УДК 004.772

Алгоритм конфигурирования многоадресных сетевых соединений в условиях компьютерной разведки

Москвин А. А.

***Постановка задачи**: не смотря на применяемые меры защиты информации, угрозы совершения компьютерных атак на вычислительные сети остаются актуальными. Одним из способов предотвращения данных угроз является сокрытие истинных IP-адресов сетевых узлов вычислительной сети посредством их динамического изменения. Однако, применение указанных мер снижает доступность сетевых узлов для легитимных пользователей, поскольку традиционно применяемые протоколы транспортного уровня TCP/UDP имеют известные ограничения, которые не гарантируют непрерывную и безопасную передачу данных. Эти ограничения снимаются посредством применения протокола транспортного уровня SCTP, способного содержать в рамках установленного соединения множество предварительно заданных IP-адресов. **Целью работы является** разработка алгоритма, позволяющего повысить доступность и защищенность сетевых узлов вычислительной сети при динамическом изменении ее IP-адресов посредством применения оптимальных параметров конфигурирования многоадресных сетевых соединений. **Используемые методы:** в работе использованы методы исследования случайных процессов, а также методы решения задач многокритериальной оптимизации. **Новизна**: элементами новизны представленного алгоритма является применение модели функционирования многоадресных сетевых соединений, основанной на математическом аппарате теории марковских процессов с дискретными состояниями и непрерывным временем, постановке и решении задачи многокритераильной оптимизации методом идеальной точки с использованием алгоритма Нелдера-Мида. **Результат**: проведенные расчеты свидетельствуют о повышении доступности и защищенности сетевых узлов в случае применения оптимальных параметров многоадресных сетевых соединений при динамическом изменении их IP-адресов. **Практическая значимость**: заключается в повышении защищенности сетевых узлов вычислительной сети за счет снижения возможности средств компьютерной разведки по выявлении истинных IP-адресов с одновременным повышением доступности сетевых узлов за счет применения оптимальных параметров конфигурации многоадресных сетевых соединений.*

***Ключевые слова:** компьютерная разведка, многоадресные сетевые соединения, многокритериальная оптимизация, повышение доступности и защищенности.*

Актуальность

Применяемые средства сетевой защиты, включая средства криптографической защиты информации, не позволяют в полной мере обеспечить требуемый уровень защищенности вычислительных сетей от реализации угроз безопасности информации (УБИ), определенных в «Банке данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю России (ФСТЭК России)», таких как «УБИ.034 Угроза использования

Библиографическая ссылка на статью:
Москвин А. А. Алгоритм конфигурирования многоадресных сетевых соединений в условиях компьютерной разведки // Системы управления, связи и безопасности. 2023. № 2. С. 102-130. DOI: 10.24412/2410-9916-2023-2-102-130

Reference for citation:
Moskvin A. A. Algorithm of multiaddress network connection configuration under conditions of computer intelligence. *Systems of Control, Communication and Security*, 2023, no. 2, pp. 102-130 (in Russian). DOI: 10.24412/2410-9916-2023-2-102-130

слабостей протоколов сетевого/локального обмена данными», «УБИ.140 Угроза приведения системы в состояние «отказ в обслуживании»», «УБИ.099 Угроза обнаружения хостов» и других угроз, направленных на идентификацию состава, структуры и алгоритмов функционирования вычислительных сетей.

Этому способствует в первую очередь статичность структурно-функциональных характеристик вычислительной сети (Internet Protocol (IP, «межсетевой протокол») адресов, Media Access Control (MAC, «управления доступом к среде») адресов, сетевых портов взаимодействия, доменных имен и т.п.) использование импортного оборудования, использование вычислительной сетью ресурсов сетей связи общего пользования, а также кризисом доверия к открытому программному обеспечению [1]. В качестве мер защиты, направленных на нивелирование вышеприведенных угроз, могут выступать меры, определенные Приказом ФСТЭК России от 25.12.2017 № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (в ред. Приказа ФСТЭК России от 26.03.2019 № 60): «Защита информационной системы (ЗИС).35 Управление сетевыми соединениями», «ЗИС.37 Перевод информационной системы в безопасное состояние», «ЗИС.8 Сокрытие архитектуры и конфигурации информационной системы».

Одной из перспективных концепций защиты вычислительных сетей, позволяющей скрывать ее истинные структурно-функциональные характеристики и формировать о ней ложное представление у злоумышленника, является концепция Moving Target Defense (MTD, «защита целей движением») [2-6].

Концепция MTD направлена на динамическое изменение компонентов вычислительных сетей в целях снижения эффективности ведения компьютерной разведки и реализации последующих деструктивных воздействий злоумышленником.

Концепция MTD подразумевает динамическое изменение параметров вычислительной сети, таких как используемые протоколы (включая протоколы маршрутизации), MAC-адреса, IP-адреса и сетевые порты, используемые для идентификации сетевых узлов, а также маршруты передачи трафика (информационные направления).

Однако, изменение структурно-функциональных характеристик вычислительной сети, в частности IP-адресов сетевых узлов, снижает их доступность не только для злоумышленников, но и для легитимных пользователей. Причиной этого являются ограничения применяемых протоколов транспортного уровня Transmission Control Protocol (TCP, «протокол управления передачей»), функциональные возможности которого описаны в Request for Comments (RFC, «заявка (запрос) на отзывы») 793, и User Datagram Protocol (UDP, «протокол пользовательских датаграмм»), RFC 768, не гарантирующих непрерывную и безопасную передачу данных при реконфигурации сетевого соединения.

Указанные ограничения снимают протоколы передачи данных, которые могут содержать в рамках установленного сетевого соединения множество предварительно заданных IP-адресов. Например, множественная адресация сетевого соединения поддерживается протоколом транспортного уровня Stream Control

№2. 2023
ISSN 2410-9916

Transmission Protocol (SCTP, «протокол передачи с управлением потоком»), RFC 4960.

В статье предложен алгоритм конфигурирования параметров многоадресных сетевых соединений, позволяющий повысить не только защищенность, но и доступность сетевых узлов вычислительной сети, поскольку в существующих способах [7-18] этого не предусмотрено.

При этом решена задача выбора оптимальных параметров многоадресных сетевых соединений, таких как количество предварительно заданных IP-адресов и времени их использования, при которых защищенность и доступность сетевых узлов вычислительной сети будет максимальной.

Анализ объекта исследования

Динамическое изменение IP-адресов сетевых узлов (СУ) вычислительной сети позволяет противостоять раскрытию злоумышленником факта передачи информации, места расположения СУ, режимов их работы, обеспечивая скрытность их функционирования, повышая тем самым их защищенность. Однако, при выполнении указанных мероприятий, доступность СУ снижается за счет применяемых протоколов передачи данных транспортного уровня.

Так, традиционно применяемый в качестве протокола передачи сообщений TCP, в рамках установленного сетевого соединения, использует только один IP-адрес, и в случае перевода вычислительной сети в безопасное состояние (рис. 1), будет происходить разрыв сетевых соединений, в том числе критически важных, что не гарантирует своевременность информационного обмена.

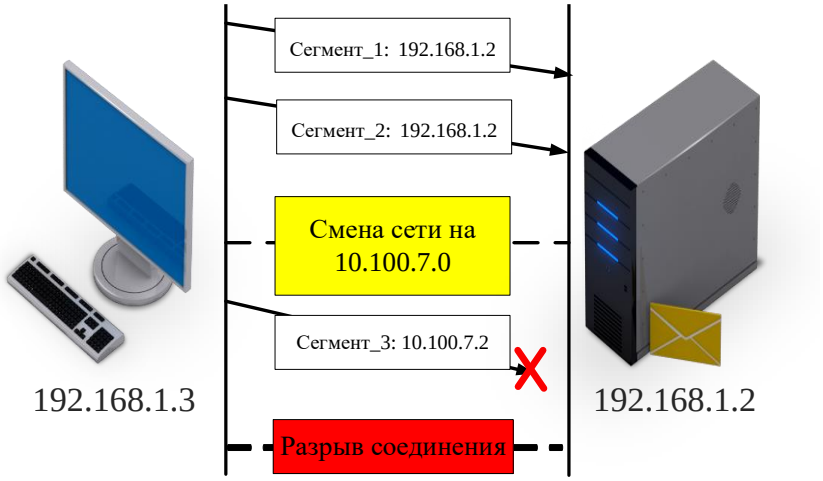


Рис. 1. Разрыв сетевого соединения TCP

Протокол передачи сообщений UDP является протоколом без подтверждения доставки датаграммы, что не гарантирует достоверную и безопасную передачу сообщений.

Протокол SCTP [19] обладает более широкими возможностями по обеспечению информационной безопасности, чем TCP и UDP, а его применение позволяет обеспечить непрерывность информационного обмена при смене IP-адресов

№2. 2023
ISSN 2410-9916

СУ вычислительной сети. Это возможно за счет многоадресности SCTP, которая позволяет осуществлять смену IP-адресов в рамках установленного сетевого соединения без из разрыва (рис. 2).

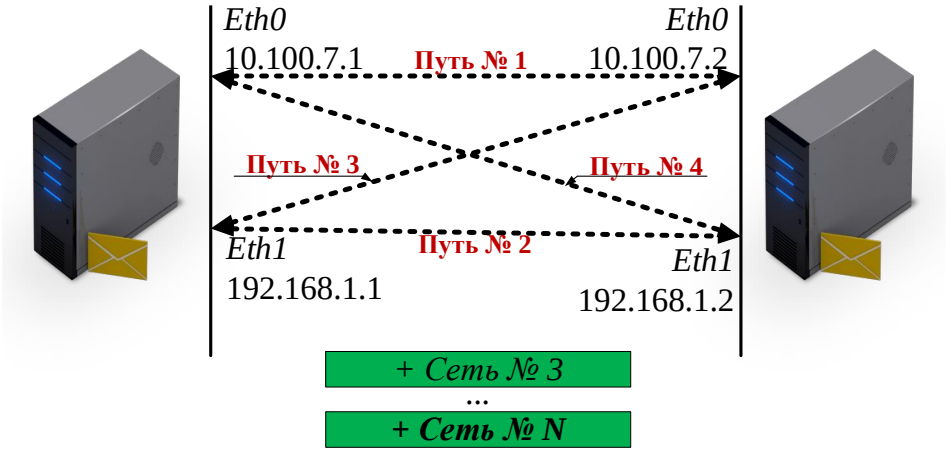


Рис. 2. Многоадресность SCTP

Еще одной особенностью данного протокола является его многопоточность (рис. 3), которая обеспечивает более надежную передачу данных. Это послужило причиной его применения в промышленной автоматизации, системах управления транспортном, электронной коммерции, системах видеонаблюдения и системах контроля и управления доступом.

