

Разработан цифровой инструмент для защиты от киберугроз на промышленных предприятиях

05.09.2025

Исследователи Санкт-Петербургского Федерального исследовательского центра РАН (СПб ФИЦ РАН) создали нейросетевой фреймворк (набор цифровых инструментов) для выявления киберугроз в системах Интернета вещей на индустриальных предприятиях.

Эксперименты на большом объеме данных промышленных систем продемонстрировали высокий уровень распознавания угроз на разных типах инфраструктуры — на 30% меньше ошибок по сравнению с существующими подобными разработками. Результаты исследования опубликованы в научном журнале [Engineering Applications of Artificial Intelligence](#).



Промышленный Интернет вещей (Industrial Internet of Things, IIoT) интегрирует «умные» технологии в промышленные процессы и включает в себя датчики, контроллеры, роботы и другие устройства, которые собирают данные в реальном времени и передают их оператору для обработки и принятия решений, а также прогнозирования возможных состояний систем. Это позволяет оптимизировать производство, снизить затраты, повысить качество продукции и прогнозировать возможные отказы оборудования и аварии.

В России внедрение IIoT также набирает обороты, особенно в отраслях нефтегазовой промышленности, энергетики, металлургии и машиностроения. Такие компании, как «Газпром нефть», «Российские железные дороги», СИБУР и Росатом активно используют промышленный Интернет вещей для мониторинга состояния оборудования, предиктивного обслуживания,

удалённого контроля и автоматического оповещения о неисправностях.

В то же время использование технологий IIoT связано с рядом рисков и угроз в цифровом пространстве: защищённость устройств может серьёзно пострадать в результате кибератак, утечек конфиденциальных данных и ошибок в программном обеспечении. В результате подобных действий со стороны злоумышленников промышленным предприятиям может быть нанесён существенный экономический ущерб.

«Для повышения эффективности выявления кибератак и снижения числа ошибок в мониторинговых индустриальных системах мы разработали фреймворк ForecaState с использованием алгоритмов искусственного интеллекта. Модели глубокого обучения нейросетей, которые мы используем, хорошо подходят для обработки больших объёмов данных, характерных для технологий IIoT. Их использование позволило на 30 процентов снизить вероятность ошибки при выявлении угроз по сравнению с существующими аналогами», — рассказывает научный сотрудник лаборатории проблем компьютерной безопасности СПб ФИЦ РАН **Диана Левшун**.

Учёные тестировали свою систему на двух больших открытых наборах данных, собранных с промышленных установок. Первый был получен с системы очистки воды и включала ежесекундные показания с датчиков. Второй набор данных включал комплексную информацию с сети электрических трансформаторов: энергонагрузка, температура масла и прочее — эти данные фиксировались каждые 15—60 минут. Различный тайминг собранной информации позволил проводить как краткосрочное, так и долгосрочное моделирование.

Для экспериментов специально выбраны данные из двух различных промышленных областей, чтобы оценить универсальность предлагаемого решения. Кроме того, авторы сравнили производительность своего решения с рядом аналогов, использующих модели прогнозирования на основе искусственного интеллекта, и с методом наивного прогноза — когда предсказывается последнее зарегистрированное значение показателя.

«Эксперименты на данных различных типов промышленных систем показывают, что наш набор инструментов может быть использован для решения самых разных задач: прогнозирование аномальной работы производственных процессов, управление энергопотреблением в системах IIoT и многих других областях. Кроме того, в отличие от некоторых специализированных подобных решений наш фреймворк является модульным — то есть его функционал может быть легко расширен и адаптирован к многообразным производственным потребностям. Эта адаптивность критически важна в быстро меняющемся ландшафте IIoT», — отмечает старший научный сотрудник лаборатории проблем компьютерной безопасности СПб ФИЦ РАН **Дмитрий Левшун**.

Применение и интеграция ForecaState могут быть реализованы в системах прогностического обслуживания на производстве для раннего выявления отказов машин, улучшения балансировки нагрузки, предотвращения аварий и техногенных катастроф, а также в системах контроля качества на производственных линиях для сокращения отходов и обеспечения стандартов качества с участием СПб ФИЦ РАН.

Исследование проведено при поддержке Исследовательского центра сильного искусственного интеллекта в промышленности Университета ИТМО.

Источник: пресс-служба [СПб ФИЦ РАН](#).