УДК 004.738.5 **DOI** 10.15622/ia.2020.19.5.5

Р.В. Максимов, С.П. Соколовский, И.С. Ворончихин

АЛГОРИТМ И ТЕХНИЧЕСКИЕ РЕШЕНИЯ ДИНАМИЧЕСКОГО КОНФИГУРИРОВАНИЯ КЛИЕНТ-СЕРВЕРНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

Максимов Р.В., Соколовский С.П., Ворончихин И.С. **Алгоритм и технические решения динамического конфигурирования клиент-серверных вычислительных сетей.**

Аннотация. Проанализированы основные факторы, обуславливающие расширение возможностей и повышение результативности сетевой разведки по идентификации состава и структуры клиент-серверных вычислительных сетей вследствие стационарности их структурно-функциональных характеристик. Вскрытые особенности защиты клиент-серверных вычислительных сетей, основанных на реализации принципов пространственного обеспечения безопасности, а также формализация и внедрение множества запрещающих регламентов обосновывают актуальность задачи динамического управления структурно-функциональными характеристиками клиент-серверных вычислительных сетей, функционирующих в условиях сетевой разведки.

Представлена математическая модель, позволяющая находить оптимальные режимы динамического конфигурирования структурно-функциональных характеристик клиент-серверных вычислительных сетей для различных ситуаций. Приведены результаты расчетов. Представлен алгоритм решения задачи динамической конфигурации структурно-функциональных характеристик клиент-серверной вычислительной сети, обеспечивающий уменьшение времени достоверности добываемых сетевой разведкой данных. Показаны результаты практических испытаний разработанного на основе алгоритма динамического конфигурирования клиент-серверных вычислительных сетей программного обеспечения. Полученные результаты свидетельствуют, что использование представленного решения по динамическому конфигурированию клиент-серверных вычислительных сетей позволяет повысить результативность защиты за счет изменения структурно-функциональных характеристик клиент-серверных вычислительных сетей в рамках нескольких подсетей. При этом достигнуто поддержание критически важных соединений, а интервалы времени изменения структурно-функциональных характеристик адаптивны к условиям функционирования и действиям злоумышленника.

Новизна разработанной модели заключается в применении математического аппарата теории марковских случайных процессов и решении уравнений Колмогорова для обоснования выбора режимов динамического конфигурирования структурно-функциональных характеристик клиент-серверных вычислительных сетей. Новизна разработанного алгоритма состоит в применении модели динамического конфигурирования структурно-функциональных характеристик клиент-серверных вычислительных сетей для динамического управления структурно-функциональными характеристиками клиент-серверной вычислительной сети в условиях сетевой разведки.

Ключевые слова: сетевая разведка, клиент-серверные вычислительные сети, технология движущейся цели, компьютерная атака, киберманеврирование

1. Введение. Развитие высоких технологий напрямую сопряжено с развитием компьютерных сетей. Все компьютерные сети по своему назначению делятся на вычислительные, информационные и смешанные. Наибольший практический интерес представляют собой вы-

числительные сети, которые предназначены для распределенного решения вычислительных задач в крупных научных центрах, предприятиях аэрокосмической отрасли и нефтегазовой промышленности, а также в оборонном секторе.

Вычислительные сети представляет собой совокупность компьютеров, соединенных между собой с каналами связи в единую систему и использующих общие ресурсы. В клиент-серверной архитектуре вычислительных сетей задания, или сетевая нагрузка, распределены между серверами (поставщиками услуг) и клиентами (клиентами). Фактически клиент и сервер – это программное обеспечение, размещенное на ЭВМ и взаимодействующее через вычислительную сеть.

В общем случае клиент-серверная вычислительная сеть (КС ВС) представляет собой совокупность клиентов, периферийного и коммуникационного оборудования, объединенного физическими линиями связи. В состав КС ВС также могут входить серверы управления данными, которые используются в совокупности с системами управления базами данных. Все эти элементы определяются идентификаторами, в качестве которых в наиболее распространенном семействе протоколов *TCP/IP* используются сетевые адреса (*IP*-адреса). Для взаимодействия с клиентами сервер выделяет необходимые ресурсы для работы и ожидает запросы на открытие соединения (или запросы на предоставляемый сервис) [1, 2]. Формат запросов клиента и сервера определяется протоколом.

Рассматриваются без детализации функций содержательной обработки информации КС ВС, элементы которых функционируют под управлением *DHCP*-сервера. Для получения элементами КС ВС сетевых параметров, таких как *IP*-адрес, время продолжительности аренды *IP*-адреса, номер подсети (маска) и других, используется протокол *DHCP* (*Dynamic Host Configuration Protocol* – протокол динамической настройки узла) [3], который позволяет автоматически назначать параметры на определенный срок, называемый временем аренды. *DHCP*-сервер функционирует на прикладном уровне эталонной модели взаимодействия открытых систем, однако он реализует распределение параметров сетевого уровня. По истечении времени аренды *IP*-адрес вновь считается свободным, и клиент обязан запросить новый или же продлить арендуемый ранее. Кроме того, клиент сам может отказаться от полученного адреса. Динамическое (по сути – автоматическое) распределение *IP*-адресов является единственным, которое позволяет централизованно управлять адресным пространством КС ВС и политикой безопасности, избегая конфликтов распределения сетевых параметров, рационально используя незадействованные или временно сво-

бодные *IP*-адреса. Процесс инициализации клиента в КС ВС известен и включает четыре этапа получения *IP*-адреса в аренду [3].

Использование именно этого клиент-серверного протокола позволяет за счет вариации параметров динамической конфигурации структурно-функциональных характеристик КС ВС в условиях сетевой разведки скрыть состав, структуру и алгоритмы функционирования КС ВС от сетевой разведки и перевести КС ВС в заранее заданную конфигурацию при реализации злоумышленником компьютерной атаки (КА).

2. Анализ объекта исследования. Конвергенция информационных технологий и инфраструктуры, приобретающих глобальный трансграничный характер, вызывает негативные процессы, которые порождают угрозы национальной безопасности государства в экономической, оборонной, информационной и других сферах.

Этому способствует:

– наращивание злоумышленниками ассортимента средств сетевой разведки и организация их непосредственного контакта с элементами КС ВС через организацию интерфейсов сетевой разведки с элементами КС ВС;

– организация составных каналов утечки и создание виртуальных точек присутствия, обусловленная открытостью архитектуры КС ВС и протоколов информационного обмена (семейства *TCP/IP*);

– использование недекларированных возможностей аппаратного и программного обеспечения, обусловленных применением в КС ВС зарубежной технологической базы.

В большинстве случаев успешной компьютерной атаке на КС ВС всегда предшествуют процессы сетевой разведки. Сетевая разведка (СР) представляет собой процесс добывания и обработки данных о КС ВС, используемых устройствах и программном обеспечении, их уязвимостях, средствах защиты, а также путях проникновения в КС ВС. СР направлена на получение структурно-функциональных характеристик КС ВС.

Под структурно-функциональными характеристиками (СФХ) в работе понимаются структура, состав, физические, логические, функциональные и технологические взаимосвязи между сегментами КС ВС, применяемые информационные технологии и особенности их функционирования.

Под динамической конфигурацией СФХ КС ВС в работе понимается такое управление сетевыми параметрами и взаимосвязями элементов КС ВС, при котором длительность стационарного состояния КС ВС изменяется адаптивно, и может быть установлено таким, что

будет меньше длительности времени сбора злоумышленником информации о структуре КС ВС ВН. Следовательно, так называемый динамический способ распределения *IP*-адресов, реализуемый протоколом *DHCP*, является разновидностью автоматического (автоматизированного) распределения и не учитывает сценариев развития и длительности времени сбора злоумышленником информации.

Периодичность динамической конфигурацией СФХ КС ВС задается декларативно и может быть определена в диапазоне от минимального до максимального значения времени работы сетевого сканера злоумышленника. Значения времени работы сетевого сканера определяется в зависимости от средств СР.

Применение в КС ВС традиционных средств защиты информации, таких как межсетевые экраны, системы обнаружения атак и вторжений, а также криптографических средств защиты, не позволяет обеспечить конфиденциальность информации о ее составе и структуре. Это обусловлено, во-первых, тем, что информационные системы (ИС) используют при передаче по КС ВС *IP*-пакетов адресную и другую служебную (технологическую) информацию [4]. Во-вторых, тем, что подавляющему большинству современных КС ВС присущи свойства детерминированности, статичности и однородности. Так, свойство статичности КС ВС заключается в наличии инвариантов структуры КС ВС, к которым можно отнести схему информационных связей и саму структуру КС ВС. Свойство однородности подразумевает наличие инвариантов состава КС ВС, к нему можно отнести множество элементов оборудования, которым представлены узлы КС ВС и установленное на узлах КС ВС программное обеспечение [5]. Свойство детерминированности сводится к наличию инвариантов алгоритмов функционирования КС ВС, к которым можно отнести интенсивность информационного обмена клиентов КС ВС, протоколы их взаимодействия, физические и логические адреса элементов КС ВС, топологию КС ВС, множество функций и иерархическую структуру клиентов КС ВС [6].

Злоумышленники, использующие данные обстоятельства, получают преимущество в использовании временного и вычислительного ресурса для ведения СР, чем достигают:

– высокой достоверности результатов СР в течение длительного времени, что позволяет осуществлять планирование, выбор времени и технологического процесса КС ВС для начала КА;

– возможности бескомпроматного применения средств СР и реализации КА в любое удобное для этого время за счет заблаговременного (планового) формирования и применения их рационального состава;

– возможности неоднократного поиска и анализа уязвимостей аппаратного и программного обеспечения с последующим их тестированием на проникновение для конкретной цели;

– возможности с небольшими ресурсными затратами проводить крупномасштабную КА после обобщения частных результатов СР.

Непосредственное влияние на возникновение данных обстоятельств оказывают, с одной стороны, требования нормативных правовых актов (НПА), определяющих топологию и типологию КС ВС, с другой стороны, требования НПА к ассортименту и особенностям применения средств защиты информации, применяемых в КС ВС.