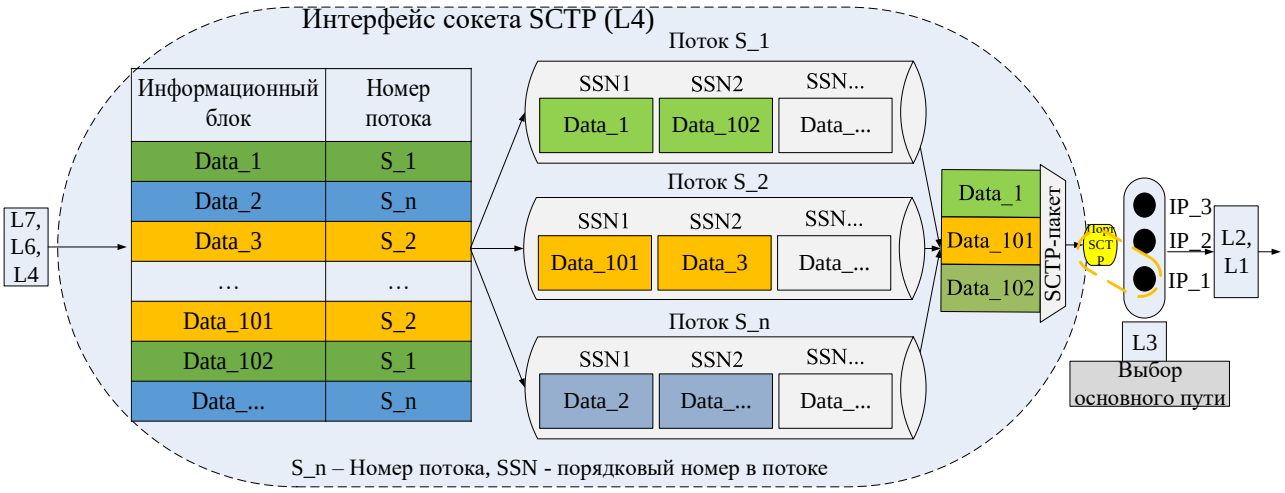


Рис. 3. Многопоточность SCTP

В рамках реализации концепции MTD, многопоточность SCTP позволит повысить защищенность сетей связи при маскировании ее структуры [20-27]. Так, основной проблемой указанных способов является избыточность маскирующего трафика, который при применении однопоточных протоколов передачи данных дает значительную нагрузку на вычислительную сеть, что не гарантирует своевременность информационного обмена.

DOI: 10.24412/2410-9916-2023-2-102-130
URL: https://sccs.intelgr.com/archive/2023-02/05-Moskvin.pdf

№2. 2023
ISSN 2410-9916

Стоит добавить, что SCTP обладает рядом преимуществ перед TCP/UDP за счет устранения следующих угроз информационной безопасности [28-34]:

1. Атаки на отказ в обслуживании (рис. 4). SCTP имеет механизм защиты от Denial of Service (DoS, «отказ в обслуживании») атак, который позволяет ограничить количество запросов, поступающих на сетевой узел и предотвратить перегрузку сети.

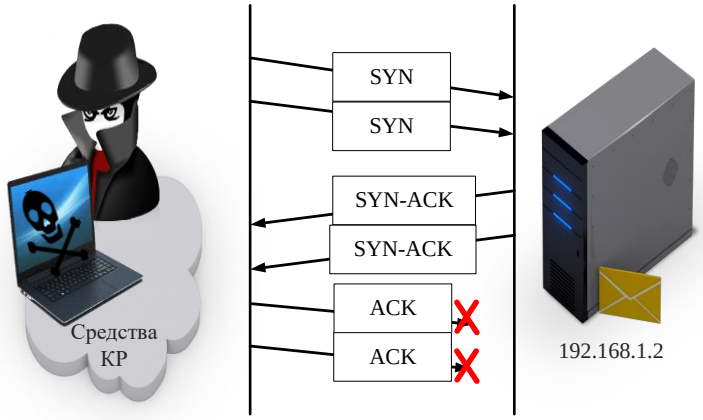


Рис. 4. Схема проведения атаки на отказ в обслуживании TCP

2. Атаки на подмену пакетов (spoofing, рис. 5) и атаки на перехват данных (sniffing). SCTP использует механизмы аутентификации и шифрования данных, что делает невозможным подмену пакетов в сети, а также позволяет защитить информацию от перехвата злоумышленниками.

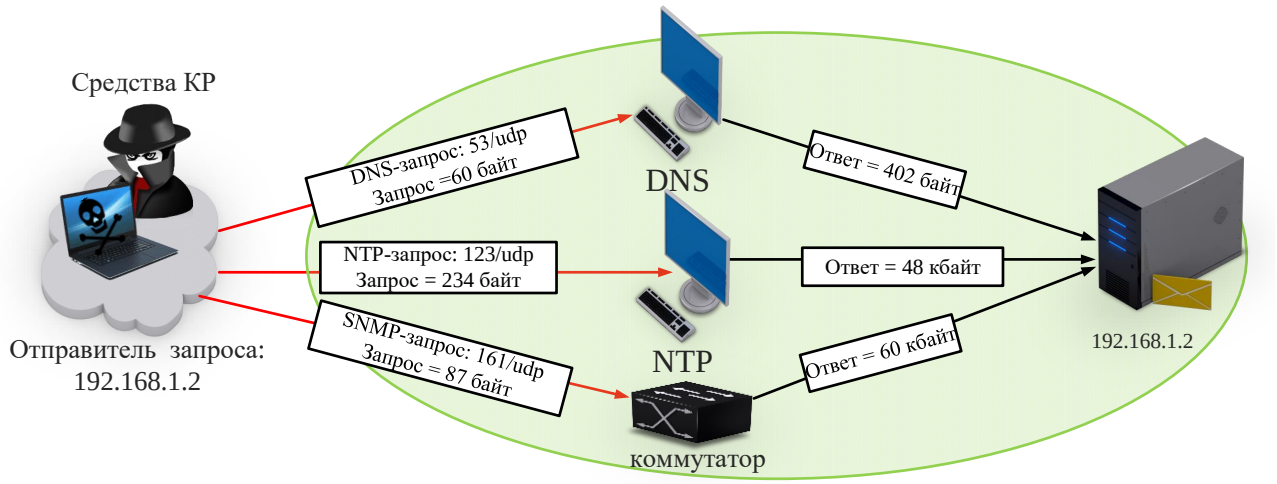


Рис. 5. Схема подмены отправителя UDP

3. Сетевая атака «блокировка головы очереди» (рис. 6) заключается в блокировке передачи данных на уровне транспортного протокола, путем занятия или задержки передачи первого пакета в очереди. SCTP имеет возможность использовать несколько потоков для передачи данных, что позволяет избежать атак подобного типа, т.е. потеря SCTP-пакета, содержащего информационные блоки одного потока, никак не повлияет на функционирование других потоков.

DOI: 10.24412/2410-9916-2023-2-102-130
URL: https://sccs.intelgr.com/archive/2023-02/05-Moskvin.pdf

№2. 2023
ISSN 2410-9916

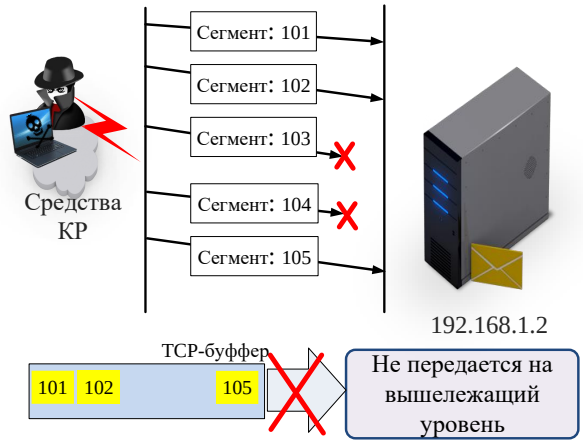


Рис. 6. Атака по типу «блокировка головы очереди» TCP

Используя функциональные возможности протоколов с множественной адресацией, возможно устранить некоторые недостатки известных способов защиты вычислительных сетей [35, 36], в основу которых положены алгоритмы динамического изменения IP-адресов.

Так, например, недостатком способа [35] является относительно низкая результативность защиты, поскольку реконфигурация сетевого соединения происходит для СУ, не имеющих критически важных сетевых соединений, и низкая доступность санкционированных СУ, поскольку при увеличении количества и интенсивности несанкционированных информационных потоков СУ вычислительной сети будут преимущественно находиться в режиме реконфигурации параметров сетевого соединения и будут недоступными для осуществления полезного информационного обмена.

А в способе [36] реконфигурация значений IP-адресов осуществляется в рамках одной подсети, что накладывает ограничение на используемый диапазон IP-адресов при их относительно большом количестве.

Алгоритм конфигурирования параметров многоадресных сетевых соединений

Предложенный алгоритм позволят повысить защищенность СУ вычислительных сетей за счет изменения IP-адресов в рамках нескольких подсетей без разрыва установленных между ними критически важных сетевых соединений, а также повысить доступность санкционированных СУ за счет смены IP-адресов в рамках предварительно задаваемого множества.

Реализация предлагаемого алгоритма конфигурирования параметров многоадресных соединений поясняется блок-схемой последовательности действий, представленной на рис. 7 и включает следующие этапы:

1. Задают исходные данные, обозначение и описание которых приведены в таблице 1.
2. Подключают СУ к сети.
3. Устанавливают многоадресное сетевое соединение между СУ.
4. Пока сетевое соединение активно:

4.1. Принимают из канала связи SCTP-пакет.
4.2. Проверяют на легитимность входящий SCTP-пакет.
4.3. В случае их совпадения, передают SCTP-пакет получателю и принимают из канала связи следующий SCTP-пакет.
4.4. В случае их несовпадения, проверяют количество неиспользованных IP-адресов (счетчик *I*).
4.5. Если *I* не равно 0, то задают очередной IP-адрес из множества доступных.
4.6. Уменьшают значение *I* на единицу и принимают из канала связи следующий SCTP-пакет.
4.7. Если *I* равно 0, то вычисляют оптимальное количество IP-адресов (параметр *K*) и время их аренды (параметр T_{max}).
4.8. Задают оптимальные параметры сетевого соединения каждому СУ, после чего принимают из канала связи следующий SCTP-пакет.
5. Формируют отчёт.

Таблица 1 – Обозначение и описание основных исходных данных

Параметры	Описание
h	Количество СУ
K	Количество предварительно заданных IP-адресов
T_{max}	Время аренды IP-адресов
T_{rec}	Время реконфигурации одного СУ
T_{scan}	Время сканирования одного СУ
I	Счетчик общего количества неиспользованных IP-адресов

Стоит отметить, что количество IP-адресов (параметр *K*) не может превышать 4095, поскольку в одном физическом соединении путем мультиплексирования могут быть организовано 4095 логических каналов, что определено стандартом 802.1Q.

Время аренды IP-адресов (T_{max}) зависит от интенсивности ведения компьютерной разведки и принимает средние значения, указанные в таблице 2, что было установлено экспериментальным путем при применении программы исследования сети и сканирования портов «Nmap» для вычислительной сети из 100 СУ.

