

УДК 004.056

Практические варианты использования машинного обучения для обеспечения безопасности информационных систем

Дронова Виктория Сергеевна dronova.vica7@gmail.com

Мазин Анатолий Викторович mazin@bmstu.ru

КФ МГТУ им. Н.Э. Баумана, Калуга, Россия

Информационная безопасность становится критически важной из-за увеличения количества кибератак и сложности методов взлома. Традиционные, основанные на статических правилах, методы часто неэффективны против современных угроз, которые требуют динамических решений. Рассмотрено применение методов машинного обучения для анализа и прогнозирования отклоняющегося от нормы состояния системы. Сделаны выводы, что машинное обучение способно выявлять шаблоны и аномалии, а также представляет собой перспективную технологию для защиты данных и инфраструктуры, предлагая ключевые подходы к обнаружению угроз.

Ключевые слова: информационная безопасность, машинное обучение, выявление аномалий, ARMA, ARIMA

Машинное обучение в области информационной безопасности разделяется на две ключевые задачи: распознавание образов и обнаружение аномалий.

Задача обнаружения аномалий фокусируется на выявлении отклонений от установленных норм. Этот метод применяется для выявления атипичного поведения, которое может указывать на потенциальные угрозы, такие как подозрительная активность в сети. Для решения таких задач используются данные, представляющие собой образцы регулярных действий, с которыми затем сравниваются новые данные. Отклонения, выявленные в процессе анализа, могут служить индикаторами вредоносной активности или нарушений безопасности [1].

Модели временных рядов, такие как ARMA и ARIMA, часто применяются для прогнозирования и обнаружения аномалий в данных, и позволяют выявлять нештатные ситуации, такие как резкое увеличение нагрузки на процессор. Модель ARMA включает три ключевых параметра: порядок авторегрессии (AR), порядок разности для обеспечения стационарности ряда и порядок скользящего среднего (MA). Эти параметры позволяют анализировать зависимости между значениями ряда и предсказывать его будущие значения. Отклонения прогноза от реальных данных могут указывать на аномалии, что позволяет своевременно реагировать на потенциальные угрозы. Если ряд нестационарен, используется модель ARIMA, которая дополнительно включает порядок дифференцирования, преобразующий данные в стационарные для лучшего прогнозирования [2].

Алгоритм машинного обучения работает следующим образом: он принимает на вход тренировочный набор данных и на основе этого набора выдает модель. Модель — это алгоритм, который, принимая новые данные в том же формате, что и обучающие данные, выдает прогноз или решение.

В данном исследовании использовалась модель ARIMA для анализа загрузки процессора, где была обнаружена повторяющаяся структура с пиками каждые 2,5 часа. Модель ARIMA с параметрами $AR = 11$, $MA = 11$ и $d = 0$, а также ARIMAX с аналогичными параметрами применялись для прогнозирования и определения аномалий [3].

Для более точного прогноза было построено 100 последних точек наблюдений, а также доверительный интервал, указывающий вероятность использования процессора в разные моменты времени. В результате применения ARIMA модель выдала прогноз, максимально близкий к реальным данным (рис. 1). При обнаружении значительных отклонений от прогноза система может классифицировать их как аномалии и инициировать предупреждения [4].

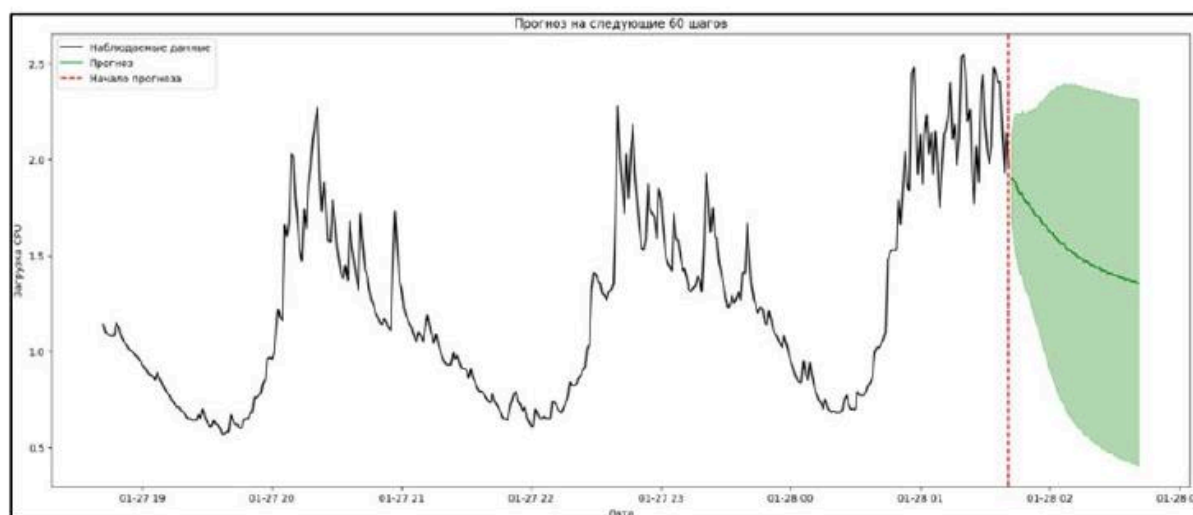


Рис. 1. Прогнозирование использования CPU в доверительном интервале для первого набора данных

Для выявления аномалий с помощью прогнозирования реальные данные сравниваются с периодически обновляемыми динамическими прогнозами. Система может предсказывать значения на 60 минут вперед каждые 30 минут, обучая новую модель ARIMA на данных, собранных за предыдущие 24 часа. В результате тестирования на первом наборе данных, ожидаемый диапазон соответствует реальному поведению процессора в заданном временном интервале, потому такой метод пошагового (инкрементального) обучения подходит практически для всех алгоритмов, так как он позволяет приблизить их к динамическому (потокковому) режиму работы несмотря на то, что изначально они разрабатывались для пакетной (статической) обработки данных.