В то же время регуляторы в качестве основных мер и рекомендаций по защите КС ВС указывают:

– сокрытие архитектуры и конфигурации информационной (автоматизированной) системы (Приказ ФСТЭК России № 239 от 25.07.2019);

– управление изменениями конфигурации информационной системы и системы защиты персональных данных (Приказ ФСТЭК России № 239 от 25.07.2019);

– перевод информационной системы или ее устройств (компонентов) в заранее определенную конфигурацию, которая обеспечивает защиту информации в случае возникновения отказов (сбоев) в защите информационной системы (Приказ ФСТЭК России № 27 от 15.02.2017).

Реализовать данные меры на текущий момент не представляется возможным, так как отсутствуют необходимые для этого технологии, и, соответственно, невозможно предъявлять требования к разработке и применению средств и систем защиты на основе этих технологий.

Внедрение ассортимента запрещающих регламентов, основанных на обнаружении и реагировании на факт ведения СР, не способны эффективно противостоять современным средствам СР [7]. В связи с этим требуются принципиально новые подходы к построению систем безопасности.

Если заменить статические параметры КС ВС динамическими, то злоумышленник не может получить окончательную и актуальную информацию, позволяющую реализовать вскрытые уязвимости программного обеспечения КС ВС. Данная концепция получила название «Защита на основе движущейся цели» (*Moving Target Defense*, *MTD*) [8-10]. Проведенный анализ научных работ в рассматриваемой предметной области [11-14] показал настолько высокую эффективность этой концепции, что за последние годы к исследованиям и разработке систем защиты в этом направлении привлечены научные кол-

лективы более чем в 30 странах мира. Существующий тренд исследований свидетельствует о том, что *MTD* может стать одной из основных парадигм построения систем информационной безопасности в ближайшем будущем.

Одним из направлений концепции *MTD* является динамическое изменение параметров КС ВС, таких как применяемые сетевые протоколы, значения *IP*- и *MAC*-адресов, номер подсети (маска), номера сетевых портов, применяемые алгоритмы шифрования, а также маршруты передачи трафика (информационные направления). Следовательно, при реализации концепции *MTD* в маскировании состава и структуры КС ВС направлением первоочередной разработки является динамическое изменение параметров сети (в рамках данной статьи – динамическое управления сетевым адресным пространством). Анализ научных работ в рассматриваемой предметной области показал, что для динамического изменения параметров КС ВС применяются методы киберманеврирования (*cyber maneuvering*) [11], которые заключаются в периодическом (синхронизированном по времени) или неуправляемом (случайном) изменении СФХ абонентов КС ВС с использованием различных способов [15-17]. При технической реализации киберманеврирования применяется *DHCP*-сервер с расширенными настройками, обеспечивающий динамическое конфигурирование СФХ КС в соответствии с разработанными алгоритмами при наступлении заданного события безопасности.

В то же время следует отметить, что известные технические решения, реализующие методы киберманеврирования, еще недостаточно проработаны и обладают существенными недостатками, а задачи приведения в соответствие таких мер защиты КС ВС (централизованному) замыслу противодействия средствам СР только начинают формулироваться отдельными авторами и их кооперациями [18-21], что обуславливает актуальность проводимого исследования.

3. Постановка задачи. Формализованную постановку задачи на динамическое конфигурирование СФХ КС ВС можно представить следующим образом:

$$< MIP, Z > \rightarrow \min P_{ABD} = \lim_{t \to \infty} P_{ABD}(t) \mid P_{ABD} \in \{P_i\},\ i = 1, 2, \ldots, h \qquad (1)$$

для минимизации вероятности вскрытия (от англ. *abduction*) структуры КС ВС злоумышленником;

$$< MIP, Z > \rightarrow \max P_{AC} = \lim_{t \to \infty} P_{AC}(t) \mid P_{AC} \in \{P_i\},\ i = 1, 2, \ldots, h \qquad (2)$$

для максимизации вероятности доступности (от англ. *access*) информации клиентам КС ВС в связи со сменой СФХ КС ВС.

В выражениях (1) и (2) введены следующие переменные:

– Z – множество внутренних параметров модели, $Z \subseteq \{S_i, \Lambda_j\}$,

где S_i = {S_1, …, S_h} – перечень моделируемых состояний КС ВС, Λ_j = {λ_1, λ_2, …, λ_J} – интенсивности потоков событий в ней;

– *MIP* – множество входных параметров модели, параметров СФХ КС ВС (от англ. *Model Input Parameters*) $MIP \subseteq \{IP, D, TM\}$, где *IP* – значение *IP*-адресов сетевых устройств вычислительной сети, являющихся клиентами *DHCP*-сервера;

– D = [1, 2, …, 32] – номер вычислительной сети *DHCP*-сервера (длина маски подсети) и клиентов КС ВС, максимальное значение составляет 32, а минимальное – 0;

– TM = [0, 1, ..., 2592000] – значение времени аренды всех *IP*-адресов вычислительной сети.

Под доступностью информации будем понимать состояние информации (ресурсов КС ВС), при котором клиенты, обладающие правами доступа, могут реализовывать их беспрепятственно. Потоки событий от клиентов к *DHCP*-серверу и от *DHCP*-сервера к клиентам представляют собой последовательность управления сетевыми параметрами и СФХ КС ВС, приводящими к изменению доступности информации клиентам и к изменению возможностей злоумышленников по вскрытию структуры КС ВС.

4. Модель динамического конфигурирования клиент-серверных вычислительных сетей. Пусть имеется КС ВС, СФХ которой могут изменяться администратором в ручном и автоматическом режимах, а также имеется узел КС ВС – *DHCP*-сервер, обеспечивающий формирование и назначение СФХ сетевым устройствам, таких как *IP*-адреса, время их аренды, маска подсети и *IP*-адрес *DHCP*-сервера, который может функционировать в том числе и в качестве средства защиты информации о составе и структуре КС ВС от СР.

Моделируемая система S с течением времени меняет свое состояние (переходит из одного состояния в другое) с интенсивностью потоков событий λ, потенциально переводящих КС ВС в состояния, когда обеспечивается или не обеспечивается скрытие структуры КС ВС при ведении СР злоумышленником. Необходимые для исследования состояния КС ВС представлены в таблице 1.

Смена состояний S_1 – S_5 обуславливается возможностью нарушения штатного режима функционирования КС ВС под воздействием на нее средств СР и КА, которые могут создавать внеочередные заявки,

влияющие на доступность информации клиентов КС ВС. В случае, если длительность цикла ведения СР меньше длительности периода стационарности СФХ КС ВС, то можно полагать, что КС ВС может быть вскрыта средствами СР. Конструктивное использование результатов СР – это КА, влияющие на ухудшение основных качеств КС ВС.

Таблица 1. Дискретные состояния КС ВС

Переменная	Состояния
S_1	Состояние покоя КС ВС. Признаки СР и КА отсутствуют
S_2	Состояние изменения СФХ (перевод КС ВС в заранее определенную конфигурацию)
S_3	Состояние обнаружения средств СР штатными средствами защиты КС ВС
S_4	Состояние идентификации средствами СР СФХ КС ВС с некоторой полнотой
S_5	Состояние невозможности вскрытия СФХ КС ВС средствами СР злоумышленника

Следовательно, для снижения результативности СР и возможности последующей реализации КА на КС ВС необходимо сокращение времени пребывания СФХ КС ВС в стационарном состоянии (так чтобы длительность времени аренды *IP*-адресов и других сетевых параметров была меньше длительности времени ведения СР). Однако это может привести к тому, что КС ВС в некоторый момент времени не сможет обеспечить доступность информации клиентам КС ВС.

Эффективность функционирования КС ВС будет оцениваться как способность КС ВС обеспечивать доступность информации клиентам КС ВС при реализации динамического конфигурирования СФХ в условиях воздействия средств СР.

Моменты возможных переходов моделируемой системы из состояния в состояние неопределенны, случайны и происходят под действием событий, характеризующихся интенсивностями λ (табл. 2). Интенсивность события λ – это среднее число событий, приходящихся на единицу времени.

Оценка эффективности процессов функционирования КС ВС при использовании динамического конфигурирования СФХ связана с необходимостью моделирования данного процесса в реальном времени, что обусловливает целесообразность использования математического аппарата марковских процессов, необходимые условия которого: потоки событий являются простейшими (обладают свойствами стационарности, ординарности и не имеют последействий). Таким образом, процесс функционирования КС ВС в условиях динамического конфи-

гурирования ее СФХ можно представить как марковский случайный процесс с дискретными состояниями и непрерывным временем.

Таблица 2. Интенсивности потоков событий

Переменная	Описание потока событий
λ_{12}	Заявки на штатное формирование и назначение СФХ клиентам КС ВС (средств СР не обнаружено)
λ_{21}	Заявки на распределение СФХ клиентам КС ВС
λ_{13}	Заявки на обнаружение средств СР
λ_{32}	Заявки на внештатное изменение СФХ клиентам КС ВС
λ_{25}	Заявки на оценку результативности защиты от средств СР
λ_{51}	Заявки на продление текущих сетевых параметров клиентам КС ВС
λ_{24}	Заявки на оценку результативности средств СР
λ_{43}	Заявки скомпрометированного средства СР на вскрытие СФХ клиентов КС ВС
λ_{41}	Заявки нескомпрометированного средства СР на вскрытие СФХ клиентов КС ВС

На рисунке 1 представлен граф состояний моделируемой системы. Рассмотрим сценарий перехода моделируемой системы из состояния S_i в состояние S_j под воздействием потоков событий с интенсивностями λ_{ij}.

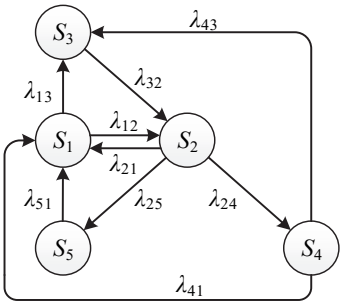

Рис. 1. Граф состояний процесса функционирования КС ВС

Пусть КС ВС функционирует в штатном режиме, между клиентами и серверами осуществляется информационный обмен, всем сетевым устройствам распределены *IP*-адреса и другие СФХ, сетевые устройства взаимодействуют между собой, воздействия средств СР отсутствуют, тогда S_1 – начальное состояние моделируемой системы (состояние покоя системы). Динамическое изменение сетевых параметров клиентов КС ВС в штатном режиме S_2 осуществляется под

воздействием λ_{12} и λ_{21} – заявок на штатное продление времени аренды *IP*-адресов и установление сетевых параметров новым клиентам. После изменения СФХ под воздействием заявок λ_{12} КС ВС переходит из состояния S_2 в состояние покоя S_1 с интенсивностью λ_{21}. В состояние S_3 система переходит под воздействием заявок на обнаружение средств СР λ_{13}. С увеличением интенсивности заявок λ_{32} на внештатное изменение СФХ клиентов КС ВС переходит из состояния S_3 в состояние S_2.

