УДК 004.942

Модель маскирования информационных направлений сетей передачи данных ведомственного назначения в условиях компьютерной разведки

Шерстобитов Р. С.

Постановка задачи: *возможность контакта средств компьютерной разведки с информационными потоками сетей передачи данных ведомственного назначения, эксплуатации недекларированных возможностей и уязвимостей программного обеспечения, а также доставки вредоносного контента во внутренние локальные сегменты обеспечивают нарушителя необходимой информацией для формирования моделей состава, связности и оперативного взаимодействия узлов сети. Одним из способов предотвращения данных угроз является маскирование информационного обмена узлов сети. Однако, существующий научно-методический аппарат по определению вероятностно-временных характеристик компрометации информационных направлений сетей передачи данных ведомственного назначения не учитывает нестационарность характеристик случайного процесса информационного обмена узлов сети в условиях компьютерной разведки.* ***Целью работы является*** *разработка модели и исследование на ее основе закономерностей функционирования сети передачи данных ведомственного назначения при реализации маскирования информационного обмена в условиях компьютерной разведки.* ***Используемые методы:*** *в работе использованы методы исследования случайных процессов.* ***Научная новизна*** *модели заключается в определении вероятностно-временных характеристик процесса функционирования сетей передачи данных ведомственного назначения при реализации маскирования информационного обмена в условиях компьютерной разведки с использованием математического аппарата теории неоднородных марковских процессов с дискретными состояниями и непрерывным временем.* ***Практическая значимость*** *модели заключается в нахождении вероятностно-временных характеристик процесса функционирования сетей передачи данных ведомственного назначения в условиях КР, необходимых для определения оптимальных значений параметров маскирования информационного обмена, с учетом нестационарности потоков сетевого трафика в информационных направлениях между узлами сети.* ***Результат:*** *разработана модель маскирования информационных направлений сетей передачи данных ведомственного назначения в условиях компьютерной разведки, которая формализована в виде неоднородного марковского случайного процесса с дискретными состояниями и непрерывным временем. Полученные выходные вероятностно-временные характеристики могут в дальнейшем выступать в качестве целевых функций при формулировании задачи векторной оптимизации параметров маскирования информационного обмена узлов сетей передачи данных ведомственного назначения в условиях компьютерной разведки.*

Ключевые слова: *сеть передачи данных, маскирование информационного обмена, компрометация, информационное направление, случайный процесс, компьютерная разведка.*

Введение

Основной особенностью построения сетей передачи данных ведомственного назначения (СПД ВН) является заимствование ресурсов связи доверенных операторов и использование в качестве транспортной составляющей сетей связи общего пользования (ССОП).

Библиографическая ссылка на статью:
Шерстобитов Р. С. Модель маскирования информационных направлений сетей передачи данных ведомственного назначения в условиях компьютерной разведки // Системы управления, связи и безопасности. 2025. № 1. С. 79-104. DOI: 10.24412/2410-9916-2025-1-079-104

Reference for citation:
Sherstobitov R. S. Model for masking information flows of departmental data transmission networks under conditions of computer reconnaissance. *Systems of Control, Communication and Security*, 2025, no. 1, pp. 79-104 (in Russian). DOI: 10.24412/2410-9916-2025-1-079-104

В связи с этим существенно возрастают возможности компьютерной разведки (КР), осуществляемой иностранными государствами, террористическими организациями, отдельными злоумышленниками с целью идентификации элементов сети связи и вскрытии структуры СПД ВН для планирования целенаправленных деструктивных воздействий и нарушения функционирования системы управления ведомством (СУВ), в интересах которой функционируют СПД ВН.

Данный факт подтверждается разработкой и принятием на государственном уровне стран-оппонентов нормативно-правовых документов, определяющих информационное пространство как арену боевых действий, а также использование отдельных подразделений для выполнения наступательных и оборонительных боевых операций («кибероперациий») в информационном пространстве («киберпространстве») совместно с традиционными видами вооруженных сил [1].

В соответствии с [1] разведывательная деятельность является критически важным компонентом планирования и проведения операций в киберпространстве и обеспечивает сбор, обработку, анализ и оценку разведывательной информации для формирования оперативной обстановки реальных или потенциальных районов ведения боевых действий. В контексте киберпространства целью формирования оперативной обстановки является отображение состава, структуры, взаимодействия элементов сети, которое графически показывает, как информационные потоки формируются и распределяются в сетях передачи данных, образуя информационные направления между узлами сети. Оценка оперативной обстановки позволяет определить приоритетные цели (англ. high payoff target, HPT) в киберпространстве для деструктивных воздействий, а также объекты для огневого поражения при ведении наземных операций. При этом, для огневого поражения необходимо знать дополнительно физическое местоположение объекта воздействия, с другой стороны для кибервоздействия необходим только доступ к ССОП и логический адрес элемента сети (IP-адрес), который определяет расположение объекта в киберпространстве.

Выявление КР узлов СПД ВН и связей между ними определяется возможностью анализа средствами разведки информационных потоков узлов сети. Информационное пространство СПД ВН, в связи с использованием ССОП, обеспечивает точки доступа КР к линиям передачи данных, позволяющим сканировать сеть и перехватывать трафик, для получения необходимых структурно-функциональных характеристик состава, связности и взаимодействия узлов сети и практически в режиме реального времени обновлять общую оперативную картину [1]. При этом, наряду с угрозами из внешней сети, существует внутренний нарушитель (доверенное устройство), а также возможность внедрения вредоносного программного обеспечения в программные средства внутренних локальных сегментов СПД ВН. Зафиксированные в 2024 году кибератаки [2], показывают, что несмотря на реализуемые в СПД ВН организационно-технические мероприятия, направленные на выявление недекларированных возможностей программного обеспечения и закрытие уязвимостей, нельзя говорить об их абсолютной эффективности.

Физическая постановка задачи

Одной из современных парадигм защиты СПД от КР является формирование у внешнего и (или) внутреннего нарушителей неверного представления об оперативной обстановке в киберпространстве, структуре информационных направлений СПД ВН и, как следствие, структуре СУВ [3]. Реализация такого подхода позволит влиять на качество решений, принимаемых нарушителем по результатам КР [4-6], предотвращать таргетированные деструктивные воздействия на объекты защиты, а также устранит антагонизм взаимодействующих сторон в условиях информационного конфликта [7]. Одним из практических методов реализации данной концепции киберобмана является маскирование информационного обмена в СПД ВН [8]. При реализации маскирования необходимо учитывать свойства потоков сетевого трафика в информационных направлениях (ИН) между конечными узлами сети. Информационный обмен узлов сети, формирующих информационные потоки различных приложений, представляет собой сложный динамический процесс, параметры которого зависят от времени, а сетевой трафик в общем случае не обладает свойством стационарности [9]. В таких условиях необходима метрика оценивания результативности маскирования в вероятностно-временной форме с учетом нестационарности параметров информационного обмена узлов СПД ВН. С точки зрения противодействия КР такой метрикой может выступать вероятность компрометации ИН, которое утилизируется ложными и реальными потоками сетевого трафика.

Однако, существующий научно-методический аппарат маскирования информационного обмена в части определения вероятностно-временных характеристик (ВВХ) компрометации ИН СПД ВН [10-18] не учитывает нестационарность характеристик случайного процесса информационного обмена узлов сети, что, в условиях КР, может привести к вскрытию средств защиты и снижению результативности маскирования.

Таким образом, для определения ВВХ оценки результативности маскирования целесообразно разработать математическую модель маскирования ИН СПД ВН в условиях КР, учитывающую нестационарный характер информационного обмена узлов сети.

Формирование параметров для моделирования

Для постановки задачи на моделирование процесса маскирования информационного обмена в СПД ВН сформулируем понятие «информационное направление СПД ВН», которая определяется следующим образом.

Введем допущение, что СПД ВН являются технической основой СУВ, на которые возложены функции по обработке и передаче информации между органами (субъектами) и объектами управления [19, 20]. Пусть для реализации замысла защиты от КР в качестве исходных данных принимается ложная структура СПД ВН, которую необходимо имитировать маскированием информационного обмена.

Имитируемая структура СПД ВН содержит совокупность из W узлов сети, имеющих IP-адреса. Для полносвязной ложной структуры максимальное количество ИН N определяется выражением:

$$N^{\max} = \frac{W(W-1)}{2}.$$

Количество реальных ИН N^{real} в имитируемой структуре СПД ВН является неуправляемым параметром (параметр внешней среды) и определяется в соответствии с принятой СУВ. С другой стороны, количество ложных ИН в имитируемой структуре СПД ВН с учетом полносвязной структуры должно удовлетворять условию:

$$N^{false} \le N^{\max} - N^{real}.$$

Введем допущение, что ИН СПД ВН физически реализуется сетевыми информационными объектами (средствами передачи и обработки данных), формирующих реальные и ложные потоки с использованием различных каналов связи.

