УДК 004.942

Математические модели маскирования структурно-динамических характеристик сетей передачи данных ведомственного назначения от компьютерной разведки

Шерстобитов Р. С.

***Постановка задачи**: Одним из способов противодействия угрозе компьютерной разведки информационных потоков является маскирование структурно-динамических характеристик сетей передачи данных ведомственного назначения. Однако, существующие подходы к аппроксимации динамических характеристик информационных потоков при реализации маскирования характеризуются низкой обобщающей способностью и необходимостью приведения нестационарных данных к стационарному виду с помощью разностных преобразований. При этом, существующий научно-методический аппарат по определению вероятностно-временных характеристик не учитывает нестационарность параметров случайного процесса оценки защищенности и доступности сетевых устройств, а также своевременности информационного обмена при реализации маскирования структурно-динамических характеристик сетей передачи данных ведомственного назначения от компьютерной разведки. **Целью работы является** разработка моделей маскирования структурно-динамических характеристик сетей передачи данных ведомственного назначения от компьютерной разведки и исследование на ее основе закономерностей функционирования сети передачи данных ведомственного назначения при реализации процедур защиты от компьютерной разведки. **Используемые методы:** в работе использованы методы машинного обучения, математической статистики, оптимизации, анализа временных рядов, исследования случайных процессов. **Новизна:** в статье предложен подход к аппроксимации динамических характеристик конструктивного сетевого трафика с использованием ансамбля из моделей рекуррентных нейронных сетей с ячейками долгой краткосрочной памяти для оценки и прогноза частотной характеристики аппроксимируемого сетевого трафика и экспоненциального закона распределения случайной величины, параметризованной выходом нейронной сети, для получения численных значений пауз между пакетами прогнозируемого маскирующего сетевого трафика. Определены вероятностно-временные характеристики процесса функционирования сетей передачи данных ведомственного назначения при реализации маскирования структурно-динамических характеристик в условиях компьютерной разведки с использованием математического аппарата теории неоднородных марковских и однородных полумарковских процессов с дискретными состояниями и непрерывным временем. **Практическая значимость**: формирование маскирующего сетевого трафика, динамические параметры которого статистически близки к конструктивному, и получение вероятностно-временных характеристик процесса функционирования сетей передачи данных ведомственного назначения в условиях компьютерной разведки и нестационарности сетевого трафика, необходимых для формализации целевых функций результативности маскирования, доступности сетевых устройств и своевременности информационного обмена при постановки задачи векторной оптимизации параметров маскирования структурно-динамических характеристик. **Результат**: разработана система моделей маскирования структурно-динамических характеристик, позволяющая исследовать функционирование сетей передачи данных ведомственного назначения в условиях компьютерной разведки.*

Библиографическая ссылка на статью:
Шерстобитов Р. С. Математические модели маскирования структурно-динамических характеристик сетей передачи данных ведомственного назначения от компьютерной разведки // Системы управления, связи и безопасности. 2026. № 1. С. 138-181. DOI: 10.24412/2410-9916-2026-1-138-181

Reference for citation:
Sherstobitov R. S. Mathematical models for masking structural and dynamic characteristics of departmental data transmission networks against computer reconnaissance. *Systems of Control, Communication and Security*, 2026, no. 1, pp. 138-181 (in Russian). DOI: 10.24412/2410-9916-2026-1-138-181

***Ключевые слова**: сеть передачи данных, структурно-динамических характеристик, компрометация, информационный поток, рекуррентная нейронная сеть, экспоненциальный закон распределения, случайный процесс, компьютерная разведка.*

Введение

Фиксируемый в последние годы рост количества и степени проработки компьютерных атак (сочетание нескольких векторов атак, использование специально разработанного вредоносного программного обеспечения, например, для подбора паролей перебором (брутфорсом), сканеры портов, эксплойты для различных уязвимостей, легитимных утилит и др.) [1]) в отношении сетей передачи данных ведомственного назначения (СПД ВН), определяется использованием сетей связи общего пользования в качестве транспортной базы для информационного обмена, а также статичностью структурных характеристик узлов сети (например, IP-адреса, MAC-адреса, сетевые порты, протоколы информационного взаимодействия), что обуславливает высокую эффективность применения средств компьютерной разведки (КР).

В таком случае, необходимо формировать у злоумышленника ложное представление о структуре (топологии) и параметрах (типологии)) СПД ВН и, как неизбежное следствие, структуре системы управления. Это позволит влиять на качество решений, принимаемых злоумышленником по результатам разведки, предотвращать деструктивные воздействия на объекты защиты или снижать их результативность и эффективность [2].

В качестве реализации такого подхода используется концепция Moving Target Defense (MTD), которая заключается в замене статических параметров сети динамическими [3-5].

Одним из практических методов реализации концепции MTD является маскирование структурно-динамических характеристик (СДХ) СПД ВН, заключающееся в маскировании структурных параметров сетевых устройств и реализации маскирования информационных потоков между элементами (сегментами) СПД ВН.

Под маскированием структурных параметров понимается сокрытие идентификаторов сетевых устройств путем расширения адресного пространства (увеличения их количества), введения ложных (маскирующих) элементов в СПД ВН и их динамического конфигурирования в условиях КР. Согласованная смена структурных параметров 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).

Под маскированием информационных потоков понимается формирование между двумя узлами, имеющими общие идентифицирующие атрибуты (например, IP-адреса, порты), маскирующего сетевого трафика (пакетов или иных единиц передачи данных), состоящего из данных приложений (пользовательский трафик) и (или) служебных данных (обеспечивающих управление соединением и передачей данных), статистически схожего с конструктивным сете-

вым трафиком по динамическим характеристикам, в течение заданного интервала времени.

Целью маскирования СДХ является сокрытие идентификаторов сетевых устройств, факта передачи конструктивного трафика в общем объеме сетевого трафика, циркулирующего между элементами (сегментами) сети, и реализация ложных структур СПД ВН.

Критерием оценки ложной структуры СПД ВН может служить степень отличия от реальной структуры. Если обратиться к теории обфускации, то такой критерий можно определить, как степень обфускации структуры. Однако для использования этого критерия необходим некий ассортимент ложных структур СПД ВН для их сравнительной оценки. В работе задача синтеза ложной структуры СПД ВН [6, 7] не ставится, а маскирование СДХ заключается в управлении параметрами маскирования и реализации ложной структуры информационных направлений СПД ВН, которая принимается в качестве исходных данных.

В то же время, с учетом целевого предназначения СПД ВН, реализация указанных мер защиты узлами сети (ложные сетевые объекты, маршрутизаторы, автоматизированные рабочие места) осуществляется в условиях ограниченных ресурсов каналов связи и сетевых устройств.

Например, при информационном обмене в условиях высокоинтенсивной КР возможно вскрытии используемых IP-адресов, что определяет необходимость реконфигурация сетевых устройств (сетевых интерфейсов), то есть перевод в заранее определенную конфигурацию, до окончания которой сетевые соединения будут недоступны. В таких условиях доступность средств обработки информации для формирования конструктивных пакетов сообщений неизбежно снижается.

Ложные элементы и маскирующий трафик, использующийся совместно с конструктивным, неделимый ресурс каналов связи и средств обработки информации, создают дополнительные ограничения на своевременность информационного обмена, так как маскирование СДХ СПД ВН характеризуется возможностью образования очередей из конструктивных и маскирующих пакетов сообщений на передатчике и приемнике, что снижает своевременность информационного обмена в СПД ВН.

Таким образом, необходимо определение оптимальных значений параметров маскирования СДХ СПД ВН (количества ложных информационных потоков, интенсивности маскирующего сетевого трафика, времени использования информационных потоков до их реконфигурации) и управление ими в динамике с учетом качества аппроксимации динамических характеристик информационных потоков, обеспечения результативности маскирования, доступности и своевременности конструктивного информационного обмена сетевых устройств, а также ресурсных ограничений на реализацию процедур защиты.

Таким образом, общая формализованная постановка проблемы маскирования СДХ СПД ВН выглядит как задача многокритериальной оптимизации параметров маскирования (X), в которой необходимо максимизировать показатели результативности маскирования (K_{mask}), своевременности информационно-

го обмена (K_{time}), доступности узлов сети (K_{avail}) СПД ВН в различных условиях функционирования (А) и ресурсных ограничениях на реализацию процедур защиты в рамках допустимого множества Q.

При этом в ходе разработки научно-методического аппарата необходимо определить типы модельных операторов (виды моделей) и их параметры.

$$\begin{cases} K_{mask}(\mathbf{X}_{mask}, \mathbf{A}_{mask}) \to \max\limits_{\mathbf{X}_{mask}, \mathbf{A}_{mask} \in Q} \\ K_{time}(\mathbf{X}_{time}, \mathbf{A}_{time}) \to \max\limits_{\mathbf{X}_{time}, \mathbf{A}_{time} \in Q} \\ K_{avail}(\mathbf{X}_{avail}, \mathbf{A}_{avail}) \to \max\limits_{\mathbf{X}_{avail}, \mathbf{A}_{avail} \in Q} \end{cases},$$

при этом

$$\mathbf{X}_{mask} = \{\mathbf{S}_{mask}, \mathbf{\Theta}_{mask}\}, \mathbf{X}_{time} = \{\mathbf{S}_{ime}, \mathbf{\Theta}_{time}\}, \mathbf{X}_{avail} = \{\mathbf{S}_{avail}, \mathbf{\Theta}_{avail}\},$$
$$\mathbf{A}_{mask} = f(\mathbf{\Theta}_{mask}), \mathbf{A}_{time} = f(\mathbf{\Theta}_{time}), \mathbf{A}_{avail} = f(\mathbf{\Theta}_{avail}),$$

где K_{mask} ($\mathbf{X}_{mask}$, $\mathbf{A}_{mask}$) – функция (модель) количественной оценки результативности маскирования СПД ВН в вероятностной метрике;

K_{time} ($\mathbf{X}_{time}$, $\mathbf{A}_{time}$) – функция (модель), характеризующая количественную оценку своевременности информационного обмена СПД ВН в вероятностной (временной) метрике;

K_{avail} ($\mathbf{X}_{avail}$, $\mathbf{A}_{avail}$) – функция (модель), характеризующая количественную оценку доступности узлов СПД ВН в вероятностной (временной) метрике;

$\mathbf{X}_{mask}$, $\mathbf{X}_{time}$, $\mathbf{X}_{avail}$ – множества управляемых факторов-аргументов (параметров функционирования СПД ВН) математических моделей, влияющих на значение целевых функций $\mathbf{K}_{mask}$, $\mathbf{K}_{time}$, $\mathbf{K}_{avail}$;

A – множества неуправляемых параметров функционирования СПД ВН, влияющих на значение целевых функций $\mathbf{X}_{mask}$, $\mathbf{X}_{time}$, $\mathbf{X}_{avail}$;

$\mathbf{S}_{mask}$, $\mathbf{S}_{time}$, $\mathbf{S}_{avail}$ – множества модельных операторов, аппроксимирующих характеристики результативности маскирования, а также своевременности информационного обмена, доступности узлов СПД ВН при реализации процедур маскирования СДХ;

$\mathbf{\Theta}_{mask}$, $\mathbf{\Theta}_{time}$, $\mathbf{\Theta}_{avail}$ – в общем случае вектора параметров соответствующих модельных операторов;

Q – допустимое множество значений целевых функций и аргументов.

Таким образом, необходима разработка математических моделей:

- аппроксимации динамических характеристик информационных потоков СПД ВН;
- оценки результативности маскирования СДХ СПД ВН;
- оценки влияния проводимых мер защиты на доступность сетевых устройств и своевременность информационного обмена в СПД ВН.

Модель аппроксимации динамических характеристик информационных потоков СПД ВН

Существующий научно-методический аппарат, разработанный в области маскирования информационного обмена и моделирования сетевого трафика основан на выборе и определении параметров функций распределения времени

ожидании моментов отправки заданных пакетов маскирующего сетевого трафика [8], либо с использованием авторегрессионных моделей на основе модели Бокса-Дженкинса [9] (интегрированная авторегрессия – скользящего среднего). Указанные модели имеют ряд недостатков, обусловленных низкой обобщающей способностью и предположении стационарности временных рядов (необходимости приведения нестационарных данных к стационарному виду с помощью разностных преобразований). Таким образом, необходим подход к аппроксимации динамических характеристик ИП СПД ВН, позволяющий получить высокую обобщающую способность для моделирования сложных нестационарных зависимостей, с одной стороны, и с другой стороны обеспечить оперативность семплирования моментов времени отправки пакетов маскирующего сетевого трафика.

В рамках моделирования необходимо на основе эмпирических данных идентифицировать модель аппроксимации динамических характеристик информационных потоков (ИП) конструктивного сетевого трафика в СПД ВН.

Общая формализованная постановка задачи структурной и параметрической идентификации модели имеет вид:

$$R_{per}(L^R, L^{Dyn}) \to \max_{\Psi},$$

где R_{per} – мера количественной оценки результативности маскирования ИП; L^R – динамические характеристики ИП конструктивного сетевого трафика; L^{Dyn} – генерируемые динамические характеристики ИП маскирующего сетевого трафика; Ψ – допустимое множество значений функций и аргументов.

Таким образом, $L^R = \{\Lambda, Z\}$, где, Λ – временной ряд частот пакетов конструктивного сетевого трафика; Z – временной ряд пауз между пакетами конструктивного сетевого трафика.

Генерируемые динамические характеристики ИП маскирующего сетевого трафика L^{Dyn} определяется выражением:

$$L^{Dyn} = \{\Lambda^{ML}, Z^{Dyn}\},$$

где, Λ^{ML} – спрогнозированный временной ряд частот пакетов маскирующего сетевого трафика; Z^{Dyn} – генерируемый временной ряд пауз между пакетами маскирующего сетевого трафика.

Для максимизации показателя результативности маскирования ИП необходимо синтезировать временной ряд частот пакетов Λ^{ML} и временной ряд задержек между пакетами маскирующего сетевого трафика Z^{Dyn}, схожие с аналогичными динамическими характеристиками конструктивного сетевого трафика Λ и Z.

Исследование информационного обмена в СПД ВН в течение времени позволяет сделать вывод, что физическая природа формирования динамических характеристик конструктивного сетевого трафика $L^R = \{\Lambda, Z\}$ представляет собой следующее: ввиду большого количества источников, в сети одновременно формируется некоторое количество n пакетов, которое регистрируется через равные промежутки времени τ. Таким образом, задержки между пакетами определяются характером работы пользователей и зависят от ряда факторов (пропускная способность сети, производительность сетевого оборудования,

очереди в операционных системах узлов сети), то есть можно говорить о существовании функциональной зависимости пауз между пакетами от частоты формирования пакетов ($\Lambda = n / \tau$). Для формирования $L^{Dyn}\{\Lambda^{ML}, Z^{Dyn}\}$ необходимо получить временной ряд пауз между пакетами маскирующего сетевого трафика Z^{Dyn}, генерируемый на основе спрогнозированного временного рядя частот пакетов маскирующего сетевого трафика Λ^{ML}.

Для получения синтетического временного ряда Z^{Dyn} пауз между отправляемыми пакетами маскирующего трафика необходимо разработать математическую модель F^{Dyn}, аппроксимирующую динамические характеристики конструктивного сетевого трафика $L^R = \{\Lambda, Z\}$, позволяющую генерировать схожий по соответствующим показателям временной ряд пауз между пакетами маскирующего сетевого трафика Z^{Dyn} с учетом прогноза возможного изменения значений временного ряда частот пакетов конструктивного сетевого трафика Λ^{ML}.

В общем виде модель F^{Dyn} аппроксимации динамических характеристик конструктивного сетевого трафика в СПД ВН представляет собой отображение входных характеристик $\{X^{Dyn}, A^{Dyn}\}$ в выходные Z^{Dyn}:

$$F^{Dyn} : \{X^{Dyn}, A^{Dyn}\} \to Z^{Dyn}.$$

Входные характеристики представляют собой множество управляемых факторов-аргументов X^{Dyn} и множество неуправляемых параметров A^{Dyn}.

Множеством управляемых параметров X^{Dyn} являются:

$$X^{Dyn} = \{\Theta^{ML}, \Theta^{Delay}, N^{dump}, N^{gen}, D^{spec}, \lambda^{fp}\},$$

где Θ^M – модельные операторы (семейство моделей) машинного обучения для прогнозирования частоты регистрации пакетов конструктивного сетевого трафика; Θ^{Delay} – модельные операторы (семейство моделей) законов распределения случайной величины задержки между пакетами маскирующего сетевого трафика; N^{dump} – длина исходного аппроксимируемого временного ряда конструктивного сетевого трафика; N^{gen} – количество прогнозируемых моделью машинного обучения частот пакетов; D^{spec} – параметр степени агрегирования исходного временного ряда; λ^{fp} – необходимая частота генерации пакетов маскирующего сетевого трафика.