Таблица 2 – Среднее время сканирования сетевых узлов

№ п/п	Режим сканирования	Время сканирования одного СУ, с
1	Quick scan	0,15
2	Ping scan	0,22
3	Intense scan	0,42
4	Intense scan, all tcp ports	37,8

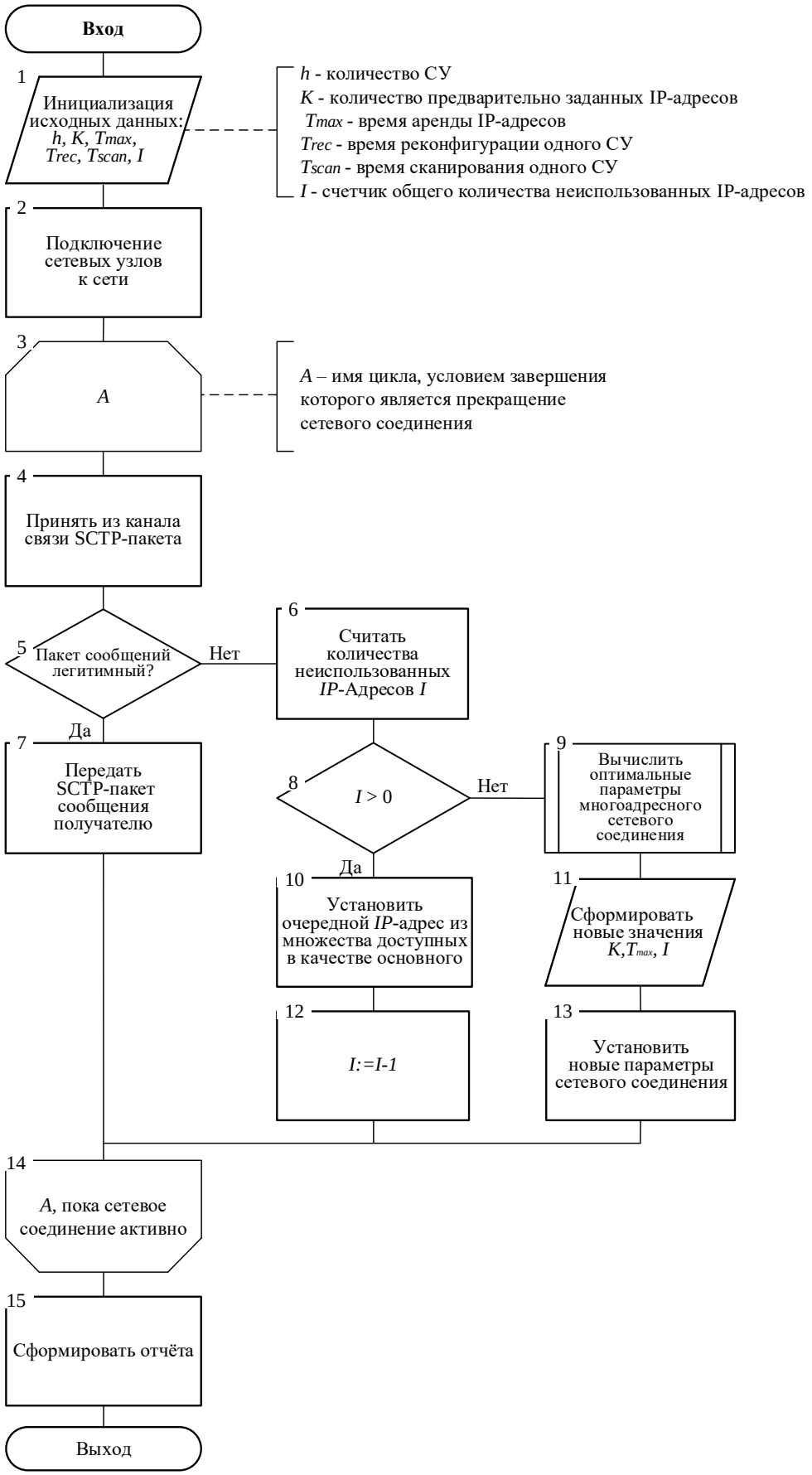
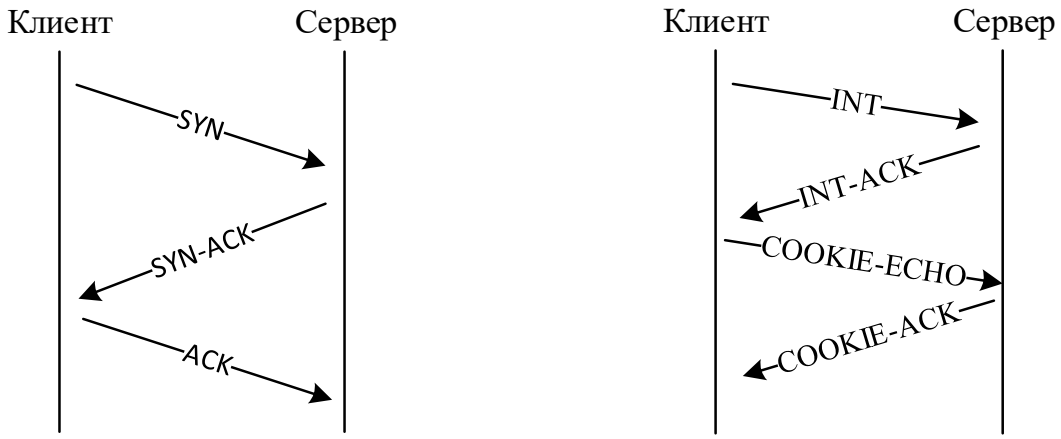


Рис. 7. Алгоритм конфигурирования параметров многоадресных сетевых соединений

Процесс установления сетевого соединения (блок 2 на рис. 7) при использовании протокола SCTP осуществляется в четыре этапа, что принципиально отличает его от других протоколов транспортного уровня (рис. 8). При этом выделение ресурсов новому сетевому соединению осуществляется только после его верификации (получения служебного пакета «COOKIE-ECHO» со специальным маркером).



а) протокол TCP б) протокол SCTP

Рис. 8. Процесс установления сетевого соединения TCP и SCTP

Для проверки состояния сетевого соединения между СУ (блок 3 на рис. 7), протоколом SCTP предусмотрена периодическая отправка служебного пакета «HEARTBEAT». Если СУ не получают эти пакеты в течение определенного времени, они могут считать, что сетевое соединение разорвано и завершить его. Служебные пакеты «HEARTBEAT» также используются для определения задержек в сети и для обнаружения ошибок передачи данных.

Для проверки на легитимность входящих сетевых пакетов (блок 5 на рис. 7) могут использоваться следующие методы:

1) аутентификация отправителя, с помощью которой определяется, является ли отправитель легитимным или нет. Это может быть достигнуто путем использования методов, предусмотренных протоколами Extensible Authentication Protocol (EAP, «расширяемый протокол аутентификации») (RFC 5254), или Remote Authentication in Dial-In User Service (RADIUS, «служба удаленной аутентификации пользователей») (RFC 2865);
2) проверка контрольной суммы пакета, с помощью которой можно определить, был ли пакет изменен в процессе передачи. Если контрольная сумма не совпадает, то пакет может быть поврежден или подделан;
3) использование Intrusion Detection System (IDS, «системы обнаружения вторжений») и Intrusion Prevention System (IPS, «системы предотвращения вторжений»), позволяющих обнаружить и предотвратить атаки на сетевые ресурсы;

4) использование фильтрации трафика, позволяющей блокировать нежелательный трафик.

Смена основного IP-адреса на один из множества доступных (блок 10 на рис. 7) осуществляется посредством использования стандартной для протокола SCTP функции «SET_PRIMARY».

В случае отсутствия доступных IP-адресов (блок 13 на рис. 7), протоколом SCTP предусмотрено добавления новых IP-адресов в установленное сетевое соединение с помощью процедуры «SET_SOCKOPT».

Вместе с этим возникает задача в определении оптимального количества предварительно заданных IP-адресов и времени их аренды (блок 9 на рис. 7), поскольку при их увеличении, также увеличивается и время реконфигурации сетевого соединения.

Так, в рамках проведенного эксперимента было выявлено, что время реконфигурации 254 СУ одной подсети составило 5 с (0,02 с на одно СУ). Соответственно, при применении многоадресных сетевых соединений, время восстановления многоадресного сетевого соединения будет увеличиваться пропорционально количеству предварительно задаваемых IP-адресов. Таким образом может возникнуть ситуация, при которой СУ будут находится в постоянной реконфигурации сетевого соединения без возможности возобновления информационного обмена.

Постановка задачи по определению оптимальных параметров многоадресных сетевых соединений

Определение оптимальных параметров конфигурирования многоадресных сетевых соединений можно сформулировать как задачу поиска оптимального количества предварительно заданных IP-адресов и времени их аренды, при которых защищенность и доступность СУ в условиях ведения компьютерной разведки будет максимальной.

Данная задача будет являться задачей многокритериальной оптимизации и в общем виде будет иметь вид:

$$\begin{cases} F_1(X^{avail}, A^{avail}) \rightarrow \max\limits_{\text{для } X^{avail}, A^{avail} \in Q} \\ F_2(X^{sec}, A^{sec}) \rightarrow \max\limits_{\text{для } X^{sec}, A^{sec} \in Q} \end{cases} \quad (1)$$

где: целевая функция F_1 характеризует «доступность» СУ, целевая функция F_2 характеризует их «защищенность»; X^{avail}, X^{sec} - множества управляемых факторов, влияющих на значения функций F_1 и F_2 соответственно; A^{avail}, A^{sec} - множества неуправляемых факторов, влияющих на значения функций F_1 и F_2 соответственно. Значения указанных функций и факторов принадлежат области допустимых значений Q.

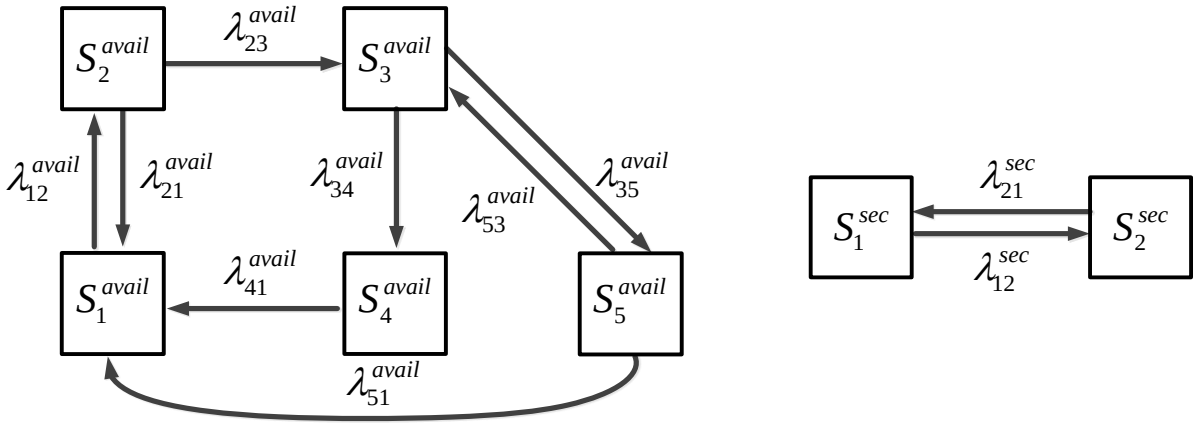
Данные целевые функции получены из представления процесса функционирования СУ (в условиях ведения компьютерной разведки) в виде двух случайных процессов [37, 38] с дискретными состояниями и непрерывным временем, при этом переход между определенными состояниями в обоих случаях

осуществляется под воздействием управляемых факторов, зависящих от количества предварительно заданных для СУ IP-адресов, а также времени их использования.

Первый случайный процесс представлен как процесс функционирования СУ с множественной адресацией (далее система L_1), где в качестве дискретных состояний выступают этапы функционирования протокола SCTP, определенные RFC 4960, а переход между этими состояниями осуществляется при возникновении в случайные моменты времени SCTP-пакетов.

