ИНТЕГРИРОВАННЫЕ МЕТОДЫ ОБНАРУЖЕНИЯ АНОМАЛИЙ В КОРПОРАТИВНЫХ СЕТЯХ: СОВРЕМЕННЫЕ СТРАТЕГИИ БЕЗОПАСНОСТИ

Kurbanov Sardor Nuriddinovich

LLC "Programmsoft", Republic of Uzbekistan, Tashkent

Аннотация:

Исследование, представленное в данном документе, посвящено актуальной теме разработки инновационных методов обнаружения аномалий в сетевом трафике корпоративных инфраструктур. В условиях постоянного эволюционирования угроз в области кибербезопасности, эффективное обнаружение аномалий в корпоративных сетях становится стратегически важным компонентом обеспечения безопасности информационных ресурсов предприятий. Настоящее исследование фокусируется на анализе современных подходов и методов, охватывая широкий спектр технологий, таких как машинное обучение, статистический анализ, глубокое обучение, а также инновационные техники анализа поведения пользователей и применение генеративных моделей.

Ключевые слова: Обнаружение аномалий, сетевая безопасность, машинное обучение, статистический анализ, глубокое обучение, анализ поведения пользователей, генеративные модели, корпоративные сети.

Целью исследований является: Основной задачей исследования является разработка интегрированных методов обнаружения аномалий в корпоративных сетях, учитывающих разнообразие современных угроз и возможностей технологий.

В задачи исследования входило: - Изучение методов анализа поведения пользователей и их применение для выявления необычных сетевых активностей.

- Разработка и анализ алгоритмов машинного обучения, включая классификацию, кластеризацию и ансамблевые методы, для эффективного обнаружения нормального и аномального трафика.
- Применение глубокого обучения, включая рекуррентные и сверточные нейронные сети, с целью выявления сложных и скрытых аномалий в динамике сетей.
- Анализ применения генеративных моделей для более точного моделирования нормального сетевого поведения.

Объектом исследования выбраны: Объектом исследования являются корпоративные сети, их топологии, трафик и сетевые протоколы, с акцентом на выявление аномалий в современной информационной среде.

Проанализированы: В рамках исследования проанализированы разнообразные подходы к обнаружению аномалий, с учетом их применимости в корпоративных сценариях. Рассмотрены успешные кейсы использования современных технологий в сетевой безопасности.

Дополнительным аспектом исследования является оценка возможности интеграции разработанных методов в существующие системы безопасности, обеспечивая удобство внедрения и минимизацию воздействия на текущую инфраструктуру предприятий.

Ожидается, что результаты данного исследования окажут важное влияние на развитие эффективных систем безопасности корпоративных сетей в условиях постоянно меняющейся киберугрозы.

В заключение подчеркивается, что разработка интегрированных методов обнаружения аномалий, объединяющих различные технологии, представляет собой ключевой элемент современных стратегий обеспечения безопасности корпоративных сетей, обеспечивая надежное реагирование на изменяющиеся угрозы и минимизацию потенциальных рисков.