УДК: 007.738.5 DOI: 10.53816/23061456_2022_5–6_67

МОДЕЛЬ КОНФИГУРИРОВАНИЯ СЕТЕВЫХ ПАРАМЕТРОВ ИНФОРМАЦИОННЫХ СИСТЕМ ДЛЯ ЗАЩИТЫ ОТ СЕТЕВОЙ РАЗВЕДКИ

MODEL FOR CONFIGURING THE NETWORK PARAMETERS OF INFORMATION SYSTEMS TO PROTECT AGAINST NETWORK INTELLIGENCE

М.А. Каплин

M.A. Kaplin

Краснодарское высшее военное училище им. С.М. Штеменко

Существующие угрозы информационной безопасности информационных систем обусловлены отсутствием превентивности применяемых средств защиты, анализирующих содержимое запросов клиентов к серверу, а также особенностями функционирования DHCP и воздействий средств злоумышленника. В этой связи открытым для поиска новых технических решений и разработки научно-методического аппарата остается вопрос соответствия защищенности информационных систем установленным требованиям безопасности объектов критической информационной инфраструктуры. Предлагаемая модель позволяет оценить защищенность информационной системы по результатам сетевого маскирования, обеспечить релевантность периодичности смены сетевых параметров компонентами информационной системы, получить ее предельные значения.
Ключевые слова: информационная система, сетевая разведка, система обнаружения атак, сетевые параметры.

Existing threats to information security of information systems due to the lack of prevention of the applied protection tools, analyzing the content of client requests to the server, as well as the peculiarities of the DHCP and the impact of malicious means. In this regard, the issue of compliance of information systems security with the established security requirements for critical information infrastructure remains open for the search for new technical solutions and the development of scientific and methodological apparatus. The proposed model makes it possible to assess information system security based on the results of network masking, to ensure the relevance of the frequency of change of network parameters by information system components, and to obtain its limiting values.
Keywords: information system, network intelligence, attack detection system, network parameters.

Повсеместная информатизация в различных сферах деятельности ведомств и организаций, обусловленная повышением эффективности в достижении поставленных целей, существенно повышает роль применяемых информационных технологий. Объединение различных информационных ресурсов на инфраструктуре сетей связи общего пользования (ССОП) существенно оптимизирует процессы информационного взаимодействия между их участниками, но, в свою очередь, увеличивает возможности деструктивных воздействий на все составляющие информационных систем [1].

Так как взаимодействие между сегментами информационных систем (ИС) осуществляется через ССОП, передача информационных потоков между ними повышает возможности сетевой разведки (СР) по вскрытию состава, структуры и алгоритмов функционирования ИС [2]. В ведомственных ИС обеспечение безопасности осуществляется в соответствии с требованиями регуляторов. При этом применение традиционных средств защиты, основанных на реализации запрещающих регламентов, вынуждают злоумышленника находить новые способы преодоления систем защиты [3]. Разработанные технологии динамического управления сетевыми параметрами абонентов клиент-серверных вычислительных сетей (КС ВС) [5–7] позволяют управлять изменениями конфигурации ИС, что, в свою очередь, обеспечивает противодействие СР еще на этапе исследования объекта атаки. Данные технологии позволяют обеспечить защищенность ИС не провоцируя злоумышленника менять стратегию преодоления систем защиты. При этом в указанных работах не рассмотрены вопросы оценки периодичности смены сетевых параметров абонентам ИС, что, в свою очередь, может привести к нерелевантной периодичности их смены, влекущей за собой угрозу вскрытия сетевых параметров ИС средствами СР, не обнаруженными системой обнаружения атак (СОА) при недостаточной частоте смены, либо к отказу в обслуживании легитимных абонентов ИС при избыточной частоте смены. К тому же сетевые адреса, высвобождаемые после смены сетевых параметров абонентам ИС, создают возможность компрометации элементов средств защиты.

Создание (эмуляция) ложных компонентов информационных систем (ЛК ИС), эмулирующие отдельные компьютеры и подсети, содержащие виртуальные узлы, предоставляемые в качестве целей для злоумышленника при осуществлении им компьютерных атак, позволяют проводить регистрацию и анализ действий злоумышленника в целях последующего противодействия компьютерным атакам, в том числе увеличения времени, необходимого для их подготовки [4]. Однако статичность сетевых параметров ЛК ИС со временем может привести к компрометации ЛК ИС.

