

РАЗРАБОТКА МЕТОДОЛОГИИ АНАЛИЗА И ПОВЫШЕНИЯ СТРУКТУРНОЙ СКРЫТНОСТИ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

Слами Али Юсуф¹

DOI:10.21681/3034-4050-2026-5-12-20

Ключевые слова: информационная безопасность, сеть передачи данных, целевые атаки (APT), демаскирующие признаки, анализ сетевого трафика.

Аннотация

Цель работы: систематизация основных угроз информационной безопасности: перехват и анализ трафика, сканирование сети, компрометация паролей, подмена доверенного объекта и отказ в обслуживании.

Метод: анализ классификаций, обобщение демаскирующих признаков по уровням модели OSI.

Результат: выявлены и классифицированы демаскирующие признаки на физическом, канальном, сетевом, транспортном и прикладном уровнях. Установлено, что наиболее информативными для нарушителя являются сетевой и транспортный уровни (топология, временные паттерны трафика). Выявлено, что целевые атаки последнего десятилетия сместили фокус на критическую инфраструктуру, включая системы промышленной автоматизации. Предложенные методы маскирования информационного обмена позволяют разорвать связь между наблюдаемым трафиком и реальными технологическими процессами. В статье систематизированы основные угрозы информационной безопасности: перехват и анализ трафика, сканирование сети, компрометация паролей, подмена доверенного объекта и отказ в обслуживании. Особое внимание уделено APT-атакам, которые характеризуются многоэтапностью, длительным скрытым присутствием и нацеленностью на промышленные системы. Материалами исследования послужили открытые данные о компьютерных атаках за 1998–2025 гг., включая инциденты Stuxnet, NotPetya, TRITON и атаку на Colonial Pipeline. Результаты: выявлены и классифицированы демаскирующие признаки на физическом, канальном, сетевом, транспортном и прикладном уровнях. Установлено, что наиболее информативными для нарушителя являются сетевой и транспортный уровни (топология, временные паттерны трафика).

Научная новизна: разработаны комплексная вероятностно-временная модель оценки скрытности, методика формирования ложных портретов на основе генетических алгоритмов и количественный показатель структурной скрытности.

Практическая значимость: возможность количественной оценки защищенности сетей, выявления уязвимых элементов и реализации активных мер маскирования при проектировании защищенных систем передачи данных.

Введение

В эпоху цифровой трансформации сети передачи данных стали ключевым элементом функционирования критической инфраструктуры, включая энергетические системы, транспорт, связь и оборонные объекты. Эффективность управления технологическими процессами и стабильность этих объектов напрямую зависят от надежности, оперативности и, что особенно важно, защищенности используемых сетей. Однако с ростом их сложности и переходом на унифицированные стеки протоколов (в частности, TCP/IP) возникает новая, чрезвычайно опасная угроза – «атаки структурной разведки» (structural reconnaissance). В отличие от традиционных атак, нацеленных на содержимое передаваемых данных, данный вид угрозы предполагает пассивный анализ сетевого трафика для извлечения внутренней операционной логики. Наблюдая за временными паттернами, топологией и интенсивностью информационных

поточков, злоумышленник может восстановить организационную структуру управления, выявить критические узлы и определить этапы технологического процесса, даже не расшифровывая сами сообщения. Это создает фундаментальное противоречие между необходимостью эффективной связи для выполнения производственных задач и потребностью скрыть информационные паттерны от технической компьютерной разведки (ТКР) вероятного противника. Существующие стандартные средства защиты информации (межсетевые экраны, системы обнаружения вторжений, антивирусы) ориентированы на блокирование известных атак или защиту семантического содержимого, но не способны противодействовать анализу структурных демаскирующих признаков, особенно в условиях сложных и продолжительных целевых атак (Advanced Persistent Threats, APT). Более того, отсутствие количественных методов оценки степени скрытности структуры сети

¹ Слами Али Юсуф, адъюнкт Военной академии связи им. Маршала Советского Союза С. М. Буденного. Санкт-Петербург, Российская Федерация. ORCID: 0009_0004_6819_2798. E-mail: alisalame654@gmail.com

не позволяет объективно определить эффективность существующих и вновь разрабатываемых механизмов защиты. В связи с этим целью данного исследования является разработка комплексной количественной методологии анализа и повышения структурной скрытности сетей передачи данных критического назначения. Для достижения этой цели в работе решаются следующие задачи: во-первых, создание вероятностно-временных моделей основных угроз, связанных с перехватом и анализом трафика, обнаружением источников информации и распознаванием структур на основе изоморфизма графов; во-вторых, разработка методики активного маскирования информационного обмена с применением интеллектуальных алгоритмов генерации ложного трафика (включая генетические алгоритмы и методы роевого интеллекта); в-третьих, проведение имитационного моделирования для количественной оценки эффективности предложенных методов. Научная новизна работы заключается в создании комплексной вероятностно-временной модели оценки скрытности и введении количественного показателя структурной скрытности $P_{i/k}$.

