УДК 004.056

Бугаенко Оксана Дмитриевна доцент кафедры информационных технологий, Северный (Арктический) федеральный университет

Карпов Александр Витальевич студент

4 курс, Северный (Арктический) федеральный университет

Россия, г. Архангельск

МЕТОДЫ ВЫЯВЛЕНИЯ СКРЫТЫХ КАНАЛОВ СВЯЗИ (DNS, ICMP, HTTP) В КОРПОРАТИВНЫХ СЕТЯХ: ОБЗОР И ЭВРИСТИЧЕСКИЕ ПОДХОДЫ

Аннотация: *в статье рассматриваются эвристические методы выявления скрытых каналов связи, реализованных средствами туннелирования в протоколах DNS, ICMP и HTTP, применительно к задачам мониторинга безопасности корпоративных сетей. Для DNS-туннелей анализируются признаки длины доменного имени, энтропии символьной строки и частоты запросов в пределах скользящего временного окна. Для ICMP-туннелей – размер полезной нагрузки Echo-сообщений и её энтропия. Для скрытых каналов на базе HTTP рассматриваются методы анализа аномалий в заголовках запросов. Приведена сравнительная таблица эвристических признаков по трём протоколам. Показано, что ни один из признаков не является достаточным в отдельности, а практически применимое обнаружение требует многопризнакового подхода с адаптацией порогов к профилю нормального трафика.*

Ключевые слова: *скрытые каналы связи, DNS-туннелирование, ICMP-туннелирование, скрытые каналы на базе HTTP, энтропия Шеннона, эвристический анализ, корпоративная сеть, обнаружение вторжений.*

Annotation: *the paper examines heuristic methods for detecting covert communication channels implemented through tunneling in the DNS, ICMP, and HTTP protocols, in the context of corporate network security monitoring. For DNS*

tunnels, the features of domain name length, character string entropy, and request frequency within a sliding time window are analysed. For ICMP tunnels – Echo message payload size and its entropy. For HTTP steganography, methods for detecting anomalies in request headers are considered. A comparative table of heuristic features across the three protocols is provided. It is shown that no single feature is sufficient on its own, and practically applicable detection requires a multi-feature approach with threshold adaptation to the normal traffic profile.

Key words: *covert channels, DNS tunneling, ICMP tunneling, HTTP steganography, Shannon entropy, heuristic analysis, corporate network, intrusion detection.*

Скрытые каналы связи – это механизмы передачи информации, использующие легитимный трафик как носитель, чтобы скрыть сам факт коммуникации [1]. В отличие от шифрования, защищающего содержимое, скрытые каналы скрывают существование обмена. Наиболее распространённые носители в корпоративных сетях – протоколы DNS, ICMP и HTTP: их трафик не блокируется на периметре, так как необходим для работы инфраструктуры [1]. Сигнатурный анализ против них малоэффективен, поэтому применяются эвристические методы, основанные на статистических признаках трафика. Целью работы является обзор таких признаков и методов обнаружения по трём указанным протоколам, а также анализ их ограничений.

DNS-туннелирование: признаки и методы обнаружения. DNS-туннелирование кодирует payload (Base32/Base64) в поддомен запроса, а ответ сервера несёт данные обратного канала [2]. DNS выбирается потому, что его трафик проходит периметр без строгой фильтрации и часто не журналируется полностью.

Ключевой признак – распределение символов в имени: легитимные имена близки к статистике естественного языка (закон Ципфа), а кодированный поддомен имеет более равномерное распределение и повышенную энтропию Шеннона [2]. Второй признак – длина: стандарт

ограничивает метку 63 октетами [4], поэтому имя длиннее типового (более 60 символов) аномально. Третий – частота уникальных запросов к домену второго уровня, выявляемая скользящим окном [3]. Надёжное обнаружение требует одновременного выполнения нескольких условий, так как каждый признак по отдельности даёт много ложных срабатываний на трафик CDN и облачных платформ.

ICMP-туннелирование: признаки и методы обнаружения. Протокол ICMP предоставляет поле данных произвольного размера в сообщениях Echo. В штатном применении команды

ping нагрузка минимальна (как правило, 32–56 байт) и статична. Туннель, напротив, заполняет поле данных кодированной полезной нагрузкой произвольного содержимого, что приводит к двум наблюдаемым аномалиям: увеличению размера поля данных сверх типового значения и росту энтропии его содержимого [2]. Согласно RFC 792, сообщения Echo не определяют формат поля данных, что и используется при организации туннеля [2]. Эвристическое правило обнаружения объединяет три условия: тип сообщения Echo (тип 0 или 8), размер нагрузки выше порогового значения и средняя энтропия за скользящее окно выше порога. Метод неприменим при шифровании нагрузки.

