**УДК 004.896**

# ПРИМЕНЕНИЕ АНСАМБЛЯ МОДЕЛЕЙ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ АНОМАЛИЙ В СЕТЕВОМ ТРАФИКЕ

**Перегородиев Д. Е.** (Университет ИТМО)
**Научный руководитель - кандидат технических наук, доцент Гусарова Н. Ф.**
(Университет ИТМО)

**Введение.** Современные киберугрозы требуют применения интеллектуальных методов анализа сетевого трафика. Традиционные подходы, основанные на сигнатурном анализе [1, 2], не справляются с новыми видами атак, такими как целевые APT-атаки или скрытый криптомайнинг. Зарубежные решения (Cisco Stealthwatch, Darktrace) активно используют машинное обучение (МО), однако их эффективность зависит от качества признаков и интерпретируемости модели. Отечественные разработки (Kaspersky, Solar) делают упор на гибридные методы, но недостаточно адаптированы для сетей с особыми требованиями к безопасности, например, военных. Научная проблема заключается в создании адаптивной системы, сочетающей высокую точность обнаружения аномалий с возможностью анализа в условиях ограниченных вычислительных ресурсов.

**Основная часть.** Предложено решение на базе ансамбля моделей Isolation Forest и Random Forest, анализирующее ключевые признаки сетевого трафика: размер пакетов, энтропию полезной нагрузки, частоту использования портов и временные интервалы. Особенность метода — автоматическая генерация признаков, включая скользящее среднее временных задержек и последовательности мелких пакетов, что повышает чувствительность к DDoS и сканированию портов. Кросс-валидация (точность 98.1%) и SHAP-анализ обеспечивают интерпретируемость, а кластеризация DBSCAN выявляет группы аномалий (например, кластер с пакетами 1506 байт и нулевой энтропией, характерный для скрытого туннелирования). Решение адаптировано для специальных сетей, имеющих высокие требования к безопасности — реализована проверка принадлежности IP-адресов к служебным подсетям, что позволило идентифицировать внешние подключения.

**Выводы.** Система успешно апробирована на реальном трафике объемом 10000 пакетов с обнаружением 49 аномалий, включая подозрительную активность на порту 61287. Практическое применение: интеграция в СОВ (Системы обнаружения вторжений) для сетей с автоматическим блокированием внешних IP и формированием отчетов. Внедрение снизит нагрузку на администраторов узлов связи за счет фильтрации ложных срабатываний. Перспективы: адаптация под IPv6 и обработка зашифрованного трафика.

**Список использованных источников:**

1. Dale J. et al. Advanced neural analysis for ransomware detection through dynamic network signature mapping. – 2024.
2. Loaiza C. et al. Dynamic temporal signature analysis for ransomware detection using sequential entropy monitoring // Authorea Preprints. – 2024.