УДК 004.8

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ПРОЕКТИРОВАНИИ ПО: ОЖИДАНИЯ, РЕАЛЬНОСТЬ, ПЕРСПЕКТИВЫ

Стариковская Н.А., Кущ М.В.

МИРЭА - Российский технологический университет, 119454, Россия, г. Москва, проспект Вернадского, 78, e-mail: starikovskaya@mirea.ru, kucsh@mirea.ru

Проводится анализ особенностей применения технологии искусственного интеллекта в проектировании информационных систем. Рассматриваются возможные области применения ИИ в проектировании ПО. Приводится обзор технологии искусственного интеллекта и машинного обучения в DevSecOps-платформах класса ASOC. Рассмотрены вопросы импортозамещения и перспективы развития технологии искусственного интеллекта и ее дальнейшего применения проектировании ИС.

Ключевые слова: нейротехнологии, искусственный интеллект, машинное обучение, сквозные цифровые технологии, DevSecOps, ASOC.

ARTIFICIAL INTELLIGENCE IN SOFTWARE DESIGN: EXPECTATIONS, REALITY, PROSPECTS

Starikovskaya N.A., Kucsh M.V.

MIREA - Russian Technological University, 119454, Moscow, 78 Vernadskogo Avenue, Russia, e-mail: starikovskaya@mirea.ru, kucsh@mirea.ru

The analysis of the application of artificial intelligence technology in the design of information systems is carried out. Possible applications of AI in software design are considered. An overview of artificial intelligence and machine learning technology in DevSecOps platforms of the ASOC class is given. The issues of import substitution and prospects for the development of artificial intelligence technology and its further application in the design of information systems are considered.

Keywords: neurotechnologies, artificial intelligence, machine learning, end-to-end digital technologies, DevSecOps, ASOC.

Введение

Нейротехнологии и технологии искусственного интеллекта включены в перечень ключевых сквозных цифровых технологий в национальной программе «Цифровая экономика Российской Федерации», реализуемой в период 2019 – 2030 гг. Развитие технологии искусственного интеллекта в России осуществляется как один из девяти федеральных проектов указанной программы.

Напомним, что сквозные цифровые технологии – это передовые научно-технические отрасли, обеспечивающие создание высокотехнологичных продуктов и сервисов и наиболее сильно влияющие на развитие экономики, радикально меняя ситуацию на существующих рынках и(или) способствуя формированию новых рынков [0]. Иными словами, речь идет о технологиях, которые имеют высокое значение и широкие возможности повсеместного применения в различных областях и способны кардинально изменить любую сферу, в которой будут внедрены. 24 ноября 2022 года на международной конференции "Путешествие в мир искусственного интеллекта" президент России Владимир Путин поставил задачу обеспечить массовое внедрение ИИ в различные сферы жизнедеятельности в предстоящие десять лет.

Технологии искусственного интеллекта и машинного обучения уже около пяти лет применяются компаниями и отделами по разработке ПО по всему миру. В 2020 году Gartner впервые включил это понятие в список самых перспективных технологий будущего – Hype Cycle for Emerging Technologies (цикл зрелости технологий).

Разработка программного обеспечения с помощью ИИ, AI-augmented Software Engineering – термин, который ввели в Gartner в 2020 году для описания процесса использования технологий искусственного интеллекта (например, машинного обучения, обработки естественного языка и др.) для ускорения циклов разработки приложений и DevOps. Ряд вендоров уже выпустил продукты для такого типа работ. Среди них Codota, Deep Code, Google, Kite, Mendix, Microsoft, OutSystems, Parasoft [2].

В России лидером в области искусственного интеллекта является ПАО Сбербанк, который запустил специальный проект Sber AI направленный на привлечение лучших идеи в этой области и их реализацию.

В данной статье будут рассмотрены возможности и перспективы применения технологии искусственного интеллекта в проектировании информационных систем.

Области применения искусственного интеллекта при разработке ПО

Применение искусственного перспективно возможно на каждом этапе проектирования ПО (рисунок 1).