Увеличение потока заявок на оценку результативности средств СР с интенсивностью λ_{24}, означает переход системы в состояние S_4, в котором злоумышленник с использованием средств СР идентифицировал состав, структуру и алгоритмы функционирования КС ВС с некоторой полнотой.

Увеличение интенсивности применения средств СР злоумышленником λ_{43} на определенном этапе приведет к компрометации средств СР и переходу системы из состояния S_4 в состояние S_3.

Процесс бескомпроматной идентификации СФХ КС ВС средствами СР злоумышленника потоком заявок с интенсивностью λ_{41} означает штатную работу КС ВС при наличии средства СР, работающего в резидентном режиме, и переход системы в состояние S_1. Переход системы из состояния S_2 в S_5 осуществляется под воздействием заявок на оценку результативности защиты от СР λ_{25} и означает отсутствие идентификации СФХ КС ВС средствами СР. Это приведет к тому, что изменение СФХ сетевых устройств КС ВС осуществляется в штатном режиме, по расписанию.

В случае привлечения для динамического распределения СФХ сетевым устройствам КС ВС *DHCP*-сервера его функционирование осуществляется в пределах одной подсети, без использования агентов-ретрансляторов, предназначенных для распределения сетевых параметров между сетевыми устройствами, которые находятся в разных подсетях. Максимальное число клиентов *DHCP*-сервера определяется выбранным классом сети, что в соответствии с рассматриваемым типом КС ВС будет составлять 255 (компьютерные сети класса *C*).

По размеченному графу состояний составлены уравнения Колмогорова – дифференциальные уравнения (3) с неизвестными функциями $p_i(t)$.

Используя известный порядок решения системы линейных дифференциальных уравнений методом Рунге – Кутты [22, 23] и учитывая вектор вероятностей начальных состояний $p_i(0)$, интервал интегрирования t_0, t_1 и число этапов интегрирования n, произведен расчет для заданных значений интенсивностей событий $\lambda_{ij} = \text{const}$ (марковский однородный процесс), что позволило получить числовые таблицы

приближенных значений p_i искомых решений $p(t)$ на некотором интервале $t \in [t_0, t_1]$. Таким образом, получены вероятностные и временные характеристики, описывающие состояния процесса функционирования КС ВС при изменении СФХ в различных условиях функционирования КС ВС (ситуациях).

$$\left.\begin{aligned}
&\frac{dp_1(t)}{dt} = \lambda_{21}p_2(t) + \lambda_{51}p_5(t) - \lambda_{12}p_1(t) + \lambda_{41}p_4(t) - \lambda_{13}p_1(t),\\
&\frac{dp_2(t)}{dt} = \lambda_{12}p_1(t) + \lambda_{32}p_3(t) - \lambda_{21}p_2(t) - \lambda_{24}p_2(t) - \lambda_{25}p_2(t),\\
&\frac{dp_3(t)}{dt} = \lambda_{13}p_1(t) - \lambda_{32}p_3(t) + \lambda_{43}p_4(t),\\
&\frac{dp_4(t)}{dt} = \lambda_{24}p_2(t) - \lambda_{43}p_4(t) - \lambda_{41}p_4(t),\\
&\frac{dp_5(t)}{dt} = \lambda_{25}p_2(t) - \lambda_{51}p_5(t),\\
&\sum_{i=1}^{5} p_i(t) = 1.
\end{aligned}\right\} \qquad (3)$$

Рассмотрим использование модели при вариациях исходных данных, определяющих следующие ситуации.

В исходной ситуации КС ВС функционирует без воздействия средств СР, в штатном режиме, СФХ сетевым устройствам распределены, осуществляется информационный обмен. По истечению времени аренды СФХ сетевых устройств КС ВС они штатно изменяются в ручном или автоматическом режиме администратором.

Ситуация C_1. КС ВС функционирует в условиях воздействия средств СР злоумышленника. Средства СР не обнаружены штатными средствами защиты КС ВС и функционируют бескомпроматно. СФХ сетевым устройствам распределены, осуществляется информационный обмен. По истечению времени аренды СФХ КС ВС они штатно изменяются в ручном или автоматическом режиме администратором. Средства СР направляют к КС ВС поток заявок на идентификацию СФХ сетевых устройств КС ВС с интенсивностью, позволяющей при постоянной интенсивности заявок на внештатное изменение СФХ сетевых устройств КС ВС, а также постоянной интенсивности заявок на обнаружение и оценку результативности обнаружения средств СР со стороны штатных средств защиты, к некоторому моменту времени вскрыть СФХ сетевых устройств КС ВС с некоторой полнотой.

Ситуация C_2. КС ВС функционирует в условиях воздействия средств СР злоумышленника. Средства СР обнаружены штатными средствами защиты КС ВС. СФХ сетевым устройствам распределены, осуществляется информационный обмен. По истечению времени аренды СФХ сетевых устройств КС ВС они штатно изменяются в ручном или автоматическом режиме администратором. При отсутствии возможности увеличения интенсивности заявок на внештатное изменение СФХ сетевых устройств КС ВС, чтобы предотвратить вскрытие средствами СР злоумышленника СФХ сетевых устройств КС ВС, штатные средства защиты наращивают интенсивность потока заявок на обнаружение средств СР и оценку результативности обнаружения средств СР.

Ситуация C_3. КС ВС функционирует без воздействия средств СР, в штатном режиме, СФХ сетевым устройствам распределены, осуществляется информационный обмен. СФХ КС ВС внештатно изменяются *DHCP*-сервером в динамическом режиме с уменьшением временных интервалов изменения СФХ. Интенсивность изменения СФХ сетевых устройств КС ВС *DHCP*-сервером может увеличиваться до тех пор, пока минимальное значение интервала времени, через который изменяются СФХ сетевых устройств, не примет пороговое значение, после прохождения которого КС ВС не сможет выполнять свою целевую функцию и будет перегружена ввиду невозможности сетевых устройств завершить текущий цикл получения распределенных им СФХ и установления ими сетевых соединений до наступления очередного цикла изменения СФХ.

При $t \to \infty$ в моделируемой системе устанавливается стационарный режим, когда КС ВС случайным образом меняет свои состояния и ее вероятности $p_1(t), p_2(t), \ldots, p_5(t)$ уже не зависят от времени и равны финальным (предельным) вероятностям.

Приближенные значения p_i на интервале $t \in [0,5]$ с фиксированным шагом интегрирования 10^3 для значений интенсивностей потоков событий ситуации C_1 имеют значения $p_1 = 0{,}2$, $p_2 = 0{,}05$, $p_3 = 0$, $p_4 = 0{,}75$, $p_5 = 0$, сплайн-интерполяция значений представлена на графиках зависимостей вероятностей состояний от времени (рис. 2).

На интервале времени [0; 1,63] графика, представленного на рисунке 2, моделируемая система находится в переходном состоянии, наблюдается всплеск значений вероятности состояния $p_2(t)$, $p_4(t)$ и значительное снижение вероятности $p_1(t)$ пребывания моделируемой системы в состоянии штатного режима функционирования, что соответствует вскрытию КС ВС с вероятностью 0,77 уже через 1,6 секунды бескомпроматного функционирования средств СР.

Это возможно при постоянной интенсивности заявок на штатное изменение СФХ сетевых устройств КС ВС, а также постоянной интенсивности заявок на обнаружение средств СР и оценку его результативности.

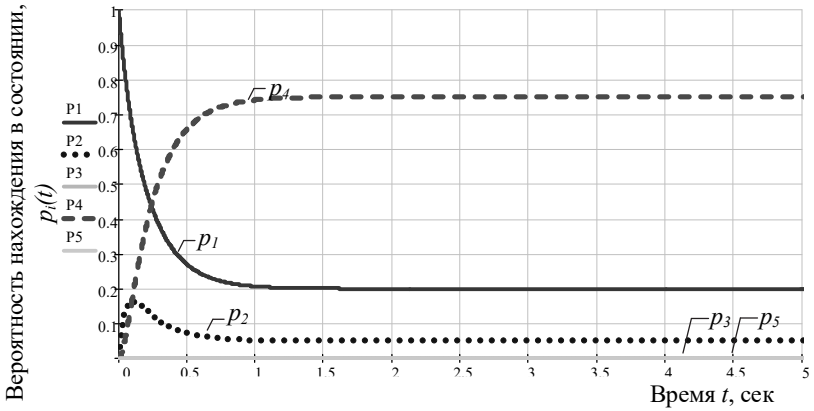

Рис. 2. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий для ситуации C_1

Финальные вероятности для ситуации C_2 имеют следующие значения $p_1 = 0{,}114$, $p_2 = 0{,}047$, $p_3 = 0{,}475$, $p_4 = 0{,}032$, $p_5 = 0{,}332$ и представлены на рисунке 3.

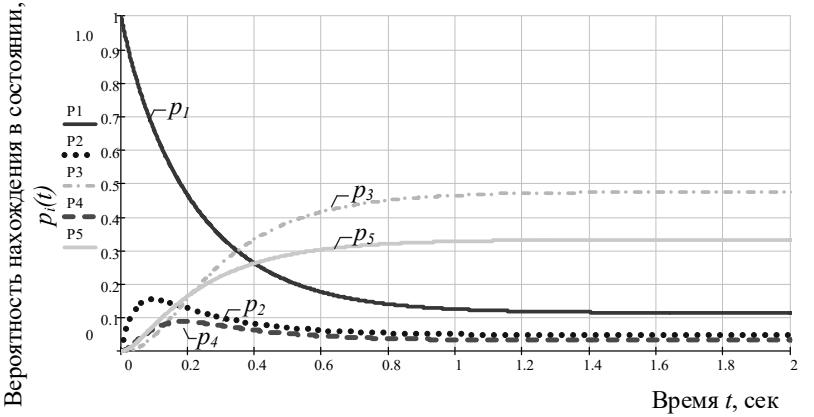

Рис. 3. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий для ситуации C_2

На рисунке 4 представлены результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий, соответствующие ситуации C_3, когда воздействия средств СР на КС ВС отсутствуют, а для динамического распределения СФХ сетевых устройств КС ВС задействован *DHCP*-сервер, постепенно уменьшающий временные интервалы, через которые осуществляется изменение СФХ до исчерпания ресурса КС ВС на реконфигурацию и последующей ее перегрузки. Данные зависимости позволяют определить пороговое значение интервала времени, через которое возможна последующая реконфигурация СФХ сетевых устройств без перегрузки системы, выполняющей свою целевую функцию, в условиях, когда воздействия средств СР отсутствуют. Финальные вероятности для ситуации C_3, для соответствующих значений интенсивностей потоков событий имеют следующие значения $p_1 = 1{,}429 \cdot 10^{-3}$, $p_2 = 2{,}02 \cdot 10^{-3}$, $p_3 = 0$, $p_4 = 0{,}997$, $p_5 = 0$.