Второй случайный процесс представлен как процесс функционирования этих же СУ в условиях ведения компьютерной разведки, а также выполнения мер по их защите (далее система L_2) посредством смены IP-адресов. Причем переход из одного состояния в другое зависит от интенсивности компьютерной разведки и частоты смены IP-адресов СУ.

В статье указанные случайные процессы рассматриваются как марковские процессы с соблюдением свойств простейшего потока событий и могут быть представлены в виде ориентированных графов для системы L_1 (рис. 9а) и L_2 (рис. 9б). Описание их дискретных состояний, а также значений интенсивностей потоков событий, переводящих системы между этими состояниями, приведено в соответствующих таблицах 3-6.



а) система L_1 б) система L_2

Рис. 9. Графы состояний систем L_1 и L_2

Таблица 3 – Дискретные состояния системы L_1

Состояние	Описание состояний
S_1^{avail}	Ожидание инициализации сетевого соединения между СУ (ожидание получения служебного SCTP-пакета «INIT»)
S_2^{avail}	Ожидание приема и передачи потока данных между СУ (ожидание получения служебного SCTP-пакета «DATA»)
S_3^{avail}	Ожидание реконфигурации сетевого соединения, либо его завершения (ожидание получения служебного SCTP-пакета «HEARTBEAT» / «SHUTDOWN»)
S_4^{avail}	Ожидание перехода СУ в состояние простоя (ожидание получения служебного SCTP-пакета» SHUTDOWN COMPLETE»)

Состояние	Описание состояний
S_5^{avail}	Состояние ожидание возобновления информационного обмена между СУ (ожидание получения служебного SCTP-пакета «HEARTBEAT ACK»)

Таблица 4 – Вероятностные характеристики процесса функционирования системы L_1

Переменная	Описание значения интенсивности
λ_{12}^{avail}	Интенсивность потока событий на инициализацию сетевого соединения
λ_{21}^{avail}	Интенсивность потока событий на отказ в инициализации сетевого соединения
λ_{23}^{avail}	Интенсивность потока событий на передачу и приема потоков данных между СУ
λ_{34}^{avail}	Интенсивность потока событий на завершение сетевого соединения между СУ
λ_{41}^{avail}	Интенсивность потока событий на закрытие сетевого соединения между СУ
λ_{35}^{avail}	Интенсивность потока событий на реконфигурации сетевого соединения
λ_{53}^{avail}	Интенсивность потока событий на возобновления информационного обмена между СУ
λ_{51}^{avail}	Интенсивность потока событий на принудительный разрыва сетевого соединения между СУ

Таблица 5 – Дискретные состояния системы L_2

Состояние	Описание состояния
S_1^{sec}	Ожидание вскрытия истинных IP-адресов СУ вычислительной сети
S_2^{sec}	Ожидание смены IP-адресов СУ вычислительной сети

Таблица 6 – Вероятностные характеристики процесса функционирования системы L_2

Переменная	Описание вероятностных характеристик
λ_{12}^{sec}	Интенсивность потока событий на вскрытие IP-адресов вычислительной сети
λ_{21}^{sec}	Интенсивность потока событий на смену IP-адресов СУ вычислительной сети

По полученным размеченным графам состояний, для вычисления вероятностно-временных характеристик моделируемых систем, составляются системы дифференциальных уравнений Колмогорова (2), (3), при этом последние уравнения заменены нормировочным условием.

$$\begin{cases} \dfrac{dp_1^{avail}(t)}{dt} = \lambda_{21}^{avail} p_2^{avail}(t) + \lambda_{41}^{avail} p_4^{avail}(t) + \lambda_{51}^{avail} p_5^{avail}(t) - \lambda_{12}^{avail} p_1^{avail}(t) \\ \dfrac{dp_2^{avail}(t)}{dt} = \lambda_{12}^{avail} p_1^{avail}(t) - (\lambda_{21}^{avail} + \lambda_{23}^{avail}) p_2^{avail}(t) \\ \dfrac{dp_3^{avail}(t)}{dt} = \lambda_{23}^{avail} p_2^{avail}(t) + \lambda_{53}^{avail} p_5^{avail}(t) - (\lambda_{34}^{avail} + \lambda_{35}^{avail}) p_3^{avail}(t) \\ \dfrac{dp_4^{avail}(t)}{dt} = \lambda_{34}^{avail} p_3^{avail}(t) - \lambda_{41}^{avail} p_4^{avail}(t) \\ \sum_{i=1}^{5} p_i^{avail}(t) = 1 \end{cases} \quad (2)$$

$$\begin{cases} \dfrac{dp_1^{sec}(t)}{dt} = \lambda_{21}^{sec} p_2^{sec}(t) - \lambda_{12}^{sec} p_1^{sec}(t) \\ p_1^{sec}(t) + p_2^{sec}(t) = 1 \end{cases} \quad (3)$$

Ввиду однородности потоков событий, переводящих системы L_1 и L_2 из одного состояния в другое, а также отсутствия в них поглощающих состояний, исследуемые процессы обладают эргодическим свойством, соответственно, имеют стационарный режим, и, как следствие, имеют финальные вероятности.

Так, финальная вероятность p_5^{avail} системы L_1 характеризует вероятность нахождения в состоянии, когда СУ будут находится в ожидании возобновления информационного обмена (состояние «недоступности» для осуществления информационного обмена), а финальная вероятность p_2^{sec} системы L_2 характеризует состояние, при котором СУ будут находится в защищенном состоянии (состояние «защищенности»).

Расчет финальных вероятностей подробно описан в [39], и в зависимости от условий функционирования СУ, будут принимать значения, представленные на графиках (рис. 10, 11):

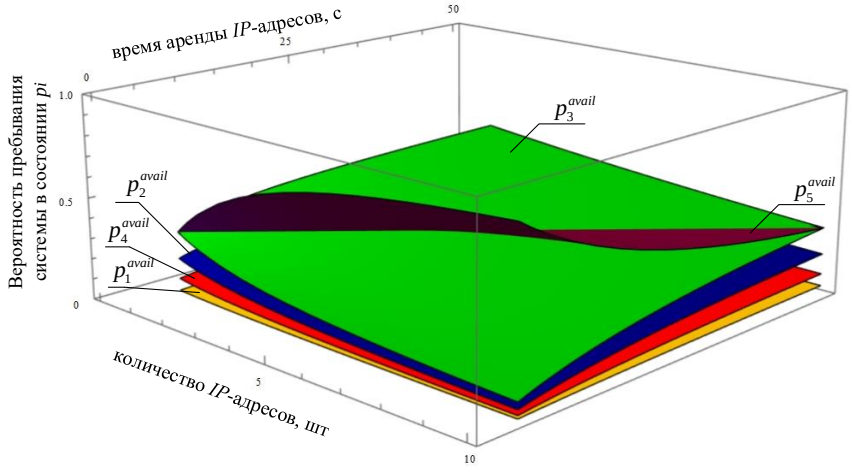


Рис. 10. Результаты расчётов зависимостей финальных вероятностей системы L_1 в зависимости от количества IP-адресов и времени их аренды

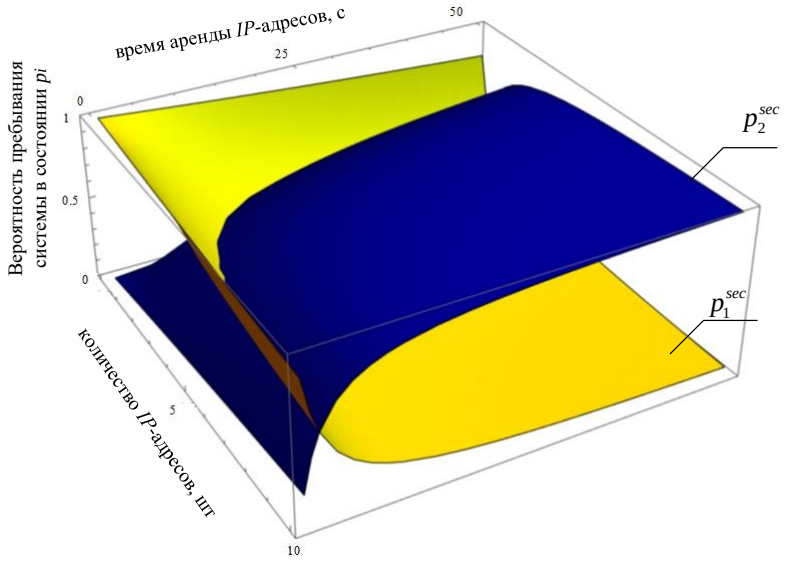


Рис. 11. Результаты расчётов зависимостей финальных вероятностей системы L_2 в зависимости от количества *IP*-адресов и времени их аренды

Значения финальных вероятностей систем L_1 и L_2 напрямую засвистят от одних и тех же параметров конфигурации многоадресных сетевых, при этом их наилучшее значения для системы L_2 будут являться наихудшими для системы L_1.

С учетом вышесказанного, задача многокритериальной оптимизации (1) примет следующий вид:

$$\begin{cases} F_1(X^{avail}, A^{avail}) = \overline{p_5^{avail}} \\ F_2(X^{sec}, A^{sec}) = p_1^{sec} \end{cases} \tag{4}$$

$$\begin{cases} F_1(X^{avail}, A^{avail}) \to \max\limits_{\text{для } X^{avail}, A^{avail} \in Q} \\ F_2(X^{sec}, A^{sec}) \to \max\limits_{\text{для } X^{sec}, A^{sec} \in Q} \end{cases} \tag{5}$$

$$X^{avail} = \{\lambda_{35}^{avail}, \lambda_{53}^{avail}, h\}, \text{при } \lambda_{35}^{avail} = y^{-1} \text{ и } \lambda_{53}^{avail} = (h \cdot T_{rec} \cdot x)^{-1} \tag{6}$$

$$X^{sec} = \{\lambda_{12}^{sec}, \lambda_{21}^{sec}, h\}, \text{при } \lambda_{12}^{sec} = y^{-1} \text{ и } \lambda_{21}^{sec} = (h \cdot T_{scan} \cdot x)^{-1} \tag{7}$$

$$A^{avail} = \{\lambda_{12}^{avail}, \lambda_{21}^{avail}, \lambda_{23}^{avail}, \lambda_{34}^{avail}, \lambda_{41}^{avail}, \lambda_{51}^{avail}, T_{rec}, T_{scan}\}, \; A^{sec} = \{T_{scan}\} \tag{8}$$

где: h – количество сетевых устройств, x – количество IP-адресов для одного СУ, y – время их аренды одним СУ, T_{scan} – время сканирования одного СУ, T_{rec} – время реконфигурации одного СУ. При этом область допустимых значений будет иметь вид:

$$Q:\begin{cases} 0<h<256, \\ 0{,}1<T_{scan}<38; 0{,}1<T_{rec}<3, \\ 1<x<4095; 0{,}01<y<86400, \\ \lambda_{12}^{avail}\geq 0, \lambda_{21}^{avail}\geq 0, \lambda_{23}^{avail}\geq 0, \lambda_{23}^{avail}\geq 0, \\ \lambda_{41}^{avail}\geq 0, \lambda_{35}^{avail}\geq 0, \lambda_{53}^{avail}\geq 0, \lambda_{51}^{avail}\geq 0, \\ \lambda_{12}^{sec}\geq 0, \lambda_{21}^{sec}\geq 0, \\ 0<F_1(X^{avail}, A^{avail})<1, \\ 0<F_2(X^{sec}, A^{sec})<1 \end{cases} \quad (9)$$

Решение задачи многокритериальной оптимизации

Поскольку задача (5) является многокритериальной, то множество возможных значений частных целевых функций будет представлять собой множество точек, образующих фронт Парето [40] в критериальном пространстве.

