# МОДЕЛЬ И МЕТОДИКА МАСКИРОВАНИЯ АДРЕСАЦИИ КОРРЕСПОНДЕНТОВ В КИБЕРПРОСТРАНСТВЕ

*Кучуров В.В.[1], Максимов Р.В.[2], Шерстобитов Р.С.[3]*

***Аннотация.*** *Формулируя требования по защите информации, регуляторы предписывают необходимость противодействовать угрозам безопасности информации, нацеленным на вскрытие структурно-функциональных характеристик информационной системы. В их числе – структура и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи между сегментами информационной системы, применяемые информационные технологии и особенности их функционирования. В качестве основных мер по защите предлагают эмуляцию ложных компонентов информационных систем, скрытие истинных информационных технологий, управление конфигурацией информационной системы и перевод ее в заранее определенную конфигурацию, обеспечивающую защиту. Однако по ряду причин такие меры не включают в базовый набор и реализуют достижение целей защиты компенсирующими средствами, формализуя и внедряя запрещающие регламенты, а также набор организационных и технических мер воздействия на источник опасности.*

***Цель исследования*** *– вскрыть и сформулировать основные направления поиска новых технических решений для маскирования структуры распределенных информационных систем в киберпространстве, реализуя маскирующий трафик с учетом требований к своевременности информационного обмена.*

***Метод исследования*** *– исследование операций в условиях неопределенности, применение теории марковских случайных процессов и решение уравнений Колмогорова для решения задачи повышения эффективности маскирующего обмена.*

***Результат исследования*** *– нахождение вероятностных и временных характеристик процесса функционирования сети передачи данных при применении технических решений по маскированию информационных систем в киберпространстве. Полученные результаты позволяют явно реализовывать меры защиты, направленные на формирование у нарушителей устойчивых ложных стереотипов об информационных системах и процессах управления, реализуемых с их помощью.*

***Ключевые слова:*** *moving target defense, компьютерная разведка, информационные направления, маскирование сетевых адресов, марковские процессы, маскирующий обмен.*

**DOI:**10.21681/2311-3456-2020-06-2-13

## Введение

Под термином «киберпространство» авторами принято определение, редуцированное из приведенного в [1]. Киберпространство – это виртуальная сетевая среда, сформированная в результате действий пользователей, программ и сервисов в сети связи общего пользования (ССОП) посредством сетей передачи данных, коммуникационных технологий и информационных систем. Информационные системы (ИС) – это совокупность территориально распределенных сегментов средств обработки информации, объединенных сетями передачи данных, с использованием коммуникационных технологий через ССОП с целью предоставления пользователям информационных ресурсов (программ и сервисов). Как правило, каждая локализованная (топологически) ИС функционирует в интересах конкретного органа управления, являющегося элементом иерархичной системы управления.

В ведомственных ИС кибербезопасность и защита киберпространства реализуется как набор мер и рекомендаций регуляторов[4,5,6]. В значимых ИС объектами, подлежащими защите от угроз безопасности информации[7], являются архитектура и конфигурация ИС (равно

4 Приказ ФСТЭК от 15.02.2017 г. № 27

5 Методический документ ФСТЭК «Меры защиты информации в государственных информационных системах» от 11.02.2014 г.

6 Приказ ФСТЭК от 25.12.2017 г. № 239

7 Банк данных угроз безопасности информации ФСТЭК России. URL: https://bdu.fstec.ru/threat

1 Кучуров Вадим Валерьевич, адъюнкт кафедры защищенных информационных технологий Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменного училища имени генерала армии С.М. Штеменко, г. Краснодар, Россия. E-mail: kuchurovv@yandex.ru

2 Максимов Роман Викторович, доктор технических наук, профессор, профессор кафедры защищенных информационных технологий Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменного училища имени генерала армии С.М. Штеменко, г. Краснодар, Россия. E-mail: rvmaxim@yandex.ru

3 Шерстобитов Роман Сергеевич, кандидат технических наук, старший преподаватель кафедры защищенных информационных технологий высшего военного орденов Жукова и Октябрьской Революции Краснознаменного училища имени генерала армии С.М. Штеменко, г. Краснодар, Россия. E-mail: scherstobitov.rs@yandex.ru

как и архитектура и конфигурация информационно-телекоммуникационной сети, АСУ):

- сокрытие архитектуры и конфигурации ИС;
- воспроизведение ложных и (или) скрытие истинных отдельных информационных технологий и (или) структурно-функциональных характеристик ИС или ее сегментов, обеспечивающее навязывание у нарушителя ложного представления об истинных информационных технологях и (или) структурно-функциональных характеристиках ИС.

По результатам анализа защищенности должно быть подтверждено, что в ИС отсутствуют уязвимости, способствующие возможности реконструкции (вскрытия) нарушителем архитектуры и конфигурации ИС.

Наряду с угрозами безопасности информации, связанными с диалоговым взаимодействием (сканированием) нарушителя и ИС (см., например, УБИ. 098, 099, 103, 132), на реконструкцию структурно-функциональных характеристик ИС нацелена угроза определения топологии ИС (УБИ. 104). Если реакцией на запросы нарушителя может быть блокирование информации или передача ложной информации, то анализ сетевого трафика может осуществляться бескомпроматно, а его результат – вскрытие топологии распределенной в киберпространстве ИС, определение важности ее узлов – может быть использован нарушителем для реализации спланированных *APT*-атак (от англ. *advanced persistent threat* – «развитая устойчивая угроза»).

При реализации мероприятий реконструкции архитектуры и конфигурации (вскрытия структурно-функциональных характеристик) ИС нарушитель стремится распределить ограниченный неоднородный ресурс средств разведки для вскрытия иерархии системы управления с требуемой полнотой, своевременностью и достоверностью. Нарушителю целесообразно осуществлять преднамеренные деструктивные воздействия на наиболее важные элементы ИС, сконцентрировав на них все усилия, а воздействия на второстепенные осуществлять при наличии свободного ресурса.

**Физическая постановка задачи**

Наилучшая стратегия защиты – формировать у нарушителя ложное (неверное) представление о схеме информационных направлений (структуре (топологии) и параметрах (типологии)) ИС и, как неизбежное следствие, структуре системы управления, в интересах которой функционирует распределенная ИС. Это позволяет влиять на качество решений, принимаемых нарушителем по результатам разведки, предотвращать деструктивные воздействия на объекты защиты или снижать их результативность и эффективность.

Такая стратегия может быть реализована посредством маскирования адресации корреспондентов и осуществления маскирующего обмена между топологически локализованными элементами (сегментами) распределенной ИС.

Маскирование адресной информации корреспондентов – это ее сокрытие путем трансляции (*NAT*, от англ. *Network Address Translation* – «преобразование сетевых адресов») истинных адресов элементов ИС и сети передачи данных (СПД), расширения адресного пространства элементов СПД (увеличение их количества) и введение ложных (маскирующих) элементов в киберпространство.

Маскирующий обмен – это упорядоченная по структуре и интенсивности совокупность ложных (маскирующих) пакетов сообщений, формируемых сетевыми информационными объектами (СИО) с целью управления демаскирующими признаками (ДМП) алгоритмов функционирования ИС и СПД, изменяющих видимую интенсивность информационного обмена между элементами СПД [2].

Основные ДМП алгоритмов функционирования ИС и СПД – это интенсивность трафика между топологически локализованными элементами (сегментами) распределенной ИС, сетевые протоколы взаимодействия и иерархические уровни (ранги) элементов ИС [3].