Множество X^{Dyn} управляемых факторов-аргументов модели включает множество модельных операторов машинного обучения Θ^{ML} и множество модельных операторов законов распределения случайной величины задержки между пакетами Θ^{Delay}:

$$\Theta^{ML} = \{\Omega_{LSTM}, \Omega_{GRU}\}, \Theta^{Delay} = \{\Omega_{Exp}\},$$

Множество модельных операторов машинного обучения Θ^{ML}, включает в себя два основных типа моделей на основе искусственных нейронных сетей (с ячейками долгой краткосрочной памяти LSTM (Long Short-Term Memory) и GRU (Gated Recurrent Unit), которые отличаются скоростью обучения и обобщающей способностью. Множество доступных модельных операторов законов распределения случайной величины задержки между пакетами Θ^{Delay} редуцировано до одного экспоненциального закона распределения исходя из следующих соображений: во-первых, экспоненциальное распределение имеет всего один

параметр и его оценка методом максимального правдоподобия является средним значением частоты событий по выборке (то есть имеет место высокая оперативность вычислений), во-вторых параметр модели имеет четкий физический смысл, сочетающийся с выходом модели машинного обучения Λ^{ML}, в-третьих, экспоненциальное распределение описывает свойства широкого класса явлений в природе, связанных с временем ожидания независимых событий.

Модели машинного обучения Ω_{LSTM} и Ω_{GRU} включают в себя свободные (обучаемые) параметры Θ_{LSTM} и Θ_{GRU}, а также гиперпараметры Θ^{gip}_{LSTM} и Θ^{gip}_{GRU} архитектур моделей машинного обучения LSTM и GRU (количество слоев в архитектурах N^{layer}_{LSTM}, N^{layer}_{GRU}; количество ячеек в архитектуре модели машинного обучения N^{cell}_{LSTM}, N^{cell}_{GRU}; длины подпоследовательностей для обучения $N^{steps}_{LSTM}, N^{steps}_{GRU}$; количество эпох обучения N^{epoch}_{LSTM}, N^{epoch}_{GRU}; параметр регуляризации модели машинного обучения N^{drop}_{LSTM}, N^{drop}_{GRU}).

Множеством неуправляемых параметров A^{Dyn} являются:

$$A^{Dyn} = \{t^{rp}_j, Z, \Lambda\}, j \in [1,..., N^{dump}], Z = \{\tau^{dyn}_1,..., \tau^{dyn}_k\}, k = N^{dump} - 1,$$

$$\tau^{dyn}_i = t^{rp}_{i+1} - t^{rp}_i, i \in [1,..., N^{dump} - 1], \Lambda = \{\lambda^{rp}_h\}, h \in [1,..., H^{dump}],$$

где: t^{rp}_i – значения моментов времени регистрации поступления пакетов конструктивного трафика на интерфейсы сетевого оборудования (источников обучающих наборов данных), а также их агрегированных характеристик; τ^{dyn}_i – значение *i*-й паузы между поступлением *i*-го и *i*-1 пакета конструктивного трафика (с); λ^{rp}_h – агрегированная частота поступления пакетов конструктивного трафика на интерфейсы сетевого оборудования (источников обучающих наборов данных) на временном шаге *h*; H^{dump} – общее значение времени агрегирования пакетов конструктивного сетевого трафика (количество временных шагов *h* поступления пакетов конструктивного трафика на интерфейсы сетевого оборудования (источников обучающих наборов данных)).

Выходные характеристики модели Z^{Dyn} представляют собой временной ряд пауз (задержек) между пакетами генерируемого маскирующего сетевого трафика на основе прогноза модели машинного обучения Λ^{ML} частотных характеристик конструктивного сетевого трафика:

$$Z^{Dyn} = F^{Delay}(\Lambda^{ML}),$$

где: F^{Delay} – функция генерации временного ряда задержек между пакетами на основе частот пакетов; Λ^{ML} – спрогнозированный временной ряд частот пакетов, [шт/(D^{spec}·с)].

Основная идея в разработанной системе моделей заключается в том, что семплирование агрегированных динамических характеристик (частот пакетов с заданной степенью укрупнения) конструктивного сетевого трафика осуществляется моделью машинного обучения (рекуррентной нейронной сетью), а непосредственная генерация пауз между пакетами осуществляется с использованием модели экспоненциального закона распределения случайной величины, параметризованной выходом нейронной сети $\Omega_{Exp}(\Lambda^{ML})$ в рамках промежутков времени, ограниченных степенью агрегирования частот D^{spec}.

Для аппроксимации конструктивного сетевого трафика моделью машинного обучения в качестве исходного массива с репрезентативными данными используется временной ряд длиной N^{dump}.

Параметр D^{spec}, определяющий степень агрегирования исходного временного ряда конструктивного сетевого трафика, влияет на долгосрочность (горизонт) прогнозирования изменения частот Λ^{ML} сетевого трафика в СПД ВН моделью машинного обучения. Например, при $D^{spec} = 1$ временной ряд Λ^{ML} имеет размерность [шт/с], при $D^{spec} = 60$ временной ряд Λ^{ML} имеет размерность [шт/мин], при $D^{spec} = 3600$ временной ряд Λ^{ML} имеет размерность [шт/ч] и так далее.

Очевидно, что при очень маленьких значениях D^{spec} прогноз машинного обучения не будет иметь смысла в связи с тем, что длительность обучения и семплирования (прогнозирования) частот будет превышать горизонт прогнозирования. При этом параметром, определяющим количество временных интервалов прогнозирования моделью машинного обучения частот пакетов Λ^{ML} со степенью агрегирования D^{spec}, является временная метрика частот пакетов сетевого трафика N^{gen}.

Фактором-аргументом, позволяющим имитировать динамические характеристики ИП и управлять нагрузкой маскирующего сетевого трафика, является частота маскирующего сетевого трафика λ^{fp}. Значение параметра λ^{fp} может зависеть от реализуемой ложной структуры СПД ВН и целей маскирования. Например, для достижения максимального сходства имитируемых (навязываемых нарушителю) ложной и реальной структуры СПД ВН, а в пределе – их биекцией (взаимно однозначным отображением), или искажения рангов (важности) пунктов управления ведомством. Параметр $\hat{\lambda}_i$ определяет значение спрогнозированной моделью машинного обучения частоты регистрации пакетов конструктивного сетевого трафика.

Необходимая для реализации замысла защиты значение частоты маскирующего сетевого трафика λ^{fp}, может естественным образом отличаться от спрогнозированных значений частот маскирующего сетевого трафика. Таким образом, допущением в работе является масштабирование значения управляемой частоты маскирующего сетевого трафика λ^{fp} на среднее значение прогнозируемой частоты конструктивного трафика.

Выражение для спрогнозированного моделью машинного обучения временного ряда частот пакетов Λ^{ML}, будет иметь вид:

$$\Lambda^{ML} = \frac{\lambda^{fp}}{\frac{1}{N^{gen}}\sum_{i}^{N^{gen}} \hat{\lambda}_i}\{\hat{\lambda}_i\} = \{\hat{\lambda}_i^*\}, i \in [1,...,N^{gen}],$$

где $\hat{\lambda}_i$ – спрогнозированная моделью машинного обучения частота генерации пакетов маскирующего сетевого трафика на i-м временном интервале прогнозирования;

$\hat{\lambda}_i^*$ – частота генерации пакетов маскирующего трафика на *i*-м временном интервале, спрогнозированной моделью машинного обучения, с учётом масштабирования на целевую интенсивность маскирования λ^{fp}.

Выражение для определения выходных характеристик модели Z^{Dyn} (временного ряда пауз между пакетами генерируемого маскирующего сетевого трафика) принимает вид:

$$Z^{Dyn} = \Omega_{Exp}(\Lambda^{ML}) = \left\{ \left[-\frac{\ln(1 - U)}{\hat{\lambda}_1^*} \right]_1, ..., \left[-\frac{\ln(1 - U)}{\hat{\lambda}_i^*} \right]_k \right\}, i = \overline{1, N^{gen}} \Rightarrow$$

$$Z^{Dyn} = \Omega_{Exp}(\Lambda^{ML}) = \left\{ \tau_{11}^{Dyn}, ..., \tau_{1n}^{Dyn}, ..., \tau_{i1}^{Dyn}, ..., \tau_{ik}^{Dyn} \right\}, k \in [1, ..., N^{sum}],$$

$$N^{sum} \approx D^{spec} \sum_{1}^{N^{gen}} (\hat{\lambda}_{N^{gen}}^*) \in N,$$

где *i* – номер временного шага; *k* – количество пауз между пакетами маскирующего сетевого трафика временного ряда Z^{Dyn} на *i*-м шаге; N^{sum} – общее количество генерируемых всей системой моделей $F^{Delay}(\Lambda^{ML})$ пауз между пакетами маскирующего сетевого трафика временного ряда Z^{Dyn} (приближенно, с округлением до натурального числа *N*); τ_i^{gen} – значение *i*-й паузы между формированием *i*-го и *i*-1 пакета маскирующего сетевого трафика; *U* – равномерно распределенная случайная величина на промежутке [0, 1].

При этом общее количество N^{sum} генерируемых всей системой моделей пауз между пакетами маскирующего сетевого трафика временного ряда Z^{Dyn} приближенно (с округлением до натурального числа *N*) равно сумме произведений частот пакетов $\hat{\lambda}_i^*$, спрогнозированных нейросетью до значения количества прогнозируемых моделью машинного обучения частот пакетов N^{gen}, на соответствующую степень агрегирования исходного временного ряда D^{spec}. То есть, на *i*-м шаге, при $D^{spec} = 60$ генерация задержек между отправкой маскирующих пакетов сетевого трафика осуществляется с использованием модели экспоненциального закона распределения в течение 1 минуты (или в среднем количестве $\hat{\lambda}_i^* D^{spec}$), параметризованной соответствующей спрогнозированной частотой пакетов $\hat{\lambda}_i^*$.

В работе, за счет близкой физической интерпретации *p*-значения статистических критериев к вероятности факта статистической близости распределений, под оценкой степени различия динамических характеристик частот конструктивного и маскирующего сетевого трафика понимается величина, обратная *p*-значению критерия Колмогорова-Смирнова (Манна-Уитни, Андерсона-Дарлинга и др.) при проверке гипотезы о статистической однородности временных рядов Λ и Λ^{ML}. То есть, задача аппроксимации свойств сетевого трафика системой моделей выражается как задача условной скалярной оптимизации через *p*-значение критерия согласия:

$$P_{compr}(\Lambda, \Lambda^{ML}) = 1 - p_{val}(\Lambda, \Lambda^{ML}) \to \min_{\Psi},$$

где P_{compr} – вероятность обнаружения средствами КР, что спрогнозированные имитируемые динамические характеристики в виде частот пакетов маскирующего сетевого трафика Λ^{ML} являются ложными, то есть, отличаются от временного ряда частот пакетов конструктивного сетевого трафика Λ;

p_{val} – p-значение, как оценка вероятности того, что наблюдаемое отклонение (статистика в используемом тесте) между двумя выборками случайно, при условии, что обе выборки принадлежат одному и тому же распределению, то есть мера статистического сходства временных рядов.

Оценка сходства временных рядов задержек между пакетами сетевого трафика Z и Z^{Dyn} определяется количеством пауз τ на i-м шаге, спрогнозированного моделью машинного обучения Θ^{ML}, что в общем виде можно формализовать выражением:

$$\{\Theta^{ML}, \Theta^{Delay}\} \rightarrow \arg\min_{\Psi} F_{Metric},$$

где F_{Metric} – метрика оценка сходства (например, средне квадратическое отклонение (MSE), корень из средне квадратического отклонения (RMSE)), Ψ – область допустимого множества значений параметров модели.

Таким образом, при использовании в качестве метрик MSE или RMSE:

$$F_{Metric} = MSE(\Theta^{ML}, \tau_i^R, \tau_i^{Dyn}) = \frac{1}{N^{train}} \sum_i^{N^{train}} \left(\tau_i^R - \tau_i^{Dyn}(\Theta^{ML})\right)^2;$$

$$F_{Metric} = RMSE(\Theta^{ML}, \tau_i^R, \tau_i^{Dyn}) = \sqrt{\frac{1}{N^{train}} \sum_i^{N^{train}} \left(\tau_i^R - \tau_i^{Dyn}(\Theta^{ML})\right)^2}.$$

Параметр N^{train} количества обучающих последовательностей, сформированных из исходного временного ряда с помощью метода скользящего окна, который не является независимым гиперпараметром, а представляет собой производную величину и определяется выражением:

$$N^{train} = N^t \cdot N^{dump} - N^{steps} + 1,$$

где параметр N^t, определяет долю исходного датасета, используемого для обучения.

Научная новизна модели заключается в том, что в отличии от известных, аппроксимация динамических характеристик конструктивного сетевого трафика осуществляется с использованием ансамбля из моделей рекуррентных нейронных сетей с ячейками долгой краткосрочной памяти для оценки и прогноза частотной характеристики аппроксимируемого конструктивного сетевого трафика и экспоненциального закона распределения случайной величины, параметризованной выходом нейронной сети, для получения численных значений пауз между пакетами прогнозируемого сетевого трафика, что позволяет решать задачу получения временного ряда маскирующего сетевого трафика статистически близкого с конструктивному.

Модель оценки вероятности компрометации маскирования структурно-динамических характеристик сетей передачи данных ведомственного назначения от компьютерной разведки

Существующие подходы к моделированию различных этапов КР в основном основаны на использовании математического аппарата случайных процессов и конечных автоматов. Этапы реализации КР элементов сети в зависимости от степени детализации и специфики воздействий злоумышленниками представляют собой конечное множество дискретных состояний, переход между которыми обусловлен наступлением существенных случайных событий с измеримыми (наблюдаемыми) параметрами, подлежащими оценке.

Цикл КР по вскрытию СДХ СПД ВН с учетом проводимых мероприятий маскирования характеризуется случайным характером компрометации реальных или ложных структурных (например, выявления корреспондирующих абонентов, количества формируемых ИП сетевого трафика в информационных направлениях) или динамических (например, интенсивности сетевого трафика, времени конфигурирования ИП) характеристик СПД ВН, а также ожиданием их компрометации. Таким образом, процесс маскирования СДХ СПД ВН в условиях КР является случайным процессом.

Исходя из вышесказанного, модель оценки вероятности компрометации маскирования СДХ СПД ВН может быть формализована в общем виде как неоднородный марковский случайный процесс ($СП_{mask}$) с дискретными состояниями и непрерывным временем.

В соответствии с теоремой Ляпунова [10] в представленной модели содержится допущение о соблюдении свойства отсутствия последействия, однако снято ограничение об однородности, то есть параметры процесса (интенсивности) в данной модели зависят от времени, следовательно, вероятность нахождения в моделируемых состояниях распределена по экспоненциальному закону распределения, а переходы из состояния в состояние определяются соответствующими интенсивностями перехода в моменты времени. Дискретные состояния представляют собой конечное множество несовместных событий, описывающих существенные свойства сети при ведении КР. Возможные траектории перехода случайного процесса $СП_{mask}$ из состояния в состояние характеризуются ориентированным графом (рис. 1).

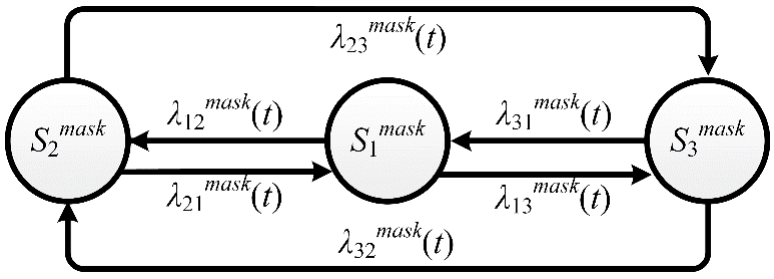

Рис. 1. Граф состояний $СП_{mask}$

Таблица 1 – Дискретные состояния СП$_{mask}$

Состояние	Описание состояний
S_1^{mask}	Ожидание компрометации маскирования структурно-динамических характеристик СПД ВН (защищенное состояния)
S_2^{mask}	Ожидание компрометации маскирования структурно-динамических характеристик СПД ВН при условии вскрытия ложных структурно-динамических характеристик СПД ВН (защищенное состояние)
S_3^{mask}	Ожидание компрометации маскирования структурно-динамических характеристик СПД ВН при условии вскрытия реальных структурно-динамических характеристик СПД ВН (незащищенное состояние)

При этом предусмотрены состояния, в которых СПД ВН будет находится как в защищенном состоянии вследствие результативного маскирования (состояния ожидания компрометации ложных или реальных СДХ СПД ВН S_1 или компрометации ложных СДХ СПД ВН S_2), так и в незащищенном состоянии вследствие нерезультативного маскирования (состояние S_3, когда скомпрометированы реальные СДХ СПД ВН).

