УДК 003.26;004.056

А.Н. Николайчук
Белорусский государственный технологический университет
Минск, Беларусь

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ СЕТЕВОЙ СТЕГАНОГРАФИИ

Аннотация. *Представлен комплексный анализ современных методов сетевой стеганографии, основанных на использовании легитимных сетевых протоколов для скрытой передачи данных. Большинство методов демонстрируют линейную зависимость времени выполнения внедрения от объема передаваемых данных.*

A.N. Nikolaichuk
Belarusian State Technological University
Minsk, Belarus

COMPARATIVE ANALYSIS OF NETWORK STEGANOGRAPHY METHODS

Abstract. *A comprehensive analysis of modern network steganography methods based on the use of legitimate network protocols for covert data transmission is presented. Most methods demonstrate a linear dependence of the implementation time on the volume of transmitted data.*

Сетевая стеганография представляет собой активно развивающуюся область информационной безопасности, которая фокусируется на скрытой передаче данных через легитимные сетевые протоколы. В условиях усиления контроля сетевого трафика, методы скрытой передачи информации приобретают особую актуальность как для защиты конфиденциальных данных, так и для проведения пентестов и анализа уязвимостей.

Среди многообразия подходов к организации скрытой коммуникации особого внимания заслуживают методы, использующие служебные поля сетевых протоколов. Одним из классических примеров такого подхода является метод скрытия данных в поле IP Identification, основанный на использовании 16-битного поля заголовка IP-пакета, изначально предназначенного для управления фрагментацией данных. Суть данного метода заключается в том, что каждый байт передаваемого сообщения кодируется в значении идентификатора отдельного IP-пакета, что обеспечивает прозрачную передачу информации через стандартные сетевые инфраструктуры [1, 2].

Поле Sequence Number в TCP заголовке, критически важное для обеспечения надежной передачи данных и предотвращения проблем повторной сборки пакетов, также может быть использовано для внедрения секретных данных. Метод работает путем кодирования информационных байтов в младшие биты Sequence Number, сохраняя естественный вид процессов TCP Handshake и передачи данных [3].

Стеганографический метод скрытия данных в DNS-запросах использует иерархическую структуру доменных имен для создания скрытых каналов связи. Преобразует каждый байт секретного сообщения в шестнадцатеричное представление и внедряет его в DNS-запросы. Данный подход может быть выявлен через анализ частоты DNS запросов и паттернов имен несуществующих доменов [4].

Метод скрытой передачи данных через ICMP пакеты использует характеристики протокола ICMP, обычно применяемого для сетевой диагностики и отчетов об ошибках. Создание скрытых каналов может быть выполнено путем внедрения информации либо в секцию данных ICMP Echo-запросов, либо в поле идентификатора [5].

Стеганография на основе временных характеристик сетевого трафика представляет собой сложный подход, который кодирует информацию во временных интервалах между последовательными сетевыми пакетами. В отличие от методов, основанных на внедрении в содержимое, временные каналы не оставляют следов в заголовках или данных пакетов. Бинарная информация может быть закодирована через вариации в задержках между пакетами, где разные временные интервалы представляют логические значения. Практическая реализация данного метода может быть затруднена потерей пакетов и необходимостью точной синхронизации времени между сообщающимися сторонами [1, 2].

Метод внедрения информации, основанный на манипуляции размером передаваемых сетевых пакетов, использует длину пакета в качестве средства организации скрытого канала связи. Фундаментальный принцип данного подхода заключается в установлении соответствия между предопределенными диапазонами размеров пакетов и специфическими значениями передаваемых данных, где вариация объема передаваемой информации служит механизмом кодирования битовых последовательностей [4].

Для оценки практической эффективности и ресурсной затратности рассмотренных методов был проведен эксперимент по передаче сообщений длиной от 25 до 100 байт. Измерялись время выполнения операции и количество сгенерированных сетевых пакетов.

Результаты эксперимента, демонстрирующие значительный разброс в производительности методов, представлены в таблице 1.