При использовании *NAT* интенсивность информационного обмена элементов СПД увеличивается за счет группировки и инкапсуляции пакетов сообщений, содержащих именные ДМП. При использовании способов расширения адресного пространства и введения ложных (маскирующих) элементов СПД интенсивность снижается соразмерно количеству дополнительных адресов и информационных направлений, используемых ими. Маскирующий обмен позволяет скрыть факт передачи конструктивного трафика и исказить (в частности – повысить) уровень иерархии («оперативно-тактическую принадлежность») соответствующих элементов ИС и СПД посредством управления ДМП алгоритмов функционирования ИС и СПД.

Совместное использование способов трансляции, расширения адресного пространства и маскирующего обмена позволяет управлять информативностью ДМП алгоритмов функционирования ИС и СПД для решения задач защиты архитектуры и конфигурации ИС. Такой подход нашел свою реализацию в динамическом изменении параметров сети (*dynamic network*) в рамках концепции *Moving Target Defense* (*MTD*) [4]. В концепции предполается замена статических параметров ИС динамическими, в результате чего нарушитель не может получить актуальную информацию, позволяющую реализовать *APT*-атаки. А защита ИС основывается не на обнаружении, а на предотвращении преднамеренных деструктивных воздействий.

Ассортимент отечественных *MTD*-решений рассмотрен в [4, 5]. В результате их применения сетевые идентификаторы (*IP*- и *MAC*-адреса) корреспондентов нельзя поставить в соответствие конкретному СИО защищаемой ИС, что снижает возможности нарушителя по реконструкции структуры ИС и *APT*-атакам на ее элементы. Реализуемая в СПД ложная структура, характеризуется совокупностью маскированных информационных направлений (передают конструктивный трафик) и маскирующих информационных направлений (передают маскирующий трафик). Ложная структура поддерживается с помощью генерации произвольного трафика, объем которого уменьшают пропорционально увеличению объема конструктивного трафика, при этом рассчитывают степень утилизации каждого маскирую-

щего ИН [2]. При изменении оперативной обстановки в рамках динамического изменения параметров сети применяют методы киберманеврирования (*cyber maneuvering*) [6], которые заключаются в адаптации ложной структуры ИС к изменившейся обстановке (условиям функционирования ИС и задачам «обмана»).

Основное технологическое препятствие для реализации маскирующего обмена – ограничения на производительность СИО и скорость передачи данных по каналам связи. Однако ограничения, снимаемые организационными мерами, не могут считаться объективными и выступать ограничениями в научных исследованиях. В работе [2] показано, что целесообразно разделять результативность маскирующего обмена (управляемость пространства ДМП ИС и СПД, его вклад в защиту архитектуры и конфигурации ИС) и эффективность маскирующего обмена (экономические и эксплуатационные затраты на него, затраты ресурсов связи, влияние на показатели эффективности связи и т.д.).

В таблице 1 представлены основные способы управления параметрами маскирующего трафика, позволяющие снизить нагрузку на принимающего абонента. Комбинация перечисленных в таблице 1 способов даст возможность снизить информативность присущих им ДМП, повысить его эффективность (не доводить маскирующий трафик до приемника, терминируя маскирующий трафик в выбранном СИО СПД (ССОП) [7].

Однако, если по какой-либо причине маскирующие пакеты сообщений не будут уничтожаться в СПД, а будут ретранслироваться абоненту-получателю, то они создадут на его входе нагрузку, ухудшая значение показателя своевременности информационного обмена (своевременность доставки сообщений).

Отказ терминации маскирующего трафика может происходить по следующим причинам:

- сбои функционирования СПД вследствие воздействия непреднамеренных помех;
- преднамеренные деструктивные воздействия на СПД (узлы ССОП);
- сбои и ошибки установления значений *MTU* узлом-отправителем;
- маршрутизация пакетов оператором ССОП по альтернативному маршруту;
- изменение параметров и структуры ССОП;
- изменение значений параметров безопасности маршрутов связи;
- изменение ИС (структуры системы управления), которую реализует СПД.

Помехи – возмущения, снижающие качество СПД: скорость передачи данных по каналам связи и доступность элементов СПД и ССОП посредством создания дополнительной (нештатной) нагрузки на процессы и устройства их реализующие.

Преднамеренные деструктивные воздействия – процесс воздействия помех (в частности, компьютерных атак), осуществляемый путем организации и реализации процедурного или декларативного воздействия источника помех (в частности, нарушителя) на элементы СПД и ССОП, которым присущи НДВ, уязвимости и открытость архитектуры.

Таким образом, возникает противоречие между расчетной (требуемой) результативностью маскирования адресации корреспондентов в киберпространстве при реализации маскирующего обмена в СПД и его эффективностью, так как к СПД справедливо предъявляют приоритетные требования по своевременности информационного обмена конструктивным трафиком между абонентами. В рамках устранения этого противоречия и получены новые научные результаты.

### Формализованная постановка задачи на моделирование оценки эффективности маскирующего обмена

Срателия защиты при реализации маскирующего обмена должна заключаться в оптимальном распределении ресурса СПД ВН для обеспечения своевременности информационного обмена (доставки сообщений) с учетом приоритетов корреспондентов (видов трафи-

Таблица 1

Способы управления параметрами маскирующего трафика

| Суть способа | Недостатки | Достоинства |
|---|---|---|
| Установка меток в маскирующих пакетах сообщений | Нагрузка на СИО | Реализуется без дополнительных технических решений |
| Фрагментация маскирующих сообщений перед передачей в СПД и уничтожение одного из фрагментов | Нагрузка на СИО | Реализуется без дополнительных технических решений |
| Трассировка маршрута *IP*-пакетов и установление значений *TTL* (*Time To Live*) и *Hop Limit* (для *IPv6*) | Прямой ДМП в заголовке и косвенный ДМП по протоколу *ICMP*, низкая результативность | Используют технологии ССОП. Исключают нагрузку на приемник. |
| Использование *Path MTU discovery*, установление относительно большого значения *MTU* и значения флага *DF* (*Do Not Fragment*) в «1» | Прямой ДМП в заголовке IPv4, косвенный ДМП по протоколу *ICMP*, *MTU Discovery Black Hole* | |
| Согласование с приемником значения *Maximum segment size* для маскирующего трафика и управление значением *MTU* | Косвенный ДМП по протоколу *ICMP* | |

ка), предотвращения задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом. При этом производительность СИО и предельная скорость передачи данных в СПД (пропускная способность каналов связи) выступают в качестве очевидных ограничений.

Своевременность информационного обмена $K_{IE}$ (от англ. (*information*) *exchange* – обмен) определяют [8] через показатели своевременности обработки $K_{Proc}$ (от англ. *processing* – обработка) и своевременности доставки $K_{Del}$ (от англ. *delivery* – доставка) следующими соотношениями:

$$K_{Proc} = P\left(T_{Proc} \le T_{Proc}^{Req}\right) \quad (1)$$

$$K_{Del} = P\left(T_{Del} \le T_{Del}^{Req}\right) \quad (2)$$

$$K_{IE} = K_{Del} \cdot K_{Proc} \quad (3)$$

Время обработки $T_{Proc}$ и время доставки $T_{Del}$ являются контекстно-зависимыми величинами, то есть требуют достаточно точно определять состав канала (каналов) связи СПД, конкретизировать функции СИО и процессов обработки (доставки) относительно уровней ЭМВОС. Так, например, процессы фрагментации (дефрагментации) пакетов сообщений могут осуществляться не только на конечных СИО, но и на транзитных, и не связаны с содержательной обработкой информации.