При этом ИН N_{ij} между i и j узлами сети определяется количеством реальных информационных потоков L_{ij}^{real} и количеством ложных информационных потоков L_{ij}^{false}:

$$N_{ij} = L_{ij}^{real} \cup L_{ij}^{false}.$$

Таким образом, все ИН в имитируемой структуре СПД ВН N определяются как объединение всех реальных и ложных информационных потоков между i и j узлами сети.

$$N = \bigcup_{i \ne j} (L_{ij}^{real} \cup L_{ij}^{false}).$$

На каждом i-м узле может содержаться r_i реальных IP-адресов и f_i ложных IP-адресов. Таким образом общее количество реальных IP-адресов R в СПД ВН будет составлять:

$$R = \sum_{i=1}^{W} r_i.$$

Общее количество ложных IP-адресов F СПД ВН будет составлять:

$$F = \sum_{i=1}^{W} f_i.$$

Осуществление информационного обмена между i и j узлами сети с использованием пар реальных или ложных IP-адресов (отправителя и получателя пакетов сообщений) образуют множество реальных L_{ij}^{real} или множество ложных L_{ij}^{false} информационных потоков:

$$L_{ij}^{real} = \{(r_i^k, r_j^m) \mid 1 \le k \le r_i, 1 \le m \le r_j\};$$
$$L_{ij}^{false} = \{(f_i^k, f_j^m) \mid 1 \le k \le f_i, 1 \le m \le f_j\},$$

где k, m – целочисленные индексы, причем k-й реальный IP-адрес отправителя и m-й реальный IP-адрес получателя могут принимать значения из множества реальных IP-адресов на i-м узле сети $\{r_i\}$ и множества реальных IP-адресов на j-м узле сети $\{r_j\}$;

k-й ложный IP-адрес отправителя и *m*-й ложный IP-адрес получателя могут принимать значения из множества ложных IP-адресов на *i*-м узле сети $\{f_i\}$ и множества ложных IP-адресов на *j*-м узле сети $\{f_j\}$.

При этом общее количество информационных потоков зависит от количества ИН в СПД ВН:

$$L = \left| L_{ij}^{real} \cup L_{ij}^{false} \right|, i, j = \overline{1, N}, i \neq j,$$

где $\left| L_{ij}^{real} \cup L_{ij}^{false} \right|$ – количество всех реальных L_{ij}^{real} и ложных L_{ij}^{false} информационных потоков между *i* и *j* узлами сети.

Реальные L_{ij}^{real} информационные потоки представляют собой последовательность конструктивного сетевого трафика, а ложные L_{ij}^{false} информационные потоки утилизируются (наполняются) маскирующим сетевым трафиком.

Под конструктивным сетевым трафиком понимается совокупность пользовательских (для реализации СУВ) и технологических (для обеспечения управляющих функций протоколов и технологий информационного обмена), пакетов сообщений, формируемых узлами сети, в целях обеспечения необходимого качества информационного обмена в ИН СПД ВН.

Под маскирующим сетевым трафиком понимается совокупность пользовательских и технологических, пакетов сообщений, формируемых узлами сети, в соответствии с замыслом защиты, в целях имитации идентификаторов конструктивного сетевого трафика в ИН СПД ВН.

При этом, в рамках исследования алгоритмы и способы формирования полей данных IP-пакетов маскирующих сообщений выступают в качестве ограничений, то есть генеративно-языковые модели для наполнения указанной части IP-пакетов маскирующих сообщений не рассматриваются.

Формирование конструктивного сетевого трафика в информационных потоках L_{ij}^{real} осуществляется с интенсивностью $\lambda_{ij}^{rp}(t)$, с учетом обеспечения необходимого качества информационного обмена в ИН СПД ВН, а также в зависимости от уровня иерархии (оперативно-тактической принадлежности) соответствующих пунктов управления (ПУ) в СУВ. Физически интенсивность конструктивного сетевого трафика $\lambda_{ij}^{rp}(t)$ в разработанной модели определяется значением количества установленных сетевых соединений (сессий) в реальных информационных потоках между *i* и *j* узлами сети в единицу времени (например, в секунду) при реализации конструктивного информационного обмена.

Формирование маскирующего сетевого трафика в информационных потоках L_{ij}^{false} осуществляется с интенсивностью $\lambda_{ij}^{fp}(t)$, с учетом обеспечения необходимой утилизации реальных и ложных ИН маскирующим сетевым трафиком, а также связности узлов сети в формируемых ложных ИН. Физически интенсивность маскирующего сетевого трафика $\lambda_{ij}^{fp}(t)$ в разработанной модели определяется значением количества установленных сетевых соединений (сессий) в ложных информационных потоках между *i* и *j* узлами сети в единицу времени (например, в секунду) при реализации маскирующего информационного обмена. Управление параметром $\lambda_{ij}^{fp}(t)$ необходимо для формирования

имитируемой структуры СПД ВН, в которой искажены (в частности – повышены) уровни иерархии соответствующих узлов ПУ.

Для удобства в статье количество потоков в рамках одного информационного направления между *i* и *j* узлами сети постоянно, следовательно, $\lambda_{ij}^{rp}(t)$, $\lambda_{ij}^{fp}(t)$ зависят только от времени.

Таким образом, под ИН СПД ВН понимается совокупность реальных и ложных информационных потоков сетевого трафика и обеспечивающих информационный обмен множества линий связи между оконечными узлами связи ПУ подразделений ведомства.

В условиях КР параметры «время z_i^k использования *k*-го реального IP-адреса отправителя и *m*-го реального IP-адреса получателя z_i^m» определяют интенсивность реконфигурации реального информационного потока U_{ij}^{real}:

$$U_{ij}^{real} = \{(z_i^k, z_j^m), z_i^k = z_j^m \mid 1 \le k \le z_i, 1 \le m \le z_j\}.$$

Соответственно, в условиях КР, параметры «время y_i^k использования *k*-го ложного IP-адреса отправителя и *m*-го ложного IP-адреса получателя y_i^m» определяют интенсивность реконфигурации ложного информационного потока U_{ij}^{false}:

$$U_{ij}^{false} = \{(y_i^k, y_j^m), y_i^k = y_j^m \mid 1 \le k \le y_i, 1 \le m \le y_j\}.$$

Реконфигурация достигается посредством ввода программным путем дополнительных виртуальных интерфейсов на внутренних (для защиты внутренней сети) и внешних (для защиты внешней сети) интерфейсах маршрутизаторов. Каждая пара корреспондентов осуществляет согласованную динамическую реконфигурацию (смену) IP-адресов и MAC-адресов. При этом согласованная реконфигурация (смена) IP-адресов и MAC-адресов 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).

Согласованность задается конфигурационным файлом, в котором перечислен весь пул адресов, последовательность смены и частота реконфигурации (например, раз в секунду, раз в минуту и т.д.). Частота реконфигурации выбирается таким образом, чтобы сканеры уязвимостей (типа nmap), анализаторы трафика (типа wireshark) не могли определить топологию (типологию) сети. Совместная согласованная смена адресов маршрутизаторов приводит к тому, что анализ трафика показывает не одно ИН, а некую структуру, структурные свойства которой (связность и интенсивность каждой связи) определяются конфигурационным файлом маршрутизатора. При этом, при условии осведомленности КР о применении такого средства защиты для достижения целей разведки нарушитель, очевидно, должен кратно увеличить свой ресурс, что неизбежно приведет к потере бескомпроматности средств КР и получение системой защиты выигрыша по ресурсу (например, времени, необходимого для реализации ответных мер).

Для учета степени воздействия на СПД ВН средств КР используется параметр «интенсивность КР сетевого трафика СПД ВН λ^{sniff}», определяющий математическое ожидание количества перехватов (сканирований) сетевого трафи-

ка в единицу времени, при допущении, что процесс разведки ИН сети формализован в виде простейшего потока.

Введем допущение, моделирующее наихудший сценарий влияния КР на СПД ВН. Так, в рамках проводимого исследования, КР является идеальным наблюдателем и способна в любой момент времени перехватить любые пакеты любого информационного потока между *i* и *j* узлами сети, ошибки в распознавании перехваченной информации отсутствуют.

Интенсивность КР сетевого трафика информационных потоков между *i* и *j* узлами сети СПД ВН определяется выражением:

$$\lambda_{ij}^{sniff} > 0$$

Таким образом, интенсивность КР сетевого трафика информационных потоков в СПД ВН в условиях идеального наблюдателя равна:

$$\Lambda^{sniff} = \bigcup_{i,j=1,N,i\neq j} \lambda_{ij}^{sniff}$$

При реализации маскирования информационного обмена и генерации маскирующего сетевого трафика с интенсивностью $\lambda_{ij}^{fp}(t)$ для имитации ложных ИН и утилизации реальных ИН необходимо учитывать динамические свойства конструктивного сетевого трафика множества приложений (сетевых протоколов) узлов СПД ВН.

Для оценки качества имитации сетевого трафика используется параметр, характеризующий качество аппроксимации динамических характеристик конструктивного сетевого трафика $p_{ij}^{idfalse}$, который является мерой статистической близости маскирующего и конструктивного сетевого трафика приложений (сетевых протоколов) узлов СПД ВН по критерию Колмогорова-Смирнова (или другим критериям, например, Хи-квадрат). *P*-значение показывает степень уверенности в статистической однородности двух временных рядов маскирующего и конструктивного трафика, определяемой по значению критерия согласия Колмогорова-Смирнова таким образом, что чем выше *p*-значение, тем ближе временные ряды, следовательно, тем ниже вероятность компрометации реальных информационных направлений, то есть выше результативность маскирования информационного обмена в СПД ВН.

Модель маскирования информационных направлений сетей передачи данных ведомственного назначения в условиях компьютерной разведки

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

Потоки сетевого трафика в ИН между узлами сети передаются в соответствии с протоколами транспортного уровня (TCP, UDP, SCTP и других). При этом переход между состояниями инициализации сетевых соединений, осуществления информационного обмена, завершения информационного обмена

или ожидания возобновления информационного обмена зависит от появления в случайный момент времени сетевых пакетов, определенных спецификацией соответствующих протоколов.

С другой стороны, цикл КР по вскрытию структуры СПД ВН с учетом проводимых мероприятий маскирования характеризуется случайным характером компрометации реальных или ложных ИН, а также ожиданием их компрометации. Таким образом, процесс маскирования ИН СПД ВН в условиях КР является случайным процессом.