Поиск наилучших значений был осуществлен методом идеальной точки, суть которого заключался в определении точки из фронта Парето, наименее отдаленной от идеальной (по заданным критериям). Под идеальной точкой понимают такую точку, компоненты которого являются максимумами частных целевых функций (5) по отдельности.

Таким образом, задача многокритериальной оптимизации (5) сводится к минимизации функции свертки (скалярной функции *R*), полученной через частные целевые функции методом отклонения от идеальной точки [41, 42] и имеющей следующий вид:

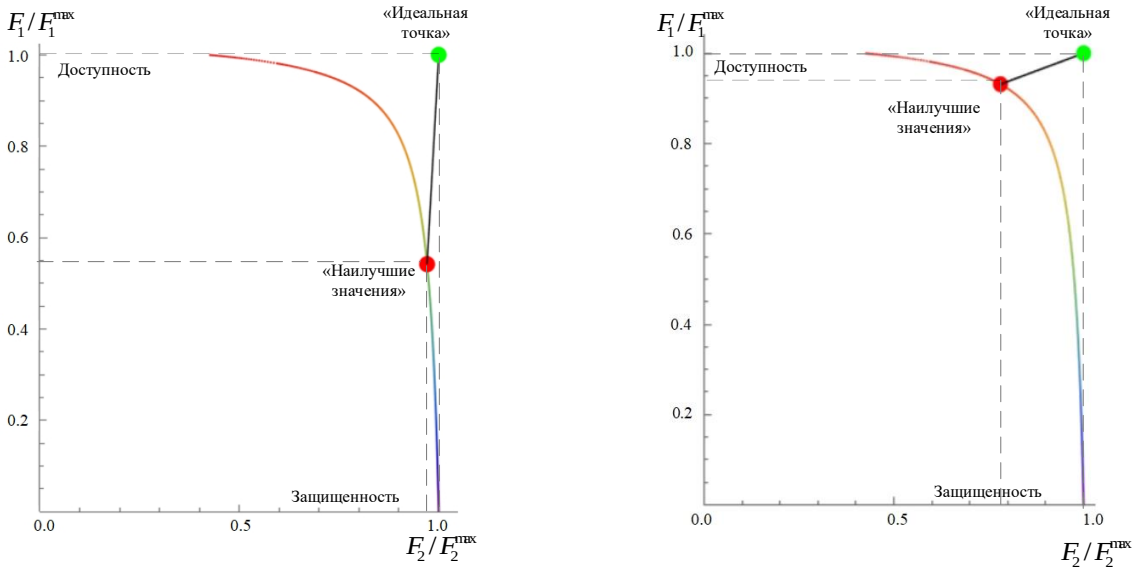
$$\begin{cases} R(X^{avail}, A^{avail}, X^{sec}, A^{sec}) = \sqrt{k_1 \cdot (\frac{F_1}{F_1^{\max}} - 1)^2 + k_2 \cdot (\frac{F_2}{F_2^{\max}} - 1)^2} \\ R(X^{avail}, A^{avail}, X^{sec}, A^{sec}) \rightarrow \min\limits_{\text{для } X^{avail}, X^{sec}, A^{avail}, A^{sec} \in Q} \end{cases} \quad (10)$$

где: k_1 и k_2 - коэффициенты значимости, полностью отражающей предпочтений лица, принимающего решение по отношению к величинам частных критериев. Они могут быть заданы экспертами или определен на основе анализа данных.

Поскольку целевые функции (5) имеют различную размерность, то была осуществлена нормировка посредством деления данных целевых функций на их максимальное значение. С условиями данной нормировки, идеальная точка будет иметь координаты (1,1).

На рис. 12 представлена визуализация критериального пространства и фронта Парето для различных коэффициентов значимости. Так, на рис. 12а преобладает важность защищенности сетевых узлов вычислительной сети ($k_2 = 0{,}8; k_1 = 1 - k_2 = 0{,}2$), а на рис. 12б преобладает важность их доступность.

№2. 2023
ISSN 2410-9916



а) значимость «защищенности» сетевых узлов

б) значимость «доступности» сетевых узлов

Рис. 12. Визуализация критериального пространства и фронта Парето для различных коэффициентов значимости

Поиск минимального значения скалярной функции R осуществлялся алгоритмом «Нелдера-Мида» [43], поскольку за счет небольшого числа переменных его сходимость по времени оказалась быстрее, чем у алгоритма «Имитации отжига» [44] и алгоритма «Роя частиц» [45].

Однако, алгоритм «Роя частиц» может быть более эффективным при решении задач при увеличении числа переменных, а также может быть полезен в задачами с нелинейными ограничениями, где он может найти оптимальное решение, которое другие алгоритмы могут пропустить.

Алгоритм «Имитации отжига» требует больше времени для нахождения оптимального решения, чем вышеупомянутые алгоритмы, однако он может быть полезен в задачах, где требуется исследовать большое пространство поиска и где есть возможность принимать худшие решения для избежания «застревания» в локальных минимумах.

Сравнительный анализ о временных затрат для (10) приведен в таблице 7.

Таблица 7 – Сравнение сходимости алгоритмов случайного поиска

№ п/п	Алгоритм	Время (мс)
1	«Нелдера-Мида»	47
2	«Имитации отжига»	406
3	«Роя частиц»	2029

Оценка эффективности применения оптимальных параметров многоадресных сетевых соединений

На выбор оптимальных параметров в блоке 9 на рис. 7 влияют условия функционирования исследуемых систем, в качестве которых могут выступать:

возможности, характер и способы ведения злоумышленником компьютерной разведки; количество СУ вычислительной сети и регламент их функционирования; наличие средств защиты информации.

Так, на рис. 13 представлено оптимальное количество IP-адресов в зависимости от времени нахождения СУ в состоянии ожидании инициализации сетевого соединения, а также времени его инициализации в условиях ведения компьютерной разведки вычислительной сети, состоящей из 100 СУ, в режиме «Intense scan» (0,42 с на 1 СУ). На рис. 14 представлено оптимальное время использования этих IP-адресов для соответствующих ситуаций.

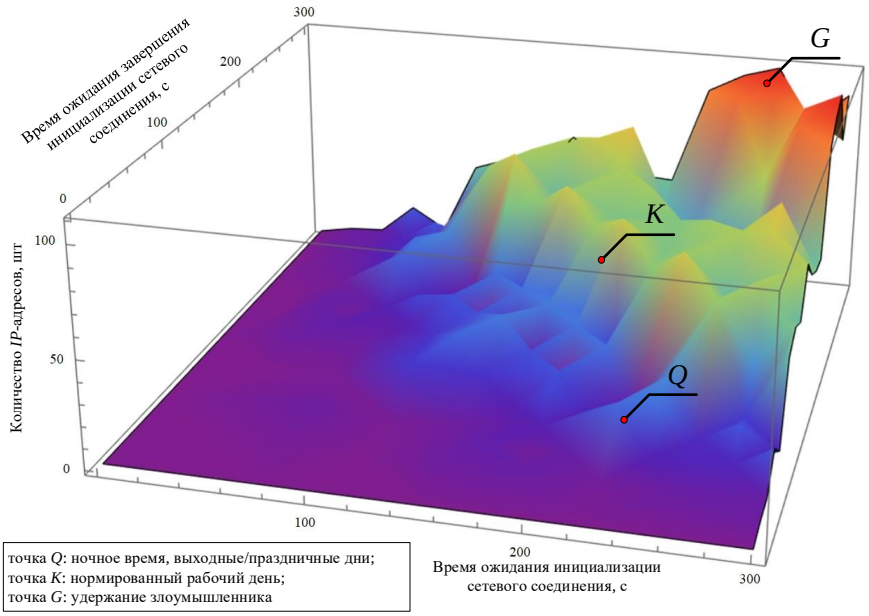


Рис. 13. Результаты расчетов оптимального количества IP-адресов СУ в зависимости от времени суток, а также легитимности новых сетевых соединений

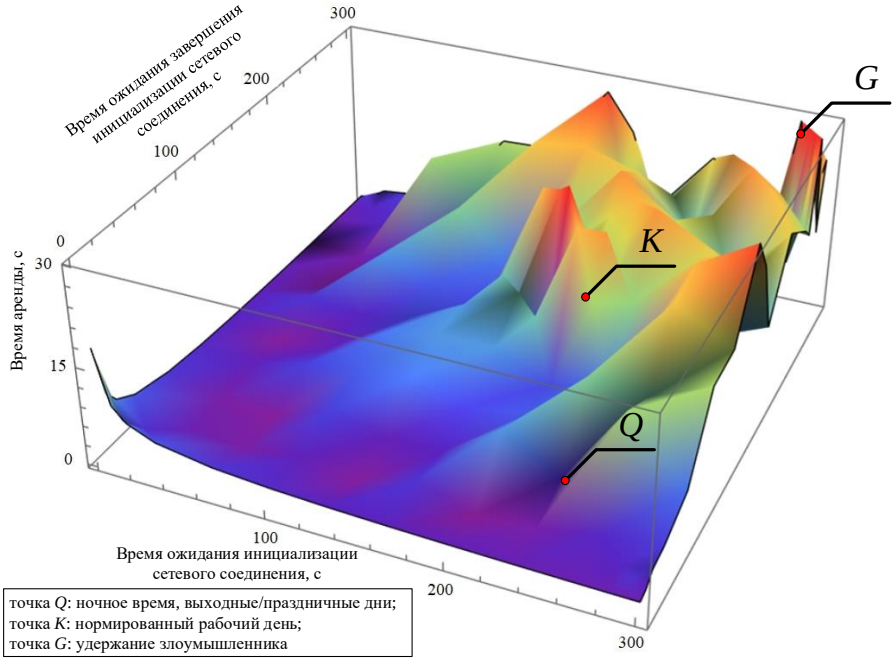


Рис. 14. Результаты расчетов оптимального количества времени аренды IP-адресов СУ в зависимости от времени суток, а также легитимности новых сетевых соединений

Так, в ситуации, когда время простоя СУ достаточно велико (например, точка *Q*: это ночь, выходные/праздничные дни), а время ожидания завершения инициализации сетевого соединения между СУ относительно невелико (а это происходит в случае установления легитимности сетевого соединения), то достаточно использовать до 6 IP-адресов с временем их аренды, не превышающих время сетевого сканирования 100 СУ в режиме «Intense scan».

Если обращение к СУ происходит значительно чаще (например, точка *K*: нормированный рабочий день), то при тех же условиях ведения компьютерной разведки, необходимо иметь от 14 IP-адресов с соответствующим времени их аренды.

Также предусмотрен случай, когда выполняются меры проактивной защиты [46-48], когда происходит удержание злоумышленника в состоянии инициализации сетевого соединения (например, точка *G*: удержание злоумышленника). В данном случае, в условиях ведения компьютерной разведки, предполагается использовать практически максимальное количество IP-адресов с максимальным временем их аренды.

На рис. 15, 16 представлены оптимальные параметры конфигурации многоадресных сетевых соединений в зависимости от интенсивности ведения компьютерной разведки, а также времени реконфигурации сетевого соединения.

