ИННОВАЦИОННЫЕ ПОДХОДЫ К ОБНАРУЖЕНИЮ АНОМАЛИЙ В КОРПОРАТИВНЫХ СЕТЯХ: МОДЕЛИРОВАНИЕ И АНАЛИЗ ТРАФИКА

Kurbanov Sardor Nuriddinovich

LLC "Programmsoft", Republic of Uzbekistan, Tashkent

Аннотация:

Научное исследование посвящено разработке эффективных моделей и алгоритмов обнаружения аномального сетевого трафика в корпоративных сетях. Исследование охватывает различные методы, включая машинное обучение, статистический анализ и глубокое обучение. Работа направлена на повышение уровня безопасности информационных систем предприятий и оперативное выявление потенциальных угроз.

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

В свете постоянно развивающихся угроз в области кибербезопасности, эффективное обнаружение аномального трафика в корпоративных сетях становится критически важным элементом обеспечения безопасности информационных ресурсов предприятий. Данное исследование фокусируется на рассмотрении различных подходов и методов, используемых для создания моделей и алгоритмов, способных автоматически выявлять необычные сетевые активности.

В контексте машинного обучения, исследуется применение алгоритмов классификации, кластеризации, и ансамблевых методов для выделения нормального и аномального трафика. Рассматриваются техники статистического анализа, включая методы временных рядов и распределенной статистики, для выявления изменений в сетевых паттернах.

Особое внимание уделяется глубокому обучению и нейронным сетям, которые могут эффективно адаптироваться к динамике современных сетей и выявлять сложные, скрытые аномалии. Рассматриваются примеры успешного

применения технологий глубокого обучения в сетевой безопасности, включая рекуррентные и сверточные нейронные сети.

Основной целью исследования является разработка и анализ эффективных моделей и алгоритмов, способных обнаруживать аномалии в сетевом трафике корпоративных сетей. Исследование направлено на повышение уровня кибербезопасности и оперативное реагирование на потенциальные угрозы в корпоративной среде.

В задачи исследования входило:

- Разработка и анализ алгоритмов машинного обучения для классификации сетевого трафика.
- Применение статистических методов для выявления временных и структурных аномалий в сетевых данных.
- Исследование применения глубокого обучения, включая рекуррентные и сверточные нейронные сети, в задаче обнаружения аномалий.
- Оценка эффективности разработанных моделей на реальных корпоративных сценариях.

Объектом исследования являются корпоративные сети, включая их структуру, трафик и сетевые протоколы. Анализируются различные типы активности в сети с целью выявления аномалий.

В рамках исследования проанализированы различные методы машинного обучения, статистического анализа и глубокого обучения, а также их применение к задачам обнаружения аномалий в корпоративных сетях. Рассмотрены примеры успешного применения этих методов на практике.

В заключении подчеркивается, что разработка и применение подобных моделей и алгоритмов представляют собой неотъемлемый элемент комплексных стратегий обеспечения безопасности корпоративных сетей, способствуя раннему обнаружению потенциальных угроз и сокращению времени реакции на инциденты.