УДК 004.942

Модель маскирования информационного обмена в сети передачи данных ведомственного назначения

Шерстобитов Р. С.

***Постановка задачи**: потребности в передачи всех видов информации между подразделениями ведомства обеспечивается универсальной транспортной сетью. В связи с этим угрозы сетевой разведки и компьютерных атак на сети передачи данных ведомственного назначения остаются актуальными. Одним из способов предотвращения данных угроз является маскирование адресной информации и реализация маскирующего обмена сетевых устройств. Однако, применение указанных мер снижает доступность сетевых узлов для осуществления конструктивного информационного обмена, поскольку ложные элементы и маскирующий трафик, совместно с конструктивным используют неделимый ресурс каналов связи и средств обработки информации сетевых устройств, а используемые протоколы транспортного уровня имеют ограничения, которые не гарантируют непрерывную передачу данных. **Целью работы является** разработка модели и исследование на ее основе закономерностей функционирования сети передачи данных ведомственного назначения при реализации маскирования информационного обмена в условиях сетевой разведки. **Используемые методы:** в работе использованы методы исследования случайных процессов. **Научная новизна** модели заключается в применении математического аппарата теории однородных полумарковских процессов с дискретными состояниями и непрерывным временем для определения вероятностно-временных характеристик процесса функционирования сетей передачи данных ведомственного назначения при реализации маскирования информационного обмена в условиях сетевой разведки. **Практическая значимость** модели заключается в нахождении вероятностно-временных характеристик процесса функционирования сетей передачи данных ведомственного назначения в условиях сетевой разведки, необходимых для определения оптимальных значений параметров сетевых соединений узлов сети при реализации маскирования информационного обмена в сетях передачи данных ведомственного назначения. **Результат**: разработана модель маскирования информационного обмена в сети передачи данных ведомственного назначения, которая формализована в виде полумарковского случайного процесса с дискретными состояниями и непрерывным временем. Полученные выходные вероятностно-временные характеристики используются в качестве целевых функций при формулировании задачи векторной оптимизации и определения оптимальных значений параметров сетевых соединений узлов сети передачи данных ведомственного назначения при реализации маскирования информационного обмена в условиях сетевой разведки.*

***Ключевые слова**: структурно-функциональные характеристики, маскирующий обмен, сетевые соединения, непрерывность информационного обмена, случайный процесс, доступность и защищенность сетевых устройств.*

Введение

На фоне обострения внешнеполитической обстановки в мире фиксируется усиление сетевой разведки (СР) и рост интенсивности информационно-технического воздействия на инфраструктуру органов государственной власти Российской Федерации.

Библиографическая ссылка на статью:
Шерстобитов Р. С. Модель маскирования информационного обмена в сети передачи данных ведомственного назначения // Системы управления, связи и безопасности. 2024. № 1. С. 1-25. DOI: 10.24412/2410-9916-2024-1-001-025

Reference for citation:
Sherstobitov R. S. The model of information exchange masking in the departmental communication network. *Systems of Control, Communication and Security*, 2024, no. 1, pp. 1-25 (in Russian). DOI: 10.24412/2410-9916-2024-1-001-025

Причем фиксируется рост сложности компьютерных атак и степень их проработки (сочетание нескольких векторов атак, использование специально разработанного вредоносного программного обеспечения, легитимных утилит и др.) [1].

В качестве основных средств СР и реализации компьютерных атак злоумышленниками используется программное обеспечение для подбора паролей перебором (брутфорсом), сканеры портов, эксплойты для различных уязвимостей [2].

Одним из факторов результативного применения указанных средств является использование сетей связи общего пользования в качестве транспортной базы для информационного обмена между территориально распределенными узлами сетей передачи данных ведомственного назначения (СПД ВН).

С другой стороны, высокая эффективность применения средств СР обуславливается статичностью элементов сети, основными из которых являются сетевые устройства (СУ), осуществляющие обработку и передачу всех видов информации.

Статичность СУ определяется постоянством множества используемых структурно-функциональных характеристик. Например, IP-адресов, MAC-адресов, сетевых портов, протоколов информационного взаимодействия.

Для защиты от угроз безопасности информации, связанных с возможностью проведения СР и компьютерных атак, в СПД ВН реализуется набор мер ФСТЭК России по сокрытию архитектуры и конфигурации СПД ВН, а также воспроизведению ложных и (или) скрытию истинных отдельных информационных технологий (структурно-функциональных характеристик) сети или ее сегментов, которые обеспечивают навязывание злоумышленнику ложного представления об истинных информационных технологиях (структурно-функциональных характеристиках) СПД ВН [3].

Физическая постановка задачи

Комплекс мероприятий по добыванию злоумышленником разведывательных сведений и их обработке очевидно выполняется в условиях ограниченного ресурса сил и средств. В таком случае, основная задача злоумышленника состоит в оптимальном распределении имеющегося потенциала для построения адекватных моделей, отражающих закономерности функционирования СПД ВН.

В таком случае, необходимо формировать у злоумышленника ложное представление о структуре (топологии) и параметрах (типологии)) СПД ВН и, как неизбежное следствие, структуре системы управления ведомством. Это позволит влиять на качество решений, принимаемых злоумышленником по результатам разведки, предотвращать деструктивные воздействия на объекты защиты или снижать их результативность и эффективность [3].

В качестве реализации такого подхода используется концепция Moving Target Defense (MTD), которая заключается в замене статических параметров сети динамическими [4-6].

Одним из практических методов реализации концепции MTD является маскирование информационного обмена, заключающееся в маскировании адресной информации сетевых устройств и реализации маскирующего информационного обмена между топологически локализованными элементами (сегментами) СПД ВН [7].

Под маскированием адресной информации СУ понимается сокрытие структурно-функциональных характеристик путем расширения адресного пространства (увеличения их количества), введения ложных (маскирующих) элементов и динамического конфигурирования параметров структурно-функциональных характеристик элементов СПД ВН. Согласованная смена параметров структурно-функциональных характеристик внешних интерфейсов СУ (IP-адресов и MAC-адресов) осуществляется «по возмущению», когда поступает управляющий сигнал от системы обнаружения атак (обнаружена компьютерная атака) или лица, принимающего решение (смена адресов как реакция на смену оперативной обстановки).

С другой стороны, наряду с угрозами безопасности информации (УБИ), связанными со сканированием средствами СР элементов сети, таких как «УБИ.098 Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб», «УБИ.099 Угроза обнаружения хостов», «УБИ.098 Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб», «УБИ.103 Угроза определения типов объектов защиты», «УБИ.132 Угроза получения предварительной информации об объекте защиты», существует угроза бескомпроматного определения топологии СПД ВН («УБИ.104 Угроза определения топологии вычислительной сети») [3, 8]. Результат ее реализации – определение важности узлов СПД ВН для осуществления злоумышленником таргетированных компьютерных атак.

Бескомпроматность реализации данной угрозы основывается на принципах использования снифферов, средств перехвата и анализа сетевого трафика, работающих преимущественно в пассивном режиме.

В таком случае, для противодействия данной угрозе в СПД ВН целесообразно реализовывать маскирующий информационный обмен.

Под маскирующим информационным обменом понимается упорядоченная по структуре и интенсивности совокупность ложных (маскирующих) пакетов сообщений, формируемых СУ с целью управления демаскирующими признаками алгоритмов функционирования СПД ВН, изменяющих видимую интенсивность информационного обмена между её элементами [9].

Основные демаскирующие признаки алгоритмов функционирования СПД ВН – это интенсивность трафика между топологически локализованными элементами (сегментами) распределенной сети передачи данных, сетевые протоколы взаимодействия и иерархические уровни (ранги) элементов СПД ВН. Маскирующий обмен позволяет скрыть факт передачи конструктивного трафика, реальные направления конструктивного информационного обмена в общем объеме трафика, циркулирующего между распределенными сегментами сети и исказить (в частности – повысить) уровень иерархии («оперативно-тактическую принадлежность») соответствующих элементов СПД ВН [9].

В настоящее время разработан ряд научно-технических предложений по динамическому конфигурированию параметров структурно-функциональных характеристик сетевых устройств [10-15], однако, задача по исследованию их доступности при реализации маскирования информационного обмена в СПД ВН не ставилась и не решалась.

При использовании протокола транспортного уровня TCP для осуществления конструктивного информационного обмена смена структурно-функциональных характеристик элементов сети, а именно IP-адресов, будет приводить к разрыву сетевых соединений между СУ, т.е. информационный обмен будет прерван.

Это связано с тем, что для данного протокола в рамках установленного сетевого соединения используется только одна пара IP-адресов отправителя и получателя. При этом сетевые устройства будут недоступны для осуществления информационного обмена до тех пор, пока не произойдет полная реконфигурации сетевых настроек всех сетевых устройств вычислительной сети.

Помимо этого, протокол TCP подвержен компьютерным атакам следующих типов: «Атака затоплением SYN-пакетами», «Атака подделкой TCP-сегмента», «Атака сбросом TCP-соединения» [16, 17].