Так, например, при ведении компьютерной разведки вычислительной сети, состоящей из 100 СУ, в режиме «Ping scan» (0,22 с на одно СУ) и в условиях быстрой реконфигурации сетевого соединения (0,02 с на одно СУ), предлагается использовать для СУ 8 IP-адресов с временем аренды 27 с (точка *B* на рис. 15, 16). При снижении интенсивности ведения компьютерной разведки снижается и необходимое количество дополнительный IP-адресов (точка *H* на рис. 15, 16).

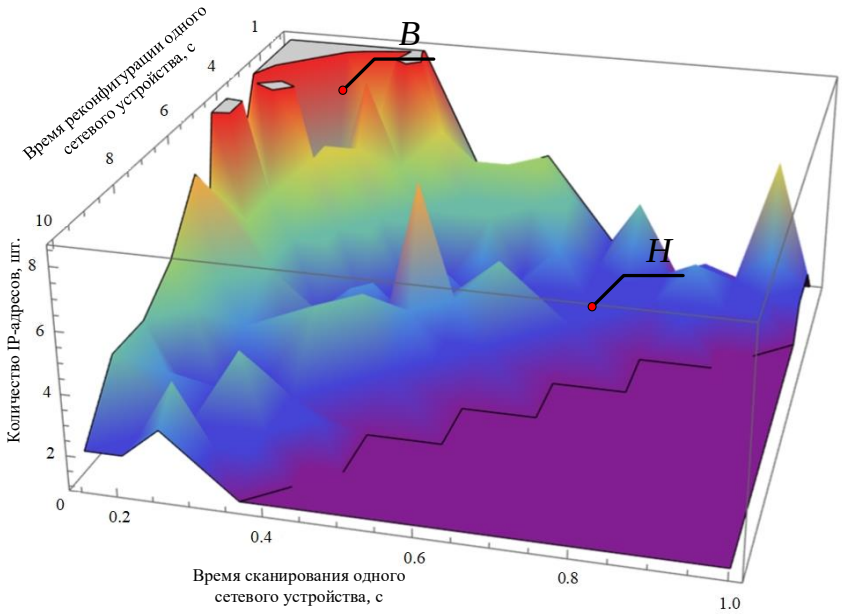


Рис. 15. Результаты расчетов оптимального количества IP-адресов в зависимости от интенсивности ведения компьютерной разведки и времени реконфигурации сетевого соединения

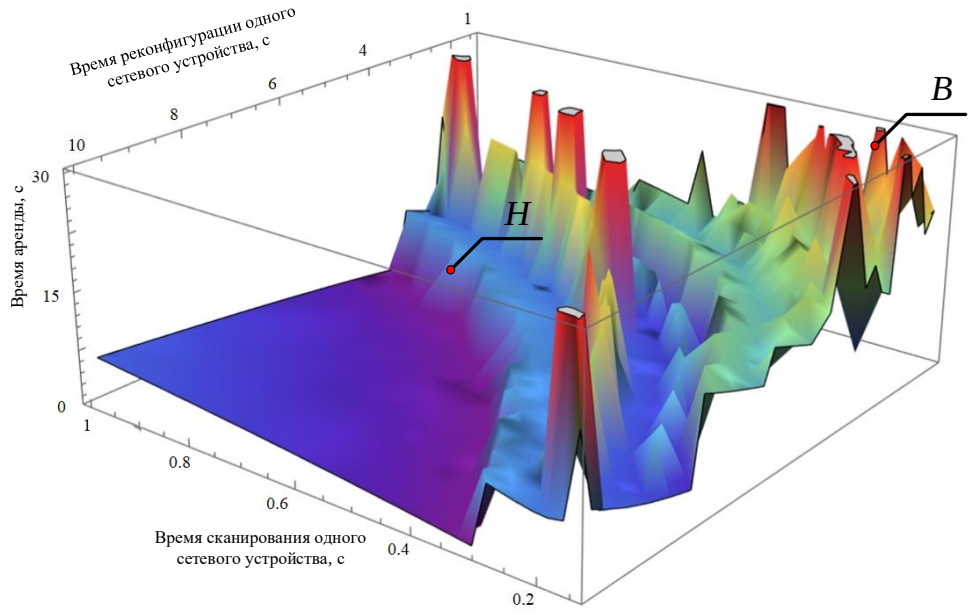
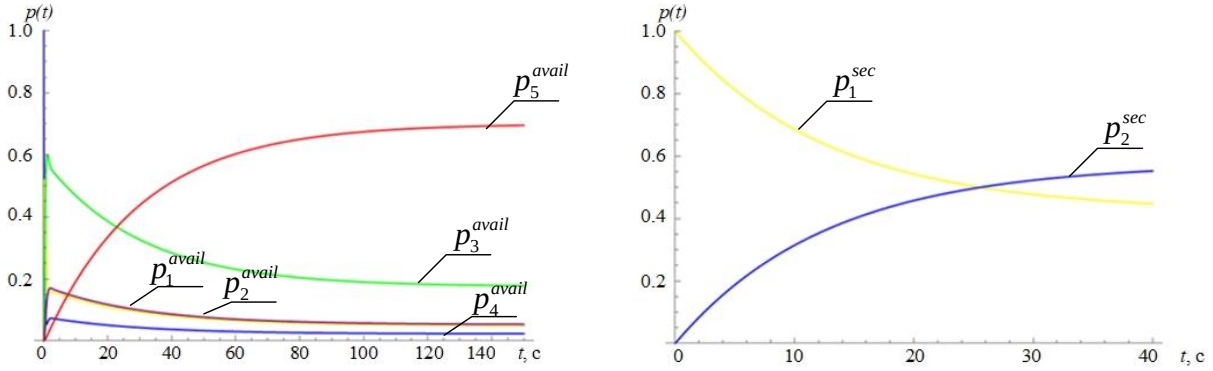


Рис. 16. Результаты расчетов оптимального количества времени аренды IP-адресов в зависимости от интенсивности ведения компьютерной разведки и времени реконфигурации сетевого соединения

Оценка эффективности применения многоадресных сетевых соединений при оптимальных параметрах оценивалась при решении уравнений (2), (3) численным методом Рунге-Кутты четверного порядка, который является более точным по сравнению с методом Эйлера, поскольку он основан на использовании нескольких точек для аппроксимации производной функции, что позволяет улучшить точность решения. Метод Эйлера основан на аппроксимации производной функции конечной разностью, причем он прост в реализации, но имеет низкую точность и может приводить к неустойчивости при решении некоторых типов ДУ.

На рис. 17, 18 представлены вероятностно-временные характеристики процесса функционирования СУ вычислительной сети, в которой ведется компьютерная разведка в режиме «Ping scan» (0,22 с на одно СУ).



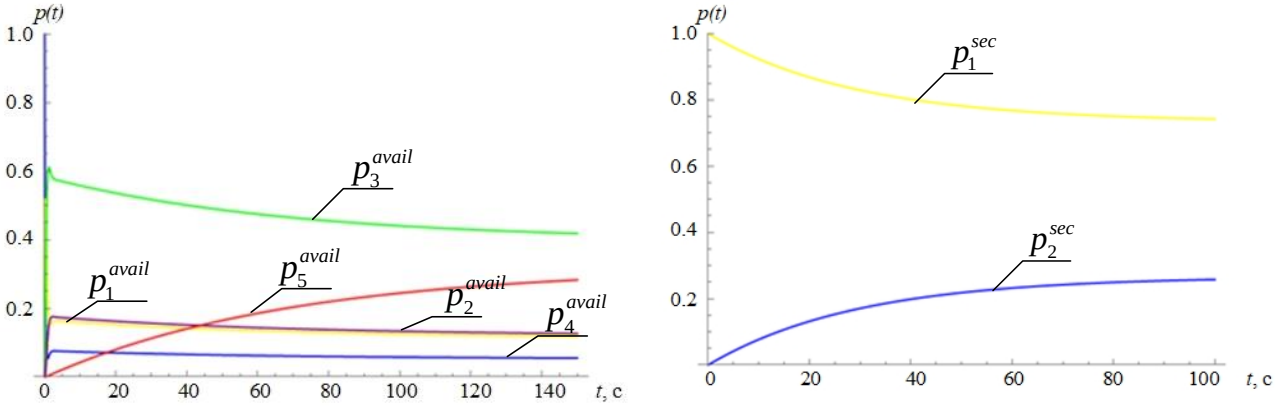
а) система L_1 б) система L_2

Рис. 17. Результаты расчетов зависимостей вероятностей $p_i(t)$ от времени ведения компьютерной разведки (без оптимальных параметров)

№2. 2023
ISSN 2410-9916

Так, в условиях применения сетевых соединений с одним IP-адресом, СУ в стационарном режиме с вероятностью 30% будет находится в состоянии непрерывного информационного обмена (состояние p_3^{avail}, рис. 17а), при этом вероятность его нахождения в защищенном состоянии будет составлять всего 45% (состояние p_1^{sec}, рис. 17б).

Однако, при применении оптимальных параметров многоадресных сетевых соединений, вероятность нахождения СУ в состоянии непрерывного информационного обмена увеличится с 30 до 50 % (Рис. 18а), а вероятность его нахождения в защищенном состоянии увеличиться с 45 до 80 % (Рис. 18б)



а) система L_1 б) система L_2

Рис. 18. Результаты расчетов зависимостей вероятностей $p_i(t)$ от времени ведения компьютерной разведки (с применением оптимальных параметров)

В таблице 8 приведена оценка эффективности применения оптимальных параметров многоадресных сетевых соединений при динамическом изменении IP-адресов вычислительной сети, состоящей из 100 СУ, функционирующей в условиях ведения различных режимов компьютерной разведки.

Таблица 8 – Оценка эффективности применения оптимальных параметров многоадресных сетевых соединений

№ п/п	Режим сканирования/время сканирования одного СУ, с	Оптимальные количество IP-адресов / время их использования, шт/с	Увеличение доступности, %	Увеличение защищенности, %
1	Quick scan / 0,15	10 / 28	23	44
2	Ping scan / 0,22	8 / 27	20	35
3	Intense scan / 0,42	6 / 26	7	23
4	Intense scan, all tcp ports / 37,8	1 / 31	0,1	0,1

DOI: 10.24412/2410-9916-2023-2-102-130
URL: https://sccs.intelgr.com/archive/2023-02/05-Moskvin.pdf

Заключение

Разработанный алгоритм позволяет повысить защищенность и доступность сетевых узлов вычислительной сети при динамическом изменении ее IP-адресов за счет применения оптимальных параметров многоадресных сетевых соединений в условиях ведения компьютерной разведки.

Выбор оптимальных параметров осуществлялся посредством минимизации функции сверки, полученной методом отклонения от идеальной точки по частным критериям, характеризующих «защищенность» и «доступность» сетевых узлов. При этом поиск минимума функции свертки реализован с помощью алгоритма «Нелдера-Мида», поскольку его сходимость по времени оказалась наименьшей. В алгоритме предусмотрен выбор наиболее значимого критерия, отражающей предпочтение лица, принимающего решение по отношению к величинам частных критериев.

Процесс функционирования СУ с множественной адресацией в условиях ведения компьютерной разведки был представлен как марковский процесс с дискретными состояниями и непрерывным временем. Причем финальные вероятности исследуемых процессов в последующем и были выбраны в качестве частных критериев.