В работах [2, 7] решены задачи снятия следующих технических ограничений:

- возникающие в связи с формированием у передающего СИО очереди из конструктивных пакетов сообщений (КПС) устраняют за счет динамического изменения длины маскирующих пакетов сообщений (МПС) и, как следствие, уменьшения времени ожидания конструктивных в очереди;
- возникающие в связи с поступлением на вход принимающего СИО одновременно пакетов сообщений от нескольких отправителей очереди из КПС и МПС устраняют за счет выбора для каждого маскирующего маршрута связи узлов-терминаторов МПС, что позволит исключить потерю КПС и необходимость их повторной передачи, что улучшит значение показателя своевременности доставки сообщений.

Тогда коэффициент эффективности маскирующего обмена в *i*-ом информационном направлении:

$$K_i^{Ef} = \frac{\bar{T}_{IE}^{AT} - \bar{T}_{IE}^{CT}}{\bar{T}_{IE}^{AT}}, \quad (4)$$

где $\bar{T}_{IE}^{AT}$ – среднее время информационного обмена общим (от англ. *aggregate* – общий) трафиком (конструктивным и маскирующим); $\bar{T}_{IE}^{CT}$ – среднее время информационного обмена конструктивным (от англ. *constructive* – конструктивный) трафиком при ограничении МПС узлами-терминаторами.

Своевременность информационного обмена можно выразить и минимизацией среднего времени нахождения элемента СПД ВН в состоянии с низкой доступностью услуг абонентам, $\bar{T}_B \to \min$ (от англ. *break* – перерыв), когда в СПД возникают очереди на обслуживание КПС и МПС. Воздействие на СИО (элемент СПД) случайных и преднамеренных помех создает дополнительную (нештатную) нагрузку на процессы связи и устройства, их реализующие. В результате воздействия случайных и преднамеренных помех $\bar{T}_B$ – длительность промежутка времени, когда абонентам недоступны от СПД услуги с требуемым качеством (среднее время простоя) – увеличивается, а доступность СПД ВН и своевременность $K_{IE}$ информационного обмена – ухудшаются.

Моменты возможных переходов СПД из состояния в состояние неопределенны и случайны. Рассмотрим переход от детерминированной постановки задачи к постановке задачи в условиях неопределенности. Тогда финальную вероятность того или иного состояния $S_i$ СПД ВН можно будет интерпретировать как среднее относительное время пребывания системы в этом состоянии.

Дано:

пусть *CP* – множество входных параметров модели μ СПД *S*, параметры контроля соединения (от англ. *Connection Parameters*) $CP \subseteq \left\{N_T, I^{AT}, I^{CT}, I^{MT}\right\}$, где $N_T$ – узел-терминатор МПС (от англ. *Node* – узел, *Terminator* – оконечное устройство); $I^{AT}$, $I^{CT}$, $I^{MT}$ – расчетная интенсивность общего трафика, конструктивного трафика, маскирующего трафика (от англ. *Intensity* – интенсивность);

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

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

*SIT* – множество параметров условий функционирования (ситуаций), поддерживаемых моделируемой системой, $SIT \subseteq \left\{I^{OT}, I^{FT}\right\}$, где $I^{OT}$ – моделируемая интенсивность конструктивного трафика от других источников (от англ. *other* – другой, дополнительный); $I^{FT}$ – моделируемая интенсивность отказов узла-терминатора (от англ. *failure* – отказ), выражаемая, например, через коэффициент $I^{FT} = \lambda_{57} / \lambda_{45}$;

*Q* – показатель эффективности функционирования СПД, $Q = \lim_{t\to\infty} P^{K_{IE}}(t)$, $P^{K_{IE}}(t) \to \max$, определяемый своевременностью информационного обмена.

Тогда содержательная постановка задачи на моделирование оценки эффективности маскирующего обмена в СПД при маскировании адресации корреспондентов в киберпространстве: разработать модель μ СПД *S*, устанавливающую закономерность изменения множества $P_i$ выходных параметров модели функционирования СПД и множества *Q* показателей эффективности функционирования СПД от множества *CP* значений входных параметров, множества *Z* значений внутренних параметров, множества *SIT* значений параметров условий функционирования. На значения параметров множеств *CP*, $P_i$, *Z*, *SIT* наложены условия их допустимости.

DOI:10.21681/2311-3456-2020-06-2-13

Тогда формальная постановка задачи на моделирование оценки эффективности маскирующего обмена в СПД при маскировании адресации корреспондентов в киберпространстве:

$$\mu : \langle S, CP, Z, SIT \rangle \to P_i$$
$$Q \left| CP \subseteq \left\{ N_T, I^{AT}, I^{CT}, I^{MT} \right\} \right. , \qquad (5)$$
$$P_i = \lim_{t \to \infty} P_i(t), SIT \subseteq \left\{ I^{OT}, I^{FT} \right\}$$

а формальная постановка задачи на оптимизацию показателей эффективности маскируемой СПД (по критерию максимизации своевременности информационного обмена):

$< S, CP, Z, SIT > \to \max P^{K_{IE}}(t) \mid P^{K_{IE}} \in \{P_i\}$,
$i = 1, 2, ..., h$ (6)

Потоки событий переводят модель μ СПД S в состояния своевременного или несвоевременного информационного обмена КПС, позволяя исследовать вероятностно-временные характеристики процессов маскирующего обмена в киберпространстве.

### Модель оценки эффективности маскирующего обмена в киберпространстве

Пусть имеется СПД ВН S, в которой реализуют маскирование адресации корреспондентов и осуществление маскирующего обмена между топологически локализованными элементами (сегментами) распределенной ИС.

Система S с течением времени меняет свое состояние (переходит из одного состояния в другое). Физически она включает в себя корреспондирующих абонентов, источники и приемники конструктивного и маскирующего трафика (СИО), средства трансляции (NAT) и расширения адресного пространства (маскираторы) СПД [9, 10], транзитные СИО СПД ССОП, узлы-терминаторы маскирующего трафика.

От передающих абонентов в СПД и далее в ССОП поступает поток событий (заявок, требований) с интенсивностью λ, потенциально переводящих модель μ СПД S в состояния, когда обеспечивается или не обеспечивается своевременность информационного обмена. Переход системы в одно из антагонистических состояний обусловливается тем, что СПД в штатных режимах функционирования справится с требуемой нагрузкой, тогда как наличие маскирующего трафика на входе приемника может создавать очереди на обработку, особенно при росте трафика от нескольких источников. Отказ терминации маскирующего трафика может происходить под воздействием непреднамеренных помех и преднамеренных деструктивных воздействий.

Примем следующие необходимые для исследования дискретные состояния $S_1$, $S_2$, ... моделируемого процесса:

$S_1$ – формирование КПС;
$S_2$ – формирование МПС;
$S_3$ – изменение текущих *IP*-адресов элемента СПД (расширение его адресного пространства);
$S_4$ – передача КПС и МПС от отправителя к получателю;
$S_5$ – терминация МПС на транзитном СИО СПД в ССОП;
$S_6$ – своевременный прием КПС;
$S_7$ – несвоевременный прием КПС.

Моменты возможных переходов моделируемой СПД при реализации маскирующего обмена из состояния в состояние неопределенны, случайны и происходят под действием событий, характеризующиеся их интенсивностями λ (см. табл. 2).