В связи с этим для маскирования адресной информации СУ и динамического конфигурирования параметров структурно-функциональных характеристик элементов СПД ВН при конструктивном информационном обмене необходимо использовать протоколы транспортного уровня, которые лишены указанных недостатков и уязвимостей. Таким протоколом транспортного уровня является SCTP (Stream Control Transmission Protocol), техническое представление которого описано в стандартах RFC (Request for Comments) 3286, 4960, 5061.

При этом возможно состояние, в котором СУ будут недоступны для осуществления конструктивного информационного обмена ввиду исчерпания всех IP-адресов из множества доступных и ожидания новых IP-адресов с целью их добавления в существующее многоадресное соединение и возобновления информационного обмена. А в случае невозможности использовать текущее соединение СУ необходима реконфигурация, в ходе которой происходит разрыв (завершение) текущих сетевых соединений и переход на другой стек IP-адресов.

С другой стороны, при организации информационного обмена количество маршрутизируемых через сети связи общего пользования IP-адресов для создания многоадресных соединений не будет сколь угодно большим. В связи с этим, при функционировании средств разведки и вскрытии истинных IP-адресов необходима реконфигурация СУ (перевод в заранее определенную конфигурацию), при которой сетевые соединения будут недоступны.

СПД ВН предназначены для конструктивного информационного обмена. С другой стороны, ложные элементы и маскирующий трафик, используя совместно с конструктивным неделимый ресурс каналов связи и средств обработки информации (сетевых устройств), создают дополнительные ограничения на конструктивный информационных обмен [9].

Так, в моменты осуществления ложных сетевых соединений и реализации маскирующего обмена, сетевые соединения для осуществления конструктивного информационного обмена будут недоступны. С другой стороны, возможна ситуация вскрытия всех ложных IP-адресов, то есть идентификация сетевой разведкой предназначения ложных IP-адресов, что наряду с вскрытием истинных IP-адресов является основанием для реконфигурации сетевых устройств (перевод в заранее определенную конфигурацию), при которой сетевые соединения будут недоступны.

Таким образом, проведенный анализ теоретических и практических аспектов маскирования адресной информации и маскирующего информационного обмена позволяет сформулировать противоречие между необходимостью реализации указанных мер для защиты структурно-функциональных характеристик СПД ВН, с одной стороны, и отсутствием научно-методического обеспечения конфигурирования параметров сетевых соединений с учетом ограниченных ресурсов каналов связи и СУ на реализацию процедур защиты, с другой стороны.

Для исследования поведения СПД ВН при различных условиях функционирования необходимо разработать модель маскирования информационного обмена сети передачи данных ведомственного назначения в условиях сетевой разведки.

Модель маскирования информационного обмена сети передачи данных ведомственного назначения в условиях сетевой разведки

Введем допущение, что СПД ВН являются технической основой системы управления ведомством, на которые возложены функции по обработке и передаче информации между органами (субъектами) и объектами управления.

При этом основными требованиями к СПД ВН являются обеспечение доступности и защищенности входящих в рассматриваемую систему компонентов.

С учетом этого, функционирование СПД ВН при реализации маскирования информационного обмена может быть представлено как случайный процесс с дискретными состояниями и непрерывным временем, отражающий функционирование СУ, между которыми установлены сетевые соединения для конструктивного и маскирующего информационного обмена (далее – система C_{avail}), и случайный процесс с дискретными состояниями и непрерывным временем, отражающий функционирование СУ в условиях ведения сетевой разведки (далее система C_{prot}). При этом множество состояний рассматриваемых систем конечно и состоит из n состояний.

Переход между состояниями в рассматриваемых случайных процессах осуществляется под воздействием управляемых и неуправляемых факторов и зависит от количества предварительно заданных сетевым устройствам истинных IP-адресов для установления многоадресных соединений и осуществления конструктивного информационного обмена, времени использования истинных IP-адресов, а также количества предварительно заданных сетевым устройствам

ложных IP-адресов для установления соединений и осуществления маскирующего информационного обмена, времени использования ложных IP-адресов.

Введем допущение, что процессы, протекающие в системах C_{avail} и C_{prot}, рассматриваются как полумарковские случайные процессы, обладающие свойствами простейшего потока событий.

Тогда функция распределения времени ожидания перехода из состояния i в состояние j $F_{ij}(t)$ под воздействием потока событий интенсивности λ_{ij} и переходные вероятности p_{ij} распределены по экспоненциальному закону и вычисляются выражениями [18-20]:

$$F_{ij}(t) = 1 - e^{-\lambda_{ij} t};$$

$$p_{ij} = \int_0^{\infty} f_{ij}(t) \prod_{k=1, k \neq j}^{n} (1 - F_{ik}(t)) dt,$$

где: $F_{ij}(t)$ – функция распределения времени ожидания перехода из состояния i в состояние j; p_{ij} – вероятность перехода из состояния i в состояние j; λ_{ij} – интенсивность потока событий, переводящих исследуемые системы из состояния i в состояние j; $f_{ij}(t)$ – плотность распределения времени ожидания перехода из состояния i в состояние j.

Система C_{avail}, отражающая функционирование СУ, между которыми установлены многоадресные сетевые соединения для конструктивного информационного обмена с маскированием адресной информации и сетевые соединения для реализации маскирующего информационного обмена представлена в виде ориентированного графа (рис. 1).

При этом дискретным состояниям, представленным в таблице 1, соответствуют вероятностные характеристики из таблицы 2.

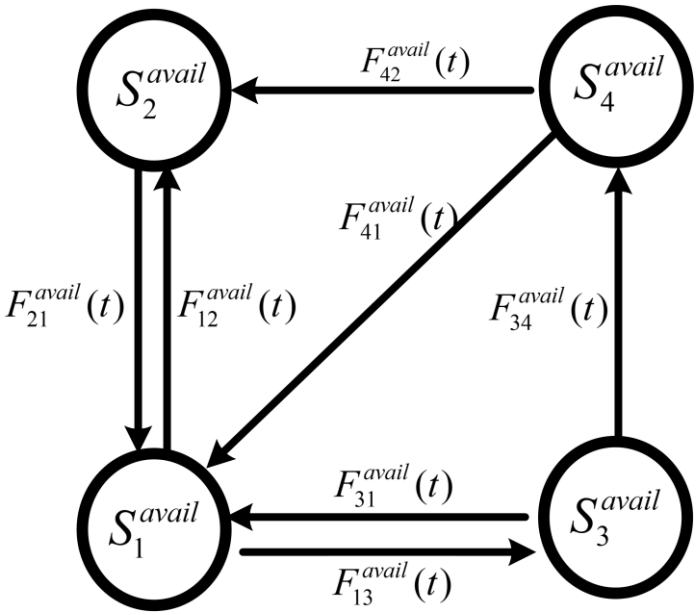

Рис. 1. Граф состояний C_{avail}

Таблица 1 – Дискретные состояния C_{avail}

Состояние	Описание состояний
S_1^{avail}	Ожидание инициализации истинного сетевого соединения и реализации конструктивного информационного обмена
S_2^{avail}	Ожидание инициализации ложного сетевого соединения и реализации маскирующего информационного обмена
S_3^{avail}	Ожидание добавления IP-адреса в сетевое соединение СУ
S_4^{avail}	Ожидание завершения реконфигурации сетевых соединений СУ

Таблица 2 – Вероятностные характеристики процесса функционирования C_{avail}

Переменная	Описание параметра
$F_{12}^{avail}(t)$	Функция распределения времени ожидания инициализации ложного сетевого соединения и реализации маскирующего информационного обмена
$F_{21}^{avail}(t)$	Функция распределения времени ожидания инициализации истинного сетевого соединения и реализации конструктивного информационного обмена
$F_{13}^{avail}(t)$	Функция распределения времени ожидания перехода СУ в недоступное состояние
$F_{31}^{avail}(t)$	Функция распределения времени ожидания добавления новых IP-адресов в существующее соединение и возобновления конструктивного информационного обмена
$F_{34}^{avail}(t)$	Функция распределения времени ожидания завершения реконфигурации сетевых соединений СУ (использование другого стека IP-адресов)
$F_{41}^{avail}(t)$	Функция распределения времени ожидания возобновления истинного сетевого соединения и реализации конструктивного информационного обмена
$F_{42}^{avail}(t)$	Функция распределения времени ожидания возобновления ложного сетевого соединения и реализации маскирующего информационного обмена

Система C_{prot}, отражающая функционирование сетевых устройств СПД ВН в условиях ведения сетевой разведки представлена в виде ориентированного графа (рис. 2). При этом дискретным состояниям, представленным в таблице 3, соответствуют вероятностные характеристики из таблицы 4.