Статья имеет следующую структуру. В первом разделе рассматриваются теоретические основы и моделирование основных угроз: угроза перехвата и анализа трафика, модель передачи сообщений в IP-сети, модель обнаружения

источников информации, а также алгоритм распознавания структур на основе изоморфизма графов. Во втором разделе представлена разработанная методика маскирования сети, включая общие положения и результаты моделирования влияния стратегий маскирования на метрики обнаружения угроз. В третьем разделе приводится количественная оценка эффективности маскирования. В заключении формулируются основные выводы и результаты исследования.

Теоретическая основа и моделирование угроз. Вероятностно-временная модель угрозы «Перехват и анализ сетевого трафика»

Для моделирования успеха наблюдателя в сборе репрезентативной выборки определим случайную величину T_c как время, необходимое для перехвата критической доли от общего сетевого потока. Процесс перехвата информации представляется в виде стохастической сети, представленной на рисунке 1 (Стохастическая сеть профильной атаки типа «Перехват и анализ сетевого трафика») [2].

Вероятность успешного перехвата к моменту времени t :

$$P_{capture}(t) = P(N(t) \geq N_{needed}) = 1 - \sum_{k=0}^{N_{needed}-1} \frac{(\lambda_{capture} \cdot t)^k e^{-\lambda_{capture}}}{k!}, \quad (1)$$

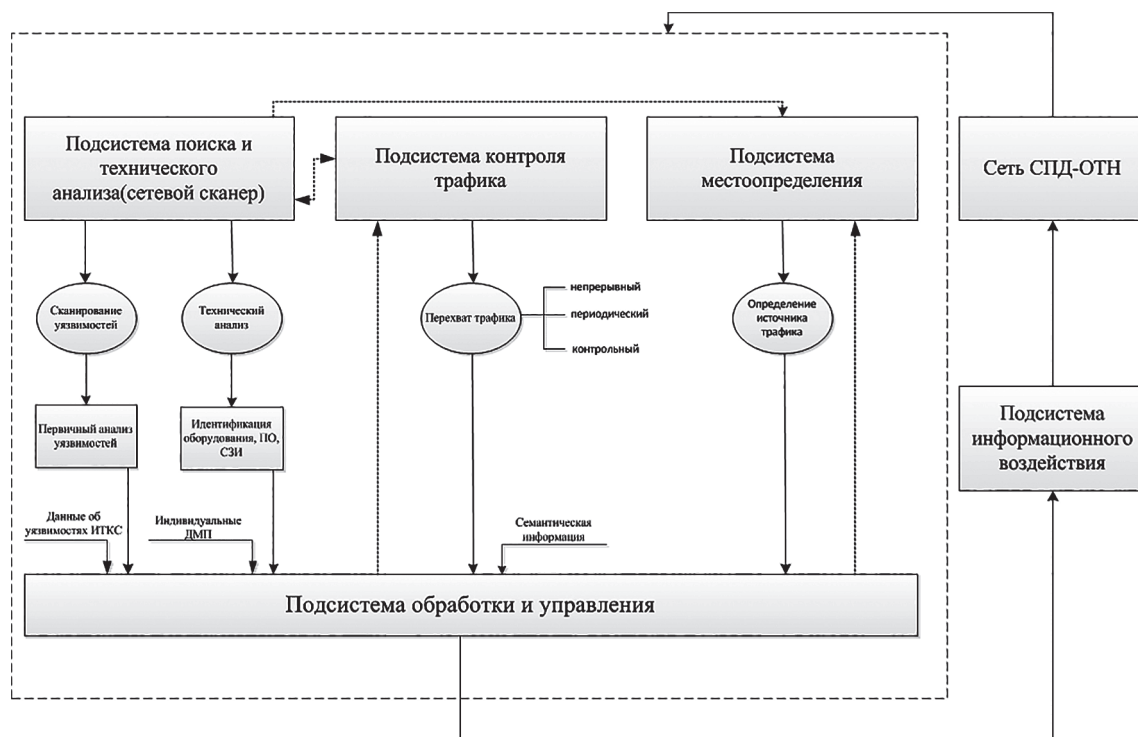


Рис. 1. Вербальная модель целевой атаки

где $P_{capture}(t)$ – вероятность того, что злоумышленник успешно перехватит репрезентативную выборку трафика за время; N_{needed} – время, прошедшее с начала атаки (перехвата); $N(t)$ – критическое количество пакетов, необходимое нарушителю для анализа структуры сети; k – промежуточная переменная суммирования (количество перехваченных пакетов); $\lambda_{capture}$ – интенсивность перехвата пакетов (пакетов/сек), характеризует технические возможности нарушителя; e – основание натурального логарифма ($\approx 2,71828$).

Эквивалентная функция стохастической сети имеет вид:

$$h(s) = \frac{w(s) \cdot m(s) \cdot l(s) \cdot P_n \cdot d(s)}{1 - (1 - P_n) \cdot z(s) \cdot l(s)}, \quad (2)$$

где $h(s)$ – эквивалентная передаточная функция всей сети в пространстве преобразования Лапласа (s – комплексная переменная); $w(s)$, $m(s)$, $l(s)$, $d(s)$, $z(s)$ – преобразования Лапласа для отдельных узлов или ветвей стохастической сети. Описывают вероятностно-временные характеристики этапов атаки (например, ожидание, обработка, передача); P_n – вероятность наличия определенного узла/пути (или успеха на конкретном шаге); $(1 - P_n)$ – вероятность отказа или отсутствия пути.