Оценка эффективности процессов функционирования СПД ВН и маскирования адресации корреспондентов связана с необходимостью моделирования 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, процессы маскирования адресации корреспондентов при реализации маскирующего обмена можно представить, как марковский случайный процесс с дискретными состояниями и непрерывным временем.

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 $\lambda_{ij}$.

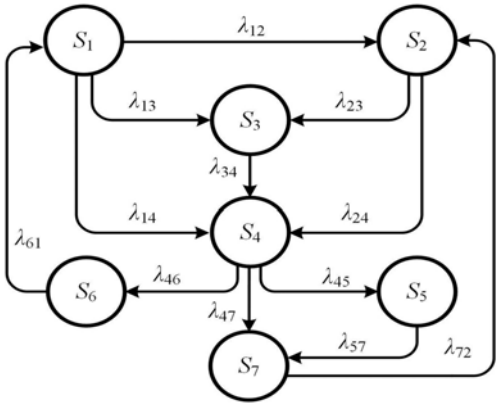


*Рис.1. Граф состояний процесса функционирования моделируемой системы*

Пусть формирование МПС происходит постоянно, чтобы скрывать факт передачи КПС, тогда $S_2$ – начальное состояние моделируемой системы. Это состояние обеспечивает результативность маскирования, интенсивность которого определяется для каждого информационного направления по модели, изложенной в [2], и является искомым с позиций обеспечения результативности [11, 12] маскирования (то есть интенсивность $\lambda_{23}$ ($\lambda_{24}$) такова, что требования по интенсивности маскирующего обмена выполняются).

Формирование КПС приведет к прерыванию формирования маскирующих ($\lambda_{12}$). Переход из $S_1$ в $S_2$ озна-

Таблица 2

Интенсивности потоков событий

| Интенсивность | Обозначение |
|---|---|
| Заявки на прерывание формирования МПС в связи с формированием КПС | $\lambda_{12}$ |
| Заявки на изменение текущих *IP*-адресов (расширение адресного пространства) КПС | $\lambda_{13}$ |
| Заявки на изменение текущих *IP*-адресов (расширение адресного пространства) МПС | $\lambda_{23}$ |
| Заявки на передачу КПС получателю без расширения адресного пространства (КПС и МПС используют один адрес отправителя) | $\lambda_{14}$ |
| Заявки на передачу МПС получателю без расширения адресного пространства (КПС и МПС используют один адрес отправителя) | $\lambda_{24}$ |
| Заявки на передачу КПС и МПС получателю с расширением адресного пространства (КПС и МПС используют множество адресов отправителя) | $\lambda_{34}$ |
| Заявки на терминацию МПС на узле-терминаторе | $\lambda_{45}$ |
| Заявки на безусловное обслуживание КПС у получателя | $\lambda_{46}$ |
| Заявки на совместное с МПС обслуживание КПС у получателя | $\lambda_{47}$ |
| Заявки на совместное с КПС обслуживание МПС у получателя, вызванные отказом терминации (узла-терминатора) | $\lambda_{57}$ |
| Квитирование, заявки на увеличение скорости передачи данных КПС вследствие своевременного приема КПС | $\lambda_{61}$ |
| Заявки на уменьшение скорости передачи данных МПС вследствие отказа терминации, возникновения очередей из КПС и МПС у получателя | $\lambda_{72}$ |

чает момент окончания формирования конструктивных и начала формирования МПС. После формирования конструктивных (маскирующих) в их заголовки включают (используя *NAT*) текущие адреса отправителя и получателя. В состоянии $S_3$ осуществляют расширение адресного пространства корреспондента (СИО) маскиратором, изменяя текущие *IP*-адреса отправителя и получателя КПС (МПС) под воздействием заявок $\lambda_{13}$ и $\lambda_{23}$ (если необходимо расширение адресного пространства – вариация, снижение информативности ДМП – корреспондентов). В состоянии $S_4$ осуществляется передача КПС и МПС от отправителя к получателю. Переход в состояние $S_4$ происходит не только из состояния расширенного адресного пространства ($\lambda_{34}$), но и в тех случаях, когда расширение адресного пространства по конструктивному ($\lambda_{13}$) или маскирующему ($\lambda_{23}$) трафику не происходит ($\lambda_{14}$ и $\lambda_{24}$). Терминацию МПС осуществляют в состоянии $S_5$. И в случае успешной терминации система переходит в состояние $S_6$ под воздействием потоков событий $\lambda_{46}$. В противном случае, то есть при отказе узла-терминатора, система переходит в состояние $S_7$ под воздействием потоков событий $\lambda_{47}$ и $\lambda_{57}$. В случае своевременного приема КПС, система может инициировать заявки на увеличение скорости передачи КПС ($\lambda_{61}$). В противном случае, то есть при несвоевременном приеме, система инициирует заявки на уменьшение скорости передачи МПС ($\lambda_{72}$).

Моделируемая СПД может находиться в состояниях $S_i$ с разной вероятностью $p_i(t)$. По размеченному графу состояний рис.1 составлены уравнения Колмогорова – дифференциальные уравнения с неизвестными функциями $p_i(t)$:

$$\left.\begin{aligned}
\frac{dp_1(t)}{dt} &= \lambda_{61}p_6(t) - \lambda_{12}p_1(t) - \lambda_{13}p_1(t) - \lambda_{14}p_1(t),\\
\frac{dp_2(t)}{dt} &= \lambda_{12}p_1(t) + \lambda_{72}p_7(t) - \lambda_{23}p_2(t) - \lambda_{24}p_2(t),\\
\frac{dp_3(t)}{dt} &= \lambda_{13}p_1(t) + \lambda_{23}p_2(t) - \lambda_{34}p_3(t),\\
\frac{dp_4(t)}{dt} &= \lambda_{14}p_1(t) + \lambda_{24}p_2(t) + \lambda_{34}p_3(t) - (\lambda_{45} + \lambda_{46} + \lambda_{47})p_4(t),\\
\frac{dp_5(t)}{dt} &= \lambda_{45}p_4(t) - \lambda_{57}p_5(t),\\
\frac{dp_6(t)}{dt} &= \lambda_{46}p_4(t) - \lambda_{61}p_6(t),\\
\frac{dp_7(t)}{dt} &= \lambda_{47}p_4(t) + \lambda_{57}p_5(t) - \lambda_{72}p_7(t),\\
\sum_{i=1}^{7} p_i(t) &= 1.
\end{aligned}\right\} \quad (7)$$

Вектор вероятностей начальных состояний марковской цепи с учетом отсутствия воздействий на СПД в начальный момент времени имеет вид:

$$p(0) = |0\ 1\ 0\ 0\ 0\ 0\ 0|, \quad (8)$$

что соответствует формированию МПС.

Задавая численные значения интенсивностей λ в соответствии с условиями функционирования ИС и СПД в киберпространстве (ситуациями *SIT*) и переходя к непрерывному времени, решается система линейных дифференциальных уравнений (7) с постоянными коэффициентами. Для решения уравнений численным методом очевидным является классический метод четвертого по-

Таблица 3

Вариация параметров модели в зависимости от условий функционирования СПД

| Признаки | Ситуации | | | |
|---|---|---|---|---|
| | $SIT_1$ | $SIT_2$ | $SIT_3$ | $SIT_4$ |
| Наличие КПС | const | – | const | const |
| Наличие МПС | – | max | max | max |
| Наличие КПС от других источников | max | const | const | const |
| Терминация МПС | – | min | min | max |

рядка – метод Рунге-Кутты с фиксированным шагом интегрирования. Применение модели заключается в вариации интенсивностей в пределах устойчивости уравнений, при этом контрастны следующие четыре ситуации SIT1 – SIT4 (см. таблицу 3).