Таблица 3 – Дискретные состояния C_{prot}

Состояние	Описание состояния
S_1^{prot}	Ожидание завершения цикла сетевой разведки
S_2^{prot}	Осуществление конструктивного информационного обмена с использованием вскрытого истинного IP-адреса
S_3^{prot}	Осуществление маскирующего информационного обмена с использованием вскрытого (частично вскрытых) ложного IP-адреса
S_4^{prot}	Осуществление маскирующего информационного обмена при вскрытии всех ложных IP-адресов

Таблица 4 – Вероятностные характеристики процесса функционирования C_{prot}

Переменная	Описание параметра
$F_{12}^{prot}(t)$	Функция распределения времени ожидания вскрытия истинного IP-адреса СУ
$F_{21}^{prot}(t)$	Функция распределения времени ожидания смены истинного IP-адреса
$F_{13}^{prot}(t)$	Функция распределения времени ожидания вскрытия ложного IP-адреса
$F_{31}^{prot}(t)$	Функция распределения времени ожидания смены ложных IP-адресов
$F_{34}^{prot}(t)$	Функция распределения времени ожидания вскрытия всех ложных IP-адресов
$F_{23}^{prot}(t)$	Функция распределения времени ожидания вскрытия ложного IP-адреса после вскрытия истинного IP-адреса
$F_{32}^{prot}(t)$	Функция распределения времени ожидания вскрытия истинного IP-адреса после вскрытия ложного IP-адреса
$F_{42}^{prot}(t)$	Функция распределения времени ожидания использования истинных IP-адресов после вскрытия всех ложных IP-адресов
$F_{41}^{prot}(t)$	Функция распределения времени ожидания реконфигурации IP-адресов

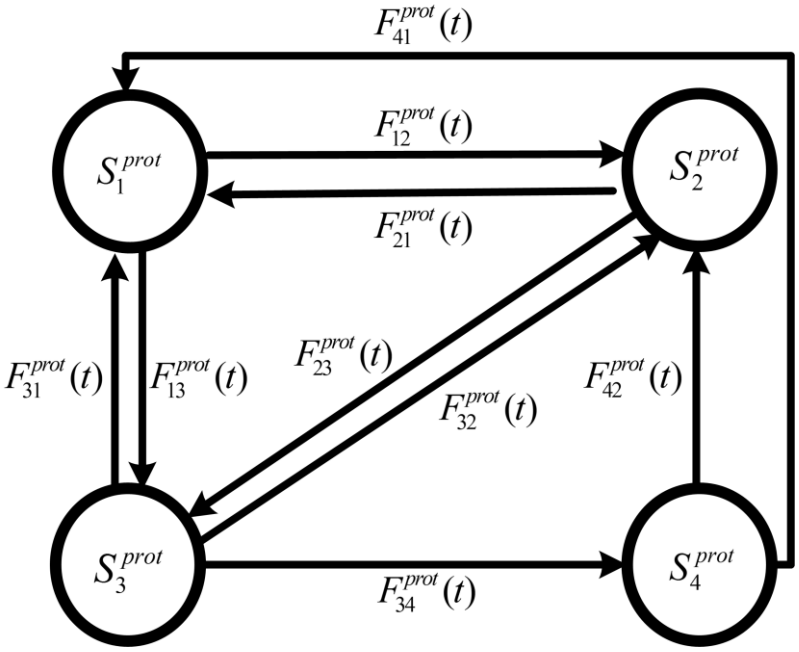

Рис. 2. Граф состояний C_{prot}

Формализация указанных случайных процессов выполняется с использованием множества входных параметров (множество M^{avail} и множество M^{prot}) и множества выходных вероятностно-временных характеристик (множество K^{avail} и множество K^{prot}):

$$M^{avail} \to K^{avail} \left| M^{avail} = \{S^{avail}, X^{avail}, L^{avail}\}; K^{avail} = \{P^{avail}, B^{avail}\}, \right.$$

$$M^{prot} \to K^{prot} \left| M^{prot} = \{S^{prot}, X^{prot}, L^{prot}\}; K^{prot} = \{P^{prot}, B^{prot}\}. \right.$$

где S^{avail} – множество дискретных состояний системы C_{avail}; S^{prot} – множество дискретных состояний системы C_{prot}; X^{avail} – множество неуправляемых (неконтролируемых) факторов системы C_{avail}; X^{prot} – множество неуправляемых (неконтролируемых) факторов системы C_{prot}; L^{avail} – множество управляемых фак-

торов системы C_{avail}; L^{prot} – множество управляемых факторов системы C_{prot}; $P^{avail} = \{P_{ij}^{avail}(t)\}$ – множество интервально-переходных вероятностей перехода C_{avail} в состояние j из состояния i в момент времени t; $P^{prot} = \{P_{ij}^{prot}(t)\}$ – множество интервально-переходных вероятностей перехода C_{prot} в состояние j из состояния i в момент времени t; $B^{avail} = \{B_{ij}^{avail}(t)\}$ – множество вероятностей первого достижения состояния j из состояния i к моменту времени t для системы C_{avail}; $B^{prot} = \{B_{ij}^{prot}(t)\}$ – множество вероятностей первого достижения состояния j из состояния i к моменту времени t для системы C_{prot}.

При этом, параметры X^{avail}, X^{prot}, L^{avail}, L^{prot} задаются как:

$$X^{avail} = \{T_{rec}, T_{add}\},$$

$$X^{prot} = \{T_{rec}, T_{cic}\},$$

$$L^{avail} = \{F_{12}^{avail}(t), F_{13}^{avail}(t), F_{21}^{avail}, F_{31}^{avail}, F_{34}^{avail}, F_{41}^{avail}(t), F_{42}^{avail}, m\},$$

$$\text{при } \lambda_{12} = (y \cdot v)/(x \cdot z), \lambda_{13} = (x \cdot z)^{-1}, \lambda_{21} = (x \cdot z)/(y \cdot v), \lambda_{31} = (m(x \cdot T_{add}))^{-1},$$

$$\lambda_{34} = (m \cdot T_{rec})^{-1}, \lambda_{41} = x/(T_{rec} \cdot m), \lambda_{42} = y/(T_{rec} \cdot m),$$

$$L^{prot} = \{F_{12}^{prot}(t), F_{13}^{prot}(t), F_{21}^{prot}(t), F_{23}^{prot}(t), F_{31}^{prot}(t), F_{32}^{prot}(t), F_{34}^{prot}(t), F_{41}^{prot}(t), F_{42}^{prot}(t), m\},$$

$$\text{при } \lambda_{12} = (x \cdot z) \cdot (m \cdot T_{cic})^{-1}, \lambda_{13} = (y \cdot v) \cdot (m \cdot T_{cic})^{-1}, \lambda_{21} = z^{-1},$$

$$\lambda_{23} = (y \cdot v) \cdot (m \cdot T_{cic})^{-1}, \lambda_{31} = v^{-1}, \lambda_{32} = (x \cdot z) \cdot (m \cdot T_{cic})^{-1},$$

$$\lambda_{34} = (v/y) \cdot (m \cdot T_{cic})^{-1}, \lambda_{41} = (x+y) \cdot m / T_{rec}, \lambda_{42} = ((x \cdot z)/(y \cdot v)) \cdot m,$$

где: m – количество СУ; x – количество истинных IP-адресов для одного СУ; y – количество ложных IP-адресов для одного СУ; z – время использования истинных IP-адресов; v – время использования ложных IP-адресов; T_{cic} – время цикла сетевой разведки злоумышленника одного СУ; T_{add} – время, затрачиваемое на добавление одного IP-адреса в существующее многоадресное соединение; T_{rec} – время, затрачиваемое на реконфигурацию сетевых соединений СУ.

Для рассматриваемых систем C_{avail} и C_{prot} целевыми вероятностно-временными характеристиками являются: вероятности перехода в состояние j из состояния i в момент времени t (интервально-переходные вероятности $P_{ij}^{avail}(t)$ и $P_{ij}^{prot}(t)$) и вероятности первого достижения состояния j из состояния i к моменту времени t ($B_{ij}^{avail}(t)$ и $B_{ij}^{prot}(t)$).