Рисунок 1 – Области применения искусственного интеллекта при разработке ПО

Рассмотрим возможности применения ИИ на разных этапах проектирования [2]:

1. Сбор технических требований. Цифровые ассистенты анализируют документы с собранными требованиями, указывают на разногласия в тексте, нестыковки в цифрах, единицах измерений, суммах и предлагают возможные решения.
2. Быстрое прототипирование. Преобразование бизнес-требований в программный код обычно занимает месяцы или даже годы. Однако машинное обучение значительно сокращает этот процесс, позволяя специалистам с меньшим опытом использовать методы разработки естественного языка или визуального интерфейса для создания прототипа.
3. Кодирование. В процессе написания кода, работающая на базе ИИ система автозаполнения предлагает рекомендации для завершения строчек кода. Интеллектуальные помощники сокращают время на создание кода на 50%. Дополнительно они могут рекомендовать обратиться к связанным документам, лучшим практикам и дать примеры кода.
4. Анализ и обработка ошибок. Виртуальный ассистент может извлекать уроки из прошлого опыта, чтобы выявлять типичные ошибки и автоматически помечать их на этапе разработки. Машинное обучение можно использовать для анализа системных журналов для быстрого и даже упреждающего выявления ошибок.
5. Автоматический рефакторинг кода. Чистый код необходим для совместной работы и долгосрочного обслуживания. По мере развития компании, программные решения могут изменяться, и остро встает вопрос о том, как модифицировать код для лучшей работы приложений. Машинное обучение используется в этом случае с целью анализа кода и автоматической оптимизации кода для легкой интерпретируемости и повышения производительности.
6. Тестирование. Автоматизированные системы тестирования используют ИИ не только для того, чтобы запускать процесс тестирования, но и для создания test кейсов.
7. Ввод в эксплуатацию. Иногда ошибки в программном коде становятся явными только после того, как программное обеспечение введено в эксплуатацию. Но AI-инструменты предотвращают подобные ситуации, проверяя статистику предыдущих релизов и логи приложений.
8. Управление проектами. Разработка программного обеспечения иногда выходит за рамки бюджета и графика. Системы продвинутой аналитики позволяют использовать данные большого количества проектов по разработке ПО для прогнозирования технических задач, необходимых ресурсов и времени на выполнение проекта. Машинное обучение может извлекать данные из прошлых проектов, такие как истории пользователей, определения функций, оценки и фактические условия, для более точного прогнозирования рабочей нагрузки и бюджета.

Технологии искусственного интеллекта и машинного обучения в DevSecOps-платформах класса ASOC

DevSecOps — это следующий этап развития DevOps, который меняет традиционное представление о роли подразделения ИБ (информационной безопасности, Security) в обеспечении качества и надежности кода. Если раньше, к примеру, специалист ИБ подключался к тестированию ПО на безопасность только после завершения основных этапов разработки, перед выпуском релиза, то сейчас его присутствие необходимо на всех этапах [3].

Методология DevSecOps находится сегодня на пике популярности. По мнению аналитиков Gartner, в 2022 году технология достигла плато продуктивности, что говорит о высоких перспективах ее дальнейшей

кастомизации. Все чаще российские компании переходят на разработку собственного ПО. Разработка приложений силами собственных программистов позволяет им быстрее реагировать на запросы пользователей, меньше зависеть от внешних факторов и таким образом сохранять гибкость и конкурентоспособность в быстро меняющейся среде.

В то же время, разрабатывая софт как для клиентов, так и для внутренних задач автоматизации, компания должна гарантировать безопасность этих программных продуктов. В тысячах строк кода могут оставаться десятки уязвимостей, которые необходимо выявить и устранить. С ростом геополитической напряженности случился и всплеск кибератак на российские ресурсы, поэтому сейчас безопасность программного обеспечения — крайне актуальная задача. Поэтому концепция DevSecOps становится более актуальной и в России.

DevSecOps-платформы класса ASOC имеют множество функциональных преимуществ, но мы остановимся на возможности настройки интеллектуального управления.

В платформу класса ASOC можно добавить инструменты анализа собранных данных. Для этого необходимо создать дополнительный функциональный модуль для консолидации, хранения и анализа полученной информации (рисунок 2).