Таблица 2 – Интенсивности потоков событий системы СП$_{mask}$

Обозначения	Интерпретация интенсивностей
$\lambda_{12}^{mask}(t)$	Интенсивность потока событий по компрометации ложных структурно-динамических характеристик СПД ВН
$\lambda_{21}^{mask}(t)$	Интенсивность потока событий по реконфигурации сети (формирование новых ложных ИП)
$\lambda_{13}^{mask}(t)$	Интенсивность потока событий по компрометации маскирования реальных структурно-динамических характеристик СПД ВН
$\lambda_{31}^{mask}(t)$	Интенсивность потока событий по реконфигурации сети (формирования новых реальных ИП)
$\lambda_{23}^{mask}(t)$	Интенсивность потока событий по компрометации реальных структурно-динамических характеристик СПД ВН после вскрытия ложных структурно-динамических характеристик СПД ВН
$\lambda_{32}^{mask}(t)$	Интенсивность потока событий по компрометации ложных структурно-динамических характеристик СПД ВН после вскрытия реальных структурно-динамических характеристик СПД ВН

Рассмотрим сценарий перехода моделируемой системы из состояния $S^{mask}{}_i$ в состояние $S^{mask}{}_j$ под воздействием потоков событий с интенсивностями $\lambda_{ij}(t)$.

Пусть нарушитель осуществляет КР постоянно, однако, реализуемые меры защиты предотвращают компрометацию реальных и ложных СДХ СПД ВН, тогда $S^{mask}{}_1$ – начальное состояние моделируемой системы, то есть начальные условия. Начальное распределение вероятностей соответствует представлению о том, что в начальный момент времени система достоверно находится в первом состоянии $P^{mask}(0) = (1, 0, 0)$. Переход из состояния $S^{mask}{}_1$ в состояние $S^{mask}{}_2$ под воздействием интенсивности потока событий $\lambda_{12}^{mask}(t)$ означает момент окончания цикла КР и компрометацию ложных СДХ СПД ВН. При нахождении в состояниях $S^{mask}{}_1$ и $S^{mask}{}_2$ обеспечивается замысел маскирования, интенсивность которого определяется для каждого ИП ($\lambda^{false}{}_{ij}$). Предполагается, что интенсивность событий $\lambda_{12}^{mask}(t)$ по компрометации ложных СДХ пропорциональ-

на доле ложных ИП в СПД ВН, то есть $N^{false}/(N^{false}+N^{real})$, а также пропорционально *p*-значению статистики об однородности усредненных динамических характеристик ложных и реальных ИП, то есть при оценке показателя результативности маскирования СПД ВН учитываются как интегральные структурные характеристики сети, так и качество аппроксимации динамических характеристик ИП. То есть, чем больше доля ложных ИП и выше правдоподобие имитации динамических характеристик ИП (при $P_{compr}\rightarrow 0$), тем выше результирующая частота событий $\lambda_{12}{}^{mask}(t)$ по вскрытию ложных СДХ СПД ВН (то есть введения злоумышленника в заблуждение).

Переход из состояния $S^{mask}{}_1$ в состояние $S^{mask}{}_3$ под воздействием интенсивности потока событий $\lambda_{13}{}^{mask}(t)$, характеризующего момент окончания цикла КР и компрометацию маскирования реальных СДХ СПД ВН. Таким образом, состояние S_3 характеризуется получением КР структуры СПД ВН, отражающей оперативное взаимодействие узлов сети с учетом уровней иерархии (важности) соответствующих узлов ПУ подразделений ведомства. Переход из состояния $S^{mask}{}_3$ в состояние $S^{mask}{}_1$ под воздействием интенсивности потока событий $\lambda_{31}{}^{mask}(t)$ характеризует реакцию системы защиты на компрометацию маскирования реальных СДХ СПД ВН и означает переход системы в защищенное состояние в связи с реконфигурацией сети (формирования новых реальных ИП). Также возможен переход из состояния $S^{mask}{}_2$ в состояние $S^{mask}{}_1$ под воздействием интенсивности потока событий $\lambda_{21}{}^{mask}(t)$, который характеризует реакцию системы защиты на компрометацию ложных СДХ СПД ВН и означает переход системы в состояние окончания цикла КР в связи с реконфигурацией сети (формирования новых ложных ИП). Переход из состояния $S^{mask}{}_2$ в состояние $S^{mask}{}_3$ под воздействием интенсивности потока событий $\lambda_{23}{}^{mask}(t)$ означает компрометацию маскирования реальных СДХ СПД ВН после вскрытия ложных СДХ СПД ВН. Переход из состояния $S^{mask}{}_3$ в состояние $S^{mask}{}_2$ под воздействием интенсивности потока событий $\lambda_{32}{}^{mask}(t)$ означает компрометацию ложных СДХ СПД ВН после компрометации маскирования реальных СДХ СПД ВН.

Перечисленные состояния описывают существенные свойства моделируемой СПД ВН при маскировании СДХ и в любой момент времени составляют полную группу событий (сумма вероятностей пребывания системы в каком-либо из состояний в любой момент времени равна 1, то есть в любой момент времени система достоверно находится в одном из множества состояний).

При моделировании случайного процесса принято допущение, согласно которому значения параметров интенсивности конструктивного λ_j^{rp} и маскирующего сетевого трафика λ_i^{fp} и равны средним значениям во всех реальных или ложных ИП по всем информационным направлениям сети, то есть:

$$\bar{\lambda}^{rp}(t)=\frac{1}{N^{real}}\sum_{j=1}^{N^{real}}\lambda_j^{rp}(t);$$

$$\bar{\lambda}^{fp}(t)=\frac{1}{N^{false}}\sum_{i=1}^{N^{false}}\lambda_i^{fp}(t),$$

где $\bar{\lambda}^{fp}(t)$ – средняя целевая (требуемая) интенсивность генерации маскирующего трафика в СПД ВН (мин$^{-1}$); $\bar{\lambda}^{rp}(t)$ – средняя интенсивность конструктивного сетевого трафика во всех ИП СПД ВН (мин$^{-1}$).

Интенсивность КР λ_{sniff} физически означает среднее количество вскрытий ложных или реальных ИП и определяется выражениями:

$$\lambda_{sniff}^{fp}(t) = K^{sniff} \cdot \bar{\lambda}^{fp^*}(t),$$

$$\lambda_{sniff}^{rp}(t) = K^{sniff} \cdot \bar{\lambda}^{rp}(t),$$

где $K^{sniff} \in [0, \ldots, 0{,}01]$ – коэффициент эффективности КР ИП на одну сессию; $\bar{\lambda}^{fp^*}(t)$ – средняя интенсивность генерации маскирующего трафика, спрогнозированная моделью машинного обучения, с учётом целевой (требуемой) средней интенсивности маскирования в СПД ВН; $\bar{\lambda}^{rp}(t)$ – средняя интенсивность конструктивного сетевого трафика в СПД ВН.

Таким образом, математическая модель исследуемого объекта представлена в виде отображения множества входных параметров случайного процесса M^{mask} во множество выходных вероятностно-временных характеристик K^{mask}.

Математическую модель функционирования системы СП$_{mask}$ можно представить в виде функции (отображения):

$$f^{mask} : M^{mask} \to K^{mask},$$

Входные неуправляемые параметры системы СП$_{mask}$ определяются конструктивным информационным обменом и воздействием КР (внешней средой) и формируют множество неуправляемых факторов A^{mask}:

$$A^{mask} = \{N^{real}, \lambda_i^{rp}(t), K^{sniff}\},$$

где, N^{real} – количество реальных ИП СПД ВН, определяемое структурой СПД ВН и СУВ (шт.); $\lambda_i^{rp}(t)$ – интенсивность конструктивного сетевого трафика в i-м реальном ИП (мин$^{-1}$); K^{sniff} – коэффициент эффективности КР ИП СПД ВН.

Совокупность внутренних параметров системы СП$_{mask}$ включает в себя два подмножества:

$$H^{mask} = \{S^{mask}, X^{mask}\},$$

Подмножество (пространство) состояний системы СП$_{mask}$:

$$S^{mask} = \{S_1^{mask}, S_2^{mask}, S_3^{mask}\},$$

Подмножество контролируемых параметров, влияющих на интенсивности потоков событий, переводящих систему из состояния в состояние:

$$X^{mask} = \{N^{false}, \lambda_i^{fp}(t), t^{if}\},$$

При этом интенсивности потоков событий, инициирующих переходы (таблица 2), представлена следующими выражениями:

$$\lambda_{12}^{mask}(t) = \lambda_{32}^{mask}(t) = (K^{sniff} \cdot \bar{\lambda}^{fp^*}(t)) \frac{N^{false}}{N^{false} + N^{real}} P_{val}\left(\bar{\lambda}^{fp^*}(t), \bar{\lambda}^{rp}(t)\right),$$

$$\lambda_{13}^{mask}(t) = \lambda_{23}^{mask}(t) = (K^{sniff} \cdot \bar{\lambda}^{rp}(t)) \frac{N^{real}}{N^{false} + N^{real}} \left(1 - P_{val}\left(\bar{\lambda}^{fp^*}(t), \bar{\lambda}^{rp}(t)\right)\right),$$

$$\bar{\lambda}^{fp*}(t) = \frac{\bar{\lambda}^{fp}(t)}{\frac{1}{N^{gen}}\sum_{i=1}^{N^{gen}}\hat{\lambda}_i}\{\hat{\boldsymbol{\lambda}}_i\}, i \in [1,...,N^{gen}],$$

$$\lambda_{31}^{mask}(t) = R^{if}\frac{1}{N^{real}},\ \lambda_{21}^{mask}(t) = R^{if}\frac{1}{N^{false}},\ R^{if} = \frac{1}{t^{if}},$$

где $\bar{\lambda}^{fp*}(t)$ – средняя интенсивности генерации маскирующего трафика, спрогнозированная моделью машинного обучения, с учётом целевой (требуемой) средней интенсивности маскирования; N^{false} – количество ложных ИП СПД ВН, определяемое имитируемой структурой (шт.); $\lambda_i^{fp}(t)$ – интенсивность маскирующего сетевого трафика в i-м ложном информационном потоке (мин$^{-1}$); t^{if} – время использования ИП (мин); R^{if} – частота реконфигурации одного ИП (мин$^{-1}$); P_{val} – мера статистической близости маскирующего и конструктивного сетевого трафика по критерию Колмогорова-Смирнова.

Таким образом, множество M^{mask} входных параметров включают в себя входные воздействия и воздействия внешней среды, а также совокупность внутренних параметров системы, то есть:

$$M^{mask} = \{S^{mask}, A^{mask}, X^{mask}\},$$

Совокупность выходных характеристик (свойств) системы, представляет собой множество безусловных вероятностей пребывания системы в соответствующих состояниях в момент времени t, после начала процесса:

$$K^{mask} = \{P^{mask}\},$$

$$P^{mask} = \{p_1^{mask}(t), p_2^{mask}(t), p_3^{mask}(t)\}.$$

В векторной форме выходом модели является вектор $\mathbf{p}^{mask}(t)$:

$$\mathbf{p}^{mask}(t) = (p_1^{mask}(t), p_2^{mask}(t), p_3^{mask}(t)).$$

Отображение f^{mask} множества входных характеристик во множество выходных с учетом неоднородности интенсивностей определяется системой дифференциальных уравнений Колмогорова:

$$\begin{cases} \frac{dp_1^{mask}(t)}{dt} = p_2^{mask}(t)\lambda_{21}^{mask}(t) + p_3^{mask}(t)\lambda_{31}^{mask}(t) - p_1^{mask}(t)(\lambda_{12}^{mask}(t) + \lambda_{13}^{mask}(t)), \\ \frac{dp_2^{mask}(t)}{dt} = p_3^{mask}(t)\lambda_{32}^{mask}(t) + p_1^{mask}(t)\lambda_{12}^{mask}(t) - p_2^{mask}(t)(\lambda_{21}^{mask}(t) + \lambda_{23}^{mask}(t)), \\ \frac{dp_3^{mask}(t)}{dt} = p_2^{mask}(t)\lambda_{23}^{mask}(t) + p_1^{mask}(t)\lambda_{13}^{mask}(t) - p_3^{mask}(t)(\lambda_{31}^{mask}(t) + \lambda_{32}^{mask}(t)), \end{cases}$$

В матричной (векторной) форме:

$$\frac{d\mathbf{p}^{mask}(t)}{dt} = \mathbf{B}^{mask}(t)\cdot\mathbf{p}^{mask}(t),$$

где, $\mathbf{B}^{mask}(t)$ – матрица интенсивностей потоков событий размерностью $\left|S^{mask}\right|$, включающая в себя элементы подмножеств A^{mask} и X^{mask}, и характеризующую систему дифференциальных уравнений:

$$\mathbf{B}^{mask}(t)=\begin{vmatrix} -(\lambda_{12}^{mask}(t)+\lambda_{13}^{mask}(t)) & \lambda_{21}^{mask}(t) & \lambda_{31}^{mask}(t) \\ \lambda_{12}^{mask}(t) & -(\lambda_{23}^{mask}(t)+\lambda_{21}^{mask}(t)) & \lambda_{32}^{mask}(t) \\ \lambda_{13}^{mask}(t) & \lambda_{23}^{mask}(t) & -(\lambda_{32}^{mask}(t)+\lambda_{31}^{mask}(t)) \end{vmatrix}.$$

Определяя значения элементов матрицы $\mathbf{B}^{mask}(t)$ в соответствии с условиями функционирования СПД, вектор вероятностей начальных состояний, систему линейных дифференциальных уравнений решают численными или аналитическими методами (например, методом Рунге-Кутты 4-го или более высоких порядков) при каждом значении времени t с заданной степенью дискретизации, а итоговое решение системы представляет собой суммарные вектора со значениями вероятностей в заданные моменты времени.

Рассмотрим решение системы дифференциальных уравнений в зависимости от различных условий функционирования СПД ВН с учетом нестационарности информационного обмена сетевых устройств.

Для расчета выходных вероятностно-временных характеристик (ВВХ) случайного процесса был использован дамп трафика, содержащий пакеты, сформированные по протоколу HTTP/HTTPS (HyperText Transfer Protocol/HyperText Transfer Protocol Secure), содержащие флаг SYN, инициирующие TCP-соединения, который был зарегистрирован в произвольно выбранном сегменте СПД ВН. Для исследования поведения системы $СП_{mask}$ полученный дамп сетевого трафика был проанализирован и в результате сформирован временной ряд за 60 минут усредненных частот конструктивного сетевого трафика в ИП из тестовой выборки $\{\bar{\lambda}^{rp}(t)\}$, $t \in [1, \ldots, 60]$, отражающий моменты существования активных сессий (с момента поступления *SYN*-пакетов до поступления пакетов с флагами *FIN* или *RST*), а также временной ряд прогнозируемых усредненных частот маскирующего сетевого трафика соответствующей длины, $\{\bar{\bar{\lambda}}(t)\}$, $t \in [1, \ldots, 60]$, генерируемый с использованием модели аппроксимации динамических характеристик конструктивного сетевого трафика на основе нейросети с LSTM-ячейками долгой краткосрочной памяти, имеющую следующую архитектуру: количество слоев в архитектуре $N^{layer} = 2$; количество ячеек в архитектуре $N^{cell} = 46$; количество эпох обучения $N^{epoch} = 16$; длина подпоследовательности для обучения $N^{steps} = 15$; параметр регуляризации $N^{drop} = 0{,}09$; длина аппроксимируемого временного ряда $N^{dump} = 1824$.

Для учета нестационарности интенсивности конструктивного сетевого трафика в момент времени t и условий функционирования СПД ВН на результативность маскирования проведена оценка влияния эффективности КР ИП, требуемой интенсивности генерации маскирующего сетевого трафика, количества ложных ИП СПД ВН, а также интенсивности реконфигурации ИП на вероятность нахождения случайного процесса $СП_{mask}$ в состоянии S_3, характеризующем компрометацию реальных СДХ СПД ВН.

Для указанных условий функционирования, при изменении коэффициента эффективности КР ИП, вероятность пребывания $СП_{mask}$ в состоянии S^{mask}_3 компрометации реальных СДХ СПД ВН с течением времени t меняется в соответствии с результатами, представленными на рис. 2, 3.