Последовательность определения указанных вероятностно-временных характеристик описана в [18], в матричной форме осуществлялось через основные характеристики полумарковских процессов по следующим выражениям:

$$\mathbf{P}^{avail}(s) = L^{-1}\{\left[\mathbf{I}^{avail} - \mathbf{p}^{avail} \times \mathbf{f}^{avail}(s)\right]^{-1} \mathbf{\Psi}^{avail}(s)\},$$

$$\mathbf{P}^{prot}(s) = L^{-1}\{\left[\mathbf{I}^{prot} - \mathbf{p}^{prot} \times \mathbf{f}^{prot}(s)\right]^{-1} \mathbf{\Psi}^{prot}(s)\},$$

$$\mathbf{B}^{avail}(s) = L^{-1}\{s^{-1} \cdot \mathbf{p}^{avail} \cdot \mathbf{f}^{avail}(s) \cdot \left(\mathbf{I}^{avail} - \mathbf{p}^{avail} \cdot \mathbf{f}^{avail}(s)\right)^{-1} \cdot \left[\mathbf{I}^{avail} \times \left(\mathbf{I}^{avail} - \mathbf{p}^{avail} \cdot \mathbf{f}^{avail}(s)\right)^{-1}\right]^{-1}\},$$

$$\mathbf{B}^{prot}(s) = L^{-1}\{s^{-1} \cdot \mathbf{p}^{prot} \cdot \mathbf{f}^{prot}(s) \cdot \left(\mathbf{I}^{prot} - \mathbf{p}^{prot} \cdot \mathbf{f}^{prot}(s)\right)^{-1} \cdot \left[\mathbf{I}^{prot} \times \left(\mathbf{I}^{prot} - \mathbf{p}^{prot} \cdot \mathbf{f}^{prot}(s)\right)^{-1}\right]^{-1}\},$$

где L^{-1} – обратное преобразование Лапласа; $\mathbf{I}^{avail}$ – единичная матрица размерности, соответствующей мощности множества дискретных состояний C_{avail}; $\mathbf{I}^{prot}$ – единичная матрица размерности, соответствующей мощности множества

дискретных состояний C_{prot}; $\mathbf{p}^{avail}$ – матрица переходных вероятностей p_{ij} C_{avail}; $\mathbf{p}^{prot}$ – матрица переходных вероятностей p_{ij} C_{prot}; $\mathbf{f}^{avail}(s)$ – матрица плотностей распределения $f_{ij}(t)$ времени ожидания переходов из состояния i в состояние j (в форме изображений) C_{avail}; $\mathbf{f}^{prot}(s)$ – матрица плотностей распределения $f_{ij}(t)$ времени ожидания переходов из состояния i в состояние j (в форме изображений) C_{prot}; «×» – операция умножения элементов матрицы; $\mathbf{\Psi}^{avail}(s)$ – вероятность того, что C_{avail} не покинет соответствующее состояние в момент времени t (в форме изображений); $\mathbf{\Psi}^{prot}(s)$ – вероятность того, что C_{prot} не покинет соответствующее состояние в момент времени t (в форме изображений).

Формирование исходных данных для моделирования

Количество узлов сети (сетевых устройств) m может зависеть от принятой структуры системы управления ведомством, от места пункта управления – организатора связи в иерархии подразделений ведомства, от замысла по защите (введению в заблуждение злоумышленника) или других условий (например, класса сети).

Для примера рассмотрим моделируемую СПД ВН, которая состоит из 20 СУ, функционирующих в условиях СР.

Управляемыми параметрами моделируемой СПД ВН являются количество x истинных IP-адресов для одного СУ, количество y ложных IP-адресов для одного СУ, время z использования истинных IP-адресов, время v использования ложных IP-адресов.

Неуправляемыми параметрами моделируемой СПД ВН являются время T_{cic} цикла сетевой разведки одного СУ, время T_{add} на добавление одного IP-адреса в существующее многоадресное соединение, время T_{rec} на реконфигурацию сетевых соединений СУ.

Задача на моделирование – исследовать различные свойства СПД ВН при реализации маскирования информационного обмена в условиях сетевой разведки и получить вероятностно-временные характеристики процесса функционирования СПД ВН.

Диапазон задаваемых истинных и ложных логических IP-адресов СУ определяется максимальным числом VLAN (Virtual Local Area Network), технологии разделения физической сети на несколько виртуальных сетей. При этом максимальное значение количества используемых адресов на одном физическом сетевом интерфейсе равно 4094, что регламентировано стандартом IEEE 802.1Q [15].

Истинные IP-адреса используются для сетевых соединений и осуществления конструктивного информационного обмена, ложные IP-адреса – для ложных сетевых соединений и реализации маскирующего информационного обмена СУ.

Время z использования истинных IP-адресов и время v использования ложных IP-адресов зависит от характеристик сети, необходимости осуществлять конструктивный или маскирующий информационный обмен. С точки зрения информационной безопасности значение параметра времени использования

истинных и ложных IP-адресов зависит от интенсивности ведения СР, которая определяется временем цикла СР $T_{cic.}$

Значения параметров времени *z* использования истинных IP-адресов и времени *v* использования ложных IP-адресов задаются с использованием DHCP-сервера при помощи опции 51 «Время аренды IP-адреса» протокола DHCP. Единицей измерения параметра является секунда.

В соответствии со стандартом RFC (Request for Comments) 2131 значения указанных параметров могут быть сколь угодно большим с учетом жизненного цикла СПД ВН (до 100 лет). В рамках исследований введено ограничение на данный параметр в 1 ч (3600 с).

Физический смысл параметра T_{cic} – время окончания ведения СР, когда завершаются запросы от средств разведки вне зависимости от режима сканирования объекта.

Экспериментальным путем были получены следующие средние значения времени цикла СР T_{cic} одного СУ в зависимости от режима использования средств СР (таблица 5).

Таблица 5 – Среднее время цикла сетевой разведки T_{cic}

№ п/п	Режим использования средств СР	Время цикла СР, с
1	Быстрое сканирование	0,3
2	Ping-сканирование	0,5
3	Интенсивное сканирование	1
4	Интенсивное сканирование, все TCP порты	30,4

Экспериментальным путем было выявлено, что среднее значение параметра времени, затрачиваемого на добавление одного истинного IP-адреса T_{add} в существующее многоадресное соединение СУ с использованием DHCP-сервера составило 0,2 с.

Время, затрачиваемое на реконфигурацию сетевых соединений одного сетевого устройства T_{rec}, в ходе которой происходит разрыв (завершение) текущего сетевого соединения и переход на другой стек IP-адресов с использованием DHCP-сервера, определено экспериментально, среднее значение составляет 3 с.

Для исследования поведения СПД ВН при различных условиях и получения вероятностно-временных характеристик полумарковского процесса рассмотрим следующие ситуации функционирования систем C_{avail}, C_{prot}.

Ситуация № 1 характеризуется наличием предварительно заданных истинных IP-адресов для истинных сетевых соединений и осуществления конструктивного информационного обмена (в данной ситуации их количество равно 4) и временем их использования 25 с. Выбор значения параметра времени использования истинных IP-адресов обусловлен значением параметра времени цикла СР T_{cic}, который равен 30 с, а также необходимостью конструктивного информационного обмена.

Ситуация № 1 характеризуется наличием кратно меньшего количества предварительно заданных ложных IP-адресов (в данной ситуации их количество равно 2) и временем их использования 15 с.

Такие условия могут быть связаны с более интенсивным режимом работы абонентов сети по конструктивному информационному обмену. В таком случае, маскирующий информационный обмен будет реализовываться в моменты простоя СУ от конструктивного информационного обмена.

Ситуация № 2 является противоположной ситуации № 1 и характеризуется наличием большего количества предварительно заданных ложных IP-адресов для ложных сетевых соединений и осуществления маскирующего информационного обмена (в данной ситуации их количество равно 4) и временем их использования 25 с. Большее значение параметра времени использования ложных IP-адресов v по отношению к времени использования истинных IP-адресов z в данном случае определено необходимостью осуществлять маскирующий обмен в СПД ВН.

Такая необходимость может быть вызвана отсутствием конструктивного информационного обмена и реализацией замысла по введению в заблуждение СР относительно структурно-функциональных характеристик СПД ВН.

Значение параметра времени цикла сетевой разведки T_{cic} в данной ситуации аналогично ситуации № 1 и равно 30 с.

С точки зрения истинных сетевых соединений и конструктивного информационного обмена, ситуация характеризуется наличием кратно меньшего количества предварительно заданных истинных IP-адресов (в данной ситуации их количество равно 2) и временем их использования 15 с.

Такие условия могут быть обусловлены менее интенсивным режимом работы абонентов сети по конструктивному информационному обмену. В таком случае, состояние простоя СУ от конструктивного информационного обмена будет чаще, что освобождает ресурсы для ложных сетевых соединений и реализации маскирующего информационного обмена.

Результаты моделирования

Результаты расчетов показывают, что недоступность истинных сетевых соединений для осуществления конструктивного информационного обмена к моменту времени t в ситуации № 1 (рис. 3) из состояния S_1^{avail} инициализации истинного сетевого соединения и реализации конструктивного информационного обмена определяется вероятностью $P_{12}^{avail}(t)$ перехода C_{avail} в состояние инициализации ложного сетевого соединения и реализации маскирующего информационного обмена S_2^{avail}, вероятностью $P_{13}^{avail}(t)$ перехода в состояние ожидания добавления IP-адреса в сетевое соединение S_3^{avail} и вероятностью $P_{14}^{avail}(t)$ перехода в состояние S_4^{avail} завершения реконфигурации сетевых соединений.

Однако, при указанных условиях функционирования и значениях управляемых и неуправляемых факторов, влияние этого состояния на общую доступность СУ СПД ВН незначительное.

Результаты расчетов показывают, что СУ СПД ВН в ситуации № 1 большую часть времени будут находиться в состоянии S_1^{avail}, доступном для истинных сетевых соединений и реализации конструктивного информационного обмена, что определяется вероятностью $P_{11}^{avail}(t)$ (рис. 3).