Для повышения результативности средств защиты целесообразно объединить эти две технологии.

Указанные недостатки, выявленные в ходе анализа работ в области противодействия сетевой разведке [8–10], обуславливают актуальность проводимого исследования.

Формализованная постановка задачи на моделирование конфигурирования сетевых параметров информационной системы

ИС представляет собой совокупность данных, технического и программного обеспечения, персонала, а также коммуникационного оборудования, соединенного физическими линиями связи. Взаимодействие между субъектами информационной системы осуществляется на основе клиент-серверной архитектуры построения вычислительных сетей. В процессе конфигурирования сетевых параметров ИС DHCP-сервер формирует и направляет каждому сетевому устройству сообщения с новыми сетевыми параметрами. При этом новые сетевые параметры задаются также и эмулированным ЛК ИС (рис. 1). Ограниченность вычислительного ресурса обусловлена длительностью времени, за которое происходит перевод клиентов ИС на новые сетевые параметры. Процесс смены сетевых параметров клиентам ИС обеспечивается протоколом DHCP (Dynamic Host Configuration Protocol), определенным в RFC 2131. По истечении времени аренды сетевых параметров или с поступлением заявок от СОА о фактах воздействия средств СР, производится реконфигурация сетевых параметров ИС.

В процессе реконфигурации сетевых параметров ИС осуществляется перевод абонентов ИС в новую подсеть. При этом высвобождаемые после смены сетевых параметров абонентов ИС IP-адреса переназначаются эмулированным в высвобождаемой подсети ЛК ИС (рис. 2).

Содержательная постановка задачи на моделирование конфигурирования сетевых параметров ИС в условиях воздействия СР: разработать модель μ ИС S, устанавливающую закономерность изменения множества P_i выходных параметров модели конфигурирования сетевых параметров ИС и множества Q показателей эффективности конфигурирования сетевых параметров ИС от множества C значений входных параметров, множества Z значений внутренних параметров, множества I значений параметров условий функционирования. На значения параметров множеств

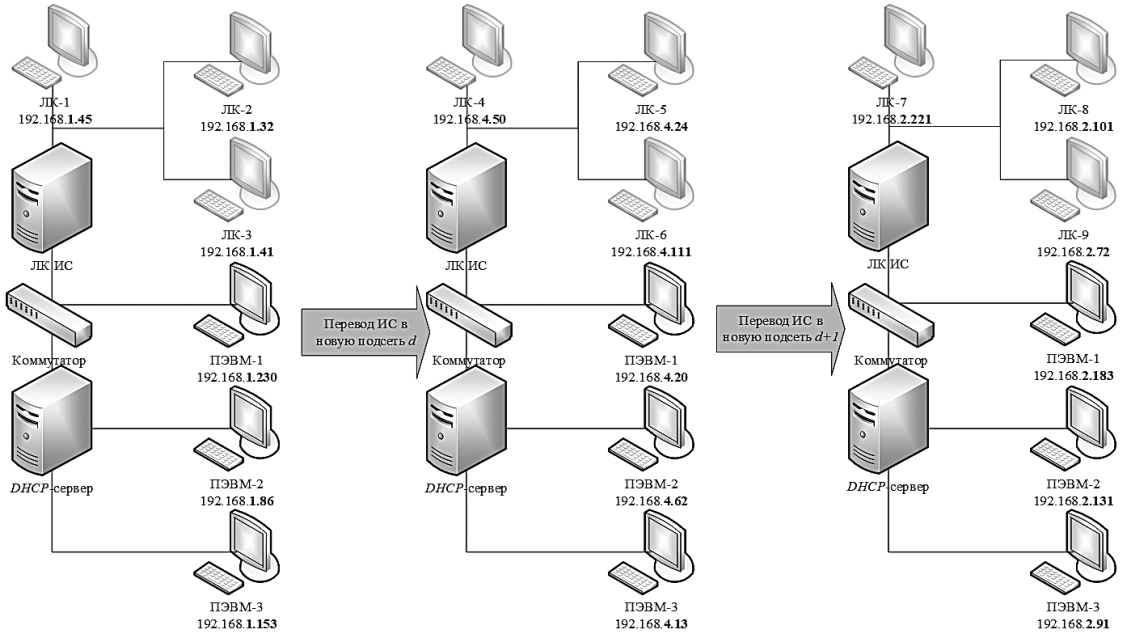

Рис. 1. Схема процесса многошаговой смены сетевых параметров клиентам и эмулированным ЛК ИС