Результаты моделирования представлены на рисунке 2. Расчеты показывают, что за время, равное одному часу работы сети, организованный нарушитель с вероятностью не хуже 0,9 способен перехватить сетевой трафик [3, 4].

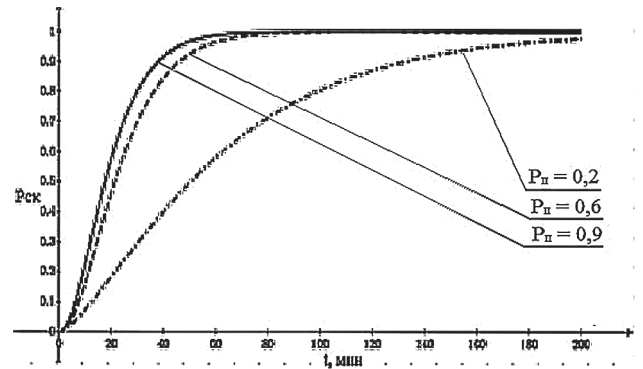


Рис. 2. Функция распределения времени анализа сетевого трафика при различных значениях вероятности доступности для перехвата трафика нарушителем в IP-сети

Модель передачи сообщений в IP-сети

Время передачи сообщения в канале зависит от пропускной способности C и объема сообщения I :

$$t = \frac{I}{C}, \quad (3)$$

где t – время передачи (с); I – объем передаваемой информации (биты, байты); C – пропускная способность канала (бит/с, байт/с).

Процесс передачи представляется стохастической сетью (рис. 3).

Эквивалентная функция определяется с использованием уравнения Мейсона. Функция распределения времени передачи аппроксимируется гамма – распределением [5]:

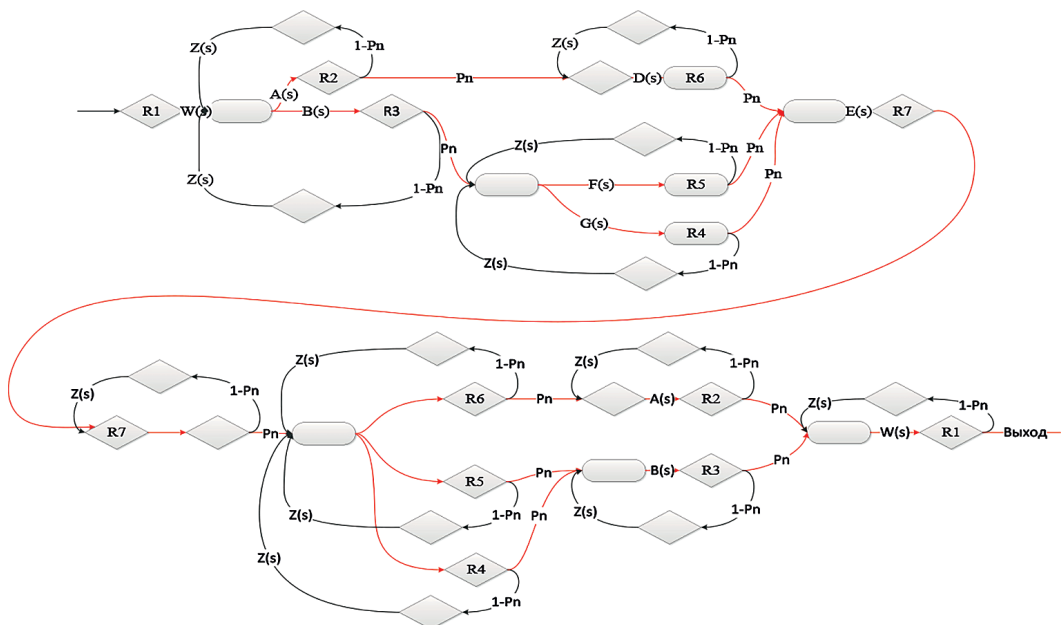


Рис. 3. Стохастическая сеть процесса передачи DBD-пакета

$$F(t) = \int_0^t \frac{\mu^\alpha}{\Gamma(\alpha)} x^{\alpha-1} e^{-\mu x} dx, \quad (4)$$

где $F(t)$ – интегральная функция распределения вероятности того, что время передачи не превысит t ; t – момент времени, для которого вычисляется вероятность; x – переменная интегрирования (время); α – параметр формы (shape parameter). Влияет на вид распределения (например, $\alpha = 1$ дает экспоненциальное распределение); μ – параметр интенсивности (rate parameter), обратный среднему времени ($\mu = 1 / \text{среднее время}$); $\Gamma(\alpha)$ – гамма-функция, обобщение факториала на действительные числа;

Результаты моделирования представлены на рисунке 4.