Оценка эффективности применения оптимальных параметров многоадресных сетевых соединений при смене IP-адресов СУ вычислительной сети показала, что, в зависимости от режима ведения компьютерной разведки, доступность СУ будет повышена до 23%, а их защищенность до 44%.

Новизна алгоритма заключается в применении модели функционирования многоадресных сетевых соединений, основанной на математическом аппарате теории марковских процессов с дискретными состояниями и непрерывным временем; постановке и решении задачи определения оптимальных параметров многоадресных сетевых соединений, при которых доступность и защищенность сетевых узлов будет максимальной.

Литература

1. Марков А. С. Важная веха в безопасности открытого программного обеспечения // Вопросы кибербезопасности. 2023. № 1 (53). С. 2–12.

2. Carvalho M., Ford R. Moving target defense for computer networks // IEEE Security & Privacy. 2014. Vol. 12. No. 2. P. 73–76.

3. Sokolovsky S. P., Voronchikhin I. S., Telenga A. P. Moving target defense for securing distributed information systems // Информатика: проблемы, методология, технологии. Сборник материалов XIX международной научно-методической конференции. Под ред. Д. Н. Борисова. 2019. С. 639–643.

4. Kanellopoulos A., Vamvoudakis K. A Moving Target Defense Control Framework for Cyber-Physical Systems // IEEE Trans. Autom. Control. 2020. Vol. 65. P. 1029–1043.

5. Sengupta S., Chowdhary A., Sabur A., Alshamrani A., Huang D., Kambhampati S. A. Survey of Moving Target Defenses for Network Security // IEEE Commun. Surv. Tutor. 2020. Vol. 22. P. 1909–1941.

6. Maximov R. V., Sokolovsky S. P., Telenga A. P. Methodology for substantiating the characteristics of false network traffic to simulate information systems // Selected Papers of the XI Anniversary International Scientific and Technical Conference on Secure Information Technologies. 2021. P. 115–124.

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

8. Соколовский С. П., Модель защиты информационной системы от сетевой разведки динамическим управлением ее структурно - функциональными характеристиками // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2020. № 7-8 (145-146). С. 62–73.

9. Maximov R. V. Sokolovsky S. P., Telenga A. P. Model of client-server information system functioning in the conditions of network reconnaissance // CEUR Workshop Proceedings. X Anniversary International Scientific and Technical Conference on Secure Information Technologies. 2019. Vol. 2603. P. 44–51.

10. Ветошкин И. С., Дрозд Ю. А., Ефимов А. А., Зорин К. М., Игнатенко А. В., Кожевников Д. А. Краснов В. А., Кузнецов В. Е., Максимов Р. В. Способ защиты вычислительной сети с выделенным сервером // Патент на изобретение RU 2449361, опубл. 27.04.2012.

11. Барабанов В. В., Ефремов А. А., Максимов Р. В. Способ защиты вычислительных сетей // Патент на изобретение RU 2696330, опубл. 31.07.2018.

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

13. Выговский Л. С., Заргаров И. А., Кожевников Д. А., Максимов Р. В., Павловский А. В., Стародубцев Ю. И., Худайназаров Ю. К., Юров И. А. Способ (варианты) защиты вычислительных сетей // Патент на изобретение RU 2307392, опубл. 27.09.2007.

14. Гаврилов А. Л., Катунцев С. Л., Максимов Р. В., Орехов Д. Н., Крупенин А. В., Медведев А. Н., Соколовский С. П. Способ защиты вычислительных сетей // Патент на изобретение RU 2682432, опубл. 19.03.2019.

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

16. Куликов О. Е., Липатников В. А, Максимов Р. В., Можаев О. А. Способ защиты информационно-вычислительных сетей от компьютерных атак // Патент на изобретение RU 2285287, опубл. 10.09.2006.

17. Гречишников Е. В., Дыбко Л. К., Ерышов В. Г., Жуков А. В., Стародубцев Ю. И. Способ обеспечения устойчивого функционирования системы связи // Патент на изобретение RU 2405184, опубл. 27.11.2010.

18. Стародубцев Ю. И., Гречишников Е. В., Комолов Д. В. Способ обеспечения устойчивости сетей связи в условиях внешних деструктивных воздействий // Патент на изобретение RU 2379753, опубл. 20.01.2010.

19. Лейкин А. В., Развитие SCTP как конвергентного транспортного протокола следующего поколения // Вестник связи. 2020. № 1. С. 13–17.

20. Голуб Б. В., Краснов В. А., Лыков Н. Ю., Максимов Р. В. Способ маскирования структуры сети связи // Патент на изобретение RU 2645292, опубл. 19.02.2018.

21. Максимов Р. В., Кучуров В. В., Шерстобитов Р. С. Модель и методика маскирования адресации корреспондентов в киберпространстве // Вопросы кибербезопасности. 2020. № 6 (40). С. 2–13.

22. Голуб Б. В., Горячая А. В., Кожевников Д. А., Лыков Н. Ю., Максимов Р. В., Тихонов С. С. Способ маскирования структуры сети связи // Патент на изобретение RU 2622842, опубл. 23.06.2017.

23. Андрианов В. И., Бухарин В. В., Кирьянов А. В., Липатников В. А., Санин И. Ю., Сахаров Д. В., Стародубцев Ю. И. Способ защиты информационно-вычислительных сетей от компьютерных атак // Патент на изобретение RU 2472211, опубл. 23.11.2011.

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

25. Берест П. А., Богачев К. Г., Выговский Л. С., Зорин К. М., Игнатенко А. В., Кожевников Д. А., Краснов В. А., Кузнецов В. Е., Максимов Р. В. Способ сравнительной оценки структур информационно-вычислительной сети // Патент на изобретение RU 2408928, опубл. 10.01.2011.

26. Макаренко С. И. Преднамеренное формирование информационного потока сложной структуры за счет внедрения в систему связи дополнительного имитационного трафика // Вопросы кибербезопасности. 2014. № 3 (4). С. 7–13.

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

28. Будников С. А., Бутрик Е. Е., Соловьев С. В. Моделирование APT-атак, эксплуатирующих уязвимость Zerologon // Вопросы кибербезопасности. 2021. № 6 (46). С. 47–61.

29. Израилов К. Е., Макарова А. К., Шестаков А.В. Обобщенная модель защиты от кибератак на VoIP //Вопросы кибербезопасности. 2023. № 2 (54). С. 109–121.

30. Бекенева Я. А. Анализ актуальных типов DDoS-атак и методов защиты от них // Известия Санкт-Петербургского государственного электротехнического университета ЛЭТИ. 2016. № 1. С. 7–14.

31. Петров М. Ю., Фаткиева Р. Р. Модель синтеза распределенных атакующих элементов в компьютерной сети // Труды учебных заведений связи. 2020. № 2. С. 113–120.

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

33. Остапенко А. Г., Тишков С. А. Исследование возможностей регулирования рисков автоматизированных систем при защите от атак типа «Отказ в обслуживании» // Информационная безопасность. 2009. № 1. С. 25–38.

34. Остапенко А. Г., Ермилов Е. В., Калашников А. О. Риск ущербности, шансы полезности и жизнестойкости компонент автоматизированных систем в условиях воздействия на них информационных угроз // Информационная безопасность. 2013. Т. 16. № 2. С. 215–218.

35. Максимов Р. В., Соколовский С. П., Ворончихин И. С. Способ защиты вычислительных сетей // Патент на изобретение RU 2716220, опубл. 06.03.2020.

36. Antonatos S., Akritidis P., Markatos E., Anagnostakis K. Defending against Hitlist Worms using Network Address Space Randomization // 2005 ACM Workshop on Rapid Malcode, USA. 2005. P. 30–40.

37. Тихонов В. И., Миронов М. А. Марковские процессы. – М.: Советское радио, 1977. – 488 с.

38. Вентцель Е. С., Овчаров Л. А. Теория случайных процессов и ее инженерные приложения. – М.: Наука, 1991. – 384 с.

39. Горбачев А. А., Соколовский С. П., Усатиков С. В. Модель функционирования и алгоритм проактивной защиты сервиса электронной почты от сетевой разведки // Системы управления, связи и безопасности. 2021. № 3. С. 60–109.

40. Ногин В. Д. Протодьяконов И. О., Евлампиев И. И. Основы теории оптимизации: Учеб. пособие для студентво втузов. – М.: Высш. Шк., 1986. – 384 с.

41. Растригин Л. А. Теория и применение случайного поиска. – Изд-во «Зинатне», Рига, 1969. – 309 с.

42. Горбачев А. А. Модель и параметрическая оптимизация проактивной защиты сервиса электронной почты от сетевой разведки // Вопросы кибербезопасности. 2022. № 3 (49). С. 69–81.

43. Nelder J., Mead R. A Simplex Method for Function Minimization // Computer Journal. 1965. P. 308–313.

44. Kennedy J., Eberhart R. Particle Swarm Optimization // Proceedings of IEEEE International Conference on Evolutionary Computation. 1995. P. 1942–1948.

45. Storn R., Price K. Differential Evolution: A simple and efficient adaptive scheme for global optimization over continuous spaces // Journal of Global Optimization. 1995. P. 1–15.

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

47. Maximov R. V., Sokolovsky S. P., Telenga A. P. Honeypots network traffic parameters modeling // SEUR Workshop Proceedings. BIT 2021 – Selected

Papers XI International Scientific and Technical Conference on Secure Information Technologies. 2021. P. 229–239.

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

References

1. Markov A. C. Important milestones in open source software security. *Voprosy kiberbezopasnosti*, 2023, vol. 1, no. 53, pp. 2–12 (in Russia).

2. Carvalho M., Ford R. Moving target defense for computer networks. *IEEE Security & Privacy*, 2014, vol. 12, no. 2, pp. 73–76.

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

4. Kanellopoulos A., Vamvoudakis K. G. A Moving Target Defense Control Framework for Cyber-Physical Systems. *IEEE Trans. Autom. Control*, 2020, vol. 65, pp. 1029–1043.

5. Sengupta S., Chowdhary A., Sabur A., Alshamrani A., Huang D., Kambhampati S. A. Survey of Moving Target Defenses for Network Security. *IEEE Commun. Surv. Tutor.*, 2020, vol. 22. pp. 1909–1941.

6. Maximov R. V., Sokolovsky S. P., Telenga A. P. Methodology for substantiating the characteristics of false network traffic to simulate information systems. *Selected Papers of the XI Anniversary International Scientific and Technical Conference on Secure Information Technologies*, 2021, pp. 115–124.

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

8. Sokolovsky S. P. Model of information system protection from network intelligence by dynamic management of its structural and functional characteristics. *Enginery Problems. Series 16. Anti-Terrorist Engineering Means*, 2020, vol. 7-8, no. 145-146, pp. 62–73 (in Russia).

9. Maximov R. V., Sokolovsky S. P., Telenga A. P. Model of client-server information system functioning in the conditions of network reconnaissance. CEUR Workshop Proceedings. *X Anniversary International Scientific and Technical Conference on Secure Information Technologies*, 2019, vol. 2603, pp. 44–51.

10. Vetoshkin I. S., Drozd J. A., Efimov A. A., Zorin K. M., Ignatenko A. V., Kozhevnikov D. A., Krasnov V. A., Kuznetsov V. E., Maksimov R. V., Method of protecting computer network having dedicated server. Patent Russia, no. RU 2449361. Publish. 27.04.2012 (in Russian).