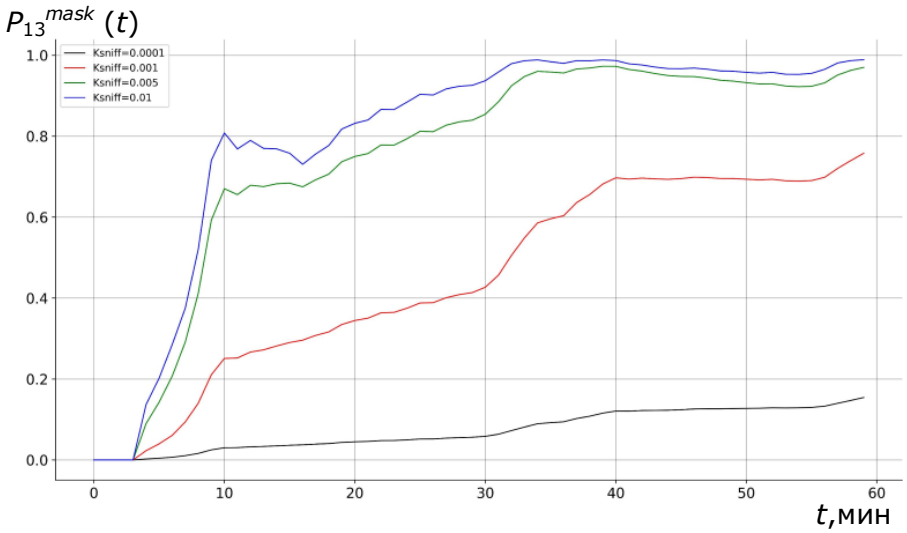

Рис. 2. Результат расчетов вероятности пребывания $СП_{mask}$ в состоянии S^{mask}_3 компрометации маскирования реальных СДХ СПД ВН в зависимости от времени при различных значениях коэффициента эффективности КР K^{sniff} в фиксированных условиях функционирования (при $\bar{\lambda}^{fp} = 150$ мин$^{-1}$, $N^{real}=N^{false}=10$ шт, $t^{if} = 10$ мин$^{-1}$)

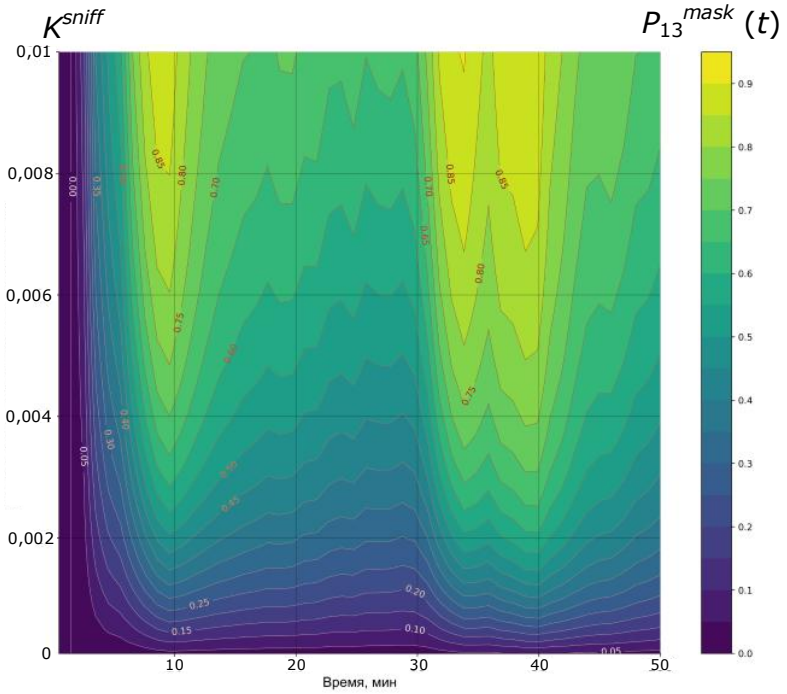

Рис. 3. Тепловая карта расчета вероятности пребывания $СП_{mask}$ в состоянии S^{mask}_3 компрометации маскирования реальных СДХ СПД ВН в зависимости от времени при варьировании значения коэффициента эффективности КР K^{sniff} в фиксированных условиях функционирования (при $\bar{\lambda}^{fp} = 150$ мин$^{-1}$, $N^{real}=N^{false}=10$ шт, $t^{if} = 10$ мин$^{-1}$)

Как видно из расчетов вероятность перехода системы $СП_{mask}$ в состояние компрометации реальных СДХ значительным образом зависит от эффективно-

сти КР злоумышленника. Так, при значении коэффициента K^{sniff} КР равного 0,001, вероятность нахождения системы в состоянии компрометации реальных структурно-динамических характеристик в течение 10 минут находится в пределах до 0,3. Однако, при увеличении значения коэффициента K^{sniff} эффективности КР до 0.01, данная оценка, через аналогичный промежуток времени, попадает в диапазон от 0,8 до 0,85.

Основными управляемыми параметрами при моделировании процесса маскирования СДХ СПД ВН является интенсивность маскирующего сетевого трафика, количество формируемых сетевыми устройствами ложных ИП, а также время реконфигурации ИП СПД ВН.

Результаты расчетов зависимости вероятности нахождения системы $СП_{mask}$ в состоянии компрометации реальных СДХ от средней интенсивности маскирующего трафика в ложных ИП представлены на рис. 4, 5.

В случае приближения значений целевой (требуемой) интенсивности генерации маскирующего сетевого трафика $\{\bar{\lambda}^{fp}(t)\}$ к значению средней интенсивности конструктивного сетевого трафика $\{\bar{\lambda}^{rp}(t)\}$, то в связи с большей однородностью ложных и реальных ИП с точки зрения динамических характеристик конструктивного и маскирующего сетевого трафика, вероятность компрометации маскирования реальных СДХ несколько снижается.

Расчет зависимости вероятности нахождения системы $СП_{mask}$ в состоянии компрометации реальных СДХ от времени t при различных значениях N^{false} показывает, что конфигурирование дополнительных ложных ИП в СПД ВН существенно снижает возможности КР по выявлению реальных СДХ СПД ВН (рис. 6, 7).

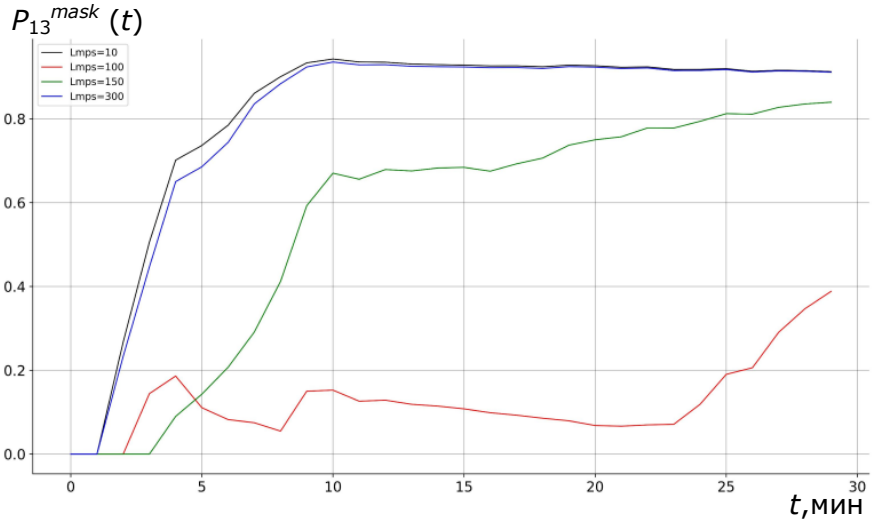

Рис. 4. Результат расчетов вероятности пребывания $СП_{mask}$ в состоянии S^{mask}_3 компрометации маскирования реальных СДХ СПД ВН в зависимости от времени при различных значениях требуемой средней интенсивности $\bar{\lambda}^{fp}$ (по временному ряду) генерации маскирующего сетевого трафика в фиксированных условиях функционирования СПД ВН (при K^{sniff} = 0,005; N^{real}=N^{false}=10 шт; t^{if} = 10 мин$^{-1}$)

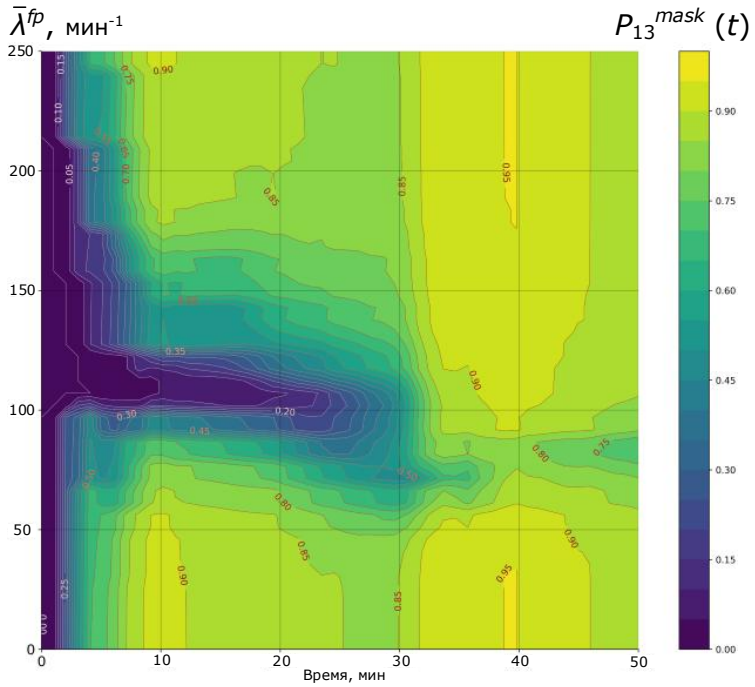

Рис. 5. Тепловая карта расчета вероятности пребывания $СП_{mask}$ в состоянии S^{mask}_3 компрометации маскирования реальных СДХ СПД ВН в зависимости от времени при варьировании значений требуемой средней интенсивности генерации маскирующего сетевого трафика в фиксированных условиях функционирования СПД ВН (при K^{sniff}=0,005; N^{real}=N^{false}=10 шт; t^{if} = 10 мин$^{-1}$)

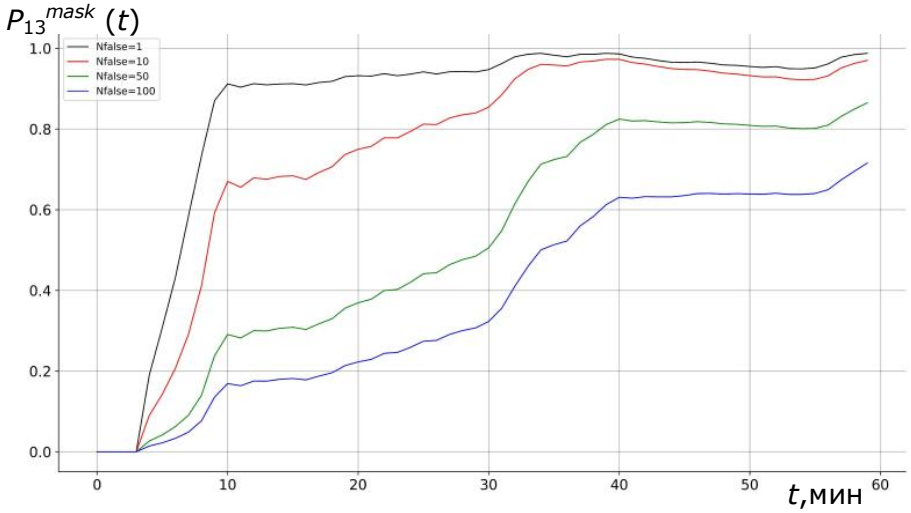

Рис. 6. Результат расчетов вероятности пребывания $СП_{mask}$ в состоянии S^{mask}_3 компрометации маскирования реальных СДХ СПД ВН в зависимости от времени при различных значениях количества ложных информационных потоков N^{false} в фиксированных условиях функционирования СПД ВН (при $\bar{\lambda}^{fp}$ = 150 мин$^{-1}$; N^{real}=10 шт; K^{sniff}=0,005; t^{if} = 10 мин$^{-1}$)

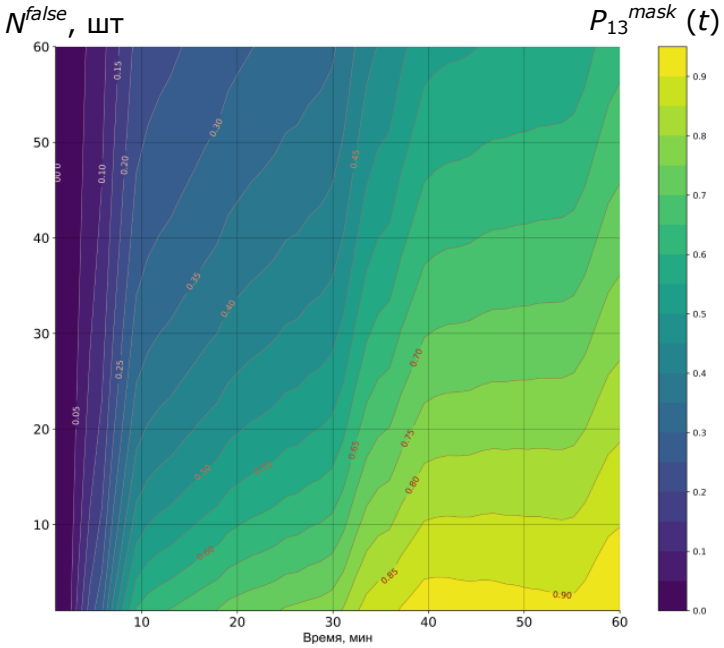

Рис. 7. Тепловая карта расчета вероятности пребывания $СП_{mask}$ в состоянии $S^{mask}{}_3$ компрометации маскирования реальных СДХ СПД ВН в зависимости от времени при варьировании значений количества ложных ИП N^{false} в фиксированных условиях функционирования (при $\bar{\lambda}^{fp}$ =150 мин$^{-1}$; K^{sniff} =0,005; N^{real} =10 шт; t^{if} =10 мин$^{-1}$)

Другой компенсирующей мерой, направленной на противодействие КР, является реконфигурация ИП СПД ВН. Как видно из расчетов вероятность перехода системы $СП_{mask}$ в состояние компрометации маскирования реальных СДХ СПД ВН значительным образом зависит от времени t^{if} использования ИП (рис. 8, 9). Так при продолжительности использования информационных потоков СПД ВН в 0,1 минуту, вероятность нахождения системы в состоянии компрометации $P^{mask}{}_3$ в течение 60 минут находится в пределах до 0,3.

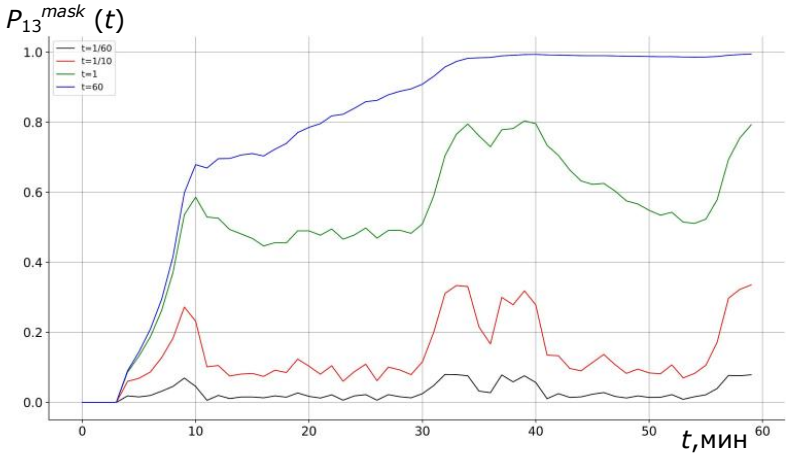

Рис. 8. Результат расчетов вероятности пребывания $СП_{mask}$ в состоянии $S^{mask}{}_3$ компрометации маскирования реальных СДХ СПД ВН в зависимости от времени при различных значениях времени t^{if} использования ИП в фиксированных условиях функционирования (при $\bar{\lambda}^{fp}$ =150 мин$^{-1}$; N^{real}=N^{false}=10 шт; K^{sniff}=0,005)

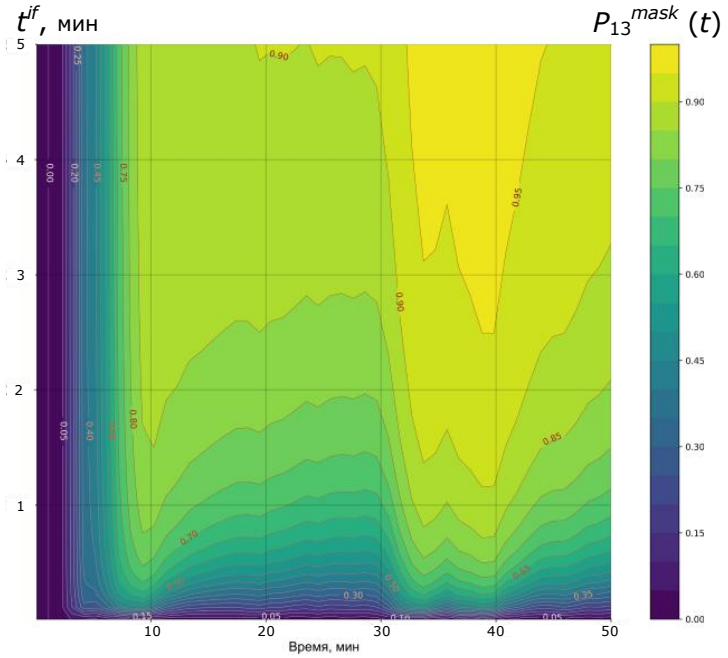

Рис. 9. Тепловая карта расчета вероятности пребывания $СП_{mask}$ в состоянии $S^{mask}{}_3$ компрометации маскирования реальных СДХ СПД ВН в зависимости от времени при варьировании значений времени использования информационных потоков t^{if} в фиксированных условиях функционирования СПД ВН (при $\bar{\lambda}^{fp}$=150 мин$^{-1}$; K^{sniff}=0,005; N^{real}=N^{false}=10 шт)

Однако, при существенном увеличении длительности использования ИП, например, 60 минут до реконфигурации, вероятность компрометации через 35 минут принимает значение 0,98.