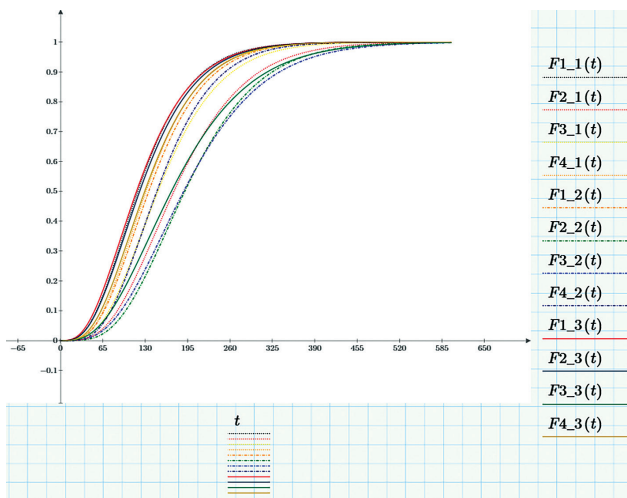


Рис. 4. Функция распределения времени доведения информации по IP-сети с увеличением объема пакета в 120 раз

Модель обнаружения источников передачи

Процесс обнаружения источников информации при сканировании сети представлен стохастической сетью (рис. 5).

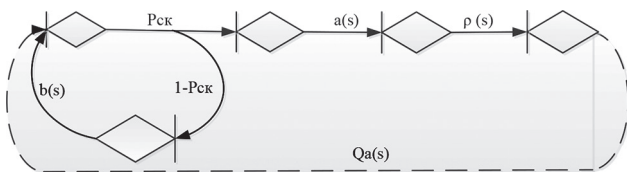


Рис. 5. Стохастическая сеть процесса функционирования подсистемы обнаружения ДМП ТКР организованного нарушителя [6].

Эквивалентная функция:

$$Q_a(s) = \frac{P_{\text{ск}} \cdot \rho \cdot a \cdot (b + s)}{[s^2 + s(a + b \cdot P_{\text{ск}}) + P_{\text{ск}} \cdot a \cdot b \cdot \rho]}. \quad (5)$$

Функция распределения времени обнаружения:

$$F(t) = \sum_{i=1}^2 \frac{P_{\text{ск}} a \rho (b + s_i)}{(2s_i + a + b P_{\text{ск}}) \cdot (-s_i)} \cdot (1 - e^{s_i t}), \quad (6)$$

где $Q_a(s)$ – преобразование Лапласа для процесса обнаружения источника при сканировании; $F(t)$ – вероятность обнаружения нарушителя к моменту времени t ; $P_{\text{ск}}$ – вероятность сканирования сети нарушителем (или вероятность срабатывания системы обнаружения на данном шаге); ρ – параметр плотности (например, плотность источников угроз или плотность сканируемых пакетов); a и b – интенсивности переходов между состояниями в марковской модели (например, a – частота начала сканирования, b – частота обнаружения); s – переменная Лапласа (s).

Модель распознавания структур информационного обмена

Для распознавания структур используется алгоритм проверки изоморфности графов (рис. 7). Вероятность обнаружения терминала [7, 8]:

$$P_i^* = 1 - e^{-\sum_{j=1}^{d_i} \lambda_{ij} \cdot p_j^*(x) dx}, \quad (7)$$

где P_i^* – вероятность обнаружения i -го терминального узла (компьютера, сервера, контроллера); d_i – степень узла i – количество его связей с соседями; λ_{ij} – интенсивность (частота) передачи пакетов между узлом i и его соседом j ; $p_j^*(x)$ – условная вероятность успешного перехвата или анализа пакета на этом соединении в момент времени x ; t – время наблюдения.

Показатель структурной скрытности:

$$P_{i/k} = \frac{w_i(k)}{N^*}, \quad (8)$$

где $P_{i/k}$ – ключевой показатель – количественная мера структурной скрытности. Значение в интервале $[0,1]$. Чем меньше значение, тем выше скрытность (лучше маскировка); $w_i(k)$ – весовая функция, отражающая количество совпадений или степень сходства между реальной структурой i и эталонной структурой k , которую пытаются восстановить нарушитель. N^* – нормировочный коэффициент (максимально возможное значение ($w_i(k)$)), отражающий общую сложность распознавания структуры

На рисунке 8 показаны два изоморфных графа (исходная и проверяемая структуры) с распределением степеней узлов. Вероятность обнаружения терминалов P_i^* рассчитана по формуле (9-2). Узлы с большей степенью (2) имеют более высокую вероятность обнаружения (0,9997), чем узлы со степенью 1 (0,9817).