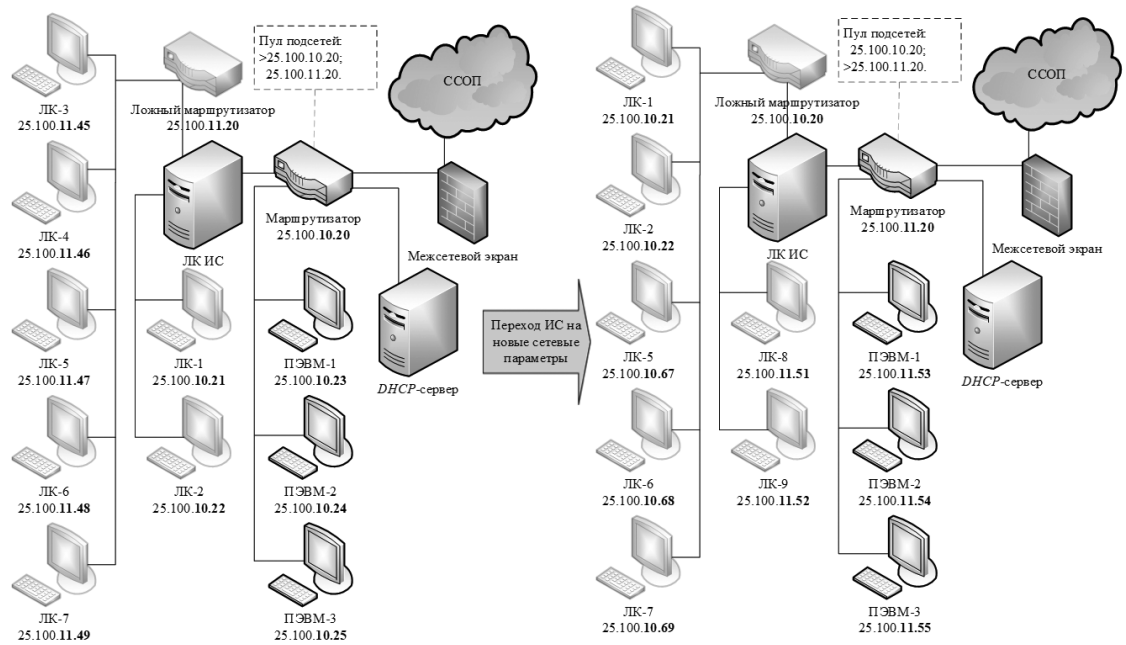

Рис. 2. Схема перевода абонентов ИС в новую подсеть и переназначения высвобожденных IP-адресов ЛК ИС

C, P_i, Z, I наложены условия их допустимости. Множество I значений параметров условий функционирования включает множество N узлов ИС (в том числе эмулированных), множество V информационных связей между узлами ИС и множество L сетевых параметров узлов ИС.

Математическая постановка задачи на моделирование конфигурирования сетевых параметров ИС в условиях воздействия СР:

$$\mu : < S, C, Z, I > \to P_i, Q \mid C \subseteq \{A, B\},$$

$$P_i = \lim_{t \to \infty} P_i(t), \quad I \subseteq \{N, V, L\}.$$

Формализованная постановка задачи на оптимизацию показателей эффективности ИС:

$$< S, C, Z, I > \min P_D^C \mid P_D^C \in \{P_i\}, i = 1,2,...,h$$

для минимизации вероятности вскрытия (от англ. Detection) структуры ИС средствами СР;

$$< S, C, Z, I > \max P_{AC}^{C} \mid P_{AC}^{C} \in \{P_i\},\ i = 1,2,...,h$$

для максимизации вероятности доступности (от англ. Access) информации клиентам ИС в связи со сменой сетевых параметров.