Результаты расчетов вероятностей нахождения случайного процесса в одном из состояний к моменту времени t для нестационарного случая показывают, что стационарные вероятности отсутствуют (значения вероятностей постоянно колеблются относительно некоторых средних значений).

Полученные результаты подтверждают влияние различных параметров функционирования СПД ВН на результативность маскирования, а также нестационарность вероятностей пребывания системы $СП_{mask}$ в моделируемых состояниях при использовании реального дампа сетевого трафика узлов СПД ВН, в связи с различными значениями средней интенсивности конструктивного $\bar{\lambda}^{rp}(t)$ в моменты времени t.

Таким образом, разработанная модель позволяет исследовать процесс функционирования СПД ВН при реализации маскирования СДХ СПД ВН с учетом нестационарности потоков сетевого трафика в информационных направлениях между конечными узлами сети, а полученные с помощью модели выходные ВВХ оценки результативности маскирования могут в дальнейшем выступать в качестве целевых функций при решении задачи векторной оптимизации параметров маскирования СДХ СПД ВН в условиях КР.

Научная новизна модели заключается в том, что в отличии от известных [11-14], оценка результативности маскирования ИП осуществляется с использованием математического аппарата теории неоднородных марковских процессов с дискретными состояниями и непрерывным временем для получения ВВХ оценки компрометации маскирования СДХ СПД ВН от КР, позволяющих исследовать функционирование СПД ВН в условиях нестационарности сетевого трафика и формализовать целевую функцию результативности маскирования при постановки задачи векторной оптимизации для определения оптимальных значений параметров маскирования СДХ СПД ВН.

Модель вероятностной оценки доступности сетевых устройств при реализации маскирования структурно-динамических характеристик сетей передачи данных ведомственного назначения

Одним из практических методов маскирования структурно-динамических характеристик в условиях константности состава, связности и оперативного взаимодействия узлов СПД ВН является сокрытие реальных структурных параметров узлов сети путем расширения адресного пространства, введения ложных элементов и динамической смене параметров сетевых соединений при переводе СПД ВН в заранее определенную конфигурацию в условиях КР.

В условиях КР, в связи со спецификой реализации реконфигурации IP-адресов, при использовании протоколов транспортного уровня (например, TCP или SCTP) возможны ситуации, когда сетевые устройства будут находится в состоянии ожидания восстановления сетевых соединений, при котором они недоступны для сетевых соединений и информационного обмена.

Проведенный анализ теоретических и практических аспектов конфигурирования параметров сетевых соединений в условиях КР позволяет сформулировать противоречие между необходимостью повышения доступности узлов СПД ВН при реализации маскирования СДХ от КР и переводе СПД ВН в заранее определенную конфигурацию, с одной стороны, и отсутствием научно-методического обеспечения оценки доступности узлов СПД ВН при реализации процедур маскирования СДХ от КР и переводе СПД ВН в заранее определенную конфигурацию с учетом нестационарности сетевого трафика, с другой стороны.

Для разрешения данного противоречия необходимо разработать математическую модель вероятностной оценки доступности сетевых устройств при реализации маскирования СДХ и переводе СПД ВН в заранее определенную конфигурацию, для получения ВВХ, позволяющих исследовать зависимость нахождения сетевых устройств в состоянии реконфигурации сетевых интерфейсов от параметров маскирования в условиях нестационарности сетевого трафика и КР.

Информационные потоки сетевого трафика в СПД ВН передаются в соответствии с протоколами транспортного уровня (TCP, UDP). При этом переход между состояниями сетевых соединений определяется появлением в случайный момент времени технологических сетевых пакетов, определенных спецификацией соответствующих протоколов. Следовательно, модель вероятностной

оценки доступности узлов сети при реализации маскирования СДХ СПД ВН может быть формализована в общем виде как неоднородный марковский случайный процесс ($СП_{avail}$) с дискретными состояниями и непрерывным временем. Система $СП_{avail}$, отражает функционирование узлов сети, при осуществлении сетевых соединений в условиях реализации маскирования СДХ.

В соответствии с теоремой Ляпунова в представленной модели содержится допущение о соблюдении свойства отсутствия последействия, однако снято ограничение об однородности, то есть параметры процесса (интенсивности) в данной модели зависят от времени, следовательно, вероятность нахождения в моделируемых состояниях (таблица 3) распределена по экспоненциальному закону распределения, а переходы из состояния в состояние определяются соответствующими интенсивностями потоков событий (заявок, требований, факторов), вызывающих переход системы из состояния в состояние в моменты времени (таблица 4). Дискретные состояния представляют собой конечное множество несовместных событий, описывающих существенные свойства системы $СП_{avail}$. Возможные траектории перехода случайного процесса $СП_{avail}$ из состояния в состояние характеризуются ориентированным графом (рис. 10).

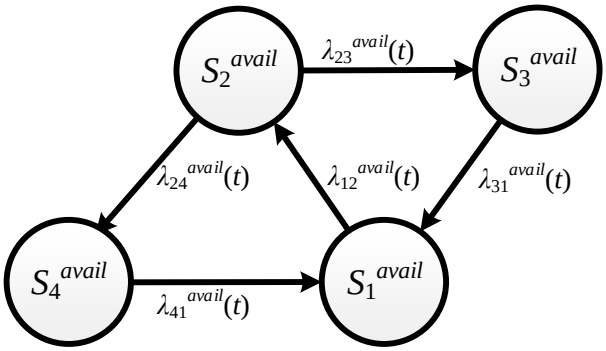

Рис. 10. Граф состояний $СП_{avail}$

Дискретные состояния определены спецификациями протоколов TCP и UDP, а переход между этими состояниями осуществляется при появлении в случайный момент времени соответствующих TCP-пакетов и UDP-сообщений.

Рассмотрим сценарий перехода моделируемой системы из состояния S_i^{avail} в состояние S_j^{avail} под воздействием потоков событий с интенсивностями $\lambda_{ij}^{avail}(t)$.

В соответствии со спецификацией протокола TCP, определено состояние S_1^{avail}, которое характеризуется ожиданием получения инициирующих сетевое соединение пакетов со служебными заголовками SYN, и является начальным состоянием моделируемой системы $СП_{avail}$ (начальным условием). Начальное распределение вероятностей соответствует представлению о том, что в начальный момент времени система достоверно находится в первом состоянии $P^{avail}(0)=(1, 0, 0, 0)$. Переход из состояния S_1^{avail} в состояние S_2^{avail} под воздействием интенсивности потока событий $\lambda_{12}^{avail}(t)$ означает момент окончания ожидания инициализации сетевого соединения (формирования логического канала), и ожидание обработки (приема, передачи) данных, характеризующееся получением пакетов со служебными заголовками DATA. После завершения

инициализации сетевого соединения (формирования логического канала) СПД ВН находятся в ожидании обработки (приема, передачи) сетевыми устройствами данных (пакетов со служебными заголовками DATA), что соответствует состоянию S_2^{avail}. Состояние S_2^{avail} характеризуется динамической сменой IP-адресов на интерфейсах, из множества («пула»), полученного от DHCP-сервера, которая может производится «по возмущению», например, когда поступает управляющий сигнал от системы обнаружения атак или от лица, принимающего решение (например, реконфигурация сети как реакция на смену оперативной обстановки). Переход из состояния S_2^{avail} в состояние S_3^{avail} под воздействием интенсивности потока событий $\lambda_{23}^{avail}(t)$ означает окончание ожидания обработки данных и начало ожидания завершения передачи информационных потоков и сетевого соединения между сетевыми устройствами СПД ВН (получение пакетов со служебными заголовками RST, FIN). Переход из состояния S_3^{avail} в состояние S_1^{avail} под воздействием интенсивности потока событий $\lambda_{31}^{avail}(t)$ характеризует завершение сетевого соединения в связи с обработкой поступающих данных сетевыми устройствами СПД ВН и переходом системы $СП_{avail}$ в состояние простоя. Переход из состояния S_2^{avail} в состояние S_4^{avail} под воздействием интенсивности потока событий $\lambda_{24}^{avail}(t)$ означает момент окончания ожидания обработки данных и начало ожидания окончания реконфигурации сетевых интерфейсов узлов сети и перевода сетевых устройств в заранее определенную конфигурацию (получение сетевыми устройствами от DHCP-сервера служебных сообщений DHCPACK, означающих окончание перевода СПД ВН в заранее определенную конфигурацию). Состояние S_4^{avail} характеризуется исчерпанием нескомпрометированных IP-адресов из ранее заданного множества и необходимостью реконфигурации сетевых интерфейсов с использованием нового пула IP-адресов, получаемого от DHCP-сервера. Перечисленные состояния описывают процесс функционирования СПД ВН при конфигурировании параметров сетевых интерфейсов узлов сети в условиях маскирования СДХ СПД ВН и в любой момент времени составляют полную группу событий (сумма вероятностей пребывания системы в каком-либо из событий в любой момент времени равна 1, то есть в каждый момент времени система достоверно находится в одном из множества состояний).

Таблица 3 – Характеристика состояний $СП_{avail}$

Состояние	**Описание состояний**
S_1^{avail}	Ожидание инициализации сетевого соединения сетевых устройств СПД ВН (ожидание получения пакетов со служебными заголовками SYN)
S_2^{avail}	Ожидание приема и передачи данных между УС (ожидание получения служебных пакетов с заголовками DATA)
S_3^{avail}	Ожидание завершения сетевого соединения (ожидание получения служебных пакетов с заголовками RST, FIN) или ожидания реконфигурации сетевых интерфейсов
S_4^{avail}	Ожидание окончания реконфигурации сетевых интерфейсов (процесс смены IP-адресов) (ожидание получения служебных пакетов DHCPACK)

Таблица 4 – Интенсивности потоков событий системы СП$_{avail}$

Переменная	**Описание параметра**
$\lambda_{12}^{avail}(t)$	Интенсивность поступления запросов на инициализацию сетевых соединений
$\lambda_{23}^{avail}(t)$	Интенсивность поступления запросов на передачу и прием информационных потоков между УС
$\lambda_{31}^{avail}(t)$	Интенсивность поступления запросов на завершение сетевых соединений
$\lambda_{24}^{avail}(t)$	Интенсивность запросов на реконфигурацию сетевых интерфейсов УС в связи со сменой IP-адресов
$\lambda_{41}^{avail}(t)$	Интенсивность запросов на возобновление информационного обмена в связи с завершением перевода сетевых устройств СПД ВН в заранее определенную конфигурацию.

Таким образом, математическую модель функционирования системы СП$_{avail}$ можно представить в виде функции (отображения):

$$f^{avail} : M^{avail} \to K^{avail}.$$

Входные неуправляемые параметры системы СП$_{avail}$ определяются структурно-динамическими параметрами конструктивного сетевого трафика, а также аппаратными и программными характеристиками сетевых устройств, осуществляющих информационный обмен в СПД ВН и формируют множество неуправляемых факторов A^{avail}:

$$A^{avail} = \{N^{real}, \bar{\lambda}^{rp}(t), \lambda_{23}^{avail}(t), \lambda_{31}^{avail}, T^{rec}\},$$

где N^{real} – количество в СПД ВН реальных ИП (количество конфигурируемых интерфейсов для конструктивного трафика), определяемое структурой СПД ВН и системой управления (шт.); $\bar{\lambda}^{rp}(t)$ – средняя интенсивность конструктивного сетевого трафика по всем ИП СПД ВН (мин$^{-1}$); T^{rec} – среднее время на реконфигурацию одного IP-адреса на сетевом интерфейсе при переводе сетевого устройства в заранее определенную конфигурацию (смене IP-адресов) (мин).

Совокупность внутренних параметров системы СП$_{avail}$ включает в себя два подмножества:

$$H^{avail} = \{S^{avail}, X^{avail}\}.$$

Подмножество (пространство) состояний системы СП$_{avail}$:

$$S^{avail} = \{S_1^{avail}, S_2^{avail}, S_3^{avail}, S_4^{avail}\}.$$

Подмножество контролируемых параметров, влияющих на интенсивности потоков событий, переводящих систему из состояния S_i^{avail} в состояние S_j^{avail}:

$$X^{avail} = \{N^{false}, \bar{\lambda}^{fp}(t), t^{ip}, U^{IP}\}.$$

При этом интенсивности потоков событий, инициирующих переходы (таблица 4) из состояния S_i^{avail} в состояние S_j^{avail}, зависят от условий функционирования СПД ВН и задаются следующими выражениями:

$$\lambda_{12}^{avail}(t) = \bar{\lambda}^{fp}(t)N^{false} + \bar{\lambda}^{rp}(t)N^{real},\ \lambda_{24}^{avail}(t) = \frac{1}{t^{ip}},\ \lambda_{23}^{avail}(t) = \frac{1}{T^{data}},$$

$$\lambda_{31}^{avail}(t) = \frac{1}{T^{serv}},\ \lambda_{41}^{avail}(t) = \frac{1}{T^{rec}U^{IP}(N^{real} + N^{false})},$$

где, U^{IP} – количество IP-адресов на сетевом интерфейсе, подлежащих реконфигурации (шт); t^{ip} – время использования IP-адресов на сетевых интерфейсах сетевых устройств СПД ВН (мин); N^{false} – количество в СПД ВН ложных ИП, определяемое имитируемой структурой (количество конфигурируемых интерфейсов для маскирующего трафика) (шт.); $\bar{\lambda}^{fp}(t)$ – средняя интенсивность маскирующего сетевого трафика по всем ИП (мин$^{-1}$); T^{data} – среднее время поступления пакетов со служебными заголовками DATA, мин; T^{serv} – среднее время поступления заявок на завершение сетевого соединения, мин.

Таким образом, множество M^{avail} входных характеристик включают в себя входные воздействия и воздействия внешней среды, а также совокупность внутренних параметров системы, то есть:

$$M^{avail} = \{S^{avail}, A^{avail}, X^{avail}\}.$$

Совокупность выходных характеристик (свойств) системы, представляет собой множество безусловных вероятностей пребывания системы в соответствующих состояниях в момент времени t, после начала процесса:

$$K^{avail} = \{P^{avail}\},$$

$$P^{avail} = \{p_1^{avail}(t), p_2^{avail}(t), p_3^{avail}(t), p_4^{avail}(t)\}.$$

В векторной форме выходом модели является вектор $\mathbf{p}^{avail}(t)$:

$$\mathbf{p}^{avail}(t) = (p_1^{avail}(t), p_2^{avail}(t), p_3^{avail}(t), p_4^{avail}(t)).$$

Отображение f^{avail} множества входных характеристик во множество выходных с учетом неоднородности интенсивностей определяется системой дифференциальных уравнений Колмогорова:

$$\begin{cases} \frac{dp_1^{avail}(t)}{dt} = p_3^{avail}(t)\lambda_{31}^{avail}(t) + p_4^{avail}(t)\lambda_{41}^{avail}(t) - p_1^{avail}(t)\lambda_{12}^{avail}(t), \\ \frac{dp_2^{avail}(t)}{dt} = p_1^{avail}(t)\lambda_{12}^{avail}(t) - p_2^{avail}(t)(\lambda_{23}^{avail}(t) + \lambda_{24}^{avail}(t)), \\ \frac{dp_3^{avail}(t)}{dt} = p_2^{avail}(t)\lambda_{23}^{avail}(t) - p_3^{avail}(t)\lambda_{31}^{avail}(t), \\ \frac{dp_4^{avail}(t)}{dt} = p_2^{avail}(t)\lambda_{24}^{avail}(t) - p_4^{avail}(t)\lambda_{41}^{avail}(t), \\ \sum_{i=1}^{4} p_i^{avail}(t) = 1. \end{cases}$$

В матричной (векторной) форме:

$$\frac{d\mathbf{p}^{avail}(t)}{dt} = \mathbf{B}^{avail}(t) \cdot \mathbf{p}^{avail}(t),$$

где $\mathbf{B}^{avail}(t)$ – матрица интенсивностей потоков событий размерностью $\left|S^{avail}\right|$, включающая в себя элементы подмножеств A^{avail} и X^{avail}, и характеризующую систему дифференциальных уравнений:

$$\mathbf{B}^{avail}(t)=\begin{vmatrix} -\lambda_{12}^{avail}(t) & 0 & \lambda_{31}^{avail}(t) & \lambda_{41}^{avail}(t) \\ \lambda_{12}^{avail}(t) & -(\lambda_{23}^{avail}(t)+\lambda_{24}^{avail}(t)) & 0 & 0 \\ 0 & \lambda_{23}^{avail}(t) & -\lambda_{31}^{avail}(t) & 0 \\ 0 & \lambda_{24}^{avail}(t) & 0 & -\lambda_{41}^{avail}(t) \end{vmatrix}.$$

Для учета параметров функционирования СПД ВН на доступность сетевых устройств при реализации маскирования СДХ СПД ВН, в условиях КР и перевода узлов сети в заранее определенную конфигурацию, проведена оценка их влияния на значения вероятности нахождения случайного процесса $СП_{avail}$ в подмножестве состояний.