Следовательно, модель маскирования ИН СПД ВН может быть формализована в общем виде как неоднородный марковский случайный процесс ($СП_{mask}$) с дискретными состояниями и непрерывным временем, исходными данными в ходе моделирования, которого являются [21]:

- пространство фазовых состояний системы (конечное множество несовместных (несовместимых) событий, описывающих существенные свойства системы и изменяющиеся «скачкообразно») (таблица 1) и возможные траектории перехода системы из состояния в состояние;
- распределение вероятностей пребывания системы в состояниях в начальный момент времени;
- интенсивности потоков событий (заявок, требований, факторов), вызывающих переход системы из состояния в состояние (таблица 2).

В соответствии с теоремой Ляпунова [22] 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).

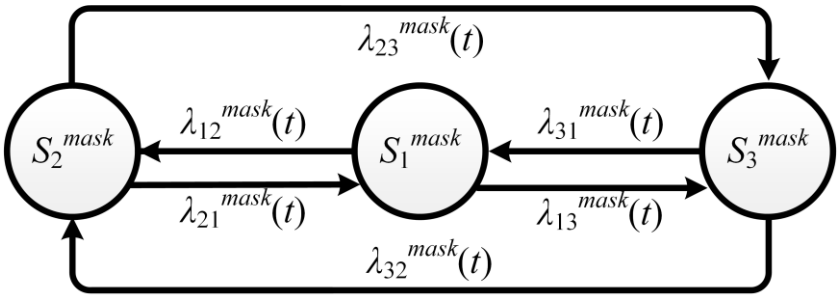

Рис. 1. Граф состояний $СП_{mask}$

Таблица 1 – Дискретные состояния $СП_{mask}$

Состояние	Описание состояний
S_1^{mask}	Ожидание компрометации ложных или реальных ИН (результативность маскирования обеспечивается)
S_2^{mask}	Ожидание компрометации реальных ИН при условии вскрытия ложных ИН (результативность маскирования обеспечивается)
S_3^{mask}	Ожидание компрометации ложных ИН при условии вскрытия реальных ИН (результативность маскирования не обеспечивается)

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

Физический смысл интенсивности λ_{ij} – математическое ожидание количества случайных событий, вызывающих переход системы из состояния S_i в состояние S_j в единицу времени. Случайная величина промежутка времени между событиями распределена по экспоненциальному закону (единственное непрерывное распределение с отсутствием последействия, или распределение с постоянной интенсивностью отказов). В этом (показательном) распределении экспонента в первой степени не меняется при интегрировании и дифференцировании, что математически и означает отсутствие последействия, а практически – вычислительную простоту (несложность). Независимость событий – это и есть отсутствие последействия. Если все потоки событий, переводящие систему из состояния в состояние, – пуассоновские и независимые, то процесс, протекающий в системе S, – марковский [22].

Таблица 2 – Интенсивности потоков событий системы $СП_{mask}$

$\lambda_{ij}(t)$	**Интерпретация интенсивностей**
$\lambda_{12}^{mask}(t)$	Интенсивность потока событий по компрометации ложных ИН
$\lambda_{21}^{mask}(t)$	Интенсивность потока событий по реконфигурации сети (формирование новых ложных ИН)
$\lambda_{13}^{mask}(t)$	Интенсивность потока событий по компрометации реальных ИН
$\lambda_{31}^{mask}(t)$	Интенсивность потока событий по реконфигурации сети (формирования новых реальных ИН)
$\lambda_{23}^{mask}(t)$	Интенсивность потока событий по компрометации реальных ИН после вскрытия ложных ИН
$\lambda_{32}^{mask}(t)$	Интенсивность потока событий по компрометации ложных ИН после вскрытия реальных ИН

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

Пусть нарушитель осуществляет КР постоянно, однако, реализуемые меры защиты предотвращают компрометацию реальных и ложных ИН СПД ВН, тогда S_1^{mask} – начальное состояние моделируемой системы $СП_{mask}$, 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_1^{mask} в состояние S_2^{mask} под воздействием интенсивности потока событий $\lambda_{12}^{mask}(t)$ означает момент окончания цикла КР и компрометацию ложных ИН. При этом нахождение в состояниях S_1^{mask} и S_2^{mask} определяет результативность маскирования, интенсивность которого определяется для каждого ИН ($\lambda_{ij}^{fp}(t)$). Предполагается, что интенсивность событий $\lambda_{12}^{mask}(t)$ по компрометации ложных ИН пропорциональна доле ложных ИН в СПД ВН (то есть, $N_{false}/(N_{false}+N_{real})$), а также пропорциональна *P*-значению статистики об однородности динамических характеристик маскирующего и конструктивного сетевого трафика в ИН. Таким образом, при оценке показателя результативности маскирования СПД ВН учитываются как интегральные характеристики сети, так и качество аппроксимации динамических характеристик конструктивного сетевого трафика на каждом ИН. То есть, чем больше доля ложных ИН и выше правдоподобие имитации динамических характеристик конструктивного сетевого трафика при генерации маскирующего, тем выше результирующая интенсивность событий $\lambda_{12}^{mask}(t)$ по вскрытию ложных ИН (введению злоумышленника в заблуждение).

Переход из состояния S_1^{mask} в состояние S_3^{mask} под воздействием интенсивности потока событий $\lambda_{13}^{mask}(t)$ означает момент окончания цикла КР и компрометацию реальных ИН. Таким образом, состояние S_3^{mask} 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_3^{mask} в состояние S_1^{mask} под воздействием интенсивности потока событий $\lambda_{31}^{mask}(t)$ характеризует реакцию системы защиты на компрометацию реальных ИН и означает переход системы в защищенное состояние в связи с реконфигурацией сети (формирования новых реальных ИН). Также возможен переход из состояния S_2^{mask} в состояние S_1^{mask} под воздействием интенсивности потока событий $\lambda_{21}^{mask}(t)$, который характеризует реакцию системы защиты на компрометацию ложных ИН и означает переход системы в состояние окончания цикла КР в связи с реконфигурацией сети (формирования новых ложных ИН). Переход из состояния S_2^{mask} в состояние S_3^{mask} под воздействием интенсивности потока событий $\lambda_{23}^{mask}(t)$ означает компрометацию реальных ИН после вскрытия ложных ИН, а переход из состояния S_3 в состояние S_2 под воздействием интенсивности потока событий $\lambda_{32}^{mask}(t)$ означает компрометацию ложных ИН после вскрытия реальных ИН.

Перечисленные состояния описывают существенные функции моделируемой СПД ВН при маскировании информационного обмена 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 исследуемого объекта представлена в виде отображения множества входных параметров случайного процесса M^{mask} во множество выходных ВВХ K^{mask}.

Тогда, 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 подмножество (пространство) неуправляемых факторов A^{mask}:

$$A^{mask} = \{N^{real}, \lambda_{ij}^{rp}(t), \lambda^{sniff}(t)\},$$

где:

N^{real} – количество реальных ИН СПД ВН, определяемое структурой СПД ВН и СУВ (шт.);

$\lambda_{ij}^{rp}(t)$ – интенсивность конструктивного сетевого трафика в реальных информационных потоках между i-м и j-м узлами сети (с$^{-1}$);

$\lambda^{sniff}(t)$ – интенсивность КР сетевого трафика СПД ВН (с$^{-1}$).

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 S_i в состояние S_j:

$$X^{mask} = \{N^{false}, \lambda_{ij}^{fp}(t), p_{ij}^{idfalse}(t), z, y\}.$$

При этом интенсивности потоков событий, инициирующих переходы (таблица 2) системы из состояния S_i в состояние S_j зависят от условий функционирования СПД ВН и задаются следующими выражениями:

$$\lambda_{12}(t), \lambda_{32}(t) = \frac{N^{false}}{N^{false} + N^{real}} \left[\sum_{i=1}^{N^{false}} \sum_{j=i+1}^{N^{false}} \frac{p_{ij}^{idfalse}(t) \lambda_{ij}^{fp}(t)}{\lambda_{ij}^{rp}(t) + \lambda_{ij}^{fp}(t)} \right] \lambda^{sniff}(t),$$

$$\lambda_{13}(t), \lambda_{23}(t) = \frac{N^{real}}{N^{false} + N^{real}} \left[\sum_{i=1}^{N_{real}} \sum_{j=i+1}^{N_{real}} \frac{(1 - p_{ij}^{idfalse}(t)) \lambda_{ij}^{rp}(t)}{\lambda_{ij}^{rp}(t) + \lambda_{ij}^{fp}(t)} \right] \lambda^{sniff}(t),$$

$$\lambda_{21} = R^{false}(t) \frac{1}{N^{false}}, \lambda_{31} = R^{real}(t) \frac{1}{N^{real}}, p_{ij}^{idfalse}(t) = f(\sup_{n \in D} \left| F_n(\lambda_{ij}^{rp}(t)) - F_n(\lambda_{ij}^{fp}(t)) \right|),$$

$$R^{false}(t) = y^{-1}, R^{real}(t) = z^{-1},$$

где N_{false} – количество ложных ИН СПД ВН, определяемое имитируемой структурой (шт.);

$\lambda_{ij}^{fp}(t)$ – интенсивность маскирующего сетевого трафика в ложных информационных потоках между i-м и j-м узлами сети (с$^{-1}$);

$R^{false}(t)$ – интенсивность реконфигурации ложного ИН (с$^{-1}$);

$R^{real}(t)$ – интенсивность реконфигурации реального ИН (с$^{-1}$);

y – время использования ложных ИН (с);

z – время использования реальных ИН (с);

$p_{ij}^{idfalse}(t)$ – параметр, характеризующий качество аппроксимации конструктивного сетевого трафика в ИН между i-м и j-м узлами сети;

D – длина анализируемого временного ряда интенсивности сетевого трафика при аппроксимации динамических характеристик конструктивного и маскирующего трафика (шт.);

$F_n(\lambda_{ij}^{fp}(t))$ – временной ряд интенсивности маскирующего трафика $\lambda_{ij}^{fp}(t)$ длиной D;

$F_n(\lambda_{ij}^{rp}(t))$ – временной ряд интенсивности конструктивного трафика $\lambda_{ij}^{rp}(t)$ длиной D.