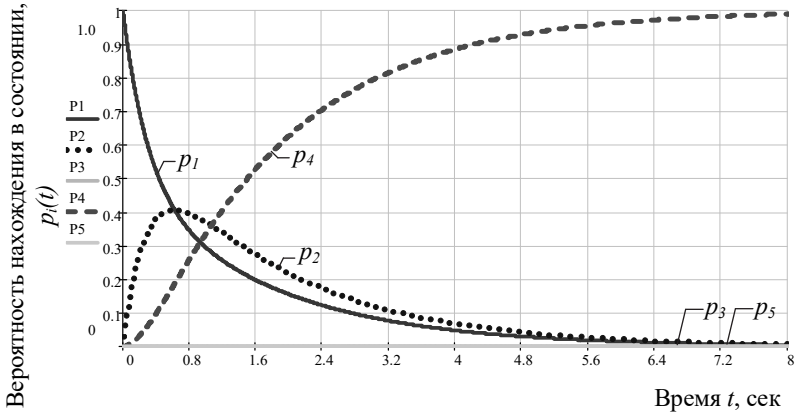

Рис. 4. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий для ситуации C_3

На рисунках 5 и 6 представлены графики зависимостей вероятностей пребывания моделируемой системы в различных состояниях от времени для ситуации C_3 при внештатном увеличении интенсивности изменения СФХ КС ВС *DHCP*-сервером в 3 и в 6 раз соответственно, по сравнению с пороговым значением.

В ситуации C_3 состояние S_3 трактуется как состояние перегрузки системы и наступления отказа в обслуживании. Пороговое значение интенсивности – это такая интенсивность изменения СФХ КС ВС *DHCP*-сервером, при которой КС ВС не сможет выполнять свою целевую функцию и будет перегружена. Сетевые устройства не могут завершить теку-

щий цикл получения распределенных им СФХ, установления сетевых соединений и передачи сообщений, до наступления очередного цикла изменения СФХ. Финальные вероятности для ситуации C_3 при внештатном увеличении интенсивности λ_{21} в 3 раза для соответствующих значений интенсивностей потоков событий имеют следующие значения $p_1 = 0{,}145$, $p_2 = 0{,}078$, $p_3 = 0$, $p_4 = 0{,}777$, $p_5 = 0$ (рис. 5).

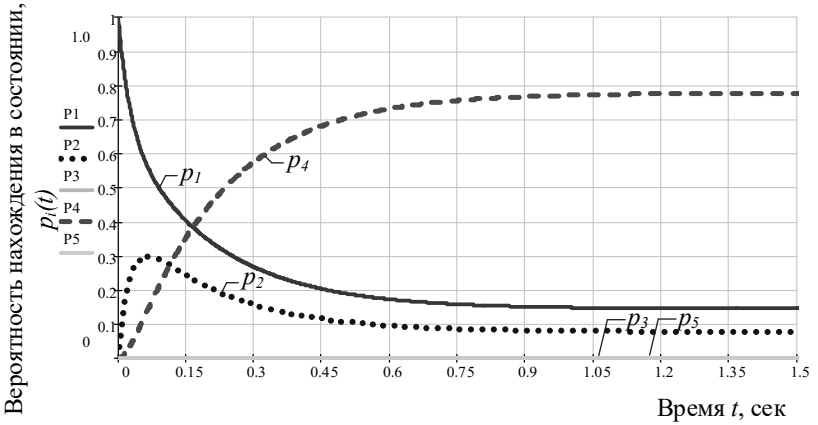

Рис. 5. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий для ситуации C_3 при внештатном увеличении интенсивности λ_{21} в 3 раза

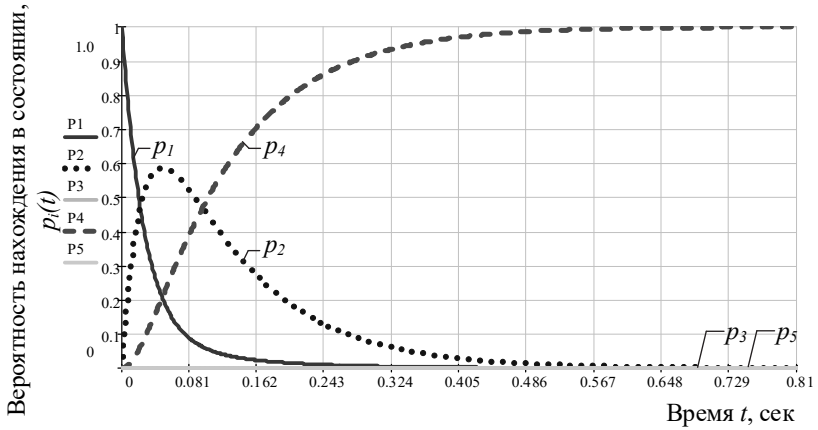

Рис. 6. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий для ситуации C_3 при внештатном увеличении интенсивности λ_{21} в 6 раз

Финальные вероятности для ситуации C_3 при внештатном увеличении интенсивности изменения СФХ КС ВС *DHCP*-сервером в 6 раз имеют следующие значения $p_1 = 0$, $p_2 = 0$, $p_3 = 0$, $p_4 = 1$, $p_5 = 0$ и представлены на рисунке 6.

Научная новизна модели заключается в применении математического аппарата теории марковских случайных процессов и решении уравнений Колмогорова для обоснования выбора режимов динамического конфигурирования структурно-функциональных характеристик клиент-серверной вычислительной сети.

Практическая значимость заключается в нахождении вероятностных и временных характеристик, описывающих состояния процесса функционирования клиент-серверной вычислительной сети при различных условиях динамического конфигурирования структурно-функциональных характеристик.

5. Алгоритм динамического конфигурирования клиент-серверных вычислительных сетей. Назначением разработанного алгоритма является динамическая конфигурация СФХ сетевых устройств КС ВС, обеспечивающая повышение результативности и снижение ресурсоемкости защиты за счет изменения значений *IP*-адресов клиентов в зависимости от условий функционирования КС ВС и действий злоумышленника в рамках задаваемого перечня подсетей без разрыва активных соединений.

Наиболее близким аналогом по своей технической сущности к представленному научно-методическому аппарату является [14], где обеспечивается повышение защищенности вычислительных сетей от несанкционированных воздействий за счет постоянного изменения *IP*-адресов в рамках одной подсети через равные, предварительно заданные интервалы времени. Это может привести к возможности вскрытия злоумышленником алгоритма изменения значений *IP*-адресов узлов защищаемой вычислительной сети и принятию им мер по обходу системы защиты.

Недостатками известных алгоритмов являются:

– относительно низкая результативность защиты КС ВС, обусловленная возможностью ложного срабатывания системы защиты и перегрузкой КС ВС [24];

– высокая ресурсоемкость защиты, обусловленная необходимостью применения дополнительного специального программного обеспечения, расходующего ресурсы сети на преобразование исходящих пакетов в свой собственный протокол, а также изменением *IP*-адресов сетевых устройств защищаемой КС ВС через фиксированные промежутки времени вне зависимости от условий функционирования и действий средств СР злоумышленника [25-29];

– относительно узкая область применения, обусловленная разрывом всех активных соединений между сетевыми устройствами при изменении СФХ КС ВС в случае обнаружения воздействия средств СР, а также изменением *IP*-адресов клиентов защищаемой вычислительной сети в рамках только одной подсети [30, 31].

Физическая (содержательная) постановка задачи. Стационарность значений СФХ сетевых устройств КС ВС, распределенных в большинстве случаев на все время функционирования КС ВС [32], позволяет злоумышленнику бескомпроматно вскрывать их средствами СР в реальном масштабе времени и в последующем успешно подвергать воздействию КА [33-36]. К тому же блокирование запросов СР штатными средствами защиты приводит к компрометации средств защиты и вынуждает злоумышленника менять пути их обхода и/или стратегию воздействия. В связи с этим для уменьшения времени актуальности и снижения достоверности добытых СР данных необходимо динамическое конфигурирование изначально стационарных СФХ сетевых устройств КС ВС с продолжительностью цикла их конфигурирования меньшей, чем продолжительность цикла добывания данных средствами СР, что заставит злоумышленника для компенсации мер защиты увеличивать интенсивность применения средств СР и в итоге приведет уже к его компрометации.

Конфигурирование СФХ *DHCP*-сервером осуществляют через интервалы времени, изменяемые адаптивно в зависимости от условий функционирования и действий злоумышленника. Другой особенностью алгоритма является то, что конфигурирование СФХ сетевых устройств КС ВС в рамках одной подсети, состоящей из относительно большого количества *IP*-адресов, накладывает ограничение на используемый диапазон их перестройки, к тому же при внештатном изменении СФХ недопустим разрыв критически важных активных соединений, например по протоколам *FTP, HTTPS, POP3, SMTP, VoIP, H.323*, между сетевыми устройствами КС ВС. В связи с этим в разработанном алгоритме для предотвращения реализации злоумышленником мер по обходу системы защиты изменение *IP*-адресов производят в рамках задаваемого диапазона подсетей без разрыва критически важных активных соединений.