Математическая модель конфигурирования сетевых параметров информационной системы в условиях воздействия сетевой разведки

Пусть имеется ИС *S*, в которой реализуют конфигурирование сетевых параметров абонентам ИС, эмуляцию ЛК ИС и осуществление штатной или внеочередной смены сетевых параметров ее клиентам в условиях воздействия СР. Физически система *S* включает в себя клиентов ИС, технические средства ЛК ИС, DHCP-сервер, технические средства системы обнаружения атак.

От передающих абонентов и далее в ИС поступает простейший поток однородных событий (заявок, требований, факторов) с интенсивностью λ, потенциально переводящих ИС в состояния, когда обеспечивается или не обеспечивается своевременность смены сетевых параметров абонентам ИС. Переход системы в одно из состояний обуславливается тем, что ИС в штатных режимах функционирования справится с требуемой нагрузкой, тогда как увеличение интенсивности воздействия средств СР и, как следствие, противодействие им может увеличить нагрузку на ИС и привести к нерелевантной частоте смены сетевых параметров абонентам ИС. Отказ смены сетевых параметров абонентам ИС может происходить под воздействием непреднамеренных и преднамеренных деструктивных воздействий (в частности — СР).

Математическая модель конфигурирования сетевых параметров ИС учитывает воздействия на ИС заявок с различной интенсивностью как от администратора сети, так и от СР.

Использование модели предполагает поиск условий релевантного конфигурирования сетевых параметров ИС и позволит перейти к вероятностной оценке защищенности структуры ИС от ее вскрытия средствами СР $P_D^C(t) \to \min$ и доступности информации клиентам ИС в связи со сменой сетевых параметров $P_{AC}^{C}(t) \to \max$.

Процесс конфигурирования сетевых параметров ИС в условиях воздействия СР можно представить как однородный марковский случайный процесс с дискретными состояниями и непрерывным временем (однородной цепью Маркова с непрерывным временем).

Учет в марковской модели времени пребывания ИС в каждом из состояний в зависимости от условий функционирования ИС позволяет исследовать динамику (моделировать процесс в реальном времени) конфигурирования сетевых параметров ИС в условиях воздействия СР.

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

– пространство дискретных состояний системы (конечное множество несовместных (несовместимых) событий, описывающих существенные свойства системы и изменяющихся «скачкообразно») (табл. 1) и возможные переходы системы из состояния в состояние (характеризуются ориентированным графом состояний моделируемой системы, представленным на рис. 3);

– распределение вероятностей пребывания системы в различных состояниях в начальный момент времени;

– интенсивности потоков событий (заявок, требований, факторов), вызывающих переход системы из состояния в состояние (табл. 2).

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

Пусть оценка результативности защиты от средств СР происходит циклично, чтобы скрывать логическую структуру ИС, тогда S_1 — начальное состояние моделируемой системы $p(0) = |1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0|$. Начальное распределение вероятностей соответствует представлению о том, что в начальный момент времени система достоверно находится в первом состоянии. Это состояние обеспечивает невозможность вскрытия функционально-логической структуры (ФЛС) ИС средствами СР, интенсивность которого определяется для каждого информационного направления и является искомым с позиций обеспечения конфигурирования сетевых пара-

Таблица 1

Дискретные состояния процесса конфигурирования сетевых параметров ИС в условиях воздействия СР

S	Интерпретация состояний
S_1	Состояние покоя системы. Сетевые параметры абонентам ИС назначены и статичны. Оценка результативности защиты от средств СР. Невозможность вскрытия функционально-логической структуры ИС средствами СР
S_2	Оценка возможности изменить структурно-функциональные характеристики ИС
S_3	Изменение сетевых параметров абонентов ИС DHCP-сервером, эмуляция ЛК ИС
S_4	Обнаружение средств СР средствами обнаружения компьютерных атак
S_5	Добывание сведений о логической структуре ИС средствами СР в диалоговом режиме, средство СР осуществляет последовательное выполнение функций сетевого сканера
S_6	Логическая структура ИС вскрыта с некоторой полнотой, оценка результативности СР злоумышленником

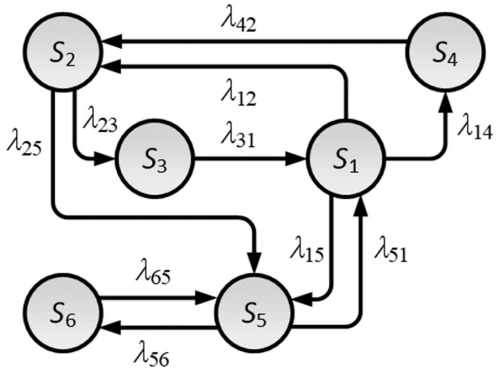

Рис. 3. Граф состояний процесса конфигурирования сетевых параметров ИС в условиях воздействия СР