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:

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

где

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

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:

$$\begin{cases} \dfrac{dp_1^{mask}(t)}{dt} = p_2^{mask}(t)\lambda_{21}^{mask}(t) + p_3^{mask}(t)\lambda_{31}^{mask}(t) - p_1^{mask}(t)(\lambda_{12}^{mask}(t) + \lambda_{13}^{mask}(t)), \\ \dfrac{dp_2^{mask}(t)}{dt} = p_3^{mask}(t)\lambda_{32}^{mask}(t) + p_1^{mask}(t)\lambda_{12}^{mask}(t) - p_2^{mask}(t)(\lambda_{21}^{mask}(t) + \lambda_{23}^{mask}(t)), \\ \dfrac{dp_3^{mask}(t)}{dt} = p_2^{mask}(t)\lambda_{23}^{mask}(t) + p_1^{mask}(t)\lambda_{13}^{mask}(t) - p_3^{mask}(t)(\lambda_{31}^{mask}(t) + \lambda_{32}^{mask}(t)), \\ \sum\limits_{i=1}^{3} p_i^{mask}(t) = 1. \end{cases}$$

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 ВН, 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.

$$\begin{cases} \frac{dp_1^{mask}(t)}{dt} = p_2^{mask}(t)R^{false}(t) + p_3^{mask}(t)R^{real}(t) - \\ -p_1^{mask}(t)(\frac{N^{false}}{N^{false}+N^{real}}\lambda_{sniff}(t)(\left[\sum_{i=1}^{N^{false}}\sum_{j=i+1}^{N^{false}}\frac{p_{ij}^{idfalse}(t)\lambda_{ij}^{fp}(t)}{\lambda_{ij}^{rp}(t)+\lambda_{ij}^{fp}(t)}\right]+\left[\sum_{i=1}^{N^{real}}\sum_{j=i+1}^{N^{real}}\frac{(1-p_{ij}^{idfalse}(t))\lambda_{ij}^{rp}(t)}{\lambda_{ij}^{rp}(t)+\lambda_{ij}^{fp}(t)}\right]), \\ \frac{dp_2^{mask}(t)}{dt} = (p_3^{mask}(t)+p_1^{mask}(t))\frac{N^{false}}{N^{false}+N^{real}}\left[\sum_{i=1}^{N^{false}}\sum_{j=i+1}^{N^{false}}\frac{p_{ij}^{idfalse}(t)\lambda_{ij}^{fp}(t)}{\lambda_{ij}^{rp}(t)+\lambda_{ij}^{fp}(t)}\right]\lambda^{sniff}(t) - \\ -p_2^{mask}(t)(R^{false}(t)+\frac{N^{real}}{N^{false}+N^{real}}\left[\sum_{i=1}^{N^{real}}\sum_{j=i+1}^{N^{real}}\frac{(1-p_{ij}^{idfalse}(t))\lambda_{ij}^{rp}(t)}{\lambda_{ij}^{rp}(t)+\lambda_{ij}^{fp}(t)}\right]\lambda^{sniff}(t)), \\ \frac{dp_3^{mask}(t)}{dt} = (p_2^{mask}(t)+p_1^{mask}(t))\frac{N^{real}}{N^{false}+N^{real}}\left[\sum_{i=1}^{N^{real}}\sum_{j=i+1}^{N^{real}}\frac{(1-p_{ij}^{idfalse}(t))\lambda_{ij}^{rp}(t)}{\lambda_{ij}^{rp}(t)+\lambda_{ij}^{fp}(t)}\right]\lambda^{sniff}(t) - \\ -p_3^{mask}(t)(R^{real}(t)+\frac{N^{false}}{N^{false}+N^{real}}\left[\sum_{i=1}^{N^{false}}\sum_{j=i+1}^{N^{false}}\frac{p_{ij}^{idfalse}(t)\lambda_{ij}^{fp}(t)}{\lambda_{ij}^{rp}(t)+\lambda_{ij}^{fp}(t)}\right]\lambda^{sniff}(t)). \end{cases}$$

Пример расчета вероятностно-временных характеристик случайного процесса СП$_{mask}$

Для расчета выходных ВВХ случайного процесса произвольно выбран сегмент СПД ВН, состоящий из 22 реальных ИН конструктивного сетевого трафика и 7 ложных ИН маскирующего сетевого трафика между i-ми и j-ми узлами сети (рис. 2).

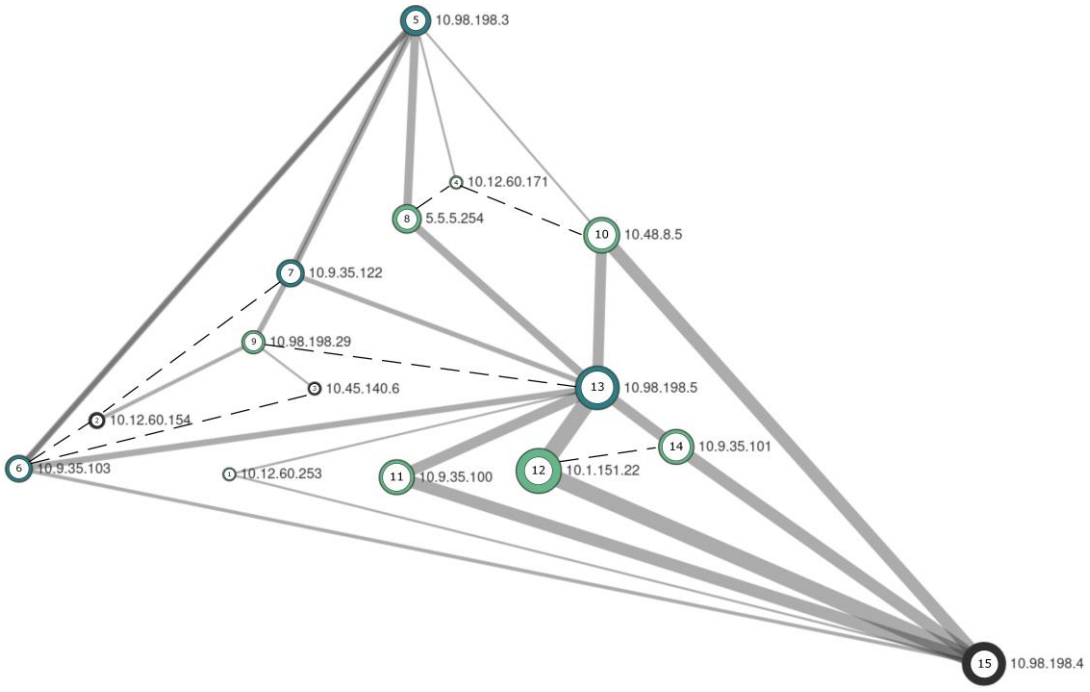

Рис. 2. Сегмент СПД ВН, используемый для моделирования СП$_{mask}$

При исследовании информационного обмена в указанном сегменте СПД ВН был произведен сбор сетевых пакетов с использованием утилиты tcpdump, в результате которого получен дамп сетевого трафика узлов сети.

В результате анализа дампа сформирован временной ряд $F_n(\lambda_{ij}^{rp}(t))$, отражающий моменты существования активных сессий (с момента поступления SYN-пакетов до поступления пакетов с флагами FIN или RST).

Агрегирование пакетов и подсчет их количества на интервале в 1 секунду, позволил проанализировать динамику инициализации сессий конструктивного информационного обмена, а также провести первичную обработку статистических данных. Для рассматриваемого временного ряда длиной $D = 1000$ с получена зависимость количества активных сессий конструктивного информационного обмена узлов сети от времени (рис. 3), и автокорреляционная функция временного ряда (рис. 4), демонстрирующую отсутствие стохастической азависимости между значениями частот, что подтверждает корректность использования математического аппарата марковских случайных процессов для моделирования процесса маскирования информационного обмена.