Для расчета выходных ВВХ случайного процесса $СП_{avail}$ в условиях нестационарности конструктивного трафика был использован дамп сетевого трафика, собранный с использованием утилиты tcpdump в сегменте СПД ВН, который применялся ранее для решения задачи аппроксимации динамических характеристик ИП конструктивного сетевого трафика и получения ВВХ компрометации маскирования СДХ СПД ВН.

Для учета нестационарности интенсивности конструктивного сетевого трафика в момент времени t сетевого трафика и условий функционирования СПД ВН на доступность узлов сети при реализации маскирования проведена оценка влияния времени использования IP-адресов t^{ip} на сетевых интерфейсах, количества IP-адресов U^{IP}, подлежащих конфигурированию на сетевом интерфейсе, количества конфигурируемых ложных ИП N^{false} (сетевых интерфейсов для маскирующего сетевого трафика), а также требуемой интенсивности маскирующего сетевого трафика $\overline{\lambda}^{fp}$ на вероятность нахождения случайного процесса $СП_{avail}$ в состоянии $S^{avail}{}_4$, характеризующем недоступность СПД ВН в зависимости от времени t.

В рассматриваемых условиях функционирования увеличение количества IP-адресов U^{IP}, подлежащих конфигурированию на сетевом интерфейсе, и количества конфигурируемых ложных ИП N^{false} (сетевых интерфейсов для маскирующего сетевого трафика), определяет увеличение вероятности пребывания $СП_{avail}$ в состоянии $S^{avail}{}_4$ отказа в обслуживании легитимных клиентов в связи с ожиданием окончания реконфигурации в диапазонах [0; 0,42].

Значения вероятности пребывания сетевых устройств в недоступном состоянии при варьировании интенсивности маскирующего обмена до 250 мин$^{-1}$ в указанных условиях функционирования достигает значения 0,21.

Как видно из рис. 14, время использования IP-адресов на сетевых интерфейсах t^{ip} значительно влияет на доступность сетевых устройств для информационного обмена.

Так увеличение времени аренды IP-адресов на сетевых интерфейсах до 3 минут 45 с и более снижает, в заданных условиях функционирования, вероятность пребывания $СП_{avail}$ в недоступном состоянии $S^{avail}{}_4$ до нуля.

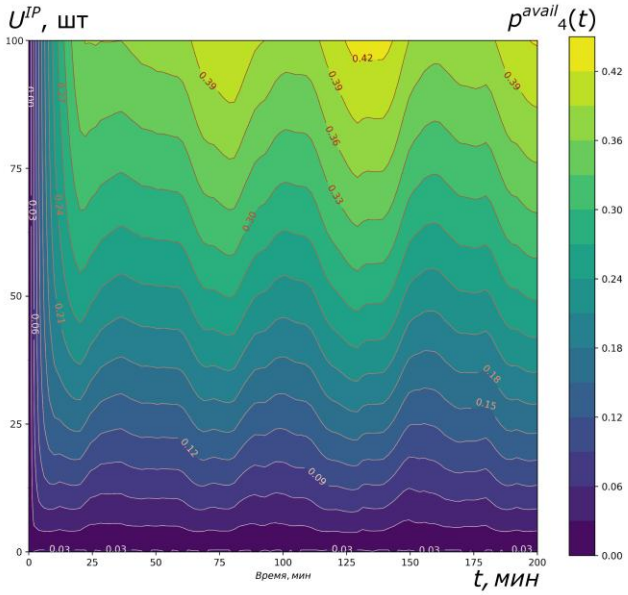

Рис. 11. Тепловая карта расчета вероятности пребывания $СП_{avail}$ в состоянии $S^{avail}{}_4$ в зависимости от времени при варьировании количества IP-адресов U^{IP}, конфигурируемых на сетевом интерфейсе, в фиксированных условиях функционирования СПД ВН: T^{data} = 10^{-4} мин; T^{serv} = 10^{-3} мин; N^{real}=10; N^{false} = 10; $\bar{\lambda}^{fp}$ = 200 $мин^{-1}$, T^{rec} = 0,005 мин; t^{ip} = 1 мин

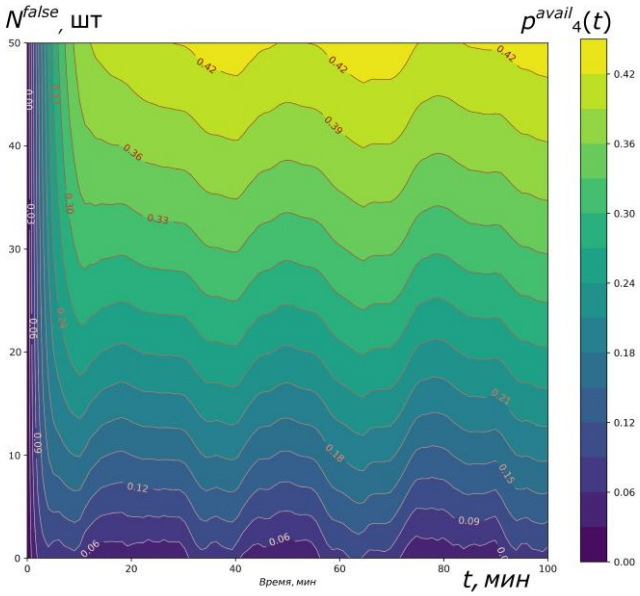

Рис. 12. Тепловая карта расчета вероятности пребывания $СП_{avail}$ в состоянии $S^{avail}{}_4$ в зависимости от времени при варьировании количества ложных ИП N^{false} в фиксированных условиях функционирования СПД ВН: T^{data} = 10^{-4} мин; T^{serv} = 10^{-3} мин; N^{real}=10; U^{IP} = 30; $\bar{\lambda}^{fp}$ =250 $мин^{-1}$; T^{rec} = 0,005 мин; t^{ip} = 1 мин

DOI: 10.24412/2410-9916-2026-1-138-181
URL: https://sccs.intelgr.com/archive/2026-01/05-Sherstobitov.pdf

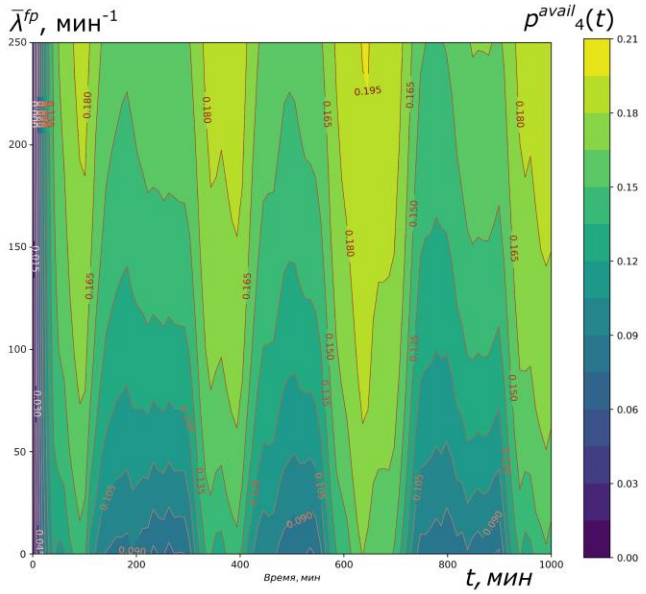

Рис. 13. Тепловая карта расчета вероятности пребывания СП$_{avail}$ в состоянии $S^{avail}{}_4$ в зависимости от времени при варьировании средней интенсивности маскирующего трафика $\bar{\lambda}^{fp}$ в фиксированных условиях функционирования СПД ВН: T^{data} = 10^{-4} мин; T^{serv} = 10^{-3} мин; N^{real}=10; N^{false} = 10; U^{IP} = 30; T^{rec} = 0,005 мин; t^{ip} = 1 мин

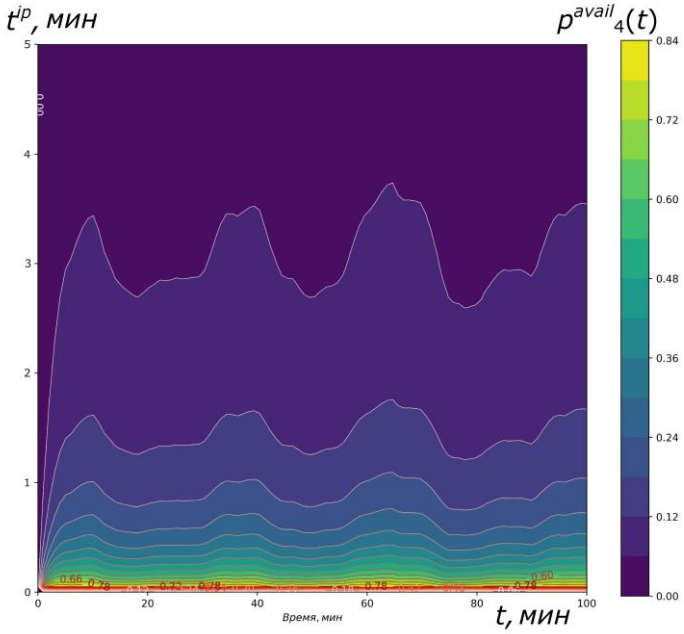

Рис. 14. Тепловая карта расчета вероятности пребывания СП$_{avail}$ в состоянии $S^{avail}{}_4$ в зависимости от времени при варьировании длительности использования IP-адресов t^{ip} на сетевых интерфейсах в фиксированных условиях функционирования СПД ВН: T^{data} = 10^{-4} мин; T^{serv} = 10^{-3} мин; $\bar{\lambda}^{fp}$ =200 мин$^{-1}$; N^{real}=10; N^{false} = 10; U^{IP} = 30; T^{rec} = 0,005 мин

С другой стороны, уменьшение времени аренды IP-адресов на сетевых интерфейсах менее 1 минуты существенно повышает вероятность пребывания $СП_{avail}$ в недоступном состоянии S^{avail}_4, значение которой достигает 0,84.

Таким образом, установлено влияние условий функционирования на доступность СПД ВН при реализации маскирования СДХ СПД от КР и переводе узлов сети в заранее определенную конфигурацию с учетом нестационарности сетевого трафика.

Использование модели позволяет исследовать процесс функционирования СПД ВН при реализации маскирования СДХ СПД от КР и переводе узлов сети в заранее определенную конфигурацию в условиях нестационарности сетевого трафика, а полученные с помощью модели выходные вероятностно-временные характеристики оценки доступности сетевых устройств при конфигурировании сетевых интерфейсов могут в дальнейшем выступать в качестве целевых функций при формулировании задачи векторной оптимизации.

Научная новизна модели заключается в том, что, в отличие от известных [15-17] оценка доступности сетевых устройств СПД ВН при реализации маскирования СДХ осуществляется с использованием математического аппарата теории неоднородных марковских процессов с дискретными состояниями и непрерывным временем для получения ВВХ, позволяющих исследовать зависимость нахождения сетевых устройств в состоянии реконфигурации сетевых интерфейсов от параметров маскирования в условиях нестационарности сетевого трафика, и формализовать целевую функцию доступности сетевых устройств при постановки задачи векторной оптимизации для определения оптимальных значений параметров маскирования СДХ СПД ВН в условиях КР.

Модель вероятностной оценки своевременности информационного обмена сетевых устройств при реализации маскирования структурно-динамических характеристик СПД ВН

Маскирование СДХ СПД ВН характеризуется возможностью образования очередей из конструктивных и маскирующих пакетов сообщений на средствах обработки информации у передающего и принимающего узлов сети, что затрудняет выполнение требований по своевременности информационного обмена конструктивными пакетами сообщений. Проведенный анализ теоретических и практических аспектов оценки своевременности информационного обмена в СПД ВН в условиях маскирования СДХ позволяет сформулировать противоречие между необходимостью обеспечения своевременности информационного обмена сетевых устройств при реализации функций маскирования, с одной стороны, и отсутствием научно-методического обеспечения оценки своевременности информационного обмена сетевых устройств в различных условиях функционирования СПД ВН при реализации маскирования СДХ от КР, с другой стороны.

Для разрешения данного противоречия необходимо разработать математическую модель оценки своевременности информационного обмена сетевых устройств, позволяющую определить вероятностно-временные характеристики

обработки конструктивного трафика в различных условиях функционирования СПД ВН при реализации маскирования СДХ от КР.

Для оценки влияния маскирования на своевременность информационного обмена конструктивным сетевым трафиком, целесообразно, в результате моделирования случайного процесса, получить аппроксимацию функции распределения обработки конструктивного трафика к моменту времени в различных условиях функционирования СПД ВН. Таким образом, модель оценки своевременности информационного обмена сетевых устройств при реализации маскирования СДХ СПД ВН может быть формализована в общем виде как однородный полумарковский случайный процесс ($СП_{time}$) с дискретными состояниями и непрерывным временем, который определяется функциями распределениями времени ожидания в соответствующих состояниях и вероятностями перехода между состояниями. Дискретные состояния $СП_{time}$ представляют собой конечное множество несовместных событий, описывающих существенные свойства СПД ВН при информационном обмене конструктивным и маскирующим сетевым трафиком. Возможные траектории перехода случайного процесса $СП_{time}$ из состояния в состояние характеризуются ориентированным графом (рис. 15)

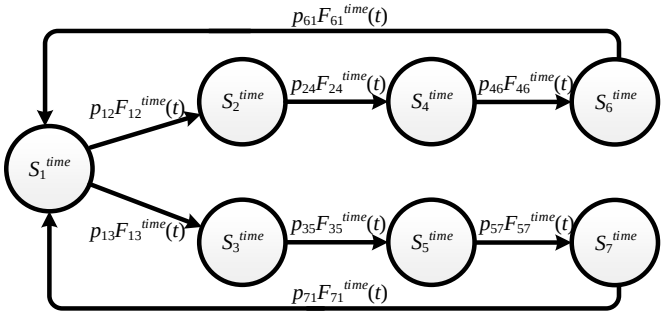

Рис. 15. Граф состояний $СП_{time}$

Таблица 5 – Дискретные состояния $СП_{time}$

Состояние	Описание состояний
S_1^{time}	Ожидание начала передачи данных (конструктивного или маскирующего сетевого трафика)
S_2^{time}	Ожидание окончания передачи конструктивного сетевого трафика
S_3^{time}	Ожидание окончания передачи маскирующего сетевого трафика
S_4^{time}	Ожидание окончания обработки конструктивного сетевого трафика
S_5^{time}	Ожидание окончания обработки маскирующего сетевого трафика
S_6^{time}	Ожидание завершения конструктивного информационного обмена
S_7^{time}	Ожидание завершения маскирующего информационного обмена

Дискретным состояниям C_{time}, соответствуют вероятностные характеристики (табл. 6).

Таблица 6 – Вероятностные характеристики $СП_{time}$

Переменная	Описание параметра
$F_{12}^{time}(t)$	Функция распределения времени ожидания поступления запросов на передачу конструктивного трафика
$F_{13}^{time}(t)$	Функция распределения времени ожидания поступления запросов на передачу маскирующего трафика
$F_{24}^{time}(t)$	Функция распределения времени ожидания окончания передачи конструктивного трафика
$F_{35}^{time}(t)$	Функция распределения времени ожидания окончания передачи маскирующего трафика
$F_{46}^{time}(t)$	Функция распределения времени ожидания окончания обработки конструктивного трафика
$F_{57}^{time}(t)$	Функция распределения времени ожидания окончания обработки маскирующего трафика
$F_{61}^{time}(t)$	Функция распределения времени ожидания завершения конструктивного информационного обмена
$F_{71}^{time}(t)$	Функция распределения времени ожидания завершения маскирующего информационного обмена

Пусть имеется СПД ВН, в которой для реализации замысла защиты реализуют маскирование СДХ. Физически СПД ВН включает в себя корреспондирующие сетевые устройства, являющиеся отправителями и приемниками конструктивного и маскирующего сетевого трафика.

