**Будущее анализатора кода: разработчики интегрируют в SafeERP машинное обучение**

В начале 2025 года, когда каждый день появляются новые приложения и миллионы строк кода, [зарубежные аналитики](https://gbhackers.com/the-growing-role-of-ai-powered-sast-in-the-developer-toolkit/) обратили внимание на быстрые и безопасные методы разработки. На сцену выходит статическое тестирование безопасности приложений (SAST), которое играет важную роль в выявлении уязвимости в исходном коде приложения до его запуска. Однако традиционные SAST-системы страдают от ложнопозитивных срабатываний, снижающих эффективность и отнимающих время разработчиков. Исследователи подчёркивают растущую роль искусственного интеллекта (ИИ) в улучшении точности SAST, что позволит разработчикам сосредоточиться на реальных угрозах безопасности.

Именно поэтому «Газинформсервис» уже сейчас работает над внедрением машинного обучения (ML-кода) для SafeERP, многофункционального комплекса защиты бизнес-приложений (1С и SAP), чтобы повысить точность SAST и обеспечить безопасность ERP-систем без лишних проверок.

Эксперт компании «Газинформсервис», специалист по внедрению SafeERP **Роман Шарапов,** отмечает: *«Ложные срабатывания в SAST-анализаторах случаются по разным причинам. Например, анализаторы могут не понимать контекст, в котором используется код, или работать только по жёстким правилам, которые не учитывают уникальность проекта. Также часто проблемы возникают из-за устаревших баз правил или особенностей библиотек, которые инструмент не распознаёт. Всё это приводит к тому, что безопасный код помечается как уязвимый».*

При такого рода «багах» тратится много времени на проверку не уязвимого кода. Исправление ложнопозитивных уязвимостей может привести к реальным уязвимостям при недостаточной компетенции разработчиков. Большое количество ложнопозитивных срабатываний снижает доверие к инструменту, а также может привести к тому, что важные уязвимости просто пропустят. Как результат — дополнительные риски и затраты для команды.

Эксперт отмечает: внедрение ИИ в статический анализатор кода SafeERP — это большой шаг в развитии статического анализа кода. Это позволит ИИ устранить ложнопозитивные срабатывания в SAST-анализаторах за счёт следующих возможностей:

**Учёт контекста кода**: ИИ анализирует, как конкретный участок кода взаимодействует с другими элементами проекта, и исключает ситуации, где предполагаемая угроза не представляет реальной опасности.

**Адаптация к проекту**: на основе данных конкретного проекта, ИИ обучается понимать особенности его структуры, используемых библиотек и стиля кодирования, снижая количество ошибочных предупреждений.

**Исторический анализ**: ИИ обрабатывает данные о предыдущих ложнопозитивных срабатываниях и использует эту информацию для повышения точности дальнейших проверок.

**Семантический анализ**: технология позволяет ИИ глубже понимать смысл кода и контекст его использования, что помогает отличать реальные угрозы от ложных.

**Кластеризация предупреждений**: ИИ объединяет схожие уведомления в группы, выделяя ключевые проблемы и упрощая анализ для разработчиков.

**Справка о компании:**

[ООО «Газинформсервис»](https://www.gaz-is.ru/) — отечественный разработчик программных и программно-аппаратных средств обеспечения информационной безопасности и комплексной инженерно-технической охраны. Компания специализируется на создании систем обеспечения информационной безопасности объектов и ИБ-систем для корпораций энергетической и транспортной отраслей, органов государственной власти, промышленных предприятий, а также учреждений финансового сектора и телекоммуникационных компаний.