Ограничения и допущения. Информация о легитимности и нелегитимности клиентов КС ВС, устанавливающих соединения, считается достоверной за счет применения комплекса средств защиты. Исходя из определения понятия легитимный, то есть соответствующий закону, под легитимностью клиента понимается его законное право находиться в составе КС ВС, установленное политикой безопасности сети, требова-

ниями и рекомендациями по обеспечению безопасности информации в КС ВС. Проверка на легитимность клиента должна производиться перед установлением соединений в КС ВС. Для получения численных оценок процесса защиты от средств СР используется разработанная модель функционирования КС ВС. Конфигурация СФХ КС ВС заключается в управлении формируемыми и распределяемыми *DHCP*-сервером значениями параметров сетевых устройств КС ВС, таких как *IP*-адреса, время продолжительности их аренды, *IP*-адрес *DHCP*-сервера, номер подсети.

Показатели и критерии. Показателем эффективности динамической конфигурации СФХ КС ВС является максимизация вероятности доступности информации клиентами КС ВС в связи со сменой СФХ $P_{AC}(t) \to \max$:

$$< MIP, Z > \to \max P_{AC} = \lim_{t \to \infty} P_{AC}(t) \mid P_{AC} \in \{P_i\},\ i = 1, 2, \ldots, h. \qquad (4)$$

Теоретическая основа алгоритма – теории систем управления, вероятности, массового обслуживания, исследования операций.

Блок-схема алгоритма динамического конфигурирования КС ВС, представленная на рисунке 7, включает следующие этапы:

1. Задают основные исходные данные, обозначение и описание которых приведены в таблице 3.

2. Подключают сетевые устройства к подсети.

3. Задают сетевым устройствам *IP*-адреса, время продолжительности их аренды $t^d_{\max}$, номер d сети *DHCP*-сервера и *IP*-адрес IP^d_{dhcp} выбранного *DHCP*-сервера, временные параметры синхронизации времени.

4. Устанавливают соединения между сетевыми устройствами.

5. Назначают установленным соединениям CIP_m.

6. Принимают из канала связи пакет сообщения.

7. Выделяют CIP_m из заголовка принятого пакета и сравнивают их с идентификаторами санкционированных информационных потоков *TS*.

8. В случае их совпадения передают пакет сообщений получателю и принимают из канала связи следующий пакет сообщения.

9. В ином случае сравнивают *IP*-адрес получателя с *FIP*.

10. В случае их несовпадения игнорируют пакет сообщений.

11. В ином случае сравнивают *IP*-адрес отправителя пакетов сообщений с каждым *IP*-адресом из множества IP^d.

12. В случае их совпадения блокируют *IP*-адрес отправителя и тем самым изолируют злоумышленника от дальнейшего информационного обмена в подсети при последующем изменении *IP*-адресов сетевых устройств.

Таблица 3. Обозначение и описание основных исходных данных

Переменная	Описание
D	Массив памяти (байт) для хранения номера подсети *DHCP*-сервера, где $D = [1, 2, \ldots, z]$, а z – максимальное количество номеров подсетей
$t^d_{\max}$	Максимальное значение времени аренды всех *IP*-адресов подсети с номером d, где d – номер подсети *DHCP*-сервера, $d = 1, 2 \ldots z$
CIP_m	Идентификатор соединения между сетевыми устройствами
C_i	Массив памяти (байт) для хранения идентификаторов соединения между сетевыми устройствами CIP_m, который содержит в себе *IP*-адрес отправителя – c, и получателя – b, тип протокола взаимодействия, порты взаимодействия, где m – максимальное допустимое количество соединений между сетевыми устройствами
CC	Массив памяти (байт) для хранения идентификаторов критически важных соединений между сетевыми устройствами, которые не подлежат разрыву, где $CC = [CIP^c_1, CIP^c_2 \ldots CIP^c_m]$, а CIP^c_m – идентификатор критических соединений между сетевыми устройствами
N_A	Массив памяти (байт) для хранения матрицы соответствия n-му *IP*-адресу сетевого устройства l-го *MAC*-адреса, где l – максимальное количество сетевых устройств в подсети, а n – максимальное допустимое значение количества *IP*-адресов сетевых устройств в подсети
d	Подмножество во множестве *IP*-адресов сетевых устройств подсети $IP^d = \{IP^d_1, IP^d_2 \ldots IP^d_n\}$
IP^d_{dhcp}	*IP*-адреса доверенных *DHCP*-серверов, где IP^d_{dhcp} – *IP*-адрес *DHCP*-сервера для подмножества d, $IP^d_{dhcp} \in IP^d$, чем обеспечивают невозможность использования ложного *DHCP*-сервера злоумышленником
FIP	Множество предварительно заданных ложных *IP*-адресов клиентов
C	Множество всех возможных соединений между сетевыми устройствами, $C = \{CIP_1, CIP_2 \ldots CIP_m\}$
A_m	Маркер активности соединения
TS	Множество идентификаторов санкционированных информационных потоков, $TS \geq 1$
FIP^d	Множество *IP*-адресов ложных клиентов вычислительной сети d, $FIP^d = \{FIP^d_1, FIP^d_2 \ldots FIP^d_n\}$, где n – максимальное допустимое количество *IP*-адресов сетевых устройств ВС

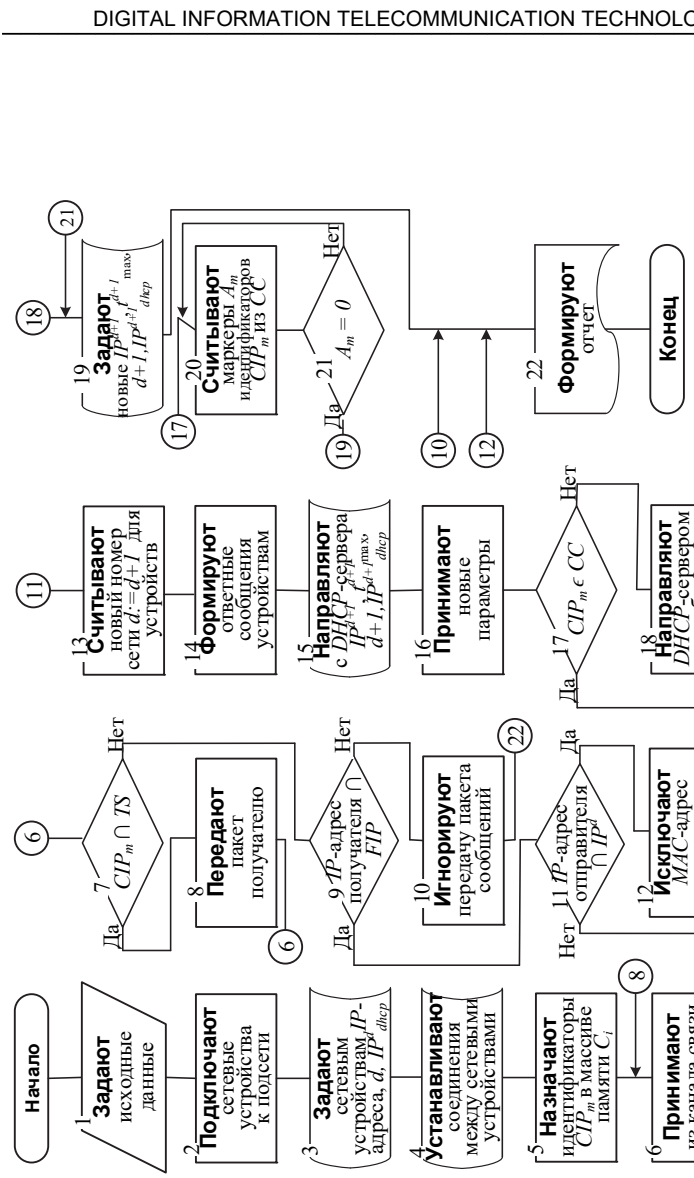

Рис. 7. Блок-схема последовательности действий, реализующих алгоритм динамического конфигурирования КС ВС

13. В ином случае изменяют СФХ сетевых устройств. Для этого считывают *DHCP*-сервером очередной номер подсети путем увеличения текущего номера сети d на единицу.

14. Формируют *DHCP*-сервером ответные сообщения каждому сетевому устройству.

15. Направляют сообщения с новыми сетевыми параметрами для каждого из сетевых устройств.

16. Принимают сообщения каждым из сетевых устройств.

17. Сравнивают, принадлежит ли идентификатор соединения между сетевыми устройствами множеству идентификаторов критических соединений.

18. В случае, если $CIP_m \notin CC$, направляют с *DHCP*-сервера сообщение сетевым устройствам, содержащее значение $t^d_{\max} = 0$ (прекращение аренды действующего *IP*-адреса).

19. Задают каждому сетевому устройству принятые новые параметры сетевой конфигурации.

20. В случае, если $CIP_m \in CC$ (прерываемые соединения является критическими), считывают маркеры активности соединений идентификаторов из множества *CC*.

21. В случае, если критическое соединение не активно ($A_m = 0$), то сетевым устройствам задают новые сетевые параметры. В ином случае ($A_m \neq 0$) вновь считывают маркеры активности соединений до тех пор, пока критическое соединение станет не активным.

22. Формируют отчет.

Для минимизации возможностей злоумышленника по реконструкции СФХ КС ВС в разработанном алгоритме в качестве функции выбора значения номера подсети *DHCP*-сервера используют последовательность чисел Фибоначчи, значение времени продолжительности аренды *IP*-адресов сетевых устройств *DHCP*-сервер выбирают случайным образом в пределах от 700 до 2592000 секунд, очередной номер подсети *DHCP*-сервера d вычисляют как $d = d+1$, а в качестве функции выбора значений *IP*-адресов сетевых устройств используют последовательность чисел Люка.

Для оценки вероятности вскрытия структуры КС ВС средствами СР в разработанном алгоритме используется модель функционирования клиент-серверной ВС в условиях ведения СР злоумышленником. При этом интенсивность потоков события λ_{25} интерпретируется как интенсивность заявок на оценку перегрузки КС ВС. Для этого рассмотрены следующие две ситуации.

Ситуация C_4. Средства СР обнаружены штатными средствами защиты КС ВС, поток заявок на обнаружение и оценку результативности обнаружения средств СР злоумышленника постоянный. Для упре-

ждения злоумышленника по вскрытию СФХ КС ВС сразу после компрометации средств СР *DHCP*-сервером увеличивается интенсивность потока заявок на внештатное изменение СФХ КС ВС. Финальные вероятности для ситуации C_4 имеют следующие значения: $p_1 = 0.353$, $p_2 = 0.294$, $p_3 = 0$, $p_4 = 0.059$, $p_5 = 0.294$ (рис. 8).