Таблица 1 – Сравнительные характеристики методов стеганографии

Метод	Длина сообщения, байт			
	25	50	75	100
	Время выполнения, с (Количество пакетов)			
IP ID	0,015 (25)	0,026 (50)	0,038 (75)	0,049 (100)
TCP Sequence	0,027 (25)	0,048 (50)	0,067 (75)	0,086 (100)
ICMP ID	0,040 (25)	0,069 (50)	0,096 (75)	0,126 (100)
ICMP Data	0,004 (1)	0,006 (2)	0,008 (3)	0,009 (4)
DNS Query	0,044 (25)	0,081 (50)	0,116 (75)	0,153 (100)
DNS TXT	0,003 (1)	0,004 (1)	0,005 (2)	0,006 (2)
Packet Sizing	0,426 (200)	0,816 (400)	1,302 (600)	1,642 (800)
Timing Channel	30,402 (200)	62,811 (400)	94,482 (600)	125,041 (800)

Большинство методов демонстрируют линейную зависимость времени выполнения от объема данных, передавая ровно 1 байт на пакет. Это предсказуемое поведение упрощает планирование операций, но создает значительный сетевой трафик при передаче больших сообщений.

Проведенное исследование методов сетевой стеганографии демонстрирует принципиальную возможность организации скрытых каналов связи путем использования служебных полей сетевых протоколов и характеристик трафика. Выбор конкретного метода стеганографии должен основываться на требованиях к скорости передачи, объему данных, уровню скрытности и особенностям сетевой инфраструктуры. Однако практическая реализация этих методов сталкивается с существенными ограничениями, обусловленными как архитектурными особенностями современных сетей, так и развитием систем обнаружения аномальной активности.

Список использованных источников

1. Николайчук А.Н., Урбанович П.П. Использование полей заголовка протокола IP для создания скрытого канала передачи данных / А.Н. Николайчук, П.П. Урбанович // Информационные технологии. Физика и математика [Электронный ресурс] : материалы 89-й научно-технической конференции профессорско-преподавательского состава, научных сотрудников и аспирантов (с международным участием), Минск, 3 – 18 февраля 2025 г. / Белорусский государственный технологический университет. – Минск : БГТУ, 2025. – С. 43–46.

2. Николайчук А.Н. Особенности стеганографических методов сокрытия информации в сетевом трафике / А.Н. Николайчук // II Международный форум по беспилотным аппаратам, 30 сентября – 2 октября 2025 г. – Минск: БГТУ, 2025. – С. 156–160.

3. Белкина, Т. А. Аналитический обзор применения сетевой стеганографии для решения задач информационной безопасности / Т.А. Белкина. – Молодой ученый, 2018. – № 11 (197) – С. 36-44.

4. Zander S. A survey of covert channels and countermeasures in computer network protocols / S. Zander, G. Armitage, P. Branch – IEEE Commun. Surv. Tutorials, 2007 – № 3, С. 44–57.

5. Галушка В.В. Сетевая стеганография на основе ICMP-инкапсуляции / С.Б. Петренкова, Я.В. Дзюба, В.А. Панченко – Инженерный вестник Дона, 2018. – № 4 (51) – 107 с.

УДК 004.8:008:34.096

Д.О. Новиков
Красноярск, Россия

ПРИНЦИПЫ, КАК ИНСТРУМЕНТ СНИЖЕНИЯ РИСКОВ ПРИ РАЗРАБОТКЕ И ИСПОЛЬЗОВАНИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: ЭТАПЫ ФОРМИРОВАНИЯ И РЕГЛАМЕНТАЦИИ

Аннотация. *Технологическое развитие, внедрение искусственного интеллекта в различные сферы требует переосмысления подхода к механизмам снижения рисков и опасностей от их использования. Одним из инструментов минимизации рисков и управления ими являются принципы, которые формируют фундамент для безопасного развития искусственного интеллекта.*

D.O. Novikov
Krasnoyarsk, Russia

PRINCIPLES AS A TOOL FOR REDUCING RISKS IN THE DEVELOPMENT AND USE OF ARTIFICIAL INTELLIGENCE: STAGES OF FORMATION AND REGULATION

Abstract. *Technological development and the introduction of artificial intelligence in various fields require a rethinking of the approach to mechanisms for reducing risks and dangers associated with their use. One of the tools for minimizing risks and managing them is the principles that form the foundation for the safe development of artificial intelligence.*