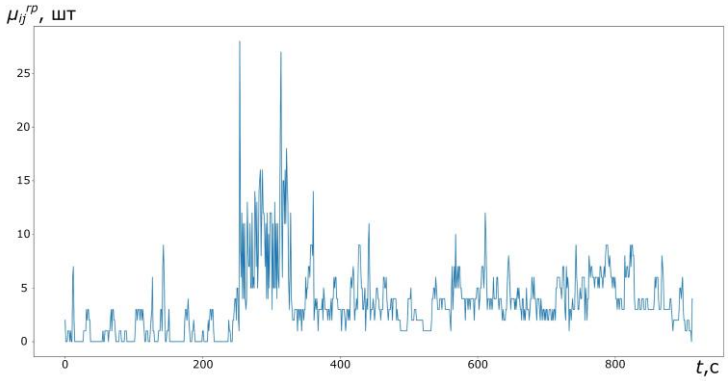

Рис. 3. Зависимость количества активных сессий конструктивного информационного обмена узлов сети от времени

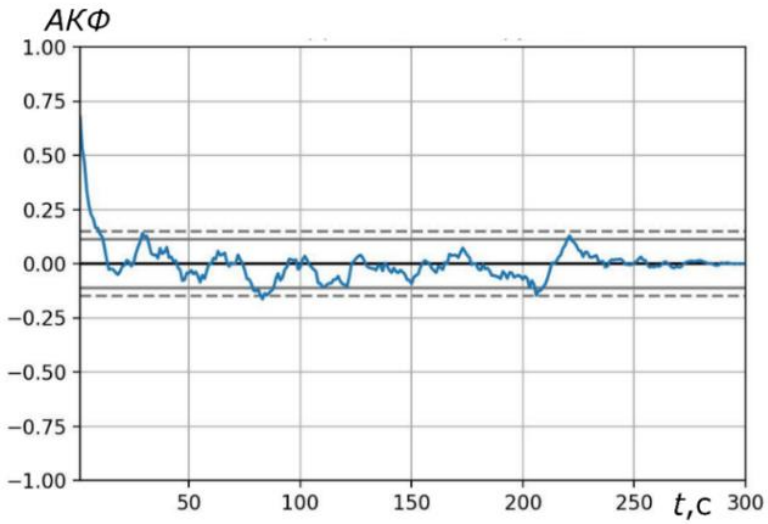

Рис. 4. График автокорреляционной функции временного ряда

№1. 2025
ISSN 2410-9916

Рассмотрим ситуацию № 1, при которой моделируемая система функционирует в стационарном режиме, то есть когда интенсивность конструктивного сетевого трафика не зависит от времени t.

При моделировании случайного процесса для ситуации № 1 принято допущение, согласно которому значения параметров λ_{ij}^{fp} и λ_{ij}^{rp}, $p_{ij}^{idfalse}$ равны средним значениям во всех реальных и ложных информационных потоках по всем ИН сети, то есть:

$$\lambda^{rp} = E(\lambda_{ij}^{rp}), \text{ где } \lambda_{ij}^{rp} = E(\lambda_{ij}^{rp}(t))$$
$$\lambda^{fp} = E(\lambda_{ij}^{fp}), \text{ где } \lambda_{ij}^{fp} = E(\lambda_{ij}^{fp}(t))$$
$$p^{idfalse} = E(p_{ij}^{idfalse}), \text{ где } p_{ij}^{idfalse} = E(p_{ij}^{idfalse}(t))$$

Таким образом, определены значения управляемых и неуправляемых параметров, определяющих условия функционирования сети: $N^{false} = 7$; $N^{real} = 22$; $\lambda^{fp} = 2$ с$^{-1}$; $\lambda^{rp} = 5$ с$^{-1}$; $R^{false} = 0{,}1$ с$^{-1}$; $R^{real} = 1$ с$^{-1}$; $p^{idfalse} = 0{,}2$; $\lambda^{sniff} = 1$ с$^{-1}$. В результате расчетов получены значения выходных ВВХ СП$_{mask}$ – вероятности нахождения случайного процесса в одном из состояний к моменту времени t (рис. 5).

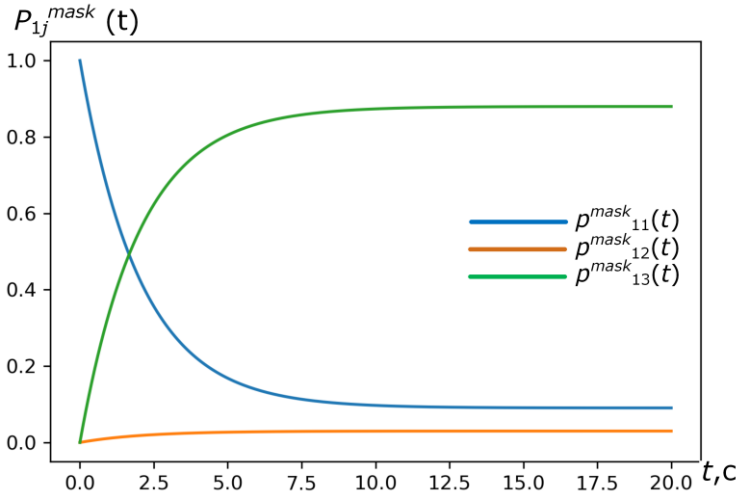

Рис. 5. Результат расчета вероятности перехода СП$_{mask}$ в состояние j из состояния S_1 к моменту времени t для ситуации № 1

Для учета параметров функционирования СПД ВН на результативность маскирования проведена оценка их влияния на значения вероятности нахождения случайного процесса СП$_{mask}$ в подмножестве состояний. В результате расчетов получены значения вероятностей пребывания в состоянии результативного (состояния S_1 или S_2) (рис. 6). и нерезультативного (состояние S_3) (рис. 7) маскирования к моменту времени t = 100 с в зависимости от качества аппроксимации динамических характеристик конструктивного сетевого трафика $p^{idfalse}$ при генерации маскирующего и интенсивности КР λ^{sniff}.

Из рисунков видно, что результативность маскирования информационного обмена существенно снижается при интенсивной КР и малых значениях критерия близости временных рядов маскирующего сетевого трафика и конструктивного сетевого трафика узлов СПД ВН.

DOI: 10.24412/2410-9916-2025-1-079-104
URL: http://sccs.intelgr.com/archive/2025-01/04-Sherstobitov.pdf

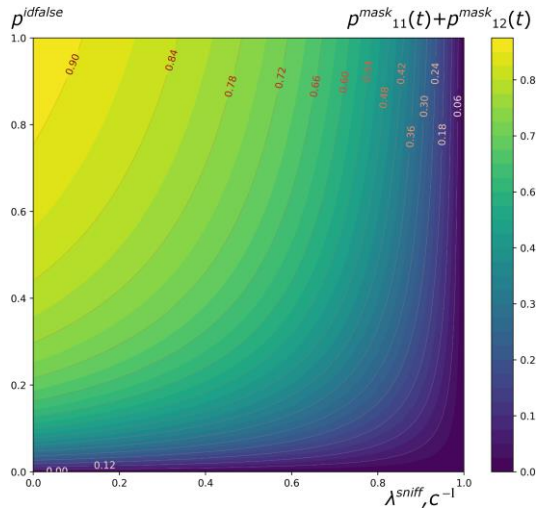

Рис. 6. Результат расчетов вероятности пребывания $СП_{mask}$ в S_1 или S_2, к t = 100 с в зависимости от интенсивности КР и качества аппроксимации конструктивного сетевого трафика

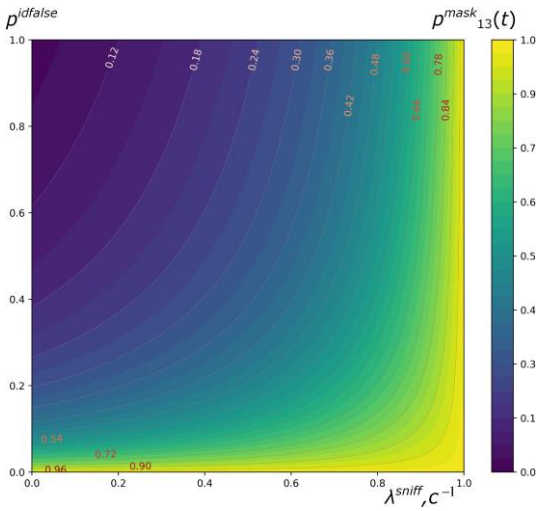

Рис. 7. Результат расчетов вероятности пребывания $СП_{mask}$ в S_3, к t = 100 с в зависимости от интенсивности КР и качества аппроксимации конструктивного сетевого трафика

Другой компенсирующей мерой, направленной на противодействие КР, является интенсивность реконфигурации ИН СПД ВН. В результате расчетов получены значения вероятностей пребывания в состоянии результативного (состояния S_1 или S_2) и нерезультативного (состояние S_3) маскирования к моменту времени t = 100 с в зависимости от интенсивности R^{real} реконфигурации реальных ИН и интенсивности λ^{sniff} КР (рис. 8, 9), а также интенсивности R^{real} реконфигурации реальных ИН и количества реальных ИН N^{real} (рис. 10, 11).

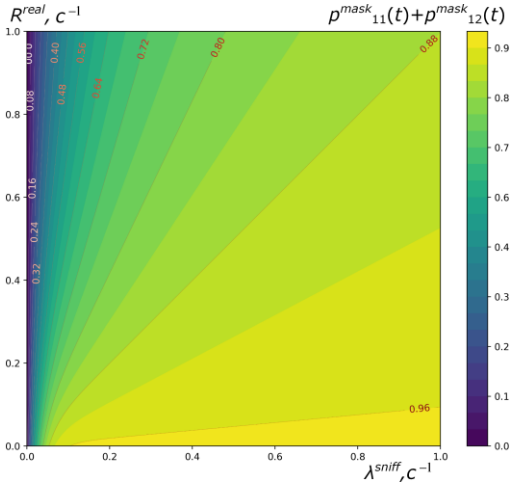

Рис. 8. Результат расчетов вероятности пребывания системы в S_1 или S_2, к t = 100 с в зависимости от интенсивности КР и интенсивности реконфигурации реальных ИН

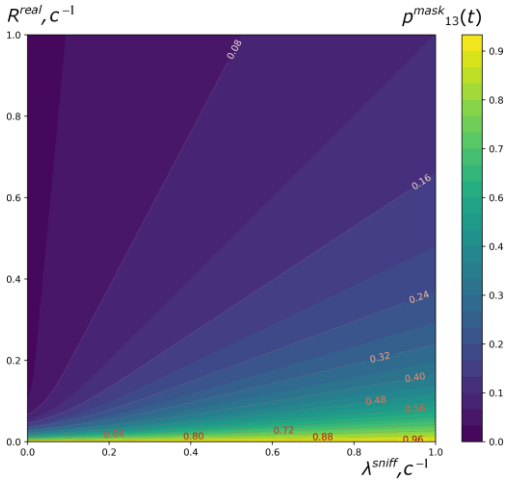

Рис. 9. Результат расчетов вероятности пребывания системы в состоянии S_3 к t = 100 с в зависимости от интенсивности КР и интенсивности реконфигурации реальных ИН