Скрытые каналы на базе HTTP: признаки и методы обнаружения. HTTP предоставляет механизмы сокрытия данных. Наиболее распространены: кодирование в заголовках (поля

User-Agent, X-Forwarded-For, нестандартные заголовки), манипуляция порядком заголовков, регистром и пробелами, а также использование поля тела запроса для передачи данных под видом легитимного контента [1]. Эвристические методы выявляют аномалии в структуре заголовков: отклонение полей от базового профиля (редкий

User-Agent, нетипичный набор заголовков), нестандартные или дублирующие поля, нетипичное соотношение размеров заголовков и тела. Ключевое ограничение: HTTP-трафик преимущественно шифруется TLS, что

делает анализ заголовков недоступным без TLS-инспекции. Без неё возможен только метаданный анализ: размер сессии, частота и ритм запросов, поле SNI.

Сравнительный анализ эвристических методов. В таблице 1 приведено сравнение эвристических признаков по трём протоколам с указанием применимости при шифровании трафика.

Таблица 1.

Сравнение эвристических методов обнаружения скрытых каналов

Протокол	**Основные признаки**	**Метод обнаружения**	**Работает при шифровании?**	**Сложность реализации**
DNS	Длина QNAME, энтропия имени, частота запросов, число уникальных поддоменов при одном домене второго уровня	Энтропийный анализ + скользящее временное окно [2; 3]	Да (DoH – частично)	Низкая
ICMP	Размер payload Echo-сообщений, энтропия содержимого, частота сообщений	Пороговый анализ + энтропия за скользящее окно [2]	Нет	Низкая
HTTP	Аномалии заголовков, нестандартные поля, User-Agent, порядок заголовков	Профилирование заголовков, сравнение с базовым профилем [1]	Нет (TLS без инспекции)	Средняя

Базовый профиль строится на исторических данных за 7–14 дней: для каждого поля заголовка рассчитываются допустимые значения и частота появления. Отклонение в виде нестандартного поля, необычного порядка заголовков или редкого User-Agent считается аномалией

Общие ограничения эвристических подходов. Главное ограничение всех методов – ложноположительные срабатывания на легитимный высокоэнтропийный трафик (CDN, облачные платформы, телеметрия), что требует адаптации порогов к профилю конкретной сети. Второе ограничение – доступность трафика: DNS over HTTPS [5] скрывает запросы внутри TLS, ICMP часто блокируется на периметре, а Скрытые каналы на базе HTTP без TLS-инспекции недоступны для анализа. Третье – компрометация агента: на скомпрометированном узле метрики могут быть подавлены или фальсифицированы.

Заключение. Анализ показывает, что эвристические методы обнаружения скрытых каналов в протоколах DNS, ICMP и HTTP обладают практической применимостью при условии многопризнакового подхода и адаптации порогов к профилю нормального трафика конкретной сети. DNS-туннелирование наиболее полно поддаётся статистическому обнаружению: комбинация энтропии, длины и частоты в скользящем окне обеспечивает уверенное обнаружение при линейной вычислительной сложности. ICMP-туннели выявляются по размеру и энтропии нагрузки, однако уязвимы к шифрованию. Скрытые каналы на базе HTTP в современных условиях требуют либо TLS-инспекции, либо ограничиваются метаданным анализом. Ни один метод не является достаточным без адаптации к фактическому профилю трафика, а полноценная защита требует их совместного применения в рамках единой подсистемы мониторинга.

Использованные источники:

1. Zander, S. A Survey of Covert Channels and Countermeasures in Computer Network Protocols / S. Zander, G. Armitage, P. Branch // IEEE Communications Surveys & Tutorials. – 2007. – Vol. 9, № 3. – P. 44–57. – DOI: 10.1109/COMST.2007.4317620.

2. Born, K. Detecting DNS Tunnels Using Character Frequency Analysis / K. Born, D. Gustafson. – 2010. – arXiv:1004.4358 [cs.CR]. – URL: https://arxiv.org/abs/1004.4358 (дата обращения: 23.05.2026).

3. Ma, X. A DNS Tunnel Sliding Window Differential Detection Method Based on Normal Distribution Reasonable Range Filtering / X. Ma, S. Guo, Z. Pan, B. Liu, K. Jiang, M. Chen, S. Tang. – 2022. – arXiv:2207.06641 [cs.CR]. – URL: https://arxiv.org/abs/2207.06641 (дата обращения: 23.05.2026).

4. Mockapetris, P. Domain Names – Implementation and Specification : RFC 1035. – IETF, 1987. – DOI: 10.17487/RFC1035.

5. Hoffman, P. DNS Queries over HTTPS (DoH) : RFC 8484 / P. Hoffman, P. McManus. – IETF, 2018. – DOI: 10.17487/RFC8484.