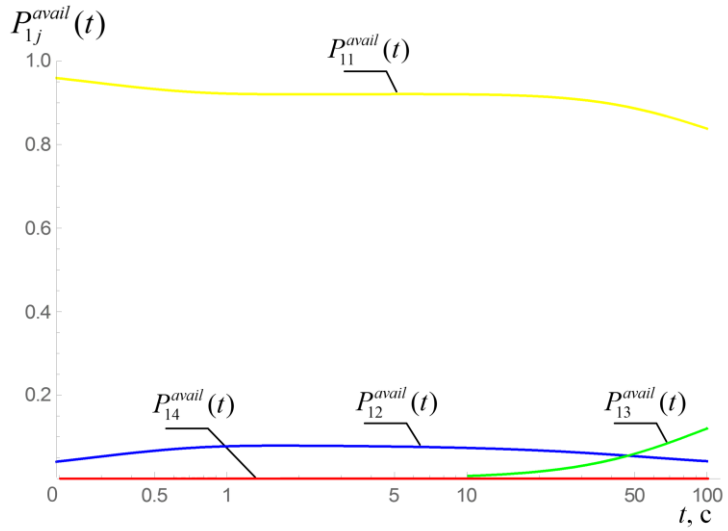

Рис. 3. Результат расчета вероятности перехода C_{avail} в состояние j из состояния S_1^{avail} к моменту времени t для ситуации № 1

В то же время, малое значение количества ложных IP-адресов и времени их использования характеризуют данную ситуацию как незащищенную от средств СР, так как большее время система функционирует в состоянии осуществления конструктивного информационного обмена с использованием вскрытого истинного IP-адреса, о чем свидетельствует существенно большие значения вероятности $P_{12}^{prot}(t)$ перехода C_{prot} из состояния завершения цикла сетевой разведки S_1^{prot} в состояние осуществления конструктивного информационного обмена с использованием вскрытого истинного IP-адреса S_2^{prot} к моменту времени t по отношению к вероятности $P_{13}^{prot}(t)$ перехода C_{prot} из состояния завершения цикла сетевой разведки S_1^{prot} в состояние осуществления маскирующего информационного обмена с использованием вскрытого (частично вскрытых) ложного IP-адреса S_3^{prot} к моменту времени t или по отношению к вероятности $P_{11}^{prot}(t)$ перехода C_{prot} из состояния завершения цикла сетевой разведки S_1^{prot} в состояние завершения цикла сетевой разведки S_1^{prot} к моменту времени t (рис. 4).

Другим состоянием C_{prot}, которым обуславливается снижение защищенности СУ СПД ВН, является состояние S_4^{prot}, при котором вскрыты все ложные IP-адреса, о чем свидетельствует вероятность $P_{14}^{prot}(t)$ перехода C_{prot} из состояния завершения цикла сетевой разведки S_1^{prot} в состояние осуществления маскирующего информационного обмена при вскрытии всех ложных IP-адресов S_4^{prot} к моменту времени t. Однако, при указанных условиях функционирования СПД ВН и значениях управляемых и неуправляемых факторов, влияние этого состояния на общую защищенность СУ незначительное.

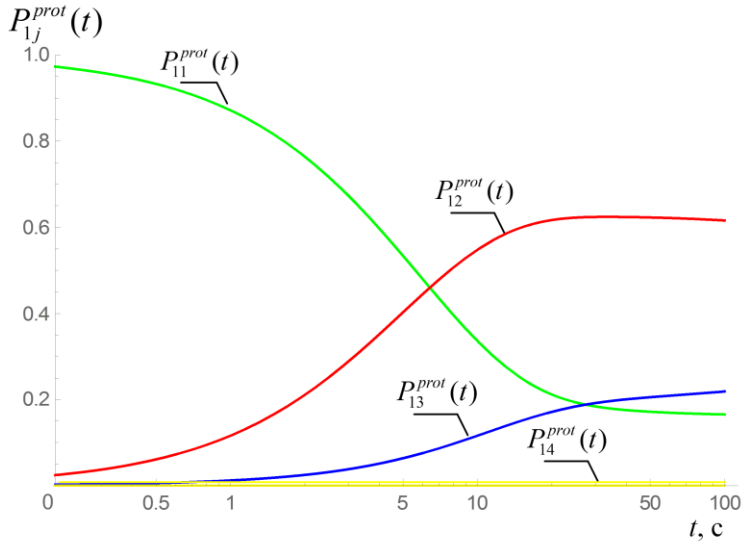

Рис. 4. Результат расчета вероятности перехода C_{prot} в состояние j из состояния S_1^{prot} к моменту времени t для ситуации № 1

Причем в первый раз система C_{prot} будет находиться в незащищенном состоянии S_2^{prot} в связи с использованием вскрытого истинного IP-адреса для конструктивного информационного обмена через 80 секунд, о чем свидетельствуют результаты расчета вероятности $B_{12}^{prot}(t)$ первого достижения системой C_{prot} состояния S_2^{prot} из состояния S_1^{prot} к моменту времени t (рис. 5).

Результаты расчетов показывают, что СУ СПД ВН в ситуации № 2 большую часть времени будут находиться в состоянии, не доступном для истинных сетевых соединений и реализации конструктивного информационного обмена.

Недоступность истинных сетевых соединений для осуществления конструктивного информационного обмена к моменту времени t в ситуации № 2 (рис. 6) из состояния S_1^{avail} инициализации истинного сетевого соединения и реализации конструктивного информационного обмена определяется большими значениями вероятности $P_{12}^{avail}(t)$ перехода C_{avail} в состояние инициализации ложного сетевого соединения и реализации маскирующего информационного обмена S_2^{avail}. Другими интервально-переходными вероятностями, определяю-

№1. 2024
ISSN 2410-9916

щими недоступность СУ СПД ВН, являются вероятность $P_{13}^{avail}(t)$ перехода C_{avail} из состояния S_1^{avail} инициализации истинного сетевого соединения и реализации конструктивного информационного обмена в состояние S_3^{avail} ожидания добавления IP-адреса в сетевое соединение и вероятность $P_{14}^{avail}(t)$ перехода из состояния S_1^{avail} инициализации истинного сетевого соединения и реализации конструктивного информационного обмена в состояние S_4^{avail} завершения реконфигурации сетевых соединений. Однако, при указанных условиях функционирования СПД ВН и значениях управляемых и неуправляемых факторов их влияние на общую доступность СУ СПД ВН незначительное.

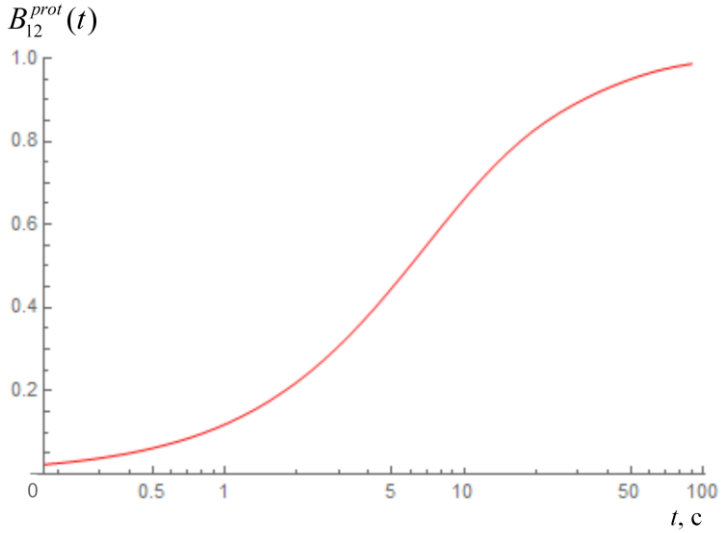

Рис. 5. Результат расчетов вероятности $B_{12}^{prot}(t)$

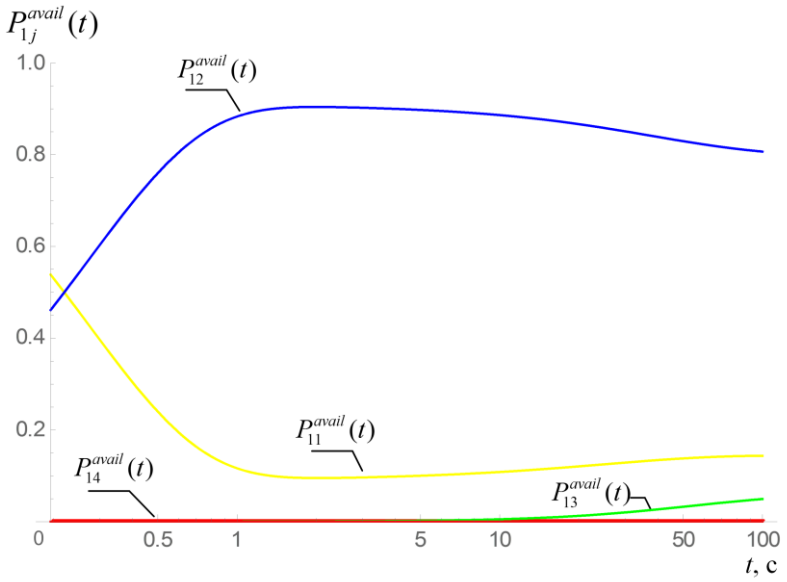

Рис. 6. Результат расчета вероятности перехода C_{avail} в состояние j из состояния S_1^{avail} к моменту времени t для ситуации № 2

Результаты расчетов показывают, что состояние, при котором система будет в недоступном состоянии для истинных сетевых соединений и осуществления конструктивного информационного обмена в связи с инициализацией ложных сетевых соединений и реализацией маскирующего информационного обмена, первый раз наступит через 2 секунды, о чем свидетельствует расчет вероятности $B_{12}^{avail}(t)$ первого достижения системы C_{prot} состояния S_2^{avail} из состояния S_1^{avail} к моменту времени t (рис. 7).