DOI: 10.24412/2410-9916-2025-1-079-104
URL: http://sccs.intelgr.com/archive/2025-01/04-Sherstobitov.pdf

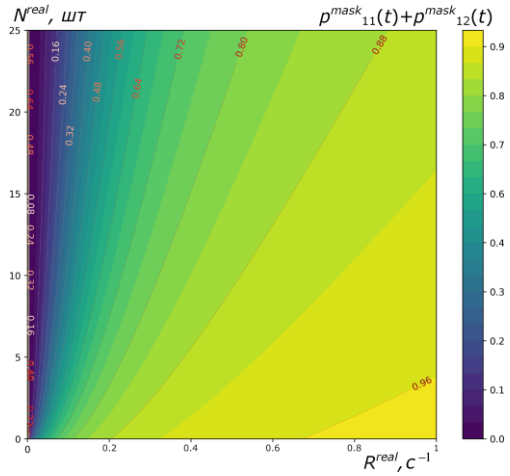

Рис. 10. Результат расчетов вероятности пребывания $СП_{mask}$ в S_1 или S_2, к t = 100 с в зависимости от интенсивности реконфигурации и количества реальных ИН

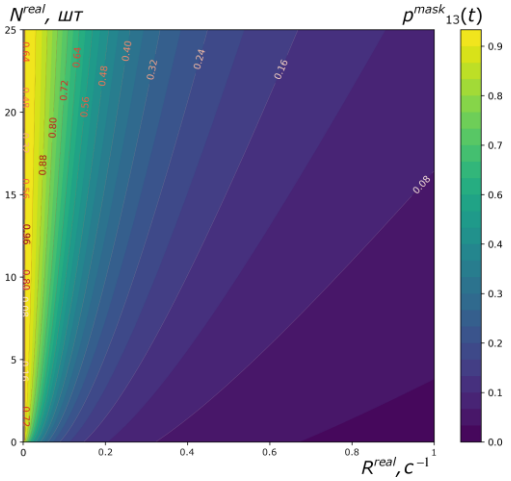

Рис. 11. Результат расчетов вероятности пребывания $СП_{mask}$ в S_3 к t = 100 с в зависимости от интенсивности реконфигурации и количества реальных ИН

Из рисунков видно, что вероятность нахождения в состоянии результативного маскирования (состояния S_1 или S_2) снижается при интенсивной КР, малых значениях интенсивности реконфигурации R^{real}, а также больших значениях количества реальных ИН СПД ВН.

Основными неуправляемыми параметрами при моделировании процесса маскирования информационного обмена в СПД ВН является интенсивность λ^{rp} конструктивного сетевого трафика между узлами сети и количество реальных ИН N^{real}.

Для реализации замысла маскирования, управляемыми параметрами определены интенсивность λ^{fp} маскирующего сетевого трафика между узлами сети и количество ложных ИН N^{false}.

В результате расчетов получены значения вероятностей пребывания системы в состоянии результативного (состояния S_1 или S_2) и нерезультативного (состояние S_3) маскирования к моменту времени t = 100 с в зависимости от интенсивности λ^{rp} конструктивного сетевого трафика и интенсивности λ^{fp} маскирующего сетевого трафика (рис. 12, 13), от интенсивности λ^{fp} маскирующего сетевого трафика и количества ложных ИН N^{false} (рис. 14, 15), а также количества ложных ИН N^{false} и количества реальных ИН N^{real}. (рис. 16, 17).

Из рисунков видно, что вероятность нахождения в состоянии результативного (состояния S_1 или S_2) маскирования существенно повышается при интенсивном маскирующем обмене узлов сети, а также формировании дополнительных ложных ИН.

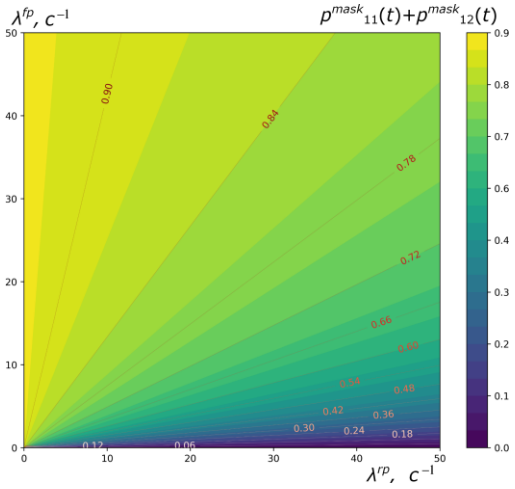

Рис. 12. Результат расчетов вероятности пребывания СП$_{mask}$ в S_1 или S_2, к t = 100 с в зависимости от интенсивностей маскирующего и конструктивного сетевого трафика

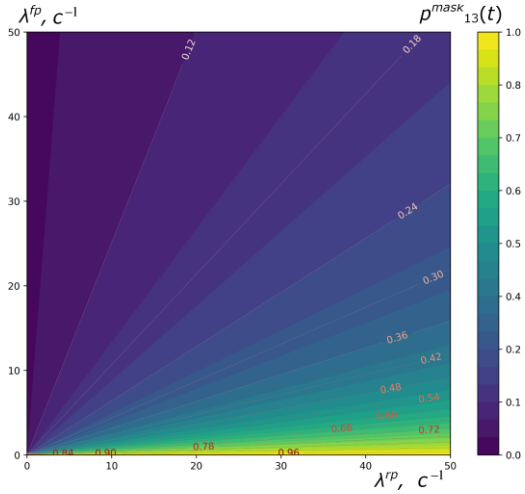

Рис. 13. Результат расчетов вероятности пребывания СП$_{mask}$ в S_3, к t = 100 с в зависимости от интенсивностей маскирующего и конструктивного сетевого трафика

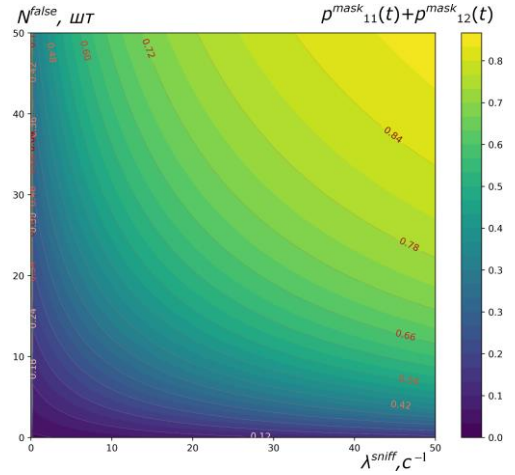

Рис. 14. Результат расчетов вероятности пребывания СП$_{mask}$ в S_1 или S_2, к t = 100 с в зависимости от интенсивности маскирующего трафика и количества ложных ИН

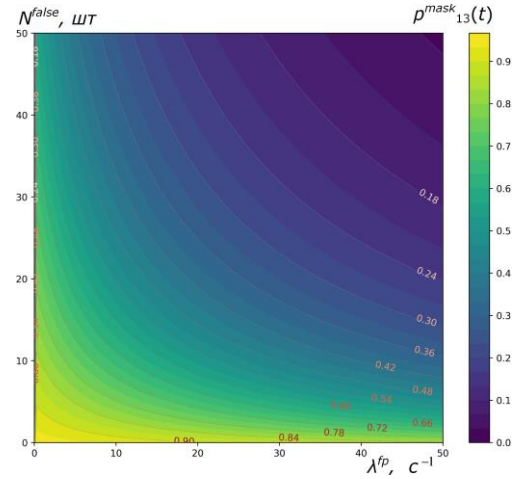

Рис. 15. Результат расчетов вероятности пребывания СП$_{mask}$ в S_3, t = 100 с в зависимости от интенсивности маскирующего трафика и количества ложных ИН

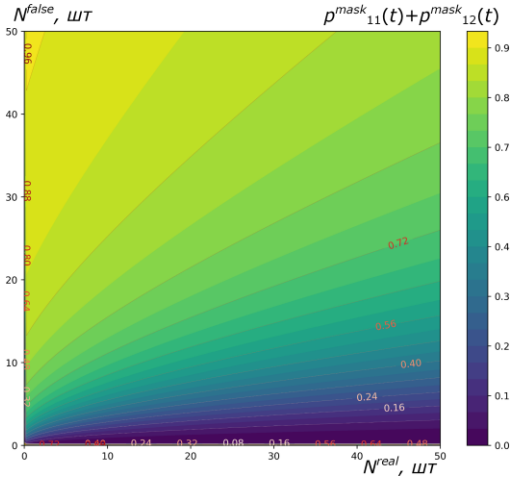

Рис. 16. Результат расчетов вероятности пребывания $СП_{mask}$ в S_1 или S_2, к t = 100 с в зависимости от количества реальных и ложных ИН

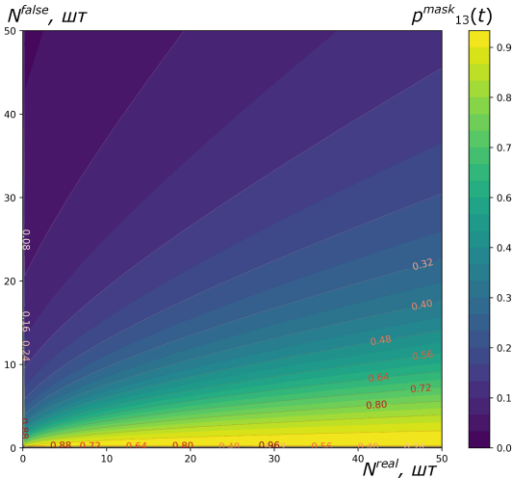

Рис. 17. Результат расчетов вероятности пребывания $СП_{mask}$ в S_3, к t = 100 с в зависимости от количества реальных и ложных ИН

Рассмотрим ситуацию № 2, при которой моделируемая система функционирует в нестационарном режиме, то есть когда интенсивность конструктивного сетевого трафика зависит от времени t. В данной ситуации снято допущение о равенстве интенсивностей конструктивного сетевого трафика на всех ИН сети, а параметр $\lambda^{rp}(t)$ определяется суммарным значением интенсивности конструктивного сетевого трафика на всех ИН сети в момент времени t.

