. 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).

35. 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).

36. 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).

37. 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).

38. 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).

39. 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).

40. 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).

41. 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).

42. 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).

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

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

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

46. Warr R.L., Collins D.H. An Introduction to Solving for Quantities of Interest in Finite-State Semi-Markov Processes. 2012. pp. 1–18.

Статья поступила 20 марта 2023 г.

Информация об авторах

Лебедкина Татьяна Владимировна – кандидат технических наук. Доцент кафедры. 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: alina031292@yandex.ru

Хорев Григорий 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: horevga@gmail.com

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

Functioning model and algorithm for configuring the addressing of false network information objects in the conditions of network reconnaissance

T. V. Lebedkina, G. A. Horev

***Purpose**: Capabilities enhancing and effectiveness improving of network reconnaissance to break information systems actualize the issues of ensure their information security. The inertial properties of the applied means of protection do not fully ensure the security of information systems from network reconnaissance and computer attacks. Spoof network information object technology is a security resource whose purpose is to be investigated or subjected to cyberattacks by an information security violator.The aim of the work is to develop a model and an algorithm to ensure the security of the information system, to provide prompt service to authorized clients with a simultaneous decrease in the quality of service requests from the attacker's tools by choosing the optimal mode of functioning of false network information objects. **Methods** used methods: formalization of the process of functioning of false network information objects in the configuration of addressing parameters under conditions of network reconnaissance by representing the process of their interaction in the form of a Markovian random process with discrete states and continuous time, as well as solving the control problem by numerical and analytical methods. **Novelty**: 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, for substantiation of the choice of optimal modes of operation of false network information objects. The novelty of the developed algorithm is the application of the presented model of functioning of false network information objects,*

statement and the decision of a direct problem of research of operations for maximization of probability of formation and sending of actual false data on requests from means of network reconnaissance. ***Result:*** *The calculations performed indicate an increase in the protection of information resources due to the timely processing of requests from the network reconnaissance tool and sending responses to it in a time not exceeding the average response time of a real network node to TCP and ARP requests. The presented algorithm makes it possible to increase the effectiveness of protection by reducing the capabilities of network reconnaissance tools to identify false network information objects by configuring addressing parameters.* ***Practical relevance****: Lies in finding the probabilistic-temporal characteristics that describe the state of the process of functioning of the false network information objects in the conditions of network reconnaissance, as well as in solving the direct problem of operations research to maximize the probability of generating and sending actual false data to requests from network reconnaissance tools, as well as reducing the possibility of compromising the means of protection.*

Key words: *network reconnaissance, false network information objects, computer attack, protocol, resilience, random process.*

Information about Authors

Tatyana Vladimirovna Lebedkina – Ph.D. of Engineering Sciences. Associate Professor at the Department. 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: alina031292@yandex.ru

Grigory Alexandrovich Horev – 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: horevga@gmail.com

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