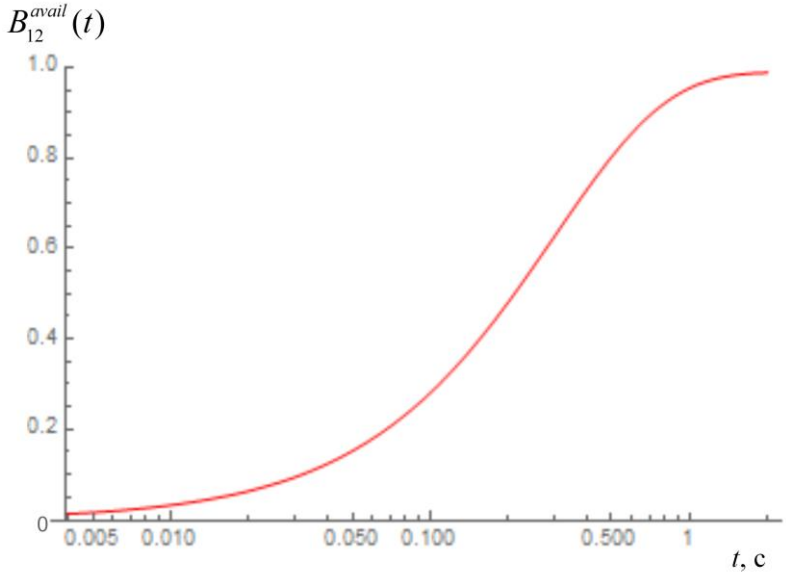

Рис. 7. Результат расчетов вероятности $B_{12}^{avail}(t)$

В то же время, большее значение количества ложных IP-адресов и времени их использования характеризуют данное состояние как защищенное от средств СР, так как большее время система функционирует в состоянии осуществления маскирующего информационного обмена с использованием вскрытого ложного IP-адреса, о чем свидетельствует вероятности $P_{13}^{prot}(t)$ перехода C_{prot} из состояния завершения цикла сетевой разведки S_1^{prot} в состояние осуществления маскирующего информационного обмена с использованием вскрытого (частично вскрытых) ложного IP-адреса S_3^{prot} к моменту времени t и вероятности $P_{11}^{prot}(t)$ перехода C_{prot} из состояния завершения цикла сетевой разведки S_1^{prot} в состояние завершения цикла сетевой разведки S_1^{prot} к моменту времени t, суммарное значение которых существенно больше вероятности $P_{12}^{prot}(t)$ перехода C_{prot} из состояния завершения цикла сетевой разведки S_1^{prot} в состояние осуществления конструктивного информационного обмена с использованием вскрытого истинного IP-адреса S_2^{prot} к моменту времени t и вероятности $P_{14}^{prot}(t)$ перехода C_{prot} из состояния завершения цикла сетевой разведки S_1^{prot} в

состояние осуществления маскирующего информационного обмена при вскрытии всех ложных IP-адресов S_4^{prot} к моменту времени t (рис. 8).

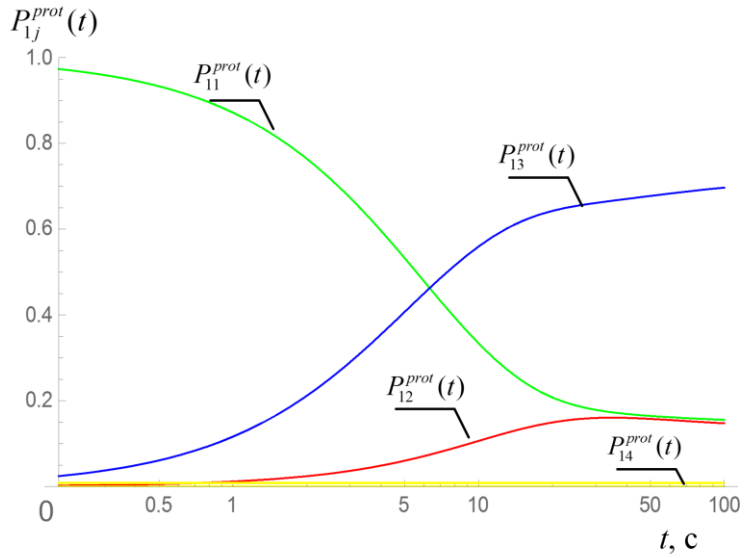

Рис. 8. Результат расчета вероятности перехода C_{prot} в состояние j из состояния S_1^{prot} к моменту времени t для ситуации № 2

На рис. 9, 10 приведены финальные вероятности для системы C_{avail} с учетом заданных значений неуправляемых факторов при варьировании количества истинных IP-адресов (x) и времени аренды истинных IP-адресов (z), а также количества ложных IP-адресов (y) и времени аренды ложных IP-адресов (v).

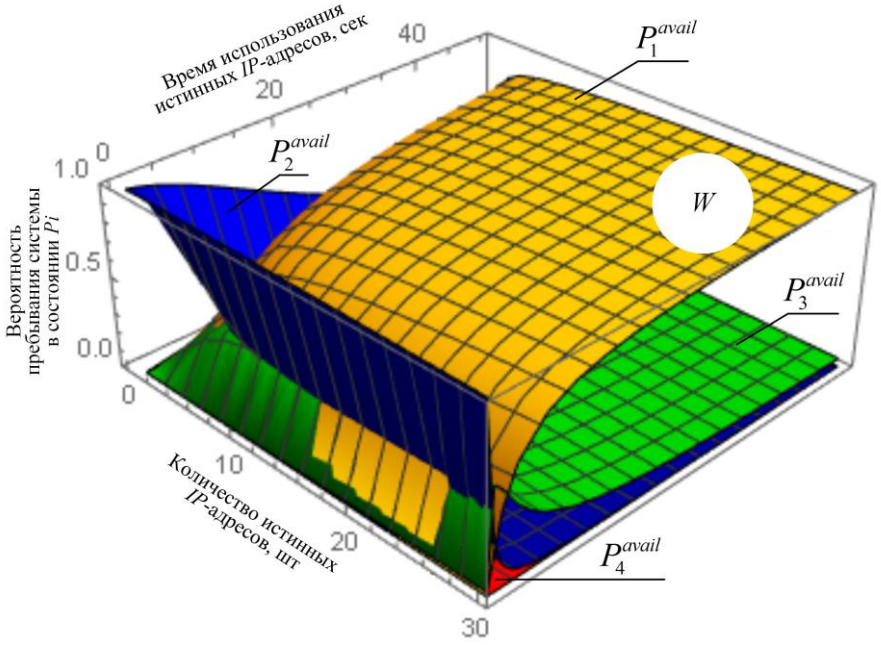

Рис. 9 – Результаты расчётов финальных вероятностей P_j^{avail} в зависимости от значений x и z

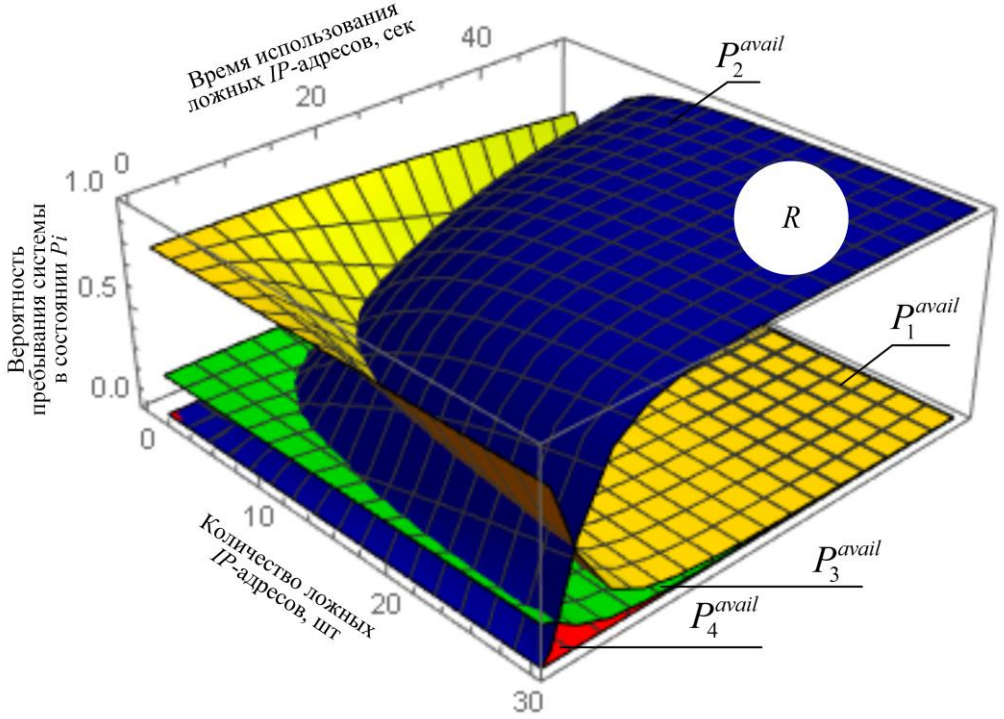

Рис. 10 – Результаты расчётов финальных вероятностей P_j^{avail}
в зависимости от значений *y* и *v*