От передающих абонентов в СПД ВН и далее в ССОП поступает простейший поток однородных событий с интенсивностью λ, потенциально переводящих СПД ВН в состояния передачи и приема конструктивного или маскирующего сетевого трафика.

Переход системы в одно из антагонистических состояний обусловливается тем, что СПД ВН в штатных режимах функционирования справится с требуемой нагрузкой, тогда как наличие маскирующего трафика при передаче конструктивного трафика может создавать дополнительную нагрузку на сетевые устройства, что приведет к образованию очередей из конструктивных и маскирующих пакетов сообщений.

На входе приемника могут также образовываться очереди из конструктивных и маскирующих пакетов сообщений, особенно при увеличении интенсивности сетевого трафика от нескольких источников.

Модель вероятностной оценки своевременности информационного обмена в СПД ВН при реализации маскирования СДХ учитывает параметры интенсивности конструктивного и маскирующего сетевого трафика в СПД ВН, объема, передаваемых за сессию данных, а также скорости (пропускной способности) передачи и обработки конструктивного и маскирующего трафика. Использование математической модели предполагает поиск условий для эффективного функционирования СПД ВН и позволит перейти к вероятностной оценке своевременности информационного обмена.

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

Пусть формирование конструктивных или маскирующих пакетов сообщений происходит не постоянно, тогда система C_{time} в начальный момент времени находится в состоянии S_1^{time} ожидания начала информационного обмена сетевых устройств. Таким образом, начальное распределение вероятностей соответствует представлению о том, что в начальный момент времени система достоверно находится в первом состоянии $P^{time}(0)=(1, 0, 0, 0, 0, 0, 0)$.

Переход из S_1^{time} в S_2^{time} означает момент окончания простоя системы и начало конструктивного информационного обмена между сетевыми устройствами СПД ВН. В состоянии S_2^{time} сетевые устройства осуществляют передачу конструктивного трафика. При этом, функция распределения времени ожидания поступления запросов на передачу конструктивного трафика $F_{12}^{time}(t)$ определяется интенсивностью сессий конструктивного сетевого трафика (λ_{12}^{time}), задаваемой для каждого информационного направления СПД ВН, в зависимости от уровня иерархии узлов связи соответствующих пунктов управления в системе управления ведомством.

Состояние S_2^{time} характеризуется ожиданием окончания передачи конструктивного трафика сетевыми устройствами. При этом, функция распределения времени ожидания окончания передачи конструктивного трафика $F_{24}^{time}(t)$ определяется интенсивностью λ_{24}^{time}, которая зависит от объема конструктивного сетевого трафика за сессию D^{real}, а также скорости V^{tr} передачи (пропускной способности) сетевого трафика в канал связи.

В состоянии S_4^{time} сетевые устройства СПД ВН осуществляют обработку поступившего от отправителей конструктивного трафика. При этом, функция распределения времени ожидания окончания обработки конструктивного трафика $F_{46}^{time}(t)$ определяется интенсивностью λ_{46}^{time}, которая зависит от объема конструктивного трафика за сессию D^{real}, а также скорости V^{rec} обработки (пропускной способности) сетевого трафика на сетевом устройстве-приемнике.

В состоянии S_6^{time} узлы СПД ВН завершили обработку конструктивного сетевого трафика и находятся в состоянии ожидания завершения информационного обмена. При этом, функция распределения времени ожидания окончания конструктивного информационного обмена $F_{61}^{time}(t)$ определяется интенсивностью λ_{61}^{time}, которая зависит от времени поступления пакетов с флагами FIN или RST, означающих завершение сетевого соединения и переход сетевых устройств в состояние простоя.

Состояние инициализации процесса передачи конструктивного сетевого трафика S_2^{time}, состояние ожидания окончания приема конструктивного информационного обмена S_4^{time} и состояние ожидания завершения конструктивного информационного обмена S_6^{time} соответствуют целевому предназначению СПД ВН. Таким образом, вероятность первого достижения состояния S_6^{time} из состояния S_1^{time} к моменту времени t определяет своевременность информационного обмена конструктивным трафиком.

Переход из S_1^{time} в S_3^{time} означает момент окончания простоя системы и начало маскирующего информационного обмена в СПД ВН. При этом, функция

распределения времени ожидания поступления запросов на передачу маскирующего трафика $F_{13}^{time}(t)$ определяется интенсивностью сессий маскирующего сетевого трафика (λ_{13}^{time}), определяемой для каждого информационного направления СПД ВН.

Состояние S_3^{time} характеризуется ожиданием окончания передачи сетевыми устройствами маскирующего трафика. При этом, функция распределения времени ожидания окончания передачи маскирующего трафика $F_{35}^{time}(t)$ определяется интенсивностью λ_{35}^{time}, которая зависит от объема маскирующего сетевого трафика за сессию D^{false}, а также скорости V^{tr} передачи (пропускной способности) сетевого трафика в канал связи.

В состоянии S_5^{time} сетевые устройства, принимающие маскирующий трафик, осуществляют его обработку. При этом, функция распределения времени ожидания окончания обработки маскирующего трафика $F_{57}^{time}(t)$ определяется интенсивностью λ_{57}^{time}, которая зависит от объема маскирующего трафика за сессию D^{false}, а также скорости V^{rec} обработки (пропускной способности) сетевого трафика на сетевом устройстве-приемнике.

В состоянии S_7^{time} узлы СПД ВН завершили обработку маскирующего сетевого трафика и находятся в состоянии ожидания завершения маскирующего информационного обмена. При этом, функция распределения времени ожидания окончания маскирующего информационного обмена $F_{71}^{time}(t)$ определяется интенсивностью λ_{71}^{time}, которая зависит от времени поступления сетевых пакетов с флагами FIN или RST, означающих завершение сетевого соединения и их переход сетевых устройств в состояние простоя.

Перечисленные состояния описывают существенные свойства моделируемой СПД ВН при осуществлении сетевыми устройствами информационного обмена конструктивным и маскирующим трафиком и в любой момент времени составляют полную группу событий (сумма вероятностей пребывания системы в каком-либо из событий в любой момент времени равна 1, то есть в каждый момент времени система достоверно находится в одном из множества состояний).

Таким образом, математическая модель оценки своевременности (оперативности) информационного обмена сетевых устройств при реализации маскирования СДХ СПД ВН представлена в виде отображения множества входных параметров случайного процесса M^{time} во множество выходных вероятностно-временных характеристик K^{time}.

Тогда, математическую модель функционирования системы $СП_{time}$ можно представить в виде функции (отображения):

$$f^{time}: M^{time} \to K^{time}.$$

Входные неуправляемые параметры системы $СП_{time}$ определяются конструктивным сетевым трафиком, характеристиками сетевых устройств, каналов передачи данных (внешней средой) и формируют подмножество (пространство) неуправляемых факторов A^{time}:

Совокупность внутренних параметров системы $СП_{time}$ включает в себя два подмножества: $H^{time} = \{S^{time}, X^{time}\}$.

Подмножество (пространство) состояний системы $СП_{time}$:

$$S^{time} = \{S_1^{time}, S_2^{time}, S_3^{time}, S_4^{time}, S_5^{time}, S_6^{time}, S_7^{time}\}.$$

Контролируемые параметры, влияющие на интенсивности потоков событий, переводящих систему из состояния S_i^{time} в состояние S_j^{time}, формируют подмножество (пространство) X^{time}.

При этом, контролируемые параметры X^{time} и неуправляемые факторы A^{time}, задаются как:

$$A^{time} = \{\bar{\lambda}^{rp}(t), N^{real}, V^{rec}, V^{tr}, D^{real}, K_{buf}^{rec}, K_{buf}^{tr}, T^{FIN}\},$$

$$F_{12}^{time}(t) = 1 - e^{-\lambda_{24}^{time} t}, F_{61}^{time}(t) = 1 - e^{-\lambda_{61}^{time} t}, F_{71}^{time}(t) = 1 - e^{-\lambda_{71}^{time} t},$$

$$при\ \lambda_{12}^{time} = \bar{\lambda}^{rp}(t) N^{real}, \lambda_{61}^{time} = \lambda_{71}^{time} = \frac{1}{T^{FIN}}.$$

$$X^{time} = \{\bar{\lambda}^{fp}(t), N^{false}, D^{false}\},$$

$$F_{13}^{time}(t) = 1 - e^{-\lambda_{13}^{time} t}, F_{35}^{time}(t) = 1 - e^{-\lambda_{35}^{time} t}, F_{57}^{time}(t) = 1 - e^{-\lambda_{51}^{time} t},$$

$$F_{24}^{time}(t) = 1 - e^{-\lambda_{12}^{time} t}, F_{46}^{time}(t) = 1 - e^{-\lambda_{46}^{time} t},$$

$$при\ \lambda_{13}^{time} = \bar{\lambda}^{fp}(t) N^{false}, \lambda_{35}^{time} = \frac{V^{tr} \cdot K_{buf}^{tr}}{(D^{real} \cdot N^{real}) + (D^{false} \cdot N^{false})},$$

$$\lambda_{57}^{time} = \frac{V^{rec} \cdot K_{buf}^{rec}}{(D^{real} \cdot N^{real}) + (D^{false} \cdot N^{false})},$$

$$\lambda_{24}^{time} = \frac{V^{tr} \cdot K_{buf}^{tr}}{(D^{real} \cdot N^{real}) + (D^{false} \cdot N^{false})}, \lambda_{46}^{time} = \frac{V^{rec} \cdot K_{buf}^{rec}}{(D^{real} \cdot N^{real}) + (D^{false} \cdot N^{false})},$$

где D^{false} – средний объем маскирующего трафика за сессию, Мбит; D^{real} – средний объем конструктивного трафика за сессию, Мбит; V^{rec} – пропускная способность (скорость) обработки данных приемника (сетевого адаптера), [Мбит/мин]; V^{tr} – пропускная способность (скорость) передачи данных в канал связи (пропускная способность сетевого адаптера или линии передачи данных) [Мбит/мин]; T^{FIN} – среднее время ожидания завершения сетевого соединения, мин, $K^{tr(rec)}_{buf}$ – коэффициент буферизации пропускной способности сетевых устройств.

Таким образом, множество M^{time} входных параметров включают в себя входные воздействия и воздействия внешней среды, а также совокупность внутренних параметров системы, то есть:

$$M^{time} = \{S^{time}, A^{time}, X^{time}\}.$$

В общем случае искомыми выходными вероятностно-временными характеристиками полумарковского процесса K^{time} являются:

$$K^{time} = \{P^{time}, G^{time}\},$$

где $P^{time}=\{P_{ij}^{time}(t)\}$ – множество интервально-переходных вероятностей пребывания системы в состоянии j из состояния i в момент времени t;

$G^{time} = \{G_{ij}^{time}(t)\}$ – множество вероятностей первого посещения системой состояния j в момент времени t, при условии, что в момент времени t=0, система находилась в состоянии i.

Определение искомых характеристик полумарковского процесса осуществляется в следующей последовательности:

– определение переходных вероятностей вложенной цепи Маркова исходя из следующего соотношения:

$$p^{time}{}_{ij} = \int_0^{\infty} f^{time}{}_{ij}(t) \prod_{k \neq i}^{n} (1 - F^{time}{}_{ik}(t)) dt,$$

где $f^{time}{}_{ij}(t) = \dfrac{dF^{time}{}_{ij}(t)}{dt}$ – функции плотности вероятности непрерывной случайной величины T_{ij} времени ожидания перехода системы из соответствующих состояний;

– определение безусловных функций распределения полного времени ожидания во всех состояниях:

$$F^{time}{}_{j}(t) = \sum_{k=1}^{n} p^{time}{}_{ij} f^{time}{}_{ij}(t);$$

– определение вероятностей того, что система не покинет соответствующие состояния в момент времени t:

$$\Psi^{time}{}_{j}(t) = 1 - F^{time}{}_{j}(t) = 1 - \sum_{k=1}^{n} p^{time}{}_{ij} f^{time}{}_{ij}(t).$$

Оценка вероятностей $P^{time}{}_{ij}(t)$ осуществляется на основе решения системы интегральных уравнений Вольтерра 2 рода с интегральным ядром разностного типа (типа «свертки»):

$$P^{time}{}_{ij}(t) = \delta_{ij} \Psi^{time}{}_{i}(t) + \sum_{k=1}^{n} p^{time}{}_{ik} \int_0^{t} f^{time}{}_{ik}(t) P^{time}{}_{jk}(t - \tau) d\tau,$$

где δ_{ij} – символ Кронекера: $\delta_{ij}=1$ при $i=j$ и $\delta_{ij}=0$ при $i \neq j$.

Применив преобразование Лапласа к системе линейных интегральных уравнений для интервально-переходных вероятностей $P_{ij}{}^{time}(t)$, получим:

$$P^{time}{}_{ij}(s) = \delta_{ij} \Psi^{time}{}_{i}(s) + \sum_{k=1}^{n} p^{time}{}_{ik} f^{time}{}_{ik}(s) P^{time}{}_{jk}(s).$$

Решение системы алгебраических уравнений в форме преобразования Лапласа в матричном виде имеют вид:

$$\mathbf{P}^{time}(s) = \left| \mathbf{I} - \mathbf{p}^{time} \times \mathbf{f}^{time}(s) \right|^{-1} \mathbf{\Psi}^{time}(s),$$

где $\mathbf{I}$ – единичная матрица размерностью n; символом $\times$ обозначено почленное произведение элементов матриц $\mathbf{p}^{time}$ и $\mathbf{f}^{time}(s)$.

Вычисление искомой матрицы с функциями распределения времени ожидания первого посещения состояний СП$_{time}$ вычисляется по выражению:

$$\mathbf{G}^{time}(s) = s^{-1} \cdot \mathbf{p}^{time} \cdot \mathbf{f}^{time}(s) \frac{\mathbf{I} \times \left(\mathbf{I} - \mathbf{p}^{time} \cdot \mathbf{f}^{time}(s) \right)}{\mathbf{I} - \mathbf{p}^{time} \cdot \mathbf{f}^{time}(s)}.$$

С использованием обратного преобразования Лапласа к матрицам $\mathbf{P}^{time}(s)$, $\mathbf{G}^{time}(s)$ определяются матрицы искомых функций $\mathbf{P}^{time}(t)$, $\mathbf{G}^{time}(t)$.

Для исследования поведения СПД ВН, влияния маскирующего сетевого трафика на своевременность конструктивного информационного обмена и получения выходных ВВХ полумарковского процесса необходимо моделирование различных условий функционирования C_{time}, которые определяются вариацией

исходных данных (параметров) – семейством реализаций λ_{ij}^{time}, (соотношением исходных данных).

Значения управляемых параметров СП$_{time}$ зависят от реализуемой ложной структуры системы управления войсками и достижения целей имитации.

Интенсивность маскирующего сетевого трафика λ_{ij}^{fp} и средний объем маскирующего трафика за сессию D_{ij}^{false} (управляемые параметры) естественным образом зависят от степени утилизации информационного направления конструктивным трафиком, выраженной неуправляемыми параметрами – интенсивностью конструктивного сетевого трафика λ_{ij}^{rp}, средним объемом конструктивного трафика за сессию D_{ij}^{real}, а также пропускной способностью канала передачи данных и сетевых устройств СПД ВН.

Для учета параметров функционирования СПД ВН на своевременность информационного обмена конструктивным сетевым трафиком при реализации маскирования СДХ проведена оценка влияния интенсивности генерации маскирующего сетевого трафика, количества, формируемых сетевыми устройствами ложных ИП, а также объема маскирующего сетевого трафика за сессию на значение вероятности $G^{time}{}_{16}(t)$ первого посещения случайного процесса C_{time} состояния S_6^{time}, характеризующем обработку приемником конструктивного сетевого трафика к моменту времени t=100 мс.

Аппроксимация функции распределения $G^{time}{}_{16}(t)$, характеризующей вероятность завершения информационного обмена в связи с окончанием передачи и обработки конструктивного трафика за время t, показала следующие зависимости (рис. 16-18).