Таблица 2

Интенсивности потоков событий

λ_{ij}	Интерпретация интенсивностей потоков событий
λ_{12}	Поток событий необходимости на эмуляцию ЛК ИС и штатную смену сетевых параметров абонентам ИС
λ_{14}	Поток событий обнаружения средств СР средствами обнаружения компьютерных атак
λ_{15}	Поток событий идентификации средствами СР структурно-функциональных характеристик ИС в диалоговом режиме (последовательные запросы сетевого сканера и ответы ИС)
λ_{23}	Поток событий на штатное или внеочередное изменение сетевых параметров абонентам ИС от DHCP-сервера, эмуляцией ЛК ИС в связи с недостаточностью результативности защиты от СР
λ_{25}	Поток событий невозможности менять логическую структуру ИС из-за нерелевантной (неадекватной, избыточной) частоты смены сетевых параметров абонентам ИС
λ_{31}	Поток событий (штатных, протокольных или внеочередных) на подтверждение сетевых параметров абонентами ИС к DHCP-серверу
λ_{42}	Поток событий необходимости принятия мер противодействия СР (заявки на оценку возможности изменить сетевые параметры абонентам ИС), опасность СР
λ_{51}	Поток событий отказа сетевого сканирования СР, вызванный функционированием средства защиты логической структуры ИС, и окончание (безуспешное) сетевого сканирования
λ_{56}	Поток событий на оценку результативности средств СР, связанный с успешным окончанием сетевого сканирования
λ_{65}	Поток событий отказа оценки результативности СР, заявки на продолжение СР

метров ИС в условиях воздействия СР (то есть, интенсивность λ_{12} (λ_{14}, λ_{15}) такова, что требования по обеспечению информационной безопасности выполняются).

Процесс конфигурирования сетевых параметров ИС в условиях воздействия СР в штатном режиме осуществляется под воздействием λ_{12}, λ_{23} и λ_{31} — заявок на эмуляцию ЛК ИС и штатной смены сетевых параметров абонентам ИС от DHCP-сервера, событий на штатное или внеочередное изменение сетевых параметров абонентам ИС от DHCP-сервера, эмуляцией ЛК ИС в связи с недостаточностью результативности защиты от СР и событий на штатное (протокольное) подтверждение сетевых параметров абонентами ИС к DHCP-серверу. После положительной оценки возможности изменить сетевые параметры (состояние S_2) под воздействием потока событий λ_{23} производится эмуляция новых ЛК ИС, перевод абонентов ИС в новую подсеть путем изменения сетевых параметров абонентам ИС, части действующих в предыдущей подсети ЛК ИС, назначению новых сетевых параметров вновь эмулированным ЛК ИС DHCP-сервером (состояние S_3), и переход в состояние покоя S_1 с интенсивностью λ_{21}, что интерпретируется как невозможность вскрытия логической структуры ИС средствами СР. При этом оставшаяся (не переведенная в новую подсеть) часть ложных компонентов ИС продолжает функционировать в предыдущей подсети, что вводит дополнительную обфускацию в информационном пространстве СР.

Под воздействием заявок низкой интенсивности λ_{15} на идентификацию средствами СР сетевых параметров ИС в диалоговом режиме, система переходит в состояние S_5, что означает штатную работу ИС при наличии воздействий СР, работающих в резидентном режиме, и проводящих добывание сведений о сетевых параметрах ИС, осуществляя последовательное выполнение функций сетевого сканера. Результативность функционирования средств защиты логической структуры с точки зрения СР интерпретируется потоком λ_{51}, под воздействием которого система переходит в режим штатного функционирования, девальвируя добытые в ходе функционирования СР сведения. Однако при низкой интенсивности λ_{12} система переходит в состояние S_6, что означает достижение средствами СР целей сканирования и вскрытие сетевых параметров ИС средствами СР с некоторой полнотой. Недостаточность полученных результатов сетевого сканирования и необходимость продолжения добывания сведений о логической структуре ИС средствами СР интерпретируется потоком событий λ_{65}.