Из рисунка 8 видно, что для предотвращения вскрытия СФХ КС ВС средствами СР необходимо увеличение интенсивности заявок на внештатное изменение СФХ КС ВС *DHCP*-сервером таким образом, чтобы цикл динамической конфигурации СФХ заканчивался ранее цикла их вскрытия средствами СР злоумышленника.

Ситуация C_5. КС ВС функционирует в условиях ведения СР злоумышленником. Средства СР не обнаружены штатными средствами защиты КС ВС, поток заявок на обнаружение и оценку результативности обнаружения средств СР злоумышленника постоянный. Для предупреждения воздействия средств СР по вскрытию СФХ КС ВС, *DHCP*-сервером осуществляется периодическое внештатное изменение СФХ КС ВС.

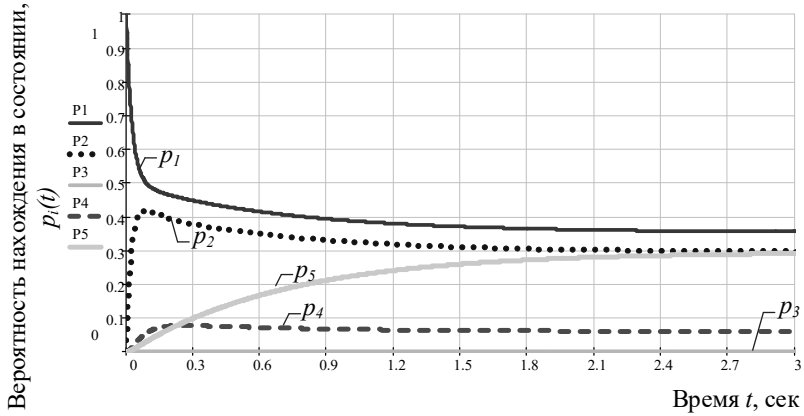

Рис. 8. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий для ситуации C_4

На интервале времени [0; 7] на рисунке 9 КС ВС находится в переходном режиме функционирования, где наблюдается всплеск значений вероятности состояния $p_2(t)$ и $p_5(t)$, а также незначительный всплеск значения вероятности состояния $p_4(t)$, что соответствует нахождению моделируемой системы в состоянии внештатного изменения СФХ КС ВС с интенсивностью потока заявок, обеспечивающей дискриминацию воздействий средств СР.

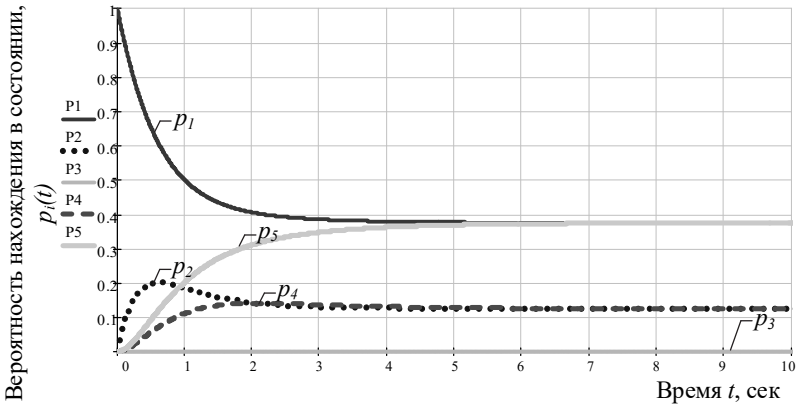

Рис. 9. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий для ситуации C_5, с низкой интенсивностью внештатного изменения СФХ КС ВС *DHCP*-сервером

Из рисунка 9 видно, что периодическое внештатное изменение с низкой интенсивностью СФ Х КС ВС *DHCP*-сервером в целях усложнения процедуры реконструкции злоумышленником алгоритма перестройки *IP*-адресов и других СФХ элементов КС ВС поможет скрыть состав, структуру и алгоритмы функционирования КС ВС от СР и переведет КС ВС в заранее заданную конфигурацию при реализации злоумышленником КА. Финальные вероятности для ситуации C_5 имеют следующие значения: $p_1 = 0.375$, $p_2 = 0.125$, $p_3 = 0$, $p_4 = 0.125$, $p_5 = 0.375$.

6. Результаты исследований. Результативность разработанного алгоритма была проверена путем его программной реализации и проведения натурного эксперимента в среде виртуализации *EVE-NG* с использованием операционных систем *Linux Kali* и *Linux Debian*.

Схема моделируемой КС ВС представлена на рисунке 10 и включает в себя две рабочие станции *Workstation* 1, 2, *DHCP*-сервер, средство СР – *Intruder* и коммутатор.

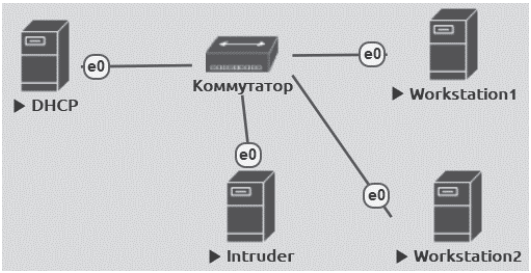

Рис. 10. Схема КС ВС

В ходе первого этапа эксперимента исследована возможность обнаружения злоумышленником изначально заданных *IP*-адресов сетевых устройств КС ВС: *DHCP*-сервера с *IP*-адресом 10.10.0.1/32 (рис. 11) и заданных им *IP*-адресов рабочих станций *Workstation* 1 и 2, имеющих значения 10.10.0.3/32 и 10.10.0.2/32 соответственно (рис. 12).

Рис. 11. Параметры *DHCP*-сервера

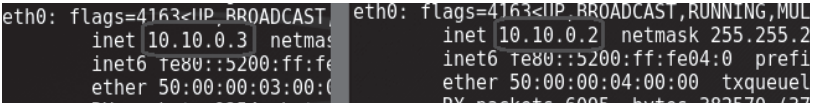

Рис. 12. Сетевые параметры рабочих станций

Для обнаружения активных *IP*-адресов в сети злоумышленником применялся сетевой сканер *NMAP* с использованием официального графического интерфейса *Zenmap*, отображающего следующую группу параметров, которая представлена на рисунке 13: «*Target*» – цель сканирования; «*Host*» – найденные устройства в сети; «*Nmap output*» – отчет и уязвимости найденных устройств в сети.

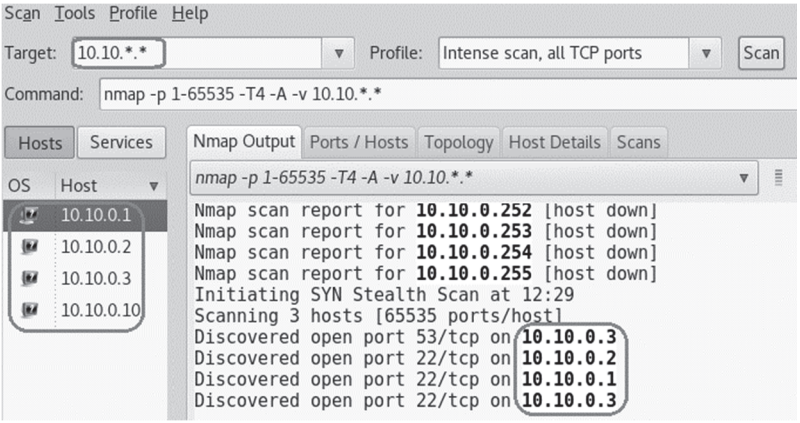

Рис. 13. Сканирование КС ВС злоумышленником

Поиск сетевых устройств осуществлялся в сети 10.10.*.*. Для идентификации узлов сети (*host detection*) злоумышленником с применением сканера *Nmap* направлялись запросы *ECHO_REQUEST* с использованием протокола *ICMP*. Применение режима *Decoy* в сканере

Nmap при каждом его запросе позволило злоумышленнику сфальсифицировать свой истинный *IP*-адрес (адрес источника). Такой набор средств сканирования достаточно эффективен и для противодействия ему необходимо применить средства анализа трафика или систем обнаружения атак.

По результатам проведенного сетевого сканирования средством *NMAP* был построен графический рисунок с изображением топологии сети и *IP*-адресами сетевых устройств КС ВС (рис. 14), а также сформирован отчет, отображающий открытые сетевые порты рабочих станций КС ВС, которые в дальнейшем могут использоваться злоумышленником в целях проведения КА (рис. 13).

В ходе второго этапа эксперимента в качестве средства защиты был применен *DHCP*-сервер, реализующий функцию динамического конфигурирования СФХ КС ВС. *DHCP*-сервером осуществлялась фиксация запросов *ECHO_REQUEST* и сравнение *IP*-адреса отправителя этих запросов с *IP*-адресами, хранящимися во множестве предварительно заданных ложных *IP*-адресов, обращение к которым исключено для легитимных клиентов КС ВС и свидетельствует о факте воздействия средств СР. В случае их совпадения *DHCP*-сервер осуществлял реконфигурацию значений ранее распределенных СФХ рабочих станций КС ВС (рис. 15), а именно значений *IP*-адресов, времени их аренды и номера подсети рабочих станций (рис. 16 и 17).

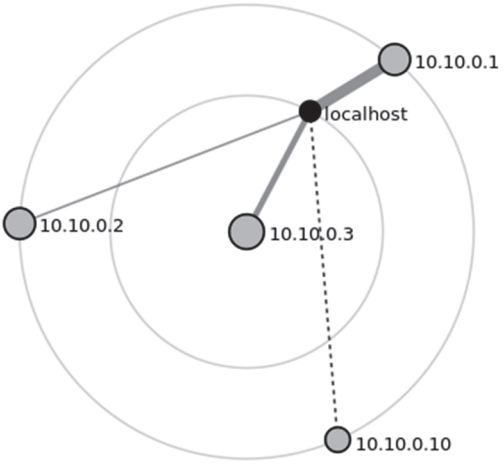

Рис. 14. Результат работы сканера *Nmap*

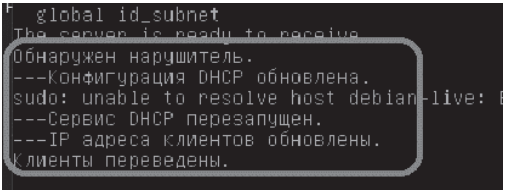

Рис. 15. Работа *DHCP*-сервера

Рис. 16. Новые сетевые параметры *DHCP*-сервера

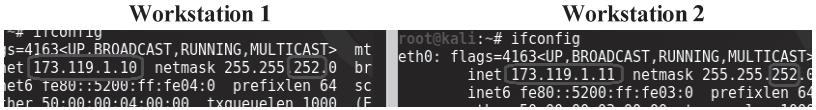

Рис. 17. Новые сетевые параметры рабочих станций

Представленная на рисунке 18 экранная форма наглядно демонстрирует, что после реконфигурации сетевых параметров рабочих станций КС ВС злоумышленник не может идентифицировать их значения. Таким образом, у него возникает необходимость повторного подбора параметров сканирования КС ВС либо расширения области сканирования, что в обоих случаях значительно увеличивает затрачиваемый им вычислительный и временной ресурс.