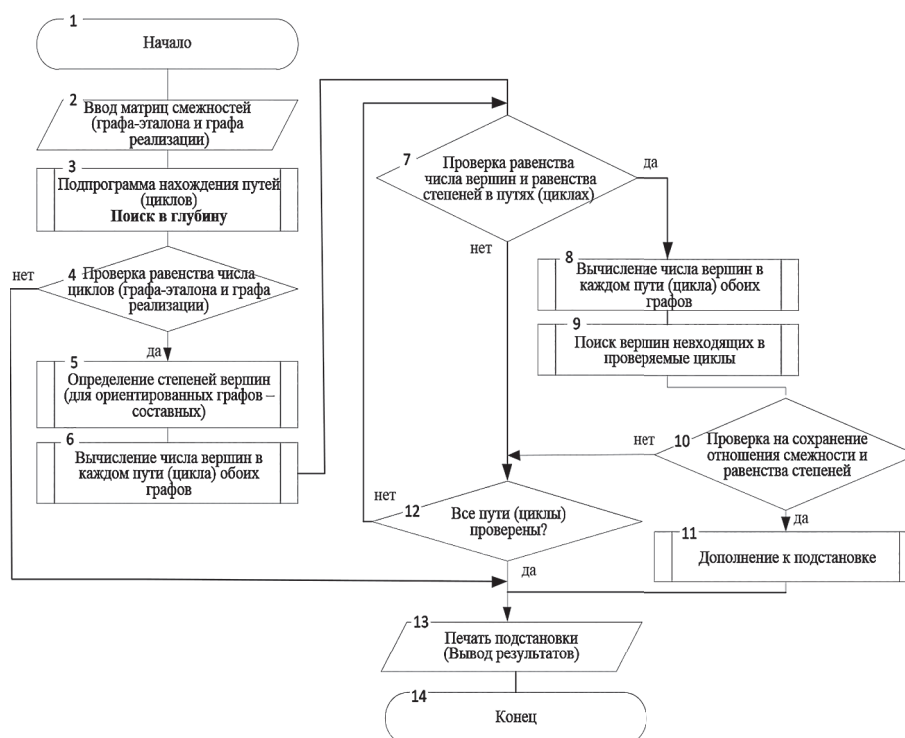


Рис. 7. Блок-схема распознавания структуры СПД ОТН



Рис. 8. Вероятность обнаружения терминалов и степени узлов графа

Результаты моделирования обнаружения источников угроз в IP-сети

Результаты моделирования, выполненного в MATLAB, показали, что предложенная модель обнаружения достигла среднего значения вероятности обнаружения 0,427 (42,7 %) по итерациям моделирования ($N = 0, 2, 4, 6, 8, 10$). В то же время средний показатель структурной скрытности источников составил 0,236 (23,6 %), что отражает баланс между обнаруживаемостью и способностью к маскировке в сети. Анализ соотношения между обнаружением и скрытностью показал, что средний балансный показатель равен 0,236. Моделирование также выявило выраженные уязвимости терминальных узлов сети: успешность распознавания уязвимостей достигла 100 % для всех восьми протестированных терминалов.

В моделировании использовались данные, классифицированные по четырем уровням: высокий, средний, низкий и очень низкий, что позволило провести комплексную оценку работы системы в условиях различного качества данных на рисунке 8 также показаны результаты моделирования на языке MATLAB [9].

В зависимости от местоположения злоумышленника относительно сети различают внутренние и внешние угрозы. Внутренние угрозы осуществляются законными пользователями сети, имеющими авторизованный доступ к ее ресурсам. Внешние угрозы исходят от хакеров, которые не имеют прямого доступа к сетевым элементам и преодолевают меры безопасности через сетевые интерфейсы [6].