Получены выходные ВВХ, при расчете которых аппроксимация зависимости частоты появления конструктивных пакетов сообщений от времени осуществлялась на основе варьирования архитектуры рекуррентной нейронной сети с LSTM-ячейками (англ. Long short-term memory) (изменялось количество слоев, ячеек, активационная функция и функция потерь).

Результаты расчетов вероятностей нахождения случайного процесса в одном из состояний к моменту времени t для нестационарного случая (рис. 18) показывают, что стационарные вероятности отсутствуют (значения вероятностей постоянно колеблются относительно некоторых средних значений). Указанные значения получены при аналогичных ситуации № 1 значениях параметров функционирования СПД ВН: N^{false} = 7; N^{real} = 22; λ^{fp} = 2 с$^{-1}$; R^{false} = 0,1 с$^{-1}$; R^{real} = 1 с$^{-1}$; $p^{idfalse}$ = 0,2; λ^{sniff} = 1 с$^{-1}$.

Для учета нестационарности параметра интенсивности конструктивного сетевого трафика в момент времени t и условий функционирования СПД ВН на результативность маскирования проведена оценка влияния качества аппроксимации конструктивного сетевого трафика, интенсивности КР, интенсивности маскирующего сетевого трафика, количества ложных и реальных ИН СПД ВН, интенсивности реконфигурации реальных ИН на вероятность нахождения случайного процесса $СП_{mask}$ в состоянии, характеризующем компрометацию реальных ИН.

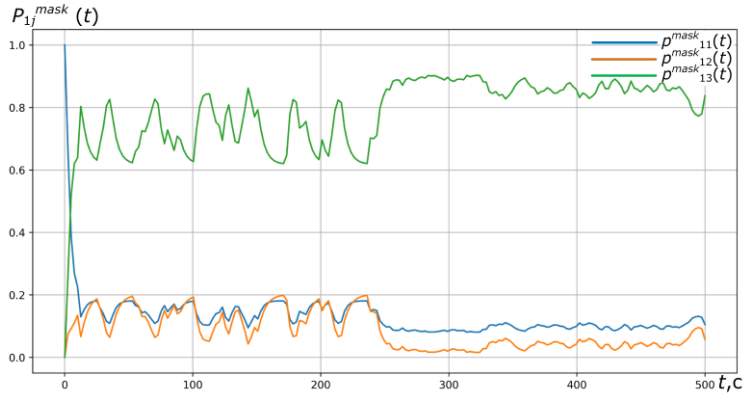

Рис. 18. Результат расчета вероятности перехода $СП_{mask}$ в состояние j из состояния S_1 к моменту времени t для ситуации № 2 (нестационарный случайный процесс)

Так, для указанных условий функционирования с учетом нестационарного характера интенсивности конструктивного сетевого трафика получены значения вероятности нахождения случайного процесса $СП_{mask}$ в состоянии S_3 к моменту времени t в зависимости от различных значений параметров:

– качества аппроксимации $p^{idfalse}$ динамических характеристик конструктивного сетевого трафика при генерации маскирующего (рис. 19) и интенсивности КР λ^{sniff} (рис. 20);
– количества ложных N_{false} (рис. 21) и реальных N^{real} (рис. 22) ИН;
– интенсивности λ^{fp} маскирующего сетевого трафика (рис. 23) и интенсивности реконфигурации R^{real} реальных ИН (рис. 24).

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 интенсивности $\lambda_{ij}^{rp}(t)$ конструктивного сетевого трафика в моменты времени t.

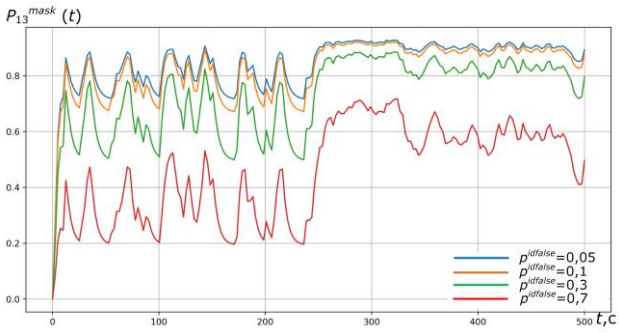

Рис. 19. Результат расчетов вероятности пребывания $СП_{mask}$ в состоянии S_3 к моменту времени t в зависимости от качества аппроксимации конструктивного трафика

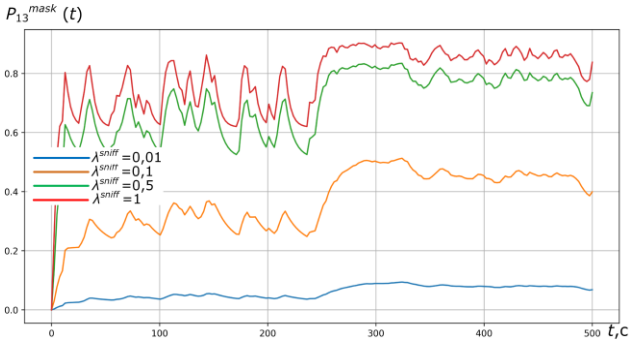

Рис. 20. Результат расчетов вероятности пребывания $СП_{mask}$ в состоянии S_3 к моменту времени t в зависимости от интенсивности КР

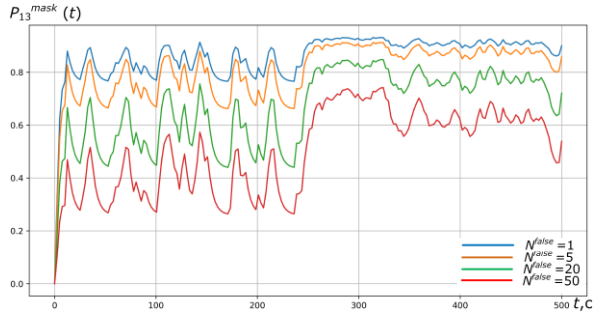

Рис. 21. Результат расчетов вероятности пребывания $СП_{mask}$ в состоянии S_3 к моменту времени t в зависимости от количества ложных ИН

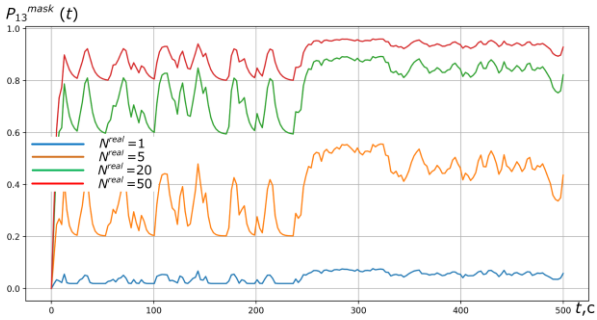

Рис. 22. Результат расчетов вероятности пребывания $СП_{mask}$ в состоянии S_3 к моменту времени t в зависимости от количества реальных ИН

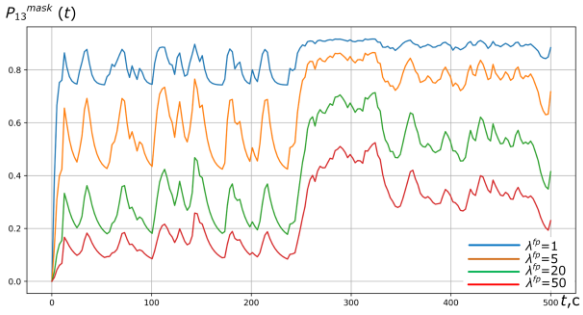

Рис. 23. Результат расчетов вероятности пребывания $СП_{mask}$ в состоянии S_3 к моменту времени t в зависимости от интенсивности маскирующего сетевого трафика

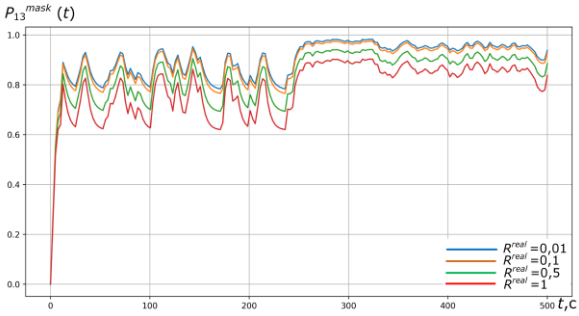

Рис. 24. Результат расчетов вероятности пребывания $СП_{mask}$ в состоянии S_3 к моменту времени t в зависимости от интенсивности реконфигурации реальных ИН

Таким образом, разработанная модель позволяет исследовать процесс функционирования СПД ВН при реализации маскирования информационного обмена 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 информационного обмена узлов СПД ВН в условиях КР.