11. Barabanov V. V., Efremov A. A., Maksimov R. V. Method of protecting computer networks. Patent Russia, no. RU 2696330. Publish. 31.07.2018 (in Russian).

12. Starodubtsev Y. I., Eryshov V. G., Korsunky V. G. Model for process of information-security monitoring in information and telecommunication systems. *Automation of Control Processes*, 2011, vol. 1, no. 23, pp. 58–61 (in Russian).

13. Vygovskij L. S., Zargarov I. A., Kozhevnikov D. A., Maksimov R. V., Pavlovskij A. V., Starodubtsev J. I., Khudajnazarov J. K., Jurov I. A. Method (variants) for protecting computer networks. Patent Russia, no. RU 2307392. Publish. 27.09.2007 (in Russian).

14. Gavrilov A. L., Katuntsev S. L., Maksimov R. V., Orekhov D. N., Krupenin A. V., Medvedev A. N., Sokolovskij S. P. Method of computer networks protection. Patent Russia, no. RU 2682432. Publish. 19.03.2019 (in Russian).

15. Buharin V. V., Kir'yanov A. V., Starodubcev Y. U. Method for protecting computer networks. *Information systems and technologies*, 2012, vol. 4, no. 72, pp. 116–121.

16. Kulikov O. E., Lipatnikov V. A., Maksimov R. V., Mozhaev O. A. Method for protecting computer networks from computer attacks. Patent Russia, no. RU 2285287. Publish. 10.10.2006 (in Russian).

17. Grechishnikov E. V., Dybko L. K., Eryshov V. G., Zhukov A. V., Starodubtsev J. I. Method for providing stable operation of communication system. Patent Russia, no. RU 2405184. Publish. 27.11.2009 (in Russian).

18. Starodubtsev J. I., Grechishnikov E. V., Komolov D. V. Method of stabilising communication networks in conditions of disruptive external effects. Patent Russia, no. RU 2379753. Publish. 20.01.2010 (in Russian).

19. Leykin A. V. SCTP evolution as the next generation converged transport protocol. *Vestnik sviazi*, 2020, vol. 1, pp. 13–17 (in Russia).

20. Golub B. V., Krasnov V. A., Lykov N. Y., Maksimov R. V. Method for masking structure of telecommunication network. Patent Russia, no. RU 2645292. Publish 19.02.2018 (in Russian).

21. Maksimov R. V., Kuchurov V. V., Sherstobitov R. S. Model and technique for abonent address masking in cyberspace. *Voprosy kiberbezopasnosti*, 2020, vol. 6, no. 40, pp. 2–13 (in Russia).

22. Golub B. V., Goryachaya A. V., Kozhevnikov D. A., Lykov N. Y., Maksimov R. V., Tikhonov S. S. Method for masking the structure of telecommunication network. Patent Russia, no. RU 2622842. Publish 23.06.2017 (in Russian).

23. Andrianov V. I., Bukharin V. V., Kir'janov A. V., Lipatnikov V. A., Sanin I. J., Sakharov D. V., Starodubtsev J. I. Method of protecting information computer networks from computer attacks. Patent Russia, no. RU 2472211. Publish 23.11.2011 (in Russian).

24. Ivanov I. I., Maksimov R. V. Etyudy tekhnologii maskirovaniya funkcional'no-logicheskoj struktury informacionnyh sistem [Etudes of the technology of masking the functional and logical structure of information systems]. *Innovacionnaya deyatel'nost' v Vooruzhennyh Silah Rossijskoj Federacii. Trudy*

vsearmejskoj nauchno-prakticheskoj konferencii, 2017, Saint Peterburg, Mititary Telecommunications Academy, 2017, pp. 147–154 (in Russian).

25. Berest P. A., Bogachev K. G., Vygovskij L. S., Zorin K. M., Ignatenko A. V., Kozhevnikov D. A., Krasnov V. A., Kuznetsov V. E., Maksimov R. V. Method for comparative assessment of information computer network. Patent Russia, no. RU 2408928. Publish 10.01.2011 (in Russian).

26. Makarenko S. I. Premeditated formation of the traffic of difficult structure due to implementation in the communication system of additional imitative traffic. *Voprosy kiberbezopasnosti*, 2014, vol. 3, no. 4, pp. 7–13 (in Russia).

27. Yazov Y. K., Serdechnyy A. L., Sharov I. A. Methodical approach for estimation of efficiency of honeypot system. *Voprosy kiberbezopasnosti*, 2014, vol. 1, no. 2, pp. 55–60 (in Russia).

28. Budnikov S. A., Butrik E. E., Soloviev S. V. Modeling of APT-attacks exploiting the zerologon vulnerability. *Voprosy kiberbezopasnosti*, 2021, vol. 6, no. 46, pp. 47–61 (in Russia).

29. Izrailov K. E., Makarova A. K., Shestakov A. V. Generalized model of protection against cyber attacks on VoIP. *Voprosy kiberbezopasnosti*, 2023, vol. 2, no. 54, pp. 109–121 (in Russia).

30. Bekeneva Y. A. Analysis of DDOS-attacks topical types and protection methods against them. *Proceedings of Saint Petersburg Electrotechnical University*, 2016, vol. 1, pp. 7–14 (in Russia).

31. Petrov M. U., Fatkieva R. R. A model of synthesis of distributed attacking elements in a computer network. *Proceedings of Telecommunication Universities*, 2020, vol. 2, pp. 113–120 (in Russia).

32. Yazov Y. K., Burushkin A. A., Panfilov A. P. Markovs models of type «Refusal in service» network attacks realization processes. *Informacionnaya bezopasnost*, 2008, vol. 1, pp. 79–84 (in Russia).

33. Ostapenko A. G., Tishkov S. A. Investigation of the possibilities of risk management of automated systems for protection against Denial-of-service attacks. *Informacionnaya bezopasnost*, 2009, vol. 1, pp. 25–38 (in Russia).

34. Ostapenko A. G., Ermilov E. V., Kalashnikov A. O. The risk of inferiority, the chances of usefulness and viability of components of automated systems under the influence of information threats on them. *Informacionnaya bezopasnost*, 2013, vol. 2, pp. 215–218 (in Russia).

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

36. Antonatos S., Akritidis P., Markatos E., Anagnostakis K. Defending against Hitlist Worms using Network Address Space Randomization. *2005 ACM Workshop on Rapid Malcode, Fairfax*, VA, USA, 2005, pp. 30–40.

37. Tihonov V. I., Mironov M. A. *Markovskie process* [Markov processes]. Moscow, 1977. 488 p. (in Russian).

38. Ventcel E. S., Ovcharov L. A. *Teoriya sluchajnyh processov i ee inzhenernye prilozheniya* [Theory of random processes and its engineering applications]. Moscow, 1991. 384 p. (in Russian).

39. Gorbachev A. A., Sokolovskij S. P., Usatikov S. V. Functioning model and algorithm of email service proactive protection from network intelligence. *Systems of Control, Communication and Security*, 2021, vol. 3, pp. 60–109 (in Russia).

40. Nogin V. D., Protod'yakonov I. O., Evlampiev I. I. *Osnovy teorii optimizacii* [Fundamentals of optimization theory]. Moscow, 1986. 384 p. (in Russian).

41. Rastrigin L. A., Baharev A. T., Zuev A. K. *Teoriya i primenenie sluchajnogo poiska* [Theory and application of random search]. Riga, 1969. 309 p. (in Russian).

42. Gorbachev A. A. Model and parametric optimization of proactive protection of the email service from network intelligence. *Voprosy kiberbezopasnosti*, 2022, vol. 3, no. 49, pp. 69–81 (in Russia).

43. Nelder J., Mead R. A Simplex Method for Function Minimization. *Computer Journal*, 1965, pp. 308–313.

44. Kennedy J., Eberhart R. Particle Swarm Optimization. *Proceedings of IEEEE International Conference on Evolutionary Computation*, 1995, pp. 1942–1948.

45. Storn R., Price K. Differential Evolution: A simple and efficient adaptive scheme for global optimization over continuous spaces. *Journal of Global Optimization*, 1995, pp. 1–15.

46. Sokolovsky S. P., Gorbachev A. A. Method for proactive protection of mail server from unsolicited emails. *Enginery Problems. Series16. Anti-Terrorist Engineering Means*, 2021, vol. 3-4, no. 154-154, pp. 31–40 (in Russia).

47. Maximov R. V., Sokolovsky S. P., Telenga A. P. Honeypots network traffic parameters modeling. SEUR Workshop Proceedings. *BIT 2021, Selected Papers XI International Scientific and Technical Conference on Secure Information Technologies*. Moscow, 2021. pp. 229–239.

48. Lebedkina T. V. Algorithm for proactive protection of file exchange information systems from network reconnaissance. *Enginery Problems. Series 16. Anti-Terrorist Engineering Means*, 2021, vol. 11-12, no. 161-162, pp. 93–101 (in Russia).

Статья поступила 15 мая 2023 г.

Информация об авторе

Москвин Артём Александрович – соискатель ученой степени кандидата технических наук. Адъюнкт. Краснодарское высшее военное училище им. генерала армии С.М. Штеменко. Область научных интересов: обеспечение информационной безопасности; синтез и системный анализ систем защиты информации критически важных объектов; маскирование информационных ресурсов интегрированных ведомственных сетей связи. E–mail: tema.kg9012@gmail.com

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

Algorithm of multiaddress network connection configuration under conditions of computer intelligence

A. A. Moskvin

Problem statement: *despite the usage of information security measures, the threats of computer attacks on computer networks remain relevant. One of the methods applied for preventing such threats is the concealment of real IP-addresses of the computer network's nodes through their dynamic changes. However, the usage of such measures lowers the network nodes' availability for legitimate users because traditionally used TCP/UPD transport layer protocols have known limitations, which do not ensure continuous and secure data transmission. These limitations can be removed by application of the SCTP transport layer protocol, which can keep a set of previously defined IP-addresses within the established connection.* ***The purpose of the work*** *is to develop the algorithm, which allows improving the availability and safety of the computer network's nodes when dynamically changing its IP-addresses by using the optimal parameters of the multiaddress network connection configuration.* ***Methods used:*** *in this paper the study of stochastic processes methods and the methods of multi-criteria optimization problems solutions are used.* ***Novelty:*** *The novelty of the presented algorithm is the application of the multiaddress network connection configuration model based on the mathematical apparatus of Markovian processes with discrete states and continuous time; and also the problem statement and multi-criteria optimization solution by application of the ideal point method and the Nelder-Mead algorithm.* ***Results:*** *calculations show the improvement in availability and safety of the network nodes when the optimal parameters of the multiaddress network connection with dynamically changing IP-addresses are applied.* ***Practical significance*** *is to improve computer networks' nodes safety by reducing the computer intelligence's ability to detect real IP-addresses with the simultaneous availability improvement by applying optimal parameters of the multiaddress network connection configuration.*

Keywords: *network intelligence, multiaddress network connection, multi-criteria optimization, availability and safety improvement.*

Information about Author

Artem Alexandrovich Moskvin – post graduate student. Krasnodar Higher Military School named after General of the Army S.M. Shtemenko. Research interests: information security; synthesis and system analysis of information security systems of critical objects; masking and simulation of information resources of integrated departmental communication networks. E–mail: tema.kg9012@gmail.com

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