По уровню эталонной модели взаимодействия открытых систем (ЭМОС) угрозы могут

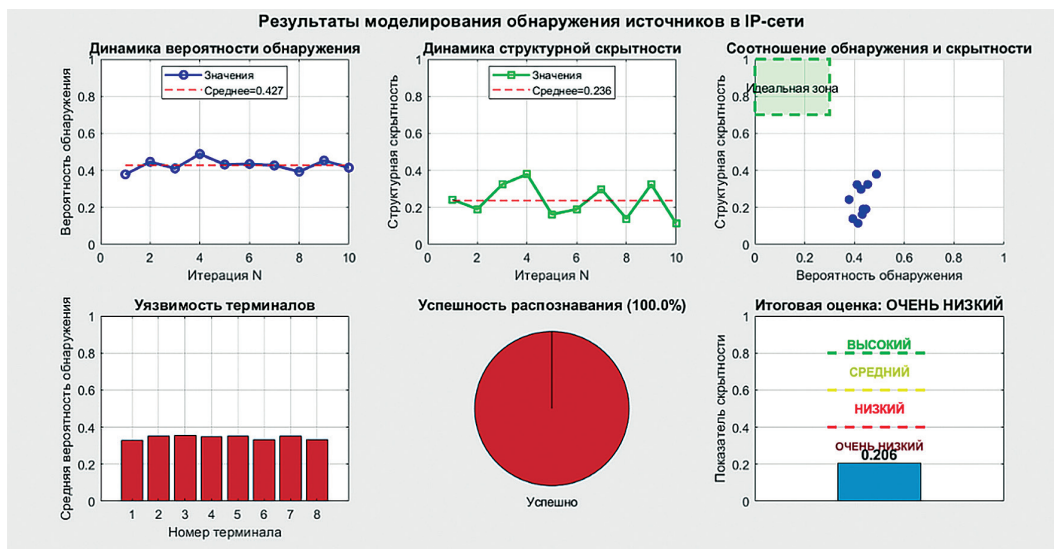


Рис. 8. Результаты моделирования обнаружения источников угроз в IP-сети

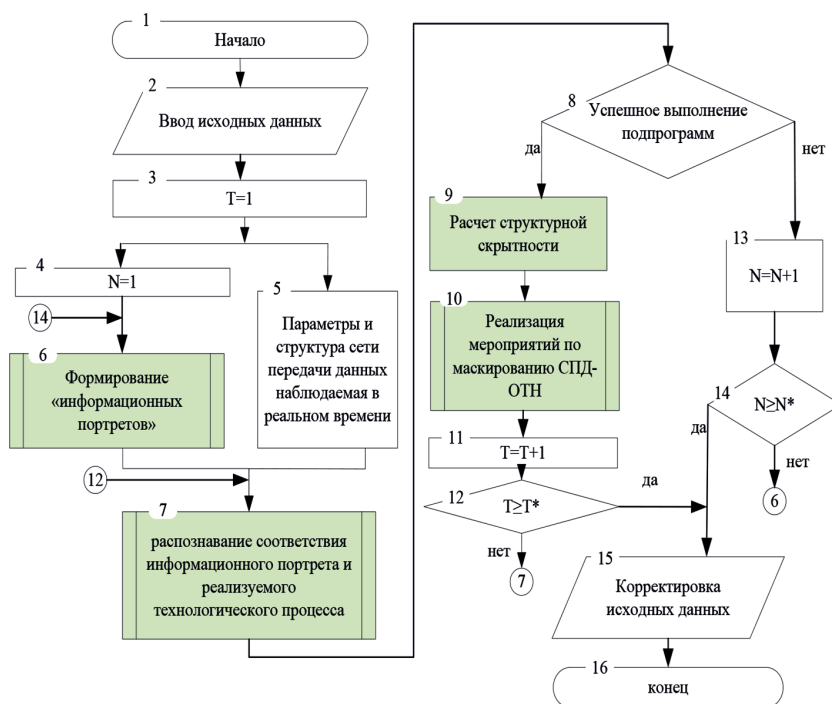


Рис. 9. Блок-схема маскирования СПД ОТН

быть реализованы на физическом, канальном, сетевом, транспортном, сеансовом, уровне представления или прикладном уровне. Каждому уровню соответствуют специфические методы реализации угроз и, соответственно, методы защиты [7].

Методика маскирования сети. Общие положения

Назначение методики – оценка вероятности распознавания структуры сети при реализации мероприятий по маскированию. Основной

показатель – вероятность распознавания структуры P_{ik} за время производственного этапа. Структура методики представлена на рисунке 9 [10, 12].

На рисунке 10 представлен комплексный анализ влияния маскирования на обнаружение сетевой активности, включающий четыре направления:

Зависимость от эффективности маскирования показывает обратную связь – чем выше эффективность маскирования, тем ниже максимальная мощность обнаружения и больше

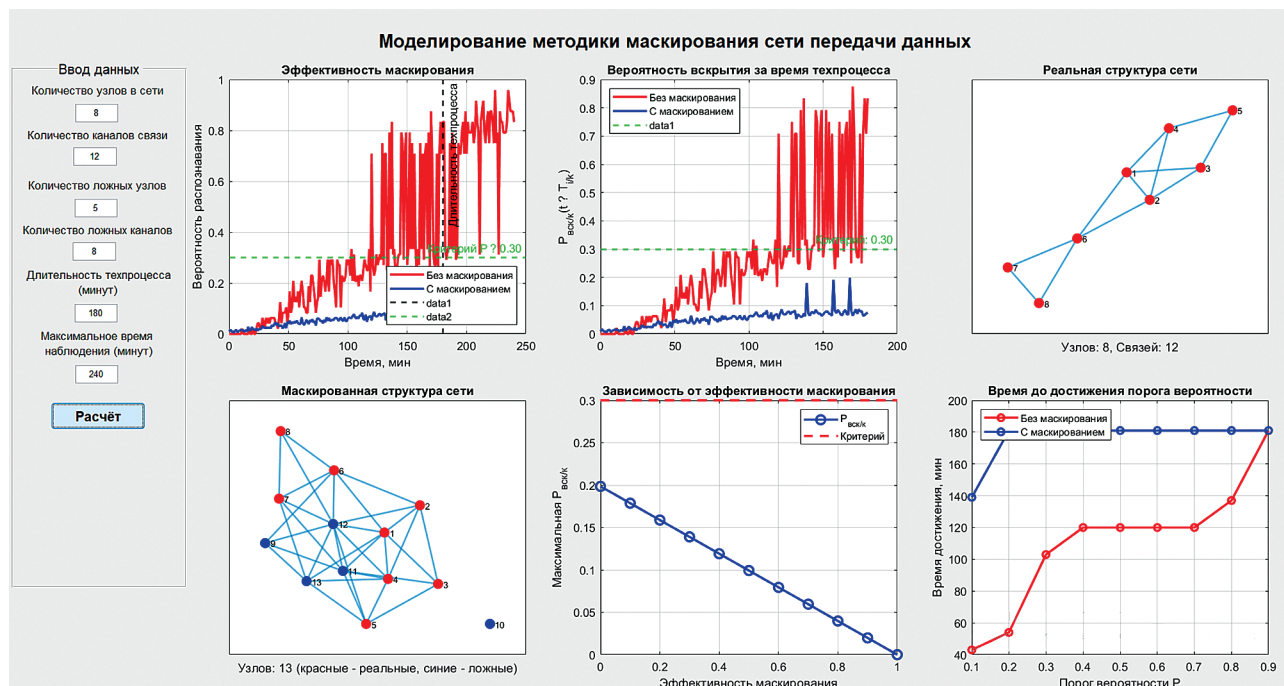


Рис. 10. Влияние стратегий маскирования на метрики обнаружения угроз

времени требуется для достижения порога обнаружения. При максимальной эффективности маскирования вероятность вскрытия снижается до 0,3 (30 %).