**Ситуация $SIT_1$.** Формирование, передача и прием только КПС: $\lambda_{14}$ = const, $\lambda_{12}$=min, $\lambda_{34}$=min, $\lambda_{47}$=min, $\lambda_{13}$ = min ($\lambda_{13}$ и $\lambda_{14}$ – антагонисты, т.к. или варьируем текущие адреса элемента СПД, или нет). Если МПС не формируются, то $\lambda_{23}$=$\lambda_{24}$= min. Тогда поток КПС к приемнику $\lambda_{14}$=$\lambda_{46}$=$\lambda_{61}$=const. $\lambda_{45}$=$\lambda_{57}$ интерпретируется как КПС других источников. Ситуация позволяет исследовать СПД без нагрузки источника МПС и найти максимальную скорость передачи. При вариации $\lambda_{45}$ ($\lambda_{57}$) исследуют обеспечение своевременности при росте трафика от других источников.

Графики зависимостей вероятностей состояний исследуемого процесса для ситуации $SIT_1$ представлены на рис. 2.

На интервале времени [0; 0,09] СПД находится в переходном режиме функционирования, где наблюдается всплеск значений вероятности состояний $p_4(t)$ и $p_6(t)$ что соответствует нахождению СПД в состоянии передачи, приема КПС и квитирования. При $t \to \infty$ в СПД устанавливается стационарный режим, когда СПД случайным образом меняет свои состояния и ее вероятности $p_1(t)$, $p_2(t)$, ..., $p_7(t)$ уже не зависят от времени и равны финальным (предельным) вероятностям.

Аналогично производят расчеты и для остальных ситуаций. Графики зависимостей вероятностей состояний исследуемого процесса для ситуаций $SIT_2$ – $SIT_4$ представлены на рисунках 3 – 5.

**Ситуация $SIT_2$.** Формирование, передача и прием только МПС (без их терминации), конструктивные не передаются ($\lambda_{12}$=$\lambda_{13}$=$\lambda_{14}$=min). $\lambda_{23}$=min ($\lambda_{23}$ и $\lambda_{24}$ – антагонисты, т.к. или варьируем текущие адреса элемента СПД, или нет). $\lambda_{34}$=0, $\lambda_{46}$=0, $\lambda_{24}$=const. $\lambda_{57}$ и $\lambda_{47}$ интерпретируется как КПС заданной (плановой) интенсивности от других источников. $\lambda_{45}$=max (искомое). $\lambda_{61}$= min, $\lambda_{72}$=const. Ситуация позволяет исследовать СПД без нагрузки источника КПС и найти максимальную скорость передачи (см. интенсивность $\lambda_{45}$) МПС при наличии заданного трафика от других источников. При увеличении $\lambda_{45}$ находим предел обеспечения своевременности при увеличении скорости передачи МПС.

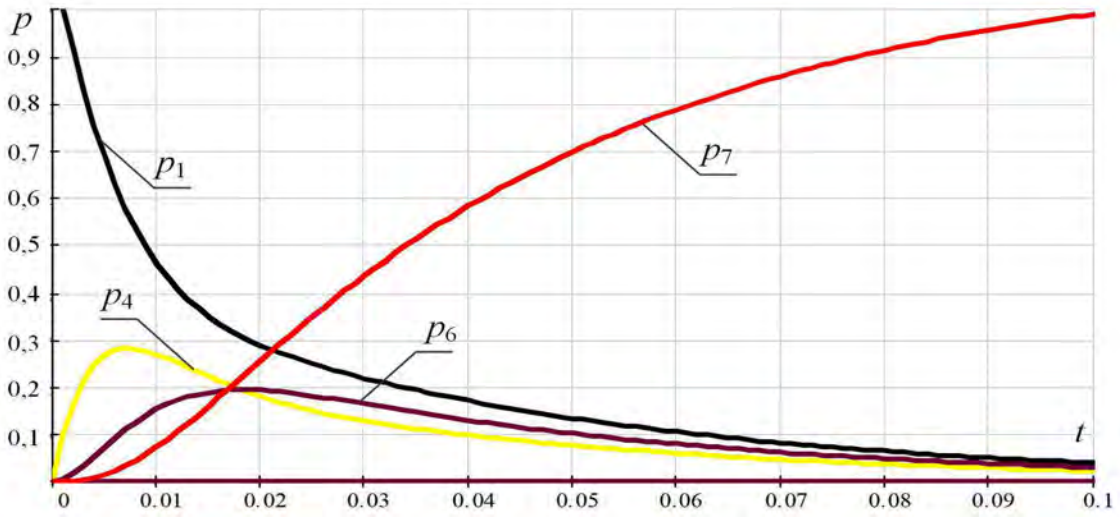


*Рис.2. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий, соответствующие ситуации $SIT_1$*

**Ситуация $SIT_3$.** Формирование, передача и прием маскирующих и КПС заданной (плановой) интенсивности. Ситуация позволяет исследовать предел обеспечения своевременности при увеличении скорости передачи МПС.

**Ситуация $SIT_4$.** Формирование, передача и прием МПС и КПС заданной (плановой) интенсивности. Ситуация позволяет исследовать предел обеспечения своевременности при увеличении скорости передачи МПС с их терминацией, предел сбоев терминации для обеспечения своевременности.

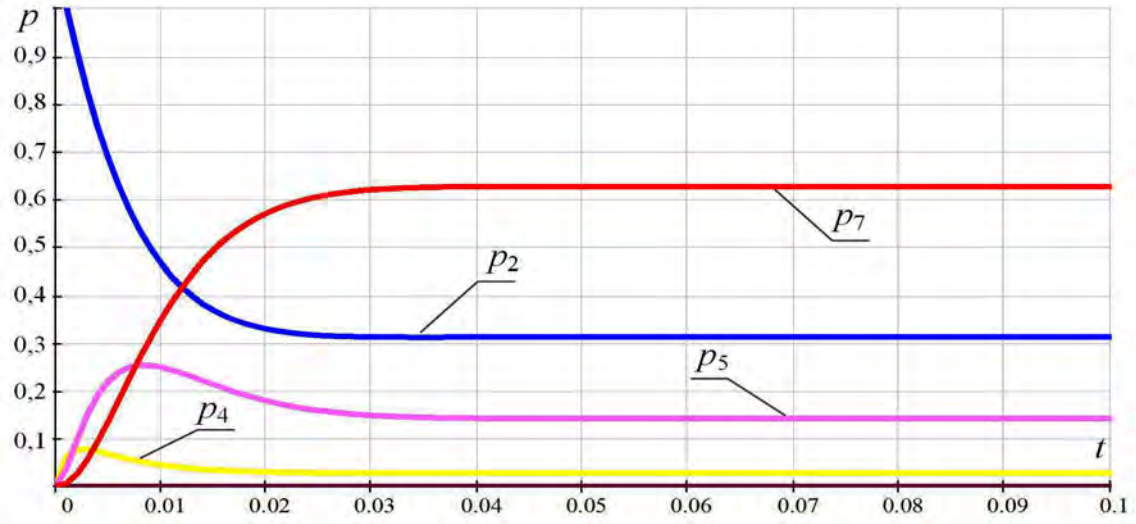


*Рис.3. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий, соответствующие ситуации $SIT_2$*