Воздействие заявок λ_{15} высокой интенсивности на идентификацию средствами СР сетевых параметров ИС в диалоговом режиме обуславливает увеличение потока событий λ_{14} обнаружения фактов воздействия СР средствами СОА, переход в состояние S_4 и увеличение потока заявок на необходимость принятия мер противодействия СР, оценку возможности изменить сетевые параметры ИС, под воздействием которых система переходит в состояние S_2. Угроза вскрытия логической структуры ИС средствами СР нивелируется увеличением потока λ_{23} на эмуляцию новых ЛК ИС, перевод абонентов ИС в новую подсеть путем изменения сетевых параметров абонентам ИС, части действующих в предыдущей подсети ЛК ИС, и назначению новых сетевых параметров вновь эмулированным ЛК ИС DHCP-сервером, и переход в состояние покоя S_1 с интенсивностью λ_{31}, что интерпретируется как невозможность вскрытия логической структуры ИС средствами СР. В описанной ситуации смена сетевых параметров абонентам ИС девальвирует полученный в ходе сканирования СР результат.

Значительное увеличение интенсивности потоков заявок на штатное (λ_{12}) и (или) на внеочередное (λ_{42}) генерирование ЛК ИС и смену структурно-функциональных характеристик (СФХ) абонентам ИС от DHCP-сервера, приводит к увеличению потока отказов возможности менять сетевые параметры ИС, в связи с нерелевантной (избыточной) периодичностью смены сетевых параметров, выраженной в отказах в обслуживании легитимных абонентов ИС (λ_{25}), переходу системы в состояние осуществления средством СР последовательного выполнения функций сетевого сканера S_5 и, в итоге, вскрытия логической структуры ИС с некоторой полнотой (состояние S_6).

По размеченному графу состояний составлена система линейных однородных дифференциальных уравнений (СЛОДУ) Колмогорова, решением которой является вектор функций $p_i(t)$:

$$\begin{cases} \dfrac{\partial p_1(t)}{\partial t} = \lambda_{31} p_3(t) + \lambda_{51} p_5(t) - \lambda_{12} p_1(t) - \lambda_{14} p_1(t) - \\ -\lambda_{15} p_1(t); \\ \dfrac{\partial p_2(t)}{\partial t} = \lambda_{12} p_1(t) + \lambda_{42} p_4(t) - \lambda_{23} p_2(t) - \lambda_{25} p_2(t); \\ \dfrac{\partial p_3(t)}{\partial t} = \lambda_{23} p_2(t) - \lambda_{31} p_3(t); \\ \dfrac{\partial p_4(t)}{\partial t} = \lambda_{14} p_1(t) - \lambda_{42} p_4(t); \\ \dfrac{\partial p_5(t)}{\partial t} = \lambda_{15} p_1(t) + \lambda_{25} p_2(t) + \lambda_{65} p_6(t) - \lambda_{51} p_5(t) - \\ -\lambda_{56} p_5(t); \\ \dfrac{\partial p_6(t)}{\partial t} = \lambda_{56} p_5(t) - \lambda_{65} p_6(t), \end{cases}$$

где $p_i(t)$ — искомые функции (вероятности нахождения системы в состоянии i в момент времени t);

λ_{ij} — интенсивности потоков событий перехода из состояния i в состояние j.

Применение модели заключается в вариации λ_{ij} в пределах устойчивости марковского процесса, описанного системой линейных дифференциальных уравнений. Характер выбранных значений интенсивностей определяется в соответствии с условиями функционирования ИС. Наибольшее практическое значение при конфигурировании сетевых параметров ИС в условиях воздействия СР имеют следующие две контрастные ситуации SIT_1 и SIT_2 (табл. 3).

Ситуация SIT_1 — генерирование ложных компонентов ИС и смена сетевых параметров абонентам ИС от DHCP-сервера осуществляется штатно через заранее рассчитанные интервалы времени. Поскольку средства СР функционируют в резидентном режиме и не идентифицированы СОА, то рассматривается, как влияют интенсивности потоков событий λ_{12} необходимости на генерирование ЛК ИС и штатную смену сетевых параметров абонентам ИС от DHCP-сервера, и λ_{23} на штатное их изменение на вероятности p_1 невозможности вскрытия логической структуры ИС средствами СР и p_6 вскрытия логической структуры ИС с некоторой полнотой.