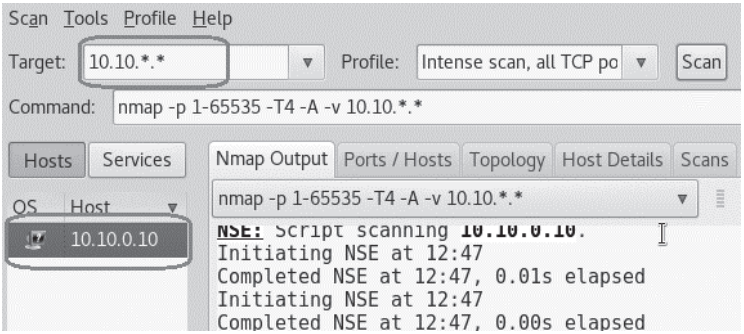

Рис. 18. Повторное сканирование КС ВС злоумышленником

7. Заключение. Расширение возможностей и повышение результативности сетевой разведки обусловлены стационарностью структурно-функциональных характеристик клиент-серверных вычис-

лительных сетей. В этой связи актуальной является задача динамического управления структурно-функциональными характеристиками клиент-серверных вычислительных сетей, функционирующих в условиях сетевой разведки.

Процесс функционирования клиент-серверной вычислительной сети в условиях динамического конфигурирования ее структурно-функциональных характеристик представлен как марковский случайный процесс с дискретными состояниями и непрерывным временем, что позволило находить оптимальные режимы для различных ситуаций.

Получены вероятностные и временные показатели, описывающие функционирование клиент-серверной вычислительной сети при различных ситуациях динамического управления ее структурно-функциональными характеристиками. Показано, что если длительность цикла динамического конфигурирования будет меньше длительности цикла сетевой разведки, то вскрытие состава и структуры сети будет сорвано, а получаемая сетевой разведкой информация не будет достоверной.

Новизна полученных результатов заключается в применении математического аппарата теории марковских случайных процессов и решении уравнений Колмогорова для обоснования выбора режимов динамического конфигурирования структурно-функциональных характеристик клиент-серверных вычислительных сетей.

Разработанные алгоритм и технические решения практически испытаны – достигнуто поддержание критически важных соединений, а интервалы времени изменения структурно-функциональных характеристик адаптивны к условиям функционирования и действиям злоумышленника.

Литература

1. *Jajodia S. et al.* Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats // Springer. 2011. 184 p.
2. *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.
3. RFC 2131. Dynamic Host Configuration Protocol. 1997. URL: https://tools.ietf.org/html/rfc2131 (дата обращения: 04.04.2020).
4. RFC 826. An Ethernet Address Resolution Protocol. 1982. URL: https://tools.ietf.org/html/rfc826 (дата обращения: 05.04.2020).
5. *Sokolovsky S.P., Telenga A.P., Voronchikhin I.S.* Moving target defense for securing Distributed Information Systems // Информатика: проблемы, методология, технологии: Сб. материалов XIX междунар. научн.-методич. конф. 2019. С. 639–643.
6. *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.
7. *Eskridge T.C. et al.* Integrated decision engine for evolving defenses // Patent US 20180309794A1, pub. 25.10.2018.

8. *Котенко И.В., Саенко И.Б., Коцыняк М.А., Лаута О.С.* Оценка киберустойчивости компьютерных сетей на основе моделирования кибератак методом преобразования стохастических сетей // Труды СПИИРАН. 2017. Вып. 6(55). С. 160–184.
9. *Jafarian J.H., Al-Shaer E., Duan Q.* Spatio-temporal address mutation for proactive cyber agility against sophisticated attackers // Proceedings of the First ACM Workshop on Moving Target Defense. 2014. pp. 69–78.
10. *MacFarland D.C., Shue C.A.* The SDN shuffle: creating a moving-target defense using host-based software-defined networking // Proceedings of the Second ACM Workshop on Moving Target Defense. 2015. pp. 37–41.
11. Cyber Maneuvering and Morphing. 2012. URL: https://defense-update.com/20120721_raytheon-to-develop-cyber-maneuver-technology-for-us-army.html (дата обращения: 31.04.2020).
12. What is Moving Target Defense. 2017. URL: https://www.cryptomove.com/what-is-mtd.html (дата обращения: 31.04.2020).
13. *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.
14. *Antonatos S., Akritidis P., Markatos E., Anagnostakis K.* Defending against Hitlist Worms using Network Address Space Randomization // 2005 ACM Workshop on Rapid Malcode. 2005. pp. 30–40.
15. *Cai G., Wang B., Wang X., Yuan Y., Li S.* An introduction to network address shuffling // 2016 18th International Conference on Advanced Communication Technology (ICACT). 2016. pp. 185–190.
16. *Luo Y.B. et al.* RPAH: Random Port and Address Hopping for Thwarting Internal and External Adversaries // Trustcom/BigDataSE/ISPA. 2015. pp. 263–270.
17. *Green M., MacFarland D.C., Smestad D.R., Shue C.A.* Characterizing network-based moving target defenses // ACM CCS Workshop on Moving Target Defense. 2015. pp. 31–35.
18. *Zhuang R., DeLoach S.A., Ou X.* Towards a theory of moving target defense // Proceedings of the First ACM Workshop on Moving Target Defense. 2014. pp. 31–40.
19. *Antonatos S., Anagnostakis K.G.* Tao: Protecting against hitlist worms using transparent address obfuscation // Communications and Multimedia Security. 2006. pp. 12–21.
20. *Wang A. et al.* Scotch: Elastically scaling up SDN control-plane using vs witch based overlay // ACM International on Conference on Emerging Networking Experiments and Technologies. 2014. pp. 403–414.
21. *Zhuang R., Bardas A.G., DeLoach S.A., Ou X.* A Theory of Cyber Attacks: A Step Towards Analyzing MTD Systems // Proceedings of the Second ACM Workshop on Moving Target Defense. 2015. pp. 11–20.
22. *Вентцель Е.С.* Исследование операций: задачи, принципы, методология. 2-е изд. // М.: Наука. 1988. 208 с.
23. *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.
24. *Zhao Z.Y., Guo Y.B., Liu W.* The Design and Research for Network Address Space Randomization in OpenFlow Network // Journal of Computer and Communications. 2015. № 3. pp. 203–211.
25. *Ganga G. et al.* Adaptor implementation for Internet Protocol address and port hopping // Patent US 20160036691A1. pub. 04.02.2016.
26. *Cruz A. et al.* Method for selection of unique next-time interval Internet Protocol address and port // Patent US 20150236752A1. pub. 20.08.2015.
27. *Fink R.A., Bubnis E.A., Keller T.E.* Method and apparatus for anonymous IP datagram exchange using dynamic network address translation // Patent US 20120117376A1. pub. 04.05.2012.
28. *Kravcov K.N.* Data transmission in networks with address space dynamic randomization // Selected Papers of the 17th International Conference on Data Analytics and Management in Data Intensive Domains. 2015. pp. 273–277.

29. *Котенко И.В., Саенко И.Б., Кушнеревич А.Г.* Архитектура системы параллельной обработки больших данных для мониторинга безопасности сетей интернета вещей // Труды СПИИРАН. 2018. Вып. 4(59). С. 5–30.
30. *Ellard D.J. et al.* Method for selection of unique next-time interval Internet Protocol address and port // Patent US 20150236752A1, pub. 20.08.2015.
31. *Котенко И.В., Саенко И.Б., Полубелова О.В.* Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Труды СПИИРАН. 2012. Вып.1 (20). С. 27–56.
32. *Maximov R.V., Krupenin A.V., Sharifullin S.R., Sokolovsky S.P.* Innovative development of tools and technologies to ensure the Russian information security and core protective guidelines // Вопросы кибербезопасности. 2019. № 1 (29). С. 10–17.
33. *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.
34. *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.
35. *Crouse M., Prosser B., Fulp E.W.* Probabilistic Performance Analysis of Moving Target and Deception Reconnaissance Defenses // Proceedings of the Second ACM Workshop on Moving Target Defense. 2015. pp. 21–29.
36. *Okhravi H. et al.* Creating a cybermoving target for critical infrastructure applications using platform diversity // International Journal of Critical Infrastructure Protection. 2015. № 5(1). pp. 30–39.

Максимов Роман Викторович — д-р техн. наук, профессор, специальная кафедра, 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. Число научных публикаций — 210. rvmaxim@yandex.ru; ул. Красина, 4, 350063, Краснодар, Россия; р.т.: +7(928)037-96-63.

Соколовский Сергей Петрович — канд. техн. наук, доцент, докторант, специальная кафедра, 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. Число научных публикаций — 200. mtd.krd@mail.ru; ул. Красина, 4, 350063, Краснодар, Россия; р.т.: +7(951)851-5408.

Ворончихин Иван Сергеевич — адъюнкт, специальная кафедра, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко. Область научных интересов: обеспечение информационной безопасности, системный анализ систем защиты информации критически важных объектов, рандомизация сетевого адресного пространства. Число научных публикаций — 22. 5.00@mail.ru; ул. Красина, 4, 350063, Краснодар, Россия; р.т.: +7 (996) 379-34-22.