Эффективность маскирования во времени: сравнение сценариев с маскированием и без него демонстрирует значительное снижение эффективности обнаружения при применении техник маскирования. Без маскирования вероятность вскрытия достигает 0,8 (80 %) за первые минуты, тогда как при маскировании она не превышает 0,3 (30 %) в течение 180 минут технологического процесса.

Вероятность вскрытия за время техпроцесса: Кривая без маскирования показывает высокую и растущую вероятность обнаружения (до 0,8 за первые минуты), тогда как при маскировании вероятность остается на низком уровне (не более 0,3 в течение 180 минут), подтверждая эффективность предложенной методики.

Реальная структура сети: Схема сети с узлами 1–13 и соединениями, иллюстрирующая контраст между реальной структурой (8 узлов, 12 связей) и её искажённым образом (13 узлов, включая 5 ложных, 8 ложных каналов), который видит система мониторинга при маскировании.

Рисунок предоставляет количественную основу для оценки стратегий маскирования через чёткие метрики: мощность обнаружения, вероятность (снижение с 0,8 до 0,3) и время (сохранение скрытности в течение 180 минут).

Оценка эффективности маскирования

Реализация мероприятий по маскированию обеспечивает снижение вероятности вскрытия структуры сети. Через 3 часа работы вероятность вскрытия не превышает 0,67 (рис. 13), что существенно затрудняет реализацию целевой атаки [11].

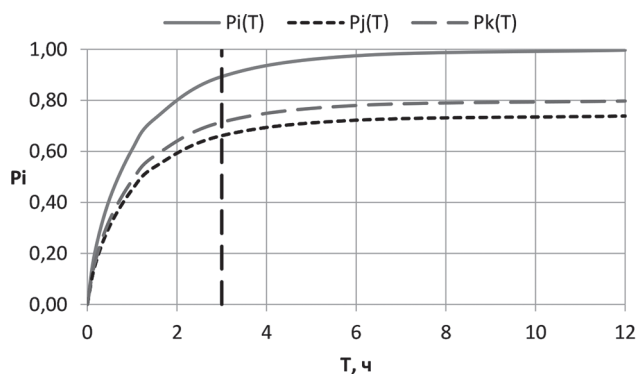


Рис.11. Функции распределения времени вскрытия k-й структуры

Заключение

В результате проведенного исследования разработана комплексная методология анализа и повышения структурной скрытности сетей передачи данных критического назначения.

1. Разработана вероятностно-временная модель угрозы «Перехват и анализ сетевого трафика» на основе стохастических сетей (рис. 1).

Установлено, что за один час работы сети нарушитель с вероятностью 0,9 способен перехватить трафик (рис. 2).

2. Построена модель передачи сообщений в IP-сети с использованием стохастического моделирования (рис. 3) и аппроксимации гамма-распределением (рис. 4), позволяющая выявлять уязвимые элементы инфраструктуры.

3. Создана модель обнаружения источников передачи при сканировании сети (формулы 5–6), показывающая, что при вероятности сканирования 0,9 время обнаружения не превышает 3,3 минуты.

4. Разработан алгоритм распознавания структур на основе проверки изоморфности графов (рис. 7) с показателем структурной скрытности P_{ilk} (формулы 7–8). Моделирование в MATLAB показало вероятность обнаружения 0,427 при скрытности 0,236 (рис. 8).

5. Предложена методика маскирования сети на основе генетических алгоритмов (рис. 9), создающая ложные информационные портреты, наблюдаемые нарушителем как «параллельная» реализация всех этапов процесса.

6. Оценка эффективности показала снижение вероятности вскрытия структуры с 0,9 до 0,67 за три часа работы (рис. 11), подтверждая обратную зависимость между маскированием и обнаружением (рис. 10).

Научная новизна: разработаны комплексная вероятностно-временная модель оценки скрытности, методика формирования ложных портретов на основе генетических алгоритмов и количественный показатель структурной скрытности.

Практическая значимость: возможность количественной оценки защищенности сетей, выявления уязвимых элементов и реализации активных мер маскирования при проектировании защищенных систем передачи данных.

Перспективы: интеграция методов машинного обучения, разработка децентрализованных протоколов скрытности и автоматизированных систем управления ложным обменом.

Разработанная методология обеспечивает комплексное решение проблемы защиты структур информационного обмена от аналитических методов технической разведки.