При прогнозировании с использованием модели ARIMAX, тренированной на другом наборе данных, наблюдался другой итоговый прогноз (рис. 2).

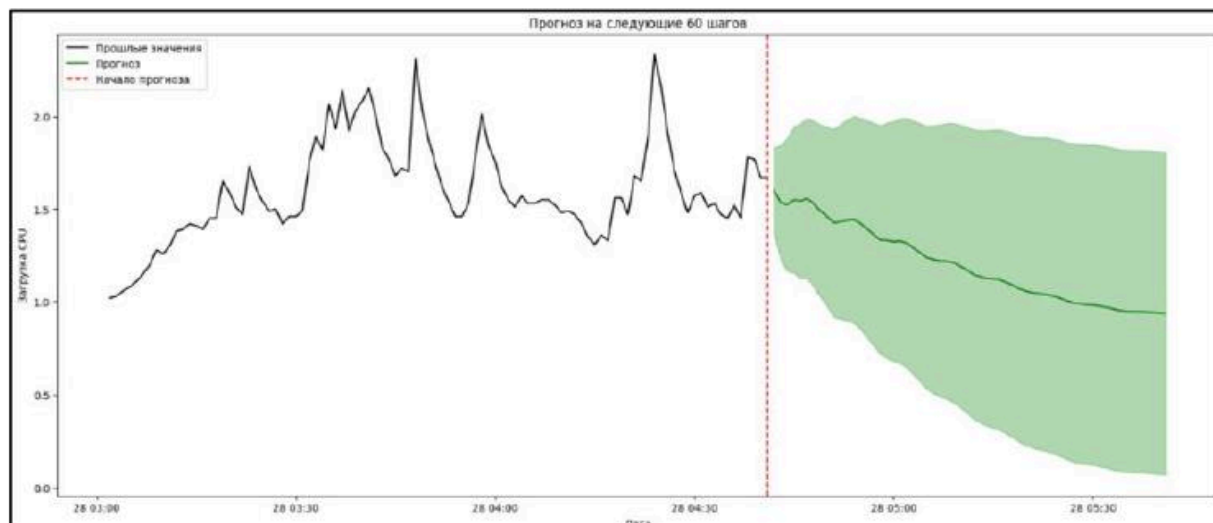


Рис. 2. Прогноз с помощью модели ARIMAX за пределами выборки для второго набора данных

При использовании модели ARIMAX, была обнаружена аномалия, которая возникает после фазы обучения модели. В исходном наборе данных на прогнозируемом участке наблюдался резкий спад, чего не учел доверительный интервал прогноза (рис. 2). Так как резкое падение наблюдаемых значений происходит в области низкой достоверности прогноза, система сгенерирует оповещение о наличии аномалии. Для этого должны быть заданы специальные пороговые условия, определяющие, насколько сильно прогнозируемые значения отличаются от фактических наблюдений, чтобы инициировать сигнал о возможной аномалии [5]. Таким образом, применение машинного обучения для обнаружения аномалий является перспективным направлением, позволяет увеличить качество мониторинга различных информационных систем и повысить их устойчивость к атакам. Такие методы можно применять для анализа состояния компонентов в DLP системах.

Литература

- [1] Лачихин А.В., Лачихина А.Б. Подходы к обучению в мультиагентных системах. *Вопросы радиоэлектроники*, 2016, № 2, с. 10–12.
- [2] Мэрфи К.П. *Вероятностное машинное обучение. Введение*. Москва, ДМК Пресс, 2022, 940 с.
- [3] Баланов А.Н. *Машинное обучение и искусственный интеллект*. Санкт-Петербург, Лань, 2024, 172 с.
- [4] Калинин М.О., Штеренберг С.И. Анализ информационной безопасности предприятия на основе мониторинга информационных ресурсов с использованием машинного обучения. *Интеллектуальные технологии на транспорте*. 2018, № 3 (15), с. 47–54.
- [5] Ангатов В.Д., Бобров А.В., Тимонин В.А., Вишняков А.С. Использование технологий машинного обучения в защите информационных систем. *Наука, техника и образование*, 2023, № 4 (92), с. 20–26.

Practical options for using machine learning to ensure the security of information systems

Dronova V.S. dronova.vica7@gmail.com

Mazin A.V. mazin@bmstu.ru

BMSTU (KB), Kaluga, Russia

Information security is becoming critically important due to the increase in cyber attacks and the complexity of hacking methods. Traditional methods based on static rules are often ineffective against modern threats that require dynamic solutions. Machine learning, capable of detecting patterns and anomalies, is a promising technology for protecting data and infrastructure, offering key approaches to threat detection.

Keywords: information security, machine learning, anomaly detection, ARMA, ARIMA