DOI 10.15622/ia.2020.19.5.5

R. MAXIMOV, S. SOKOLOVSKY, I. VORONCHIKHIN

ALGORITHM AND TECHNICAL SOLUTIONS FOR DYNAMIC CONFIGURATION OF CLIENT-SERVER COMPUTING NETWORKS

Maximov R., Sokolovsky S., Voronchikhin I. **Algorithm and Technical Solutions for Dynamic Configuration of Client-Server Computing Networks.**

Abstract. The main factors that determine the expansion of capabilities and increase the effectiveness of network intelligence to identify the composition and structure of client-server computer networks due to the stationarity of their structural and functional characteristics are analyzed. The substantiation of an urgent problem of dynamic management of structurally-functional characteristics of the client-server computer networks functioning in the conditions of network reconnaissance is resulted on the grounds of the revealed protection features of client-server computer networks at the present stage that is based on realization of principles of spatial safety maintenance, and also formalization and introduction of forbidding regulations.

The mathematical model allowing to find optimum modes for dynamic configuration of structurally-functional characteristics of client-server computer networks for various situations is presented. Calculation results are given. An algorithm is presented that makes it possible to solve the problem of dynamic configuration of the structural and functional characteristics of a client-server computer network, which reduces the reliability time of data obtained by network intelligence. The results of practical tests of software developed on the basis of the dynamic configuration algorithm of client-server computer networks are shown. The obtained results show that the use of the presented solution for the dynamic configuration of client-server computer networks allows to increase the effectiveness of protection by changing the structural and functional characteristics of client-server computer networks within several subnets without breaking critical connections through time intervals that are adaptively changed depending on the functioning conditions and the attacker's actions.

The novelty of the developed model lies in the application of the mathematical apparatus of the Markov's theory of random processes and Kolmogorov's solution of equations to justify the choice of dynamic configuration modes for the structural and functional characteristics of client-server computer networks. The novelty of the developed algorithm is the use of a dynamic configuration model for the structural and functional characteristics of client-server computer networks for the dynamic control of the structural and functional characteristics of a client-server computer network in network intelligence.

Keywords: Network Intelligence, Client-server Computer Networks, Moving Target Technology, Computer Attack, Cybermaneuvering

Maximov Roman — Ph.D., Dr.Sci., Professor, Special 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. The number of publications — 210. rvmaxim@yandex.ru; 4, Krasina str., 350063, Krasnodar, Russia; office phone: +7(928)037-96-63.

Sokolovsky Sergey — Ph.D., Associate Professor, Doctoral Student, Special Department, Krasnodar Higher Military School named after General of the Army S.M. Shtemenko. Research interests: nformation security, synthesis and system analysis of information security systems of critical objects, masking and simulation of information resources of integrated departmental communication networks. The number of publications — 200. mtd.krd@mail.ru; 4, Krasina str., 350063, Krasnodar, Russia; office phone: +7(951)851-5408.

Voronchikhin Ivan — Ph.D. Student, Special Department, Krasnodar Higher Military School named after General of the Army S.M. Shtemenko. Research interests: information security, system analysis of information security systems of critical objects, network address space randomization. The number of publications — 22. 5.00@mail.ru; 4, Krasina str., 350063, Krasnodar, Russia; office phone: +7 (996) 379-34-22.

References

1. Jajodia S. et al. Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats. Springer. 2011. 184 p.
2. Voronchikhin I.S., Ivanov I.I., Maximov R.V., Sokolovsky S.P. [Masking the structure of distributed information systems in cyberspace]. *Voprosy kiberbezopasnosti – Cybersecurity issues*. 2019. vol. 6 (34). pp. 92–101. (In Russ).
3. RFC 2131. Dynamic Host Configuration Protocol. 1997. Available at: https://tools.ietf.org /html/rfc2131 (accessed: 04.04.2020).
4. RFC 826. An Ethernet Address Resolution Protocol. 1982. Available at: https://tools.ietf.org /html/rfc826 (accessed: 05.04.2020).
5. Sokolovsky S.P., Telenga A.P., Voronchikhin I.S. [Moving target defense for securing Distributed Information Systems] *Informatika: problemy, metodologija, tehnologii: Sb. materialov XIX mezhdunar. nauchn.-metodich. konf.* [Informatics: problems, methodology, technologies: collection of materials of the XIX international scientific and methodological conference]. 2019. pp. 639–643.
6. 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]. *Innovacii – Innovations*. 2018. vol. 3(233). pp. 28–35. (In Russ).
7. Eskridge T.C. et al. Integrated decision engine for evolving defenses. Patent US 20180309794A1, pub. 25.10.2018.
8. Kotenko I.V., Saenko I.B., Kozinak M.A., Louth O.S. [Estimation of cyber stability of computer networks based on simulation of cyber attacks using stochastic network transformation method]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2017. vol. 6(55). pp. 160–184. (In Russ).
9. Jafarian J.H., Al-Shaer E., Duan Q. Spatio-temporal address mutation for proactive cyber agility against sophisticated attackers. *Proceedings of the First ACM Workshop on Moving Target Defense.* 2014. pp. 69–78.
10. MacFarland D.C., Shue C.A. The SDN shuffle: creating a moving-target defense using host-based software-defined networking. Proceedings of the Second ACM Workshop on Moving Target Defense. 2015. pp. 37–41.
11. Cyber Maneuvering and Morphing. 2012. Available at: https://defense-update.com/20120721_raytheon-to-develop-cyber-maneuver-technology-for-us-army.html (accessed: 31.04.2020).
12. What is Moving Target Defense. 2017. Available at: https://www.cryptomove.com/what-is-mtd.html (accessed: 31.04.2020).
13. Maximov R.V., Sokolovsky S.P. Voronchikhin I.S. *Sposob zashchity vychislitel'nih setey* [Method of Protection of Computer Networks]. Patent Russia, no. 2716220, 06.03.2020. (In Russ.).
14. Antonatos S., Akritidis P., Markatos E., Anagnostakis K. Defending against Hitlist Worms using Network Address Space Randomization. 2005 ACM Workshop on Rapid Malcode. 2005. pp. 30–40.
15. Cai G., Wang B., Wang X., Yuan Y., Li S. An introduction to network address shuffling. 2016 18th International Conference on Advanced Communication Technology (ICACT). 2016. pp. 185–190.
16. Luo Y.B. et al. RPAH: Random Port and Address Hopping for Thwarting Internal and External Adversaries. Trustcom/BigDataSE/ISPA. 2015. pp. 263–270.
17. Green M., MacFarland D.C., Smestad D.R., Shue C.A. Characterizing network-based moving target defenses. ACM CCS Workshop on Moving Target Defense. 2015. pp. 31–35.

18. Zhuang R., DeLoach S.A., Ou X. Towards a theory of moving target defense. Proceedings of the First ACM Workshop on Moving Target Defense. 2014. pp. 31–40.
19. Antonatos S., Anagnostakis K.G. Tao: Protecting against hitlist worms using transparent address obfuscation. Communications and Multimedia Security. 2006. pp. 12–21.
20. Wang A. et al. Scotch: Elastically scaling up SDN control-plane using vs witch based overlay. ACM International on Conference on Emerging Networking Experiments and Technologies. 2014. pp. 403–414.
21. Zhuang R., Bardas A.G., DeLoach S.A., Ou X. A Theory of Cyber Attacks: A Step Towards Analyzing MTD Systems. Proceedings of the Second ACM Workshop on Moving Target Defense. 2015. pp. 11–20.
22. Ventcel' E.S. *Issledovanie operacij: zadachi, principy, metodologija* [Operations research: objectives, principles, and methodology]. M.: Nauka. 1988. 208 p. (In Russ).
23. Maximov R.V., Orehov D.N., Sokolovsky S.P. [Model and algorithm of functioning of the client-server information system in the conditions of network intelligence]. *Sistemy upravlenija, svjazi i bezopasnosti – Management, communication and security systems.* 2019. vol. 4. pp. 50–99. (In Russ).
24. *Zhao Z.Y., Guo Y.B., Liu W.* The Design and Research for Network Address Space Randomization in OpenFlow Network. *Journal of Computer and Communications*. 2015. vol. 3. pp. 203–211.
25. Ganga G. et al. Adaptor implementation for Internet Protocol address and port hopping. Patent US 20160036691A1. pub. 04.02.2016.
26. Cruz A. et al. Method for selection of unique next-time interval Internet Protocol address and port. Patent US 20150236752A1. pub. 20.08.2015.
27. Fink R.A., Bubnis E.A., Keller T.E. Method and apparatus for anonymous IP datagram exchange using dynamic network address translation. Patent US 20120117376A1. pub. 04.05.2012.
28. Kravcov K.N. Data transmission in networks with address space dynamic randomization. Selected Papers of the 17th International Conference on Data Analytics and Management in Data Intensive Domains. 2015. pp. 273–277.
29. Kotenko I.V., Saenko I.B., Kushnerevich A.G. [Architecture of a parallel big data processing system for monitoring the security of Internet of things networks]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2018. vol. 4(59). pp. 5–30. (In Russ).
30. Ellard D.J. et al. Method for selection of unique next-time interval Internet Protocol address and port. Patent US 20150236752A1, pub. 20.08.2015.
31. Kotenko I.V., Saenko I.B., Polubelova O.V. [Applying information and security event management technology to protect information in critical infrastructures]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2012. vol. 1(20). pp. 27–56. (In Russ).
32. Maximov R.V., Krupenin A.V., Sharifullin S.R., Sokolovsky S.P. [Innovative development of tools and technologies to ensure the Russian information security and core protective guidelines]. *Cybersecurity issues*. 2019. vol. 1(29). pp. 10–17.
33. Krupenin A.V., Sokolovsky S.P., Horev G.A., Kalach A.V. [Masking channel-level identifiers for proactive protection of integrated special-purpose communication networks]. *Vestnik Voronezhskogo instituta FSIN Rossii – Bulletin of the Voronezh Institute of the Federal penitentiary service of Russia.* 2018. vol. 3. pp. 81–89. (In Russ).
34. Sherstobitov R.S., Sharifullin S.R., Maksimov R.V. [Masking integrated communication networks for departmental purposes]. *Sistemy upravlenija, svjazi i bezopasnosti – Systems of Control, Communication and Security.* 2018. vol. 4. pp. 136–175. (In Russ).
35. Crouse M., Prosser B., Fulp E.W. Probabilistic Performance Analysis of Moving Target and Deception Reconnaissance Defenses. Proceedings of the Second ACM Workshop on Moving Target Defense. 2015. pp. 21–29.
36. Okhravi H. et al. Creating a cybermoving target for critical infrastructure applications using platform diversity. *International Journal of Critical Infrastructure Protection*. 2015. vol. 5(1). pp. 30–39.