На рис. 11, 12 приведены финальные вероятности для системы C_{prot} с учетом заданных значений неуправляемых факторов при варьировании количества истинных IP-адресов (*x*) и времени аренды истинных IP-адресов (*z*), а также количества ложных IP-адресов (*y*) и времени аренды ложных IP-адресов (*v*).

Так, при увеличении количества истинных IP-адресов и увеличении времени их аренды, и при уменьшении количества ложных IP-адресов и времени аренды ложных IP-адресов, СУ СПД ВН (например, область значений *W*) в стационарном режиме будут находится преимущественно в состоянии, доступном для инициализации истинных сетевых соединений и реализации конструктивного информационного обмена (рис. 9 и 10, вероятность P_1^{avail}), но незащищенном для СПД ВН состоянии (рис. 11 и 12, вероятность P_2^{prot}, вероятность P_4^{prot}). И наоборот, при увеличении количества ложных IP-адресов и времени аренды ложных IP-адресов, и при уменьшении количества истинных IP-адресов и уменьшении времени их аренды СУ СПД ВН (например, область значений *R*) в стационарном режиме будут находится преимущественно в состоянии недоступном для инициализации истинных сетевых соединений и реализации конструктивного информационного обмена (рис. 9 и 10, вероятность P_2^{avail}, вероят-

ность P_3^{avail}, вероятность P_4^{avail}), но защищенном для СПД ВН состоянии (рис. 11 и 12, вероятность P_1^{prot}, вероятность P_3^{prot}).

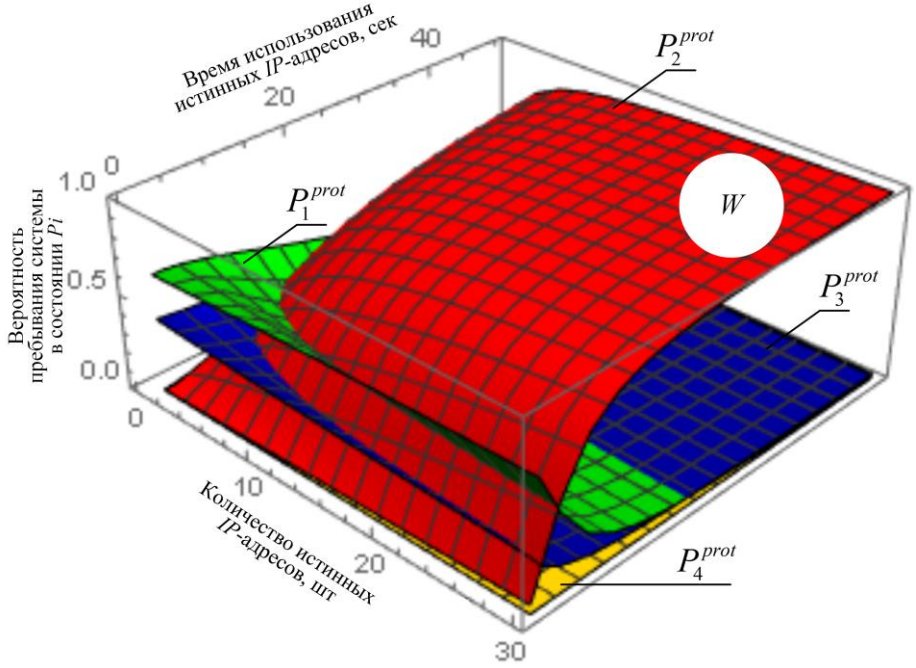

Рис. 11 – Результаты расчётов финальных вероятностей P_j^{prot} в зависимости от значений *x* и *z*

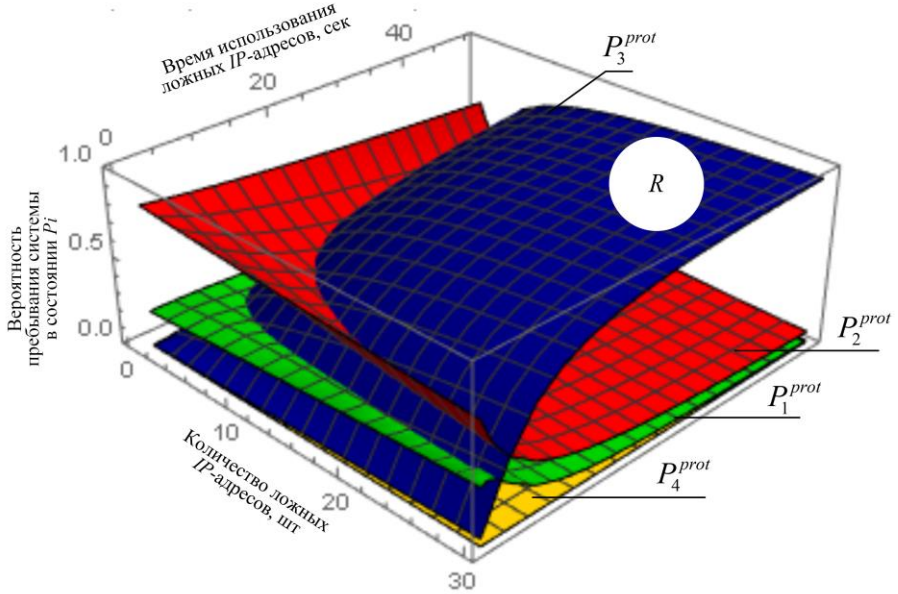

Рис. 12 – Результаты расчётов финальных вероятностей P_j^{prot} в зависимости от значений *y* и *v*

DOI: 10.24412/2410-9916-2024-1-001-025
URL: https://sccs.intelgr.com/archive/2024-01/01-Sherstobitov.pdf

Результаты расчётов показывают, что при заданных условиях функционирования СУ СПД ВН показатели защищенности и доступности являются антагонистами и конкурируют за ограниченный ресурс каналов связи и средств обработки информации, следовательно, актуальной становится задача определения таких значений управляемых параметров сетевых соединений СУ СПД ВН в различных условиях функционирования при реализации маскирования информационного обмена в условиях ведения СР, при которых СПД ВН находится в Парето-оптимальном состоянии (улучшение одного параметра невозможно без ухудшения другого с учетом заданных ограничений).

Состояния S_2^{avail}, S_3^{avail}, S_4^{avail} системы C_{avail} возможно охарактеризовать как состояния, при которых СУ будут не доступны для истинных сетевых соединений конструктивного информационного обмена. С другой стороны, состояние S_1^{avail} возможно охарактеризовать как состояние, при которых СУ будут находиться в состоянии доступном для истинных сетевых соединений конструктивного информационного обмена. Таким образом, финальная вероятность нахождения системы в состоянии S_1^{avail} может рассматриваться как целевая функция (показатель), характеризующая критерий «доступности» СУ СПД ВН.

Состояние S_2^{prot} системы C_{prot} возможно охарактеризовать как состояние, при котором СУ будут находиться в незащищенном состоянии. Таким образом, финальная вероятность нахождения системы в множестве состояний, за исключением состояния S_2^{prot}, может рассматриваться как целевая функция (показатель), характеризующая критерий «защищенности» СУ СПД ВН.

Тогда задача определения оптимальных значений управляемых параметров сетевых соединений СУ СПД ВН в различных условиях функционирования при реализации маскирования информационного обмена в условиях СР может быть сформулирована как максимизация целевых функций, характеризующих критерии «доступности» и «защищённости».

Таким образом, формализованная постановка задачи многокритериальной оптимизации будет иметь вид:

$$\begin{cases} F_1(L^{avail}, X^{avail}) \rightarrow \max\limits_{\text{для } L^{avail}, X^{avail} \in Q} \\ F_2(L^{prot}, X^{prot}) \rightarrow \max\limits_{\text{для } L^{prot}, X^{prot} \in Q} \end{cases},$$

где: X^{avail} – множество неуправляемых (неконтролируемых) факторов системы C_{avail}; X^{prot} – множество неуправляемых (неконтролируемых) факторов системы C_{prot}; L^{avail} – множество управляемых факторов системы C_{avail}; L^{prot} – множество управляемых факторов системы C_{prot}.