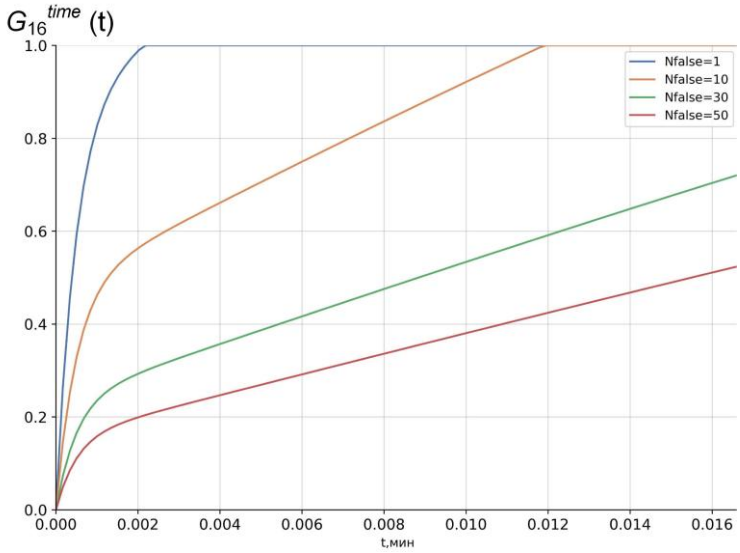

Рис. 16. Результат расчета функции распределения $G^{time}{}_{16}(t)$ вероятности обработки конструктивного трафика при варьировании количества ложных ИП за 100 мс в фиксированных условиях функционирования СПД ВН: N^{real} = 10 шт; V^{rec}=V^{tr} =10800 Мбит/мин; D^{false} = 1 Мбит; D^{real} = 3 Мбит; $K^{tr}{}_{buf}$ = $K^{rec}{}_{buf}$=1; T^{FIN} = 10^{-3} с; $\bar{\lambda}^{rp} = 200$ мин$^{-1}$; $\bar{\lambda}^{fp} = 200$ мин$^{-1}$

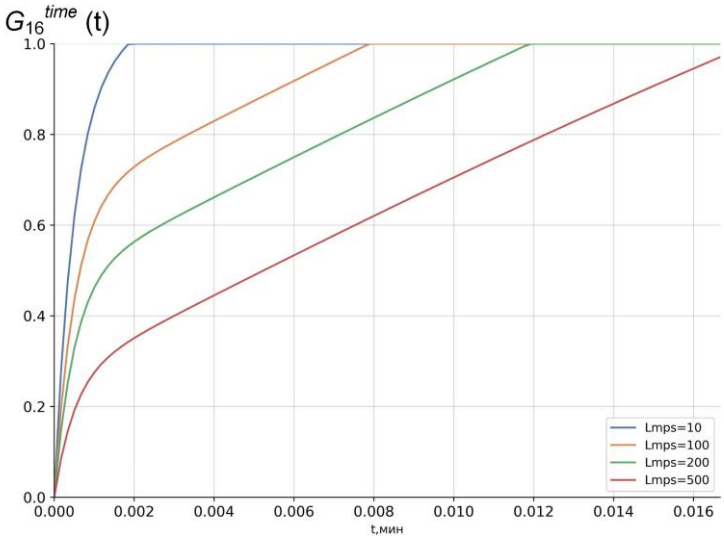

Рис. 17. Результат расчета функции распределения $G^{time}_{16}(t)$ вероятности обработки конструктивного трафика при варьировании средней интенсивности маскирующего сетевого трафика за 100 мс в фиксированных условиях функционирования СПД ВН: $N^{real} = N^{false}$ =10 шт; V^{rec}=V^{tr} =10800 Мбит/мин; D^{false} = 1 Мбит; D^{real} = 3 Мбит; $K^{tr}_{buf} = K^{rec}_{buf}$=1; T^{FIN} = 10^{-3} с; $\bar{\lambda}^{rp}$ = 200 мин$^{-1}$

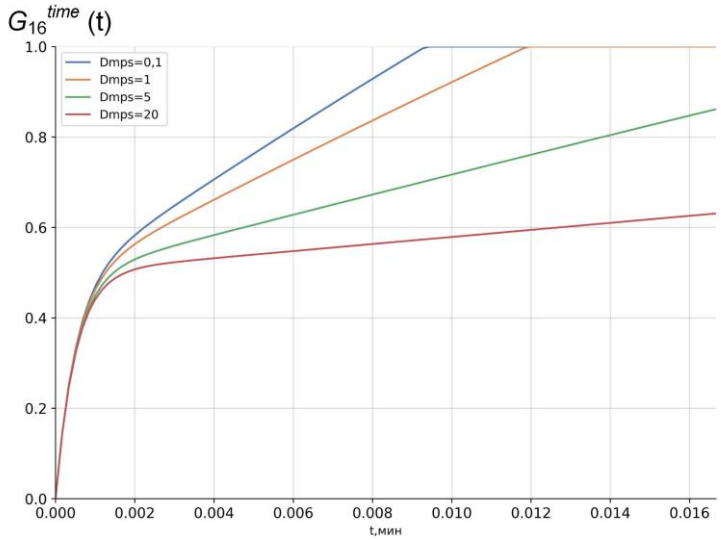

Рис. 18. Результат расчета функции распределения $G^{time}_{16}(t)$ вероятности обработки конструктивного трафика при варьировании объема маскирующего сетевого трафика за сессию за 100 мс в фиксированных условиях функционирования СПД ВН: $N^{real} = N^{false}$ =10 шт; V^{rec}=V^{tr} =10800 Мбит/мин; D^{real} = 3 Мбит; $K^{tr}_{buf} = K^{rec}_{buf}$=1; T^{FIN} = 10^{-3} с; $\bar{\lambda}^{rp}$ = 200 мин$^{-1}$; $\bar{\lambda}^{fp}$ = 200 мин$^{-1}$

Как следует из расчетов, вероятность обработки конструктивного трафика на приемнике при заданных условиях функционирования СПД ВН существенно зависит от интенсивности маскирующего сетевого трафика, количества, формируемых ложных ИП, а также объемов передаваемого маскирующего сетевого трафика.

Таким образом, установлено влияние параметров функционирования СПД ВН на своевременность информационного обмена в условиях КР при реализации маскирования СДХ СПД ВН.

Разработанная математическая модель оценки своевременности информационного обмена сетевых устройств позволяет определить вероятностно-временные характеристики обработки конструктивного трафика в различных условиях функционирования СПД при реализации маскирования структурно-динамических характеристик СПД ВН от КР.

Научная новизна модели заключается в том, что в отличии от известных [18, 19], в ней оценка своевременности информационного обмена сетевых устройств при реализации маскирования СДХ, осуществляется с использованием математического аппарата теории однородных полумарковских процессов с дискретными состояниями и непрерывным временем для получения ВВХ, позволяющих исследовать зависимость своевременной обработки сетевого трафика от условий функционирования СПД ВН и формализовать целевую функцию своевременности информационного обмена при постановки задачи векторной оптимизации для определения оптимальных параметров маскирования СДХ СПД ВН в условиях КР.

Вывод

Предложенные математические модели позволяет исследовать процесс функционирования СПД ВН при реализации маскирования СДХ СПД ВН и решают задачу аппроксимации динамических характеристик ИП, определения ВВХ оценки результативности маскирования и доступности узлов СПД ВН, с учетом нестационарности сетевого трафика, а также своевременности информационного обмена в условиях КР.

Направлением дальнейших исследований является разработка алгоритмов оптимизации параметров маскирования СДХ с учетом результативности маскирования, а также доступности сетевых устройств и своевременности информационного обмена в условиях реализации мер защиты СПД ВН, а также оценка эффективности их применения**.**

Литература

1. CODE RED 2026: Актуальные киберугрозы для российских организаций // Официальный информационный ресурс ПАО «Группа Позитив» [Электронный ресурс]. 2026. – URL: http://ptsecurity.com/research/analytics/russia-cyberthreat-landscape-2026/#id1 (дата обращения 14.01.2026).

2. Давыдов А. Е., Максимов Р. В., Савицкий О. К. Защита и безопасность ведомственных интегрированных инфокоммуникационных систем. – М.: Воентелеком, 2017. – 536 с.

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

4. 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.

5. 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.

6. Горбачев А. А. Маскирование топологических свойств вычислительных сетей. Часть 1 // Вопросы кибербезопасности. 2024. № 6 (64). С. 130–139. doi: 10.21681/2311-3456-2024-6-130-139

7. Горбачев А. А. Маскирование топологических свойств вычислительных сетей. Часть 2 // Вопросы кибербезопасности. 2025. № 1 (65). С. 63–72. doi: 10.21681/2311-3456-2025-1-63-72

8. Денисов Д. С. Модель и алгоритм имитации трафика службы электронной почты в ведомственных информационных системах // Электронный сетевой политематический журнал «Научные труды КубГТУ». 2024. № 5. С. 74–96. doi: 10.26297/2312-9409.2024.5.7.

9. Горбачев А. А., Лысенко Д. Э. Алгоритм имитации динамических характеристик трафика веб-сервиса // Вопросы кибербезопасности. 2024. № 4 (62). С. 104–115.

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

11. 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: 10.21681/2311-3456-2019-6-92-101.

12. Максимов Р. В., Орехов Д. Н., Соколовский С. П. Модель и алгоритм функционирования клиент-серверной информационной системы в условиях сетевой разведки // Системы управления, связи и безопасности. 2019. № 4. С. 50–99. doi: 10.24411/2410-9916-2019-10403.

13. Горбачев А. А., Соколовский С. П., Усатиков С. В. Модель функционирования и алгоритм проактивной защиты сервиса электронной почты от сетевой разведки // Системы управления, связи и безопасности. 2021. № 3. С. 60–109. doi: 10.24412/2410-9916-2021-3-60-109.

14. Ерышов В. Г., Ильина Д. В. Марковская модель процесса компьютерной разведки, осуществляющей несанкционированный доступ и получение конфиденциальной информации из информационных систем организаций // Волновая электроника и инфокоммуникационные системы: сборник статей XXV Международной научной конференции. – Санкт-Петербург, 2022. – С. 17–21.

15. Горбачев А. А., Соколовский С. П., Каплин М. А. Определение оптимальных параметров конфигурирования информационных систем в

условиях сетевой разведки // Вопросы кибербезопасности. 2022. № 4 (50). С. 80–90. doi: 10.21681/2311-3456-2022-4-80-90.

16. 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.

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

18. Лебедкина Т. В., Хорев Г. А. Модель функционирования и алгоритм конфигурирования адресации ложных сетевых информационных объектов в условиях сетевой разведки // Системы управления, связи и безопасности. 2023. № 2. С. 23–62. doi: 10.24412/2410-9916-2023-2-23-62.

19. 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.

References

1. CODE RED 2026: Current cyber threats for Russian organizations. *Oficial'nyj informacionnyj resurs PAO* «*Gruppa Positiv*» [The official information resource of Group Positive PJSC]. 2026. Available at: http://ptsecurity.com/research/analytics/russia-cyberthreat-landscape-2026/#id1 (accessed 14 January 2026) (in Russian).

2. Davydov A. E., Maksimov R. V., Savickiy O. K. *Zaschita i bezopasnost' vedomstvennych integrirovannych infokommunikacionnych system* [Protection and safety of the departmental integrated information and communication systems]. Moscow, Voentelecom, 2017. 536 p. (in Russian).

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

4. 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.

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

6. Gorbachev A. A. Masking of topological properties of computer networks in network reconnaissance conditions. Part 1. *Voprosy kiberbezopasnosti*, 2024, vol. 6, no. 64, pp. 130–139. doi: 10.21681/2311-3456-2024-6-130-139 (in Russia).

7. Gorbachev A. A. Masking of topological properties of computer networks in network reconnaissance conditions. Part 2. *Voprosy kiberbezopasnosti*, 2025, vol. 1, no. 65, pp. 63–72. doi: 10.21681/2311-3456-2025-1-63-72 (in Russia).

8. Denisov D. S. Model and algorithm for simulating email service traffic in departmental information systems. *Elektronnii setevoi politematicheskii jurnal* «*Nauchnie trudi KubGTU*», 2024, no. 5, pp. 74–96. doi: 10.26297/2312-9409.2024.5.7 (in Russian).

9. Gorbachev A. A., Lisenko D. E. Algorithm for simulating dynamic traffic characteristics web service. *Voprosy kiberbezopasnosti*, 2023, vol. 4, no. 62, pp. 104–115 (in Russia).

10. 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).

11. Voronchikhin I. S., Ivanov I. I., Maximov R. V., Sokolovsky S. P. Masking of Distributed Information Systems Structure in Cyber Space. *Voprosi Kiberbezopasnosti*, 2019, vol. 6, no. 34, pp. 92–101. doi: 10.21681/2311-3456-2019-6-92-101 (in Russian).

12. Maximov R. V., Orekhov D. N., Sokolovsky S. P. Model and Algorithm of Client-Server Information System Functioning in Network Intelligence Conditions. *Systems of Control, Communication and Security*, 2019, no. 4, pp. 50–99. doi: 10.24411/2410-9916-2019-10403 (in Russian).

13. Gorbachev A. A., Sokolovsky S. P., Usatikov S. V. Functioning model and algorithm of email service proactive protection from network intelligence. *Systems of Control, Communication and Security*, 2021, no. 3, pp. 60–109 (in Russian). doi: 10.24412/2410-9916-2021-3-60-109.

14. Eryshov V. G., Il'ina D. V. *Markovskaya model' processa komp'yuternoj razvedki, osushchestvlyayushchej nesankcionirovannyj dostup i poluchenie konfidencial'noj informacii iz informacionnyh sistem organizacij* [Markov model of a computer intelligence process that performs unauthorized access and acquisition of confidential information from organizational information systems]. *Volnovaya elektronika i infokommunikacionnye sistemy: sbornik statej XXV Mezhdunarodnoj nauchnoj konferencii* [Wave Electronics and Infocommunication Systems: Proceedings of the XXV International Scientific Conference]. Saint-Petersburg, 2022, pp. 17–21 (in Russian).

15. Gorbachev A. A., Sokolovsky S. P., Kaplin M. A. Determination of optimal parameters for configuring information systems in the conditions of network. *Voprosy kiberbezopasnosti*, 2022, vol. 4, no. 50, pp.80–90 (in Russia).

16. 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).

17. 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).

18. Lebedkina T. V., Horev G. A. Functioning model and algorithm for configuring the addressing of false network information objects in the conditions of

network reconnaissance. *System of Control, Communication and Security*, 2023. vol. 2, pp. 23–62 (in Russian).

19. 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).

Статья поступила 20 февраля 2026 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 объектов; маскирование информационных ресурсов интегрированных ведомственных сетей связи. E-mail: scherstobitov.rs@yandex.ru

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

Mathematical models for masking structural and dynamic characteristics of departmental data transmission networks against computer reconnaissance

R. S. Sherstobitov

Problem Statement: *one of the methods to counter the threat of computer reconnaissance of information flows is masking the structural and dynamic characteristics of departmental data transmission networks. However, existing approaches to approximating the dynamic characteristics of information flows during masking implementation are characterized by low generalization capability and the necessity of converting non-stationary data to a stationary form using differencing transformations. At the same time, the existing scientific and methodological framework for determining probabilistic-temporal characteristics does not account for the non-stationarity of parameters of the random process assessing the security and availability of network devices, as well as the timeliness of information exchange during the implementation of masking of structural and dynamic characteristics of departmental data transmission networks against computer reconnaissance.* ***The purpose of the work*** *is to develop models for masking structural and dynamic characteristics of departmental data transmission networks against computer reconnaissance and to investigate, based on these models, the patterns of functioning of a departmental data transmission network during the implementation of computer reconnaissance protection procedures.* ***Methods used:*** *the work employs methods of machine learning, mathematical statistics, optimization, time series analysis, and random process research.* ***Novelty****: the article proposes an approach to approximating the dynamic characteristics of legitimate network traffic using an ensemble of recurrent neural network models with Long Short-Term Memory (LSTM) cells to evaluate and predict the frequency characteristic of the approximated network traffic, and an exponential distribution law of a random variable parameterized by the neural network output to obtain numerical values of pauses between packets of the predicted masking network traffic. The probabilistic-temporal characteristics of the functioning process of departmental data transmission networks during the implementation of masking of structural and dynamic characteristics under conditions of computer reconnaissance have been determined using the mathematical apparatus of the theory of non-homogeneous Markov and homogeneous semi-Markov processes with discrete states and continuous time.* ***Practical significance:*** *formation of masking network traffic whose dynamic parameters are statistically close to legitimate traffic, and obtaining probabilistic-temporal characteristics of the functioning process of departmental data transmission networks under conditions of computer reconnaissance and network traffic non-stationarity, necessary for formalizing the objective functions of masking effectiveness, network device availability, and timeliness of information exchange when formulating the problem of vector optimization of masking parame-*

ters for structural and dynamic characteristics. ***Result:*** *a system of models for masking structural and dynamic characteristics has been developed, allowing the investigation of the functioning of departmental data transmission networks under conditions of computer reconnaissance.*

Keywords: *data transmission network, structural and dynamic characteristics, compromise, information flow, recurrent neural network, exponential distribution law, random process, computer reconnaissance.*

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.