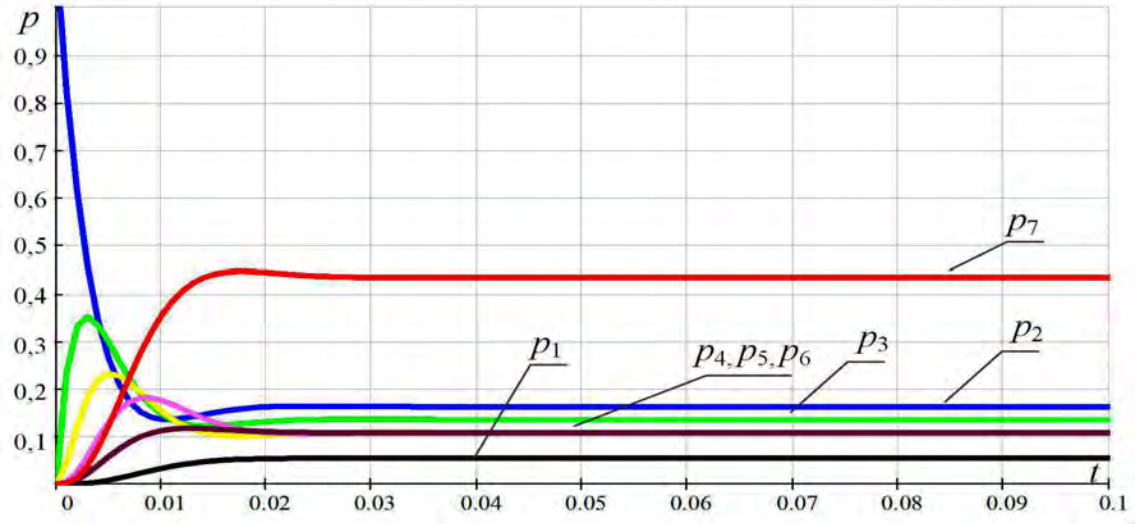


*Рис.4. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий, соответствующие ситуации $SIT_3$*

DOI:10.21681/2311-3456-2020-06-2-13

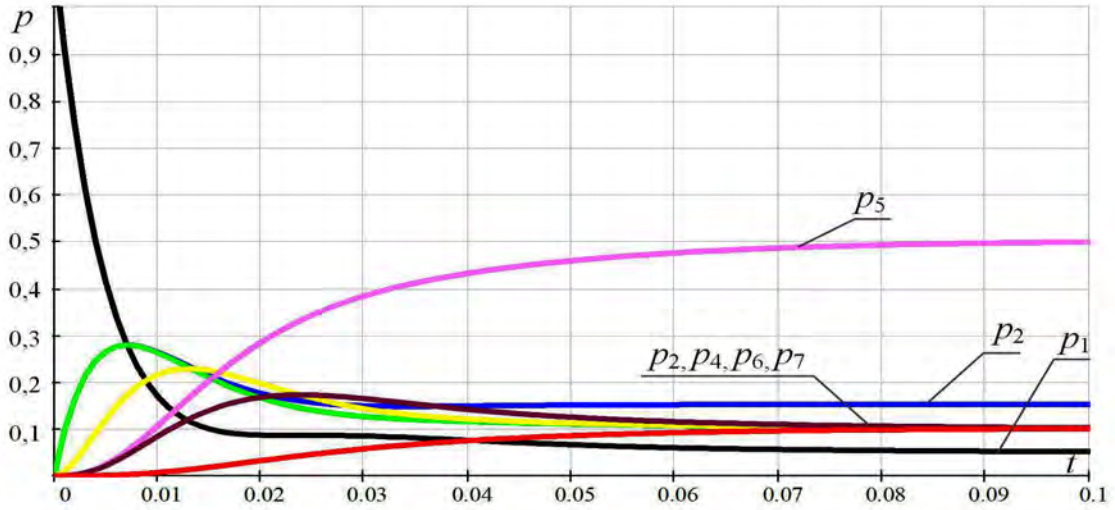


*Рис.5. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий, соответствующие ситуации $SIT_4$*

Конструктивное использование модели очевидным образом приводит к методике маскирования адресации корреспондентов в киберпространстве, в частности, при реализации ложных информационных систем [13-17]. Процесс защиты принимающего абонента (СИО) От перегрузки в соответствии с методикой сводится к максимизации $p_6(t)$ вероятности (и среднего времени) значения показателя своевременности информационного обмена $P^{K_{IE}}(t) \to \max$, что предполагает адаптивное управление [18] ложным трафиком при условии выполнения требований к результативности маскирующего обмена.

Показатель результативности маскирующего обмена (достижение целей имитации) – сходство имитируемых (ложных, навязываемых противнику) схемы СПД и структуры системы управления, выражаемое через коэффициент сходства $K_{Sim} \geq K_{Sim}^{Req}$ (от англ. *similarity* – сходство, *requirement* – требование). Такое сходство в пределе – их биекция (взаимно однозначное отображение). Вскрывая с высокой полнотой схему СПД средствами компьютерной разведки, нарушитель вскрывает ложную структуру, чем и достигается его дезинформация и устранение конфликта [19].

Возможно также задание коэффициента сходства в виде целевой функции $K_{Sim} \to \max$. Такой способ определения коэффициента сходства применим в случаях, когда определить требования к нему невозможно (нецелесообразно) и структура сети маскирующего обмена выбирается из числа альтернатив по результатам сравнения каждой альтернативы со структурой имитируемой системы управления. Или в виде целевой функции $K_{Sim} \to \min$, когда структура сети маскирующего обмена выбирается из числа альтернатив [20] по результатам сравнения каждой альтернативы со структурой истинной, маскируемой системой управления. Если обратиться к теории обфускации, которая в настоящее время применяется в области программирования (от англ. *obfuscate* – скрывать, запутывать), то критерий $K_{Sim} \to \min$ можно определить, как степень обфускации структуры СПД. С учетом того, что структурная связность элементов СПД и их количество регулируются системой защиты путем маскирования адресной информации корреспондентов и реализацией маскирующего обмена, результативность вскрытия нарушителем ложной структуры СУ можно представить следующим выражением:

$$P_{Abd}^{SysCont} = P_{NetInt}^{n} P\left(K_{Sim} \geq K_{Sim}^{Req}\right), \quad (9)$$

где $P_{Abd}^{SysCont}$ – характеристика результативности вскрытия структуры системы управления (от англ. abduction – вскрытие); $P_{NetInt}^{n}$ – характеристика полноты добытых разведданных (от англ. *network intelligence* – компьютерная разведка), где $n = 1..N$ – структурные элементы СПД, характеризующиеся ценностью для нарушителя и взаимной связностью.

Упрощенно выражение (9) можно представить в виде

$$P_{Abd}^{SysCont} \approx P\left(K_{Sim} \geq K_{Sim}^{Req}\right), \quad (10)$$

что будет означать наиболее жесткие для системы защиты условия $P_{NetInt}^{n} \to 1$, когда нарушителя можно считать внутренним, допущенным к штатным средствам ИС.

## Выводы

Представленная математическая модель оценки эффективности маскирующего обмена в киберпространстве учитывает влияние и характер воздействия на СПД информационных потоков от передающего к принимающему абоненту, фоновую нагрузку ИС, отказы системы маскирования, которые способны снизить доступность

принимающего абонента и ухудшить значение показателя своевременности информационного обмена в ИС.

Научная новизна модели заключается в применении математического аппарата теории марковских случайных процессов и решении уравнений Колмогорова для исследования и решения задачи повышения эффективности маскирующего обмена при маскировании адресации корреспондентов в киберпространстве за счет обеспечения своевременности информационного обмена конструктивными сообщениями.