Теоретическая значимость модели заключается в том, что, в отличие от известных ([15], в которой используются однородные марковские случайные процессы для решения задач обеспечения динамического управления ресурсами и устранения демаскирующих признаков средств защиты информации, [16], в которой используются однородные марковские случайные процессы для управления параметрами сетевых соединений клиент-серверной информационной системы в условиях КР, [17], в которой используются однородные марковские случайные процессы для моделирования почтовых сеансов и оптимального конфигурирования параметров функционирования систем электронной почты, [18], в которой используются однородные марковские случайные процессы для моделирования процесса несанкционированного доступа КР к ресурсам

информационных систем) применяется математический аппарат теории неоднородных марковских процессов с дискретными состояниями и непрерывным временем для определения ВВХ оценки результативности маскирования ИН СПД ВН, позволяющий учитывать нестационарность сетевого трафика и использовать полученные ВВХ для определения оптимальных значений параметров маскирования информационного обмена узлов СПД ВН в условиях КР.

Вывод

Предложенная математическая модель позволяет исследовать процесс функционирования СПД ВН в условиях КР и, в отличие от известных [15-18], решает задачу определения ВВХ оценки результативности маскирования ИН СПД ВН, с учетом нестационарности потоков сетевого трафика, с использованием математического аппарата теории неоднородных марковских процессов с дискретными состояниями и непрерывным временем.

Направлением дальнейших исследований является разработка алгоритма оптимального конфигурирования параметров маскирования информационного обмена узлов сети, а также оценка эффективности их применения**.**

Литература

1. Joint Chiefs of Staff. Cyberspace operations. Joint Chiefs of Staff (US); 19 2022 Dec 19. Joint Publication No.: JP 3-12. Official Website of the Joint Chiefs of Staff [Электронный ресурс]. URL: https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series (дата обращения: 01.12.2024).

2. Актуальные киберугрозы: 1 квартал 2024 года // Официальный информационный ресурс ПАО «Группа Позитив» [Электронный ресурс]. 2024. – URL: http://ptsecurity.com.ru-ru/research/analytics/cybersecurity-threatscape-2024-q1/ (дата обращения 11.11.2024).

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

4. 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.

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

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

7. Макаренко С. И. Динамическая модель двунаправленного информационного конфликта с учетом возможностей сторон по наблюдению, захвату и блокировке ресурса // Системы управления, связи и безопасности. 2017. № 1. С. 60-97. doi: 10.24411/2410-9916-2017-10106.

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

9. Шелухин О. И., Ерохин С. Д., Ванюшина А. В. Классификация IP-трафика методами машинного обучения. – М.: Горячая линия – Телеком, 2023. – 284 с.

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

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

12. Гугин А. Ю., Иванов И. И., Крупенин А. В., Кучуров В. В., Максимов Р. В. Мультисервисный маршрутизатор с функцией маскирования информационных направлений // Патент на полезную модель RU 191373, опубл. 02.08.2019.

13. Максимов Р. В., Починок В. В., Шерстобитов Р. С., Ворончихин И. С., Лысенко Д. Э., Теленьга А. П., Горбачев А. А. Способ маскирования структуры сети связи // Патент на изобретение RU 2794532, опубл. 20.04.2023.

14. Максимов Р. В., Соколовский С. П., Теленьга А. П. Способ защиты вычислительных сетей // Патент на изобретение RU 2789810, опубл. 10.02.2023.

15. 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.

16. 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.

17. 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.

18. 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.

19. Боговик А. В., Игнатов В. В. Эффективность систем военной связи и методы ее оценки. – СПб.: ВАС, 2006. – 183 с.

20. Макаренко С. И. Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки. Монография. – СПб.: Наукоемкие технологии, 2020. – 337 с.

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

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

References

1. Joint Chiefs of Staff. Cyberspace operations. Joint Chiefs of Staff (US); 19 2022 Dec 19. Joint Publication No.: JP 3-12. *Official Website of the Joint Chiefs of Staff*. Available at: https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series (accessed: 1 December 2024).

2. Current cyber threats: 1st quarter 2024. *Oficial'nyj informacionnyj resurs PAO « Gruppa Positiv»* [The official information resource of Group Positive PJSC]. 2023. Available at: http://ptsecurity.com.ru-ru/research/analytics/cybersecurity-threatscape-2024-q1 (accessed 11 November 2024) (in Russian).

3. Sherstobitov R. S., Maksimov R. V., Sharifullin S. R. Masking of Departmental-purpose Integrated Communication Networks. *System of Control, Communication and Security*, 2018, vol. 4, pp. 136-175 (in Russian).

4. 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.

5. 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).

6. Telenga A. P. Masking Metastructures of Information Systems in Cyberspace. *Voprosi Kiberbezopasnosti*, 2023, no. 5(57), pp. 50-59 (in Russian).

7. Makarenko S. I. Dynamic Model of the Bi-directional Information Conflict to Take into Account Capabilities of Monitoring, Capturing and Locking of Information Resources. *Systems of Control, Communication and Security*, 2017, no. 1, pp. 60-97. doi: 10.24411/2410-9916-2017-10106 (in Russian).

8. Sherstobitov R. S. The Model of Information Exchange Masking in the Departmental Communication Network. *Systems of Control, Communication and Security*, 2024, no. 1, pp. 1-25. doi: 10.24412/2410-9916-2024-1-001-025 (in Russian).

9. Sheluhin O. I., Erohin S. D., Vanyushina A. V. *Klassifikaciya IP-trafika metodami mashinnogo obucheniya* [Classification of IP Traffic Using Machine Learning Methods]. Moscow, Goryachaya liniya. Telekom Publ., 2023. 284 p. (in Russian).

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

11. Golub B. V., Krasnov V. A., Likov N. Yu., Maksimov R. V. *Sposob Maskirovaniya Strukturi Seti Svyazi* [Method of Masking the Structure of the Communication Network]. Patent Russia, no. 2645292, 2018.

12. Gugin A. Yu., Ivanov I. I., Krupenin A. V., Kuchurov V. V., Maksimov R. V. *Mul'tiservisnyj marshrutizator s funkciej maskirovaniya informacionnyh napravlenij* [Multiservice Router with Information Direction Masking Function]. Utility Model Patent Russia, no 191373, 2019.

13. Maksimov R. V., Pochinok V. V., Sherstobitov R. S., Voronchihin I. S., Lysenko D. E., Telen'ga A. P., Gorbachev A. A. *Sposob maskirovaniya struktury seti*

svyazi [Method for Masking the Structure of a Communication Network]. Patent Russia, no 2794532, 2023.

14. Maksimov R. V., Sokolovskij S. P., Telen'ga A. P. *Sposob zashchity vychislitel'nyh setej* [Method for Protecting Computing Networks]. Patent Russia, no. 2789810, 2023.

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

16. 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).

17. 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.

18. 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).

19. Bogovik A. V., Ignatov V. V. *Effektivnost' sistem voennoj svyazi i metody ee ocenki* [Effectiveness of Military Communication Systems and Methods of Its Assessment]. Saint-Petersburg, 2006. 183 p (in Russian).

20. Makarenko S. I. *Modeli sistemy svjazi v uslovijah prednamerennyh destabilizirujushhih vozdejstvij i vedenija razvedki* [Models of the Communication System in the Conditions of Deliberate Destabilizing Influences and Intelligence]. Saint-Petersburg, Naukoemkie tekhnologii Publ., 2020. 337 p. (in Russian).

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

22. 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).

Статья поступила 16 декабря 2024 г.

Информация об авторе

Шерстобитов Роман Сергеевич – кандидат технических наук. Докторант. Краснодарское высшее военное училище им. генерала армии С.М. Штеменко. Область научных интересов: обеспечение информационной безопасности; синтез и системный анализ систем защиты информации критически важных объек-

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

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

Model for masking information flows of departmental data transmission networks under conditions of computer reconnaissance

R. S. Sherstobitov

Problem statement: *the ability of computer intelligence systems to interact with information flows of departmental data transmission networks and to exploit undeclared capabilities and vulnerabilities of software, as well as to deliver malicious content to internal local segments, provides the intruder with the necessary information to form models of the composition, connectivity, and operational interaction of network nodes. One of the ways to prevent these threats is to mask the information exchange of network nodes. However, the existing scientific and methodological framework for determining the probabilistic and temporal characteristics of the compromise of information channels in departmental data transmission networks does not take into account the non-stationarity of the characteristics of the random process of information exchange among network nodes under computer intelligence.* ***The purpose of the work*** *is model development and study the functioning of the departmental data transmission networks in the realization of information exchange masking in the conditions of computer intelligence.* ***Methods used****: the methods of random processes examination are used****.*** ***The scientific novelty*** *of the model lies in the application of mathematical apparatus of the non-homogeneous Markov processes theory with discrete states and continuous time to determine the probabilistic and temporal characteristics of the process of departmental data networks functioning in the implementation of information exchange masking in the conditions of computer intelligence.* ***Practical significance*** *of the model is the finding the probabilistic-temporal characteristics of the process of departmental data transmission networks functioning in the conditions of computer intelligence, which are necessary for determining the optimal values of the masking parameters.* ***Result****: the model for masking information channels of departmental data transmission networks under conditions of computer reconnaissance has been developed, which is formalized as a Markov random process with discrete states and continuous time. The obtained output probabilistic-temporal characteristics could be used as an objective function in the formulation of the vector optimization problem and optimal values of network connection parameters of nodes of the departmental data transmission network in the implementation of information exchange masking in the conditions of computer intelligence.*

Keywords: *data transmission network, information exchange masking, compromise, information flow, random process, computer intelligence.*

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.