Указанные параметры являются общими для целевых функций F_1 и F_2, а их значения принадлежат области допустимых значений Q.

Целевая функция F_1 характеризует «доступность» СУ СПД ВН:

$$F_1(L^{avail}, X^{avail}) = P_1^{avail}.$$

Целевая функция F_2 характеризует «защищенность» СУ СПД ВН:

$$F_2(L^{prot}, X^{prot}) = \overline{P_2^{prot}}.$$

Использование модели позволяет исследовать различные свойства СПД ВН при реализации маскирования информационного обмена СПД ВН в условиях сетевой разведки, а полученные с помощью модели выходные вероятностно-временные характеристики могут в дальнейшем выступать в качестве целевых функций при формулировании задачи векторной оптимизации.

Научная новизна модели заключается в применении математического аппарата теории однородных полумарковских процессов с дискретными состояниями и непрерывным временем для определения вероятностно-временных характеристик процесса функционирования СПД ВН при реализации маскирования информационного обмена в условиях сетевой разведки.

Практическая значимость модели заключается в нахождении вероятностно-временных характеристик процесса функционирования СПД ВН в условиях сетевой разведки, необходимых для определения оптимальных значений параметров сетевых соединений СУ при реализации маскирования информационного обмена в СПД ВН.

Вывод

Предложенная модель позволяет исследовать процесс функционирования СПД ВН при реализации маскирования информационного обмена в условиях сетевой разведки с учетом конфигурировании параметров сетевых соединений СУ, имеющих множественную адресацию. Модель формализована в виде полумарковского случайного процесса с дискретными состояниями и непрерывным временем, при этом выходные характеристики определяются через основные характеристики полумарковского процесса с экспоненциальным законом распределения.

Направлением дальнейших исследований является определение оптимальных значений параметров сетевых соединений СУ при реализации маскирования информационного обмена в СПД ВН в условиях сетевой разведки, а также оценка эффективности их применения**.**

Литература

1. Отчет об исследовании серии кибератак на органы государственной власти Российской Федерации // Официальный информационный ресурс ООО «Солар Секьюрити» [Электронный ресурс]. URL: http://rt-solar.ru/analytics/reports/2203 (дата обращения 22.11.2023).

2. Статистика сетевых атак // Официальный информационный ресурс АО «Лаборатория Касперского» [Электронный ресурс]. 2023. – URL: http://statistics.securelist.ru/2023 (дата обращения 24.11.2023).

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

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. Зайцев Д.В., Зуев О. Е., Крупенин А. В., Максимов Р. В., Починок В. В., Шарифуллин С.Р., Шерстобитов Р. С. Способ маскирования структуры сети связи // Патент на изобретение RU 2682105, опубл. 14.03.2019.

8. Теленьга А. П. Маскирование метаструктур информационных систем в киберпространстве // Вопросы кибербезопасности. 2023. № 5 (57). С. 50-59.

9. Шерстобитов Р. С., Шарифуллин С. Р., Максимов Р. В. Маскирование интегрированных сетей связи ведомственного назначения // Системы управления, связи и безопасности. 2018. № 4. С. 136-175.

10. 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.

11. 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.

12. Максимов Р. В., Соколовский С. П., Ворончихин И. С., Гритчин А. Д., Боядкин М. С., Игнатенко А. В. Способ защиты вычислительных сетей // Патент на изобретение RU 2726900, опубл. 16.07.2020.

13. 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.

14. Москвин А. А., Максимов Р. В., Горбачев А. А. Модель, оптимизация и оценка эффективности применения многоадресных сетевых соединений в условиях сетевой разведки // Вопросы кибербезопаности. 2023. № 3 (55). С. 13-22.

15. Москвин А. А. Алгоритм конфигурирования многоадресных соединений в условиях компьютерной разведки // Системы управления, связи и безопасности. 2023. № 2. С. 102-130.

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

17. 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.

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

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

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

References

1. An investigation report of a series of cyber attacks on Russian Federation public authorities. *Oficial'nyj informacionnyj resurs OOO «Solar Security»* [The official information resource of Solar Securiry LLC]. Available at: http://rt-solar.ru / analytics/reports/2203 (accessed 22 November 2023) (in Russian).

2. Network attack statistics. *Oficial'nyj informacionnyj resurs AO «Laboratoriia Kasperskogo»* [The official information resource of Kaspersky Lab JSC]. 2023. Available at: http://statistics.securelist.ru/2023 (accessed 24 November 2023) (in Russian).

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

4. Kanellopoulos A., Vamvoudakis K. 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. P. 115–124.

7. Zaicev D. V, Zuev O. E., Krupenin A. V., Maksimov R. V., Pochinok V. V., Sharifullin S. R., Sherstobitov R. S. Method for masking the structure of telecommunication network. Patent Russia, no RU 2682105. Publish 14.03.2019 (in Russian).

8. Telenga A. P. Masking metasrtructures of information system in cyberspace. *Voprosy kiberbezopasnosti*, 2023, vol. 5, no. 57, pp. 50-59 (in Russia).

9. Sherstobitov R. S., Maksimov R. V., Sharifullin S. R. Masking of departmental-purpose integrated communication networks. *System of Control, Communication and Security*, 2018, vol. 4, pp. 136-175 (in Russian).

10. 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).

11. Sokolovsky S. P. Model of information system protection from network intelligence by dynamic management of its structural and functional characteristics. *Voprosy oboronnoj tekhniki. Seriya 16: Tekhnicheskie sredstva protivodejstviya terrorizmu*, 2020, vol. 7-8, no. 145-146, pp. 62–73 (in Russia).

12. Maksimov R. V., Sokolovskij S. P., Voronchihin I. S., Gritchin A. D., Boiadkin M.S., Ignatenko A.V. Method of protecting computer networks. Patent Russia, no RU 2726900. Publish 16.07.2020 (in Russian).

13. 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).

14. Moskvin A. A., Maksimov R. V., Gorbachev A. A. Model, optimization and efficiency evaluation of application multicast network connections in conditions of network intelligence. *Voprosy kiberbezopasnosti*, 2023, vol. 3, no. 55, pp.13-22 (in Russia).

15. Moskvin A. A. Algorithm of multiaddress network connection configuration under conditions of computer intelligence. *System of Control, Communication and Security*, 2023, vol. 2, pp. 102-130 (in Russian).

16. 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).

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

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

19. 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).

20. 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).

Статья поступила 6 декабря 2023 г.

Информация об авторе

Шерстобитов Роман Сергеевич – кандидат технических наук. Докторант. 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 объек-

тов; маскирование информационных ресурсов интегрированных ведомственных сетей связи. E–mail: scherstobitov.rs@yandex.ru

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

The model of information exchange masking in the departmental communication network

R. S. Sherstobitov

Problem statement: *the need to transmit all types of information between departmental divisions is provided by a universal transportation network. In this regard, the threats of network reconnaissance and computer attacks on departmental data transmission networks are still relevant. One of the ways to prevent these threats is masking of address information and realization of masking exchange of network devices. However, the application of these measures reduces the availability of network nodes for the implementation of constructive information exchange, because false elements and masking traffic utilizes in conjunction with the constructive indivisible resource of communication channels and information processing network devices, and the transport layer protocols used have restrictions that do not guarantee continuous data transmission.* ***The purpose of the work*** *is to model development and study the functioning of the data transmission network of departmental purpose in the realization of information exchange masking in the conditions of network reconnaissance.* ***Methods used****: in the work the methods of research of random processes are used.* ***The scientific novelty*** *of the model lies in the application of mathematical apparatus of the theory of homogeneous semi-Markov processes with discrete states and continuous time to determine the probabilistic and temporal characteristics of the process of functioning of departmental data networks in the implementation of information exchange masking in the conditions of network reconnaissance.* ***Practical significance*** *of the model is to identify the probabilistic-temporal characteristics of the process of functioning of data transmission networks of departmental purpose in the conditions of network reconnaissance, necessary for determining the optimal values of the parameters of network connections of network nodes in the realization of information exchange masking in data transmission networks of departmental purpose.* ***Result****: the model of information exchange masking in the departmental communication network, which is formalized in the form of a semi-Markov random process with discrete states and continuous time. The obtained output probabilistic-temporal characteristics are used as target functions in the formulation of the vector optimization problem and optimal values of network connection parameters of nodes of the data transmission network of departmental purpose in the implementation of information exchange masking in the conditions of network reconnaissance.*

Keywords: *structural and functional characteristics, masking exchange, network connections, continuity of information exchange, random process, availability and security of network devices.*

Information about Author

Roman Sergeevich Sherstobitov – Ph.D. of Engineering Sciences. Doctoral 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: scherstobitov.rs@yandex.ru

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