Практическая значимость заключается в нахождении вероятностных и временных характеристик, описывающих состояния процесса функционирования сети передачи данных в различных условиях, которые необходимо использовать при синтезе ложных информационных систем для решения задач дезинформации нарушителя относительно архитектуры и конфигурации объектов защиты.

**Литература**


1. Марков А.С., Цирлов В.Л. Руководящие указания по кибербезопасности в контексте ISO 27032 // Вопросы кибербезопасности. 2014. № 1(2). С. 28-35.
2. Максимов Р.В., Шерстобитов Р.С., Шарифуллин С.Р. Маскирование интегрированных сетей связи ведомственного назначения [Электронный ресурс] // Системы управления, связи и безопасности. Электрон. журн. 2018. № 4. С. 136-175. Режим доступа: http://sccs.intelgr.com/archive/2018-04/08-Sherstobitov.pdf.
3. 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. 11-12 октября 2017 года. СПб.: ВАС, 2017. 358с.
4. Ворончихин И.С., Иванов И.И., Максимов Р.В., Соколовский С.П. Маскирование структуры распределенных информационных систем в киберпространстве // Вопросы кибербезопасности. 2019. № 6 (34). С. 92-101. DOI: https://doi.org/10.21681/2311-3456-2019-6-92-101.
5. Максимов Р.В., Соколовский С.П., Ворончихин И.С. Алгоритм и технические решения динамического конфигурирования клиент-серверных вычислительных сетей // Информатика и автоматизация. 2020. № 5 (19). С. 1018-1049. DOI: https://doi.org/10.15622/ia.2020.19.5.5.
6. Beraud, P., Cruz, A., Hassell, S., & Meadows, S. (2011). Using cyber maneuver to improve network resiliency. 2011 - MILCOM 2011 Military Communications Conference, 1121-1126.
7. Способ маскирования структуры сети связи. Пат. 26822105 Рос. Федерация, МПК G06F / Зайцев Д.В., Зуев О.Е., Крупенин А.В., Максимов Р.В., Починок В.В., Шарифуллин С.Р., Шерстобитов Р.С.; заявитель и патентообладатель Краснодарское высшее военное училище (RU). № 2018112925; заявл. 09.04.2018; опубл. 14.03.2019, Бюл. № 8.
8. Боговик А.В., Игнатов В.В. Эффективность систем военной связи и методы ее оценки. СПб.: ВАС, 2006. 183 с.
9. Соколовский С.П. Модель защиты информационной системы от сетевой разведки динамическим управлением ее структурно-функциональными характеристиками // Вопросы оборонной техники. Серия 16 противодействие терроризму. 2020. № 7-8. С. 62-73.
10. Соколовский С.П., Крупенин А.В., 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.
11. Марков А.С., Горшков Ю.Г., Матвеев В.А., Цирлов В.Л. Современные тренды в области кибербезопасности / Безопасные информационные технологии. Сборник трудов Седьмой всероссийской научно-технической конференции / под. ред. В.А. Матвеева. М.: МГТУ им. Н.Э. Баумана, 2016. 345 с. илл.
12. Maximov R.V., Sokolovsky S.P., Gavrilov A.L. Hiding Computer Network Proactive Security Tools Unmasking Features. In CEUR Workshop Proceedings, 2017, Vol-2081 (Selected Papers of the VIII All-Russian Scientific and Technical Conference on Secure Information Technologies, BIT 2017). P. 88-92.
13. Krupenin A., Maximov R., Sharifullin S., Sokolovsky S. Innovative Development of Tools and Technologies to Ensure the Russian Information Security and Core Protective Guidelines // Voprosy kiberbezopasnosti [Cybersecurity issue], 2019, №1 (29), pp. 10-17. DOI: 10.21681/2311-3456-2019-1-10-17.
14. Bilinski M., Gabrys R., Mauger J. Optimal Placement of Honeypots for Network Defense. In: Bushnell L., Poovendran R., Başar T. (eds) Decision and Game Theory for Security. GameSec 2018. Lecture Notes in Computer Science, vol 11199. Springer, Cham. 2018. DOI: https://doi.org/10.1007/978-3-030-01554-1_7.
15. Chee Keong NG, Lei Pan, Dr. Yang Xiang. Honeypot Frameworks and Their Applications: A New Framework. In SpringerBriefs on Cyber Security Systems and Networks. Springer, Singapore. 2018. DOI: 10.1007/978-981-10-7739-5.
16. Wang, Y., Guo, Y., Zhang, L. et al. SWIM: An Effective Method to Perceive Cyberspace Situation from Honeynet. Arabian Journal for Science and Engineering. 2018. Vol. 43. P. 6863. DOI: 10.1007/s13369-017-2904-5.
17. Вишневский А.С. Обманная система для выявления хакерских атак, основанная на анализе поведения посетителей веб-сайтов // Вопросы кибербезопасности. 2018. № 3 (27). С. 8-17. DOI: 10.21681/2311-3456-2018-3-54-62.
18. Iskolnyy B.B., Maximov R.V., Sharifullin S.R. Survivability Assessment of Distributed Information and Telecommunication Networks // Selected Papers of the VIII All-Russian Conference with International Participation «Secure Information Technologies» (BIT 2017). Bauman Moscow Technical University. December 6-7, 2017, Moscow, Russia. P. 59-65.

19. Евневич Е.Л., Фаткиева Р.Р. Моделирование информационных процессов в условиях конфликтов // Вопросы кибербезопасности. 2020. № 2 (36). С. 92-101. DOI: 10.21681/2311-3456-2020-2-42-49.
20. Кубарев А.В., Лапсарь А.П., Федорова Я.В. Повышение безопасности эксплуатации значимых объектов критической инфраструктуры с использованием параметрических моделей эволюции // Вопросы кибербезопасности. 2020. № 1 (35). С. 8-17. DOI: /10.21681/2311-3456-2020-01-08-17.

# MODEL AND TECHNIQUE FOR ABONENT ADDRESS MASKING IN CYBERSPACE

*Kuchurov V.V.[8], Maximov R.V.[9], Sherstobitov R.S.[10]*

***Abstract.***

*Regulators charge to counter information security threats against the structural and functional characteristics of the information system to ensure the information security requirements. These requirements include information system structure and composition, information technologies and functioning characteristics, physical and logical, functional and technological interconnections between information system segments. They order false components of information system emulation as a basic step of protection, as well as information technologies hiding, information system configuration management and its switching to predetermined configuration that provides a protection. However that steps are not included into basic set and they protection aims are reached with compensative assets, formalizing and implementing inhibitory orders and set of organizational and technical measures on threat source.*

*The **purpose** of research – to disclose and to state main ways of search of new technical solutions for structure masking of distributed information systems in cyberspace implementing masking traffic taking into account the requirements for the timeliness of information exchange.*

*The **method** of research – operations research in the face of uncertainty, the application of the theory of Markov processes and Kolmogorov equation for solving the problem of increasing the efficiency of masking exchange.*

*The **result** of research – finding the probabilistic and temporal characteristics of the functioning process of the data transmission network when applying technical solutions for information systems masking in cyberspace. The results obtained make it possible to explicitly implement protection measures aimed at forming persistent false stereotypes among violators about information systems and control processes implemented with their help.*

***Keywords:*** *moving target defense, computer reconnaissance, information directions, network address masking, Markov processes, masked exchange.*