Ситуация SIT_2 — осуществляется внеочередное генерирование ЛК ИС и смена сетевых параметров абонентам ИС от DHCP-сервера в связи с поступлением заявок от СОА. Поскольку средства СР идентифицированы СОА, то рассматривается, как влияют интенсивности потоков событий λ_{42} необходимости принятия мер противодействия СР, и λ_{23} на внеочередное генерирование ЛК ИС и штатную смену сетевых параметров абонентам ИС от DHCP-сервера, на вероятности p_1 невозможности вскрытия логичесокй структуры ИС средствами СР и p_6 ее вскрытия с некоторой полнотой.

Для получения оценки переходных процессов в ситуациях SIT_1 и SIT_2 перейдем к решению СЛОДУ численным методом. Исходные данные для расчета: СЛОДУ, вектор вероятностей начальных состояний, нормировочное условие, значения интенсивностей потоков событий задаем постоянными в соответствии с выбранными условиями функционирования ИС.

В ситуации SIT_1 на интервале времени [0; 9,1] с ИС находится в переходном режиме функционирования, где наблюдается всплеск значений вероятности состояния $p_6(t)$, что интерпретируется как нахождение ИС в состоянии невозможности вскрытия логической структуры ИС средствами СР. Значительное уменьшение периодичности генерирования ЛК ИС и штатной смены сетевых параметров абонентам ИС от DHCP-сервера (интенсивность потока событий $\lambda_{12} < 3$) приводит ко вскрытию сетевых параметров ИС средствами СР с некоторой полнотой (рис. 4).

В ситуации SIT_2 на интервале времени [0; 2,87] с ИС находится в переходном режиме функционирования, где наблюдается всплеск

Таблица 3

Вариация параметров модели в зависимости от условий функционирования ИС

Признаки	Ситуации	
	SIT_1	SIT_2
Штатная смена сетевых параметров	min	max
Наличие СР	min	max
Обнаружение средств СР средствами СОА	min	max

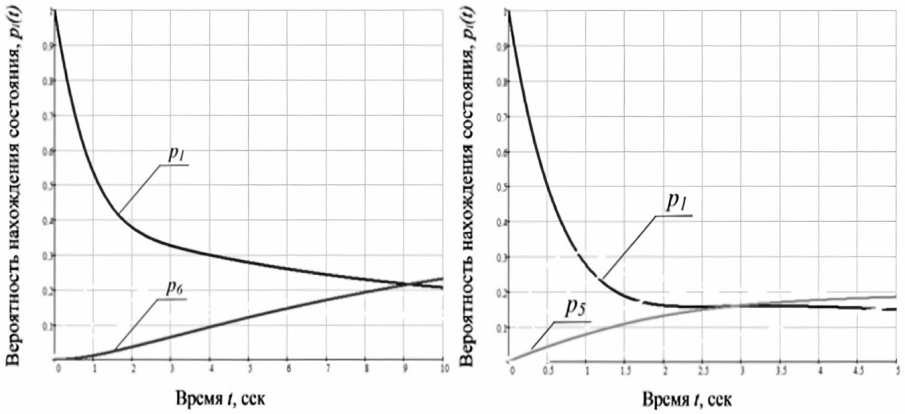

Рис. 4. Результаты расчета зависимостей вероятностей состояний p_1 и p_6 (в ситуации SIT_1), p_1 и p_5 (в ситуации SIT_2) от времени для значений интенсивностей событий

значений вероятности состояния $p_5(t)$, что интерпретируется как нахождение ИС в состоянии доступности информации клиентам ИС (рис. 4). Значительное увеличение периодичности генерирования ЛК ИС и штатной смены сетевых параметров абонентам ИС от DHCP-сервера (интенсивность потока событий $\lambda_{12} > 324$) приводит к увеличению отказов возможности менять логическую структуру ИС из-за нерелевантной (неадекватной, избыточной) частоты смены сетевых параметров абонентам ИС в связи с угрозой отказа в обслуживании легитимных абонентов.