Литература

1. Привалов А. А., Лаут О. С. Моделирование компьютерных атак и нарушителя. – М.: Воениздат, 2015. – 234 с.
2. Петров П. П. Угрозы информационной безопасности в военных сетях // Кибербезопасность. – 2021. – № 3. – С. 45–52.
3. Сидоров С. С. Методы технической разведки в киберпространстве. СПб.: Наука, 2019.
4. Кузнецов К. К. Анализ сетевого трафика для вскрытия структуры управления // Вопросы защиты информации. – 2022. – № 1. – С. 33–40.
5. Соколов А. В. Теоретические основы скрытности информационных систем. М.: Горячая линия–Телеком, 2018.
6. Smith J., Brown T. Graph-based analysis of network security // Computer Networks. – 2019. – Vol. 158. – Pp. 1–15.
7. Garcia M. Vulnerability assessment of IP-based military networks // Military Communications Conference. – 2022. – Pp. 1–6.
8. Chen L. Rapid source detection in adversarial network environments // IEEE Transactions on Information Forensics and Security. – 2020. – Vol. 15. – Pp. 2345–2356.
9. Корнеев Г. А. Теория графов в задачах распознавания структур. М.: Физматлит, 2017.
10. SpiderNet: Enabling Bot Identification in Network Topology Obfuscation Against Link Flooding Attacks // IEEE/ACM Transactions on Networking. – 2025. – Vol. 33. – No. 1. – Pp. 99–113.
11. WADCS: Weibull-attentive deep learning model for enhanced cyber security // Journal of King Saud University – Computer and Information Sciences. – 2025. – Vol. 37. – No. 1.
12. Stallings W. Cryptography and Network Security: Principles and Practice. 8th ed. New York: Pearson, 2020. – 832 p.

DEVELOPMENT OF A METHODOLOGY FOR ANALYZING AND IMPROVING THE STRUCTURAL SECRECY OF DATA TRANSMISSION NETWORKS

Slami Ali Yusuf²

Keywords: information security, data transmission network, targeted attacks (APT), unmasking signs, analysis of network traffic.

² Slami Ali Yusuf, Adjunct of the Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny. St. Petersburg, Russian Federation. ORCID: 0009_0004_6819_2798. E-mail: alisalame654@gmail.com

Abstract

Goal: systematization of the main threats to information security: interception and analysis of traffic, network scanning, compromise of passwords, spoofing of a trusted object, and denial of service.

Method: analysis of classifications, generalization of unmasking features by levels of the OSI model.

Result: unmasking signs at the physical, channel, network, transport and application layers are identified and classified. It is established that the network and transport layers (topology, temporal traffic patterns) are the most informative for the attacker. It is revealed that targeted attacks of the last decade have shifted the focus to critical infrastructure, including industrial automation systems. The proposed methods of masking information exchange make it possible to break the connection between the observed traffic and real technological processes. Particular attention is paid to APT attacks, which are characterized by multi-stage, long-term covert presence, and targeting industrial systems. The study materials were based on open data on computer attacks for 1998–2025, including the Stuxnet, NotPetya, TRITON incidents, and the attack on the Colonial Pipeline. Results: unmasking signs at the physical, channel, network, transport, and application layers were identified and classified.

Scientific novelty: a complex probabilistic-temporal model for assessing stealth, a method for forming false portraits based on genetic algorithms and a quantitative indicator of structural secrecy have been developed.

Practical significance: the ability to quantify the security of networks, identify vulnerable elements and implement active masking measures in the design of secure data transmission systems.

References

1. Privalov A. A., Laut O. S. Modelirovanie komp'yuternyh atak i narushitelya. – M.: Voenizdat, 2015. – 234 p.
2. Petrov P. P. Ugrozy informacionnoj bezopasnosti v voennyh setyah // Kiberbezopasnost'. – 2021. – No. 3. Pp. 45–52.
3. Sidorov S. S. Metody tehnichej razvedki v kiberprostranstve. SPb.: Nauka, 2019.
4. Kuznecov K. K. Analiz setevogo trafika dlya vskrytiya struktury upravleniya // Voprosy zashchity informacii. – 2022. – No. 1. – Pp. 33–40.
5. Sokolov A. V. Teoreticheskie osnovy skrytnosti informacionnyh sistem. M.: Goryachaya liniya–Telekom, 2018.
6. Smith J., Brown T. Graph-based analysis of network security // Computer Networks. – 2019. – Vol. 158. – P. 1–15.
7. Garcia M. Vulnerability assessment of IP-based military networks // Military Communications Conference. – 2022. – Pp. 1–6.
8. Chen L. Rapid source detection in adversarial network environments // IEEE Transactions on Information Forensics and Security. – 2020. – Vol. 15. – Pp. 2345–2356.
9. Korneev G. A. Teoriya grafov v zadachah raspoznavaniya struktur. M.: Fizmatlit, 2017.
10. SpiderNet: Enabling Bot Identification in Network Topology Obfuscation Against Link Flooding Attacks // IEEE/ACM Transactions on Networking. – 2025. – Vol. 33. – No. 1. – Pp. 99–113.
11. WADCS: Weibull-attentive deep learning model for enhanced cyber security // Journal of King Saud University – Computer and Information Sciences. – 2025. – Vol. 37. – No. 1.
12. Stallings W. Cryptography and Network Security: Principles and Practice. 8th ed. New York: Pearson, 2020. – 832 p.