## References

1. Markov A.S., Cirlov V.L. Rukovodyashchie ukazaniya po kiberbezopasnosti v kontekste ISO 27032 // Voprosy kiberbezopasnosti. – 2014. – № 1(2). – S. 28-35.
2. Maximov R.V., Sherstobitov R.S., Sharifullin S.R. Maskirovanie integrirovannyh setej svyazi vedomstvennogo naznacheniya [Elektronnyj resurs] // Sistemy upravleniya, svyazi i bezopasnosti. – Elektron. zhurn. – 2018. – № 4. – S. 136-175. – Rezhim dostupa : http://sccs.intelgr.com/archive/2018-04/08-Sherstobitov.pdf.
3. Ivanov I.I., Maximov R.V. Etyudy tekhnologii maskirovaniya funkcional'no-logicheskoj struktury informacionnyh sistem / Innovacionnaya deyatel'nost' v Vooruzhennyh Silah Rossijskoj Federacii: Trudy vsearmejskoj nauchno-prakticheskoj konferencii. 11-12 oktyabrya 2017 goda. – SPb.: VAS, 2017 – 358s.
4. Voronchixin I.S., Ivanov I.I., Maksimov R.V., Sokolovskij S.P. Maskirovanie struktury` raspredelenny`x informacionny`x sistem v kiberprostranstve // Voprosy` kiberbezopasnosti. – 2019. № 6 (34). – S. 92-101. DOI: https://doi.org/10.21681/2311-3456-2019-6-92-101.
5. Maximov R.V., Sokolovskij S.P., Voronchixin I.S. Algoritm i texnicheskie resheniya dinamicheskogo konfigurirovaniya klient-serverny`x vy`chislitel`ny`x setej // Informatika i avtomatizaciya. 2020. № 5 (19). C. 1018-1049. DOI: https://doi.org/10.15622/ia.2020.19.5.5.

8 Vadim Kuchurov, postgraduate, Krasnodar Higher Military School, Krasnodar, Russian Federation. E-mail: kuchurovv@ yandex.ru

9 Roman Maximov, Dr.Sc.(Eng.), Professor, Professor of Department of Protected Information Technology, Krasnodar Higher Military School, Krasnodar, Russian Federation. E-mail: rvmaxim@yandex.ru

10 Roman Sherstobitov, Ph.D., Senior Lecturer of Department of Protected Information Technology, Krasnodar Higher Military School, Krasnodar, Russian Federation. E-mail: scherstobitov.rs@yandex.ru

6. Beraud, P., Cruz, A., Hassell, S., & Meadows, S. (2011). Using cyber maneuver to improve network resiliency. 2011 - MILCOM 2011 Military Communications Conference, 1121-1126.
7. Sposob maskirovaniya struktury` seti svyazi. Pat. 26822105 Ros. Federaciya, MPK G06F / Zajcev D.V., Zuev O.E., Krupenin A.V., Maksimov R.V., Pochinok V.V., Sharifullin S.R., Sherstobitov R.S.; zayavitel` i patentoobladatel` Krasnodarskoe vy`sshee voennoe uchilishhe (RU). – № 2018112925; zayavl. 09.04.2018; opubl. 14.03.2019, Byul. № 8.
8. Bogovik A.V., Ignatov V.V. E`ffektivnost` sistem voennoj svyazi i metody` ee ocenki. – SPb.: VAS, 2006. – 183 s.
9. Sokolovskij S.P. Model` zashhity` informacionnoj sistemy` ot setevoj razvedki dinamicheskim upravleniem ee strukturno-funkcional`ny`mi xarakteristikami // Voprosy` oboronnoj texniki. Seriya 16 protivodejstvie terrorizmu. 2020. № 7-8. – S. 62-73.
10. Sokolovskij S.P., Krupenin A.V., Xorev G.A., Kalach A.V. Maskirovanie identifikatorov kanal`nogo urovnya sredstv proaktivnoj zashhity` integrirovanny`x setej svyazi special`nogo naznacheniya // Vestnik Voronezhskogo instituta FSIN Rossii. 2018. № 3. – S. 81-89.
11. Markov A.S., Gorshkov YU.G., Matveev V.A., Cirlov V.L. Sovremennye trendy v oblasti kiberbezopasnosti // Bezopasnye informacionnye tekhnologii. Sbornik trudov Sed'moj vserossijskoj nauchno-tekhnicheskoj konferencii / pod. red. V.A. Matveeva. – M.: MGTU im. N.E. Baumana, 2016. 345 s. – ill.
12. Maximov R.V., Sokolovsky S.P., Gavrilov A.L. Hiding Computer Network Proactive Security Tools Unmasking Features. In CEUR Workshop Proceedings, 2017, Vol-2081 (Selected Papers of the VIII All-Russian Scientific and Technical Conference on Secure Information Technologies, BIT 2017). P. 88-92.
13. Krupenin A., Maximov R., Sharifullin S., Sokolovsky S. Innovative Development of Tools and Technologies to Ensure the Russian Information Security and Core Protective Guidelines // Voprosy kiberbezopasnosti [Cybersecurity issue], 2019, №1 (29), pp. 10-17. DOI: 10.21681/2311-3456-2019-1-10-17.
14. Bilinski M., Gabrys R., Mauger J. Optimal Placement of Honeypots for Network Defense. In: Bushnell L., Poovendran R., Başar T. (eds) Decision and Game Theory for Security. GameSec 2018. Lecture Notes in Computer Science, vol 11199. Springer, Cham. 2018. DOI: https://doi.org/10.1007/978-3-030-01554-1_7.
15. Chee Keong NG, Lei Pan, Dr. Yang Xiang. Honeypot Frameworks and Their Applications: A New Framework. In SpringerBriefs on Cyber Security Systems and Networks. Springer, Singapore. 2018. DOI: https://doi.org/10.1007/978-981-10-7739-5.
16. Wang, Y., Guo, Y., Zhang, L. et al. SWIM: An Effective Method to Perceive Cyberspace Situation from Honeynet. Arabian Journal for Science and Engineering. 2018. Vol. 43. P. 6863. DOI: https://doi.org/10.1007/s13369-017-2904-5.
17. Vishnevskij A.S. Obmannaya sistema dlya vy`yavleniya xakerskix atak, osnovannaya na analize povedeniya posetitelej veb-sajtov // Voprosy` kiberbezopasnosti. – 2018. № 3 (27). – S. 8-17. DOI: https://doi.org/10.21681/2311-3456-2018-3-54-62.
18. Iskolnyy B.B., Maximov R.V., Sharifullin S.R. Survivability Assessment of Distributed Information and Telecommunication Networks // Selected Papers of the VIII All-Russian Conference with International Participation «Secure Information Technologies» (BIT 2017). Bauman Moscow Technical University. December 6-7, 2017, Moscow, Russia. P. 59-65.
19. Evnevich E.L., Fatkieva R.R. Modelirovanie informacionny`x processov v usloviyax konfliktov // Voprosy` kiberbezopasnosti. – 2020. № 2 (36). – S. 92-101. DOI: https://doi.org/10.21681/2311-3456-2020-2-42-49.
20. Kubarev A.V., Lapsar` A.P., Fedorova Ya.V. Povy`shenie bezopasnosti e`kspluatacii znachimy`x ob``ektov kriticheskoj infrastruktury` s ispol`zovaniem parametricheskix modelej e`volyucii // Voprosy` kiberbezopasnosti. – 2020. № 1 (35). – S. 8-17. DOI: https://doi.org/10.21681/2311-3456-2020-01-08-17.