Снизить нагрузку на данное состояние сервера возможно путем эмуляции ЛК ИС взамен переведенных в новую подсеть узлов ИС и оставления в предыдущей подсети ЛК ИС, подвергнутых сканированию сетевой разведкой, что, в свою очередь, введет дополнительную неопределенность на информационном поле СР. Данный подход предоставит выигрыш во времени, позволяющий перевести на новые сетевые параметры абонентов ИС, и, как следствие, обеспечить функционирование ИС, не приводящее к отказу в обслуживании ее легитимных абонентов.

Выводы

Предложенная модель позволяет находить вероятностные и временные характеристики, описывающие состояния процесса конфигурирования сетевых параметров информационной системы в различных ситуациях, которые необходимо использовать при синтезе структур ложных сетевых компонентов для решения задач дезинформации противника относительно структуры и конфигурации объектов защиты. При этом выбор ситуаций обусловлен особенностями процессов ведения сетевого сканирования злоумышленником.

Литература

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

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

3. Давыдов А.Е. Защита и безопасность ведомственных интегрированных инфокоммуникационных систем: монография / А.Е. Давыдов, Р.В. Максимов, О.К. Савицкий. — Москва: Воентелеком, 2015. 520 с.

4. Lei C. Moving Target Defense Techniques: A Survey / C. Lei, H. Zhang, J. Tan, Y. Zhang, X. Liu // Security and Communication Networks. 2018. Vol. 2. P. 1–25.

5. Максимов Р.В., Шерстобитов Р.С., Катунцев С.Л., Шарифуллин С.Р., Каплин М.А. Программный модуль управления интенсивностью маскирующего трафика: свидетельство о государственной регистрации программы для ЭВМ № 2018660295 от 21 августа 2018 года.

6. Каплин М.А. Модель верификации результативности маскирования структуры информационных систем // Информатика: проблемы, методы, технология: сборник статей XXI международной научно-технической конференции. — Воронеж. 2021. С. 737–746.

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

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

9. Ворончихин И.С. Динамическое изменение структурно-функциональных характеристик информационной системы в целях снижения эффективности сетевой разведки // Безопасные информационные технологии: Безопасные информационные технологии: сборник трудов Десятой Международной научно-технической конференции. — Москва. 2019. С. 81–87.

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

Referense

1. Maximov R.V. Innovative information technologies in the context of ensuring national security of the state / R.V. Maximov, S.P. Sokolovsky, S.R. Sharifullin, V.P. Chernoles // Innovations. 2018. № 3 (233). P. 28–35.

2. Voronchikhin I.S. Masking the structure of distributed information systems in cyberspace / I.S. Voronchikhin, I.I. Ivanov, R.V. Maximov, S.P. Sokolovsky // Cybersecurity issues. 2019. № 6 (34). P. 92–101.

3. Davydov A.E. The Protection and Security of Departmental Integrated Information and Communication Systems: monograph / A.E. Davydov, R.V. Maximov, O.K. Savickij. — Moscow: Voentelekom, 2015. 520 p.

4. Lei C. Moving Target Defense Techniques: A Survey / C. Lei, H. Zhang, J. Tan, Y. Zhang, X. Liu // Security and Communication Networks. 2018. Vol. 2. P. 1–25.

5. Maximov R.V. Sherstobitov R.S., Katuncev S.L., Sharifullin S.R., Kaplin M.A. Software module for controlling the intensity of masking traffic: certificate of state registration of the program for ECM 2018660295 from 21.08.2018.

6. Kaplin M.A. Model for verification of performance of information systems structure masking // Computer science: problems, methods, technology: collection of articles of the XXI International Scientific and Technical Conference. — Voronezh. 2021. P. 737–746.

7. Patent for the invention RU 2716220. Method of protection of computer networks: publ. 06.03.20: Byul. № 7 / R.V. Maksimov, S.P. Sokolovsky, I.S. Voronchikhin. 33 p.

8. Maksimov R.V. Algorithm and technical solutions for dynamic configuration of client-server computer networks / R.V. Maksimov, S.P. Sokolovsky, I.S. Voronchikhin // Informatics and automation. 2020. № 5. P. 1018–1049.

9. Voronchikhin I.S. Dynamic change of structural and functional characteristics of an information system in order to reduce the effectiveness of network intelligence // Safe information technologies: Safe information technologies: proceedings of the Tenth International Scientific and Technical Conference. — Moscow. 2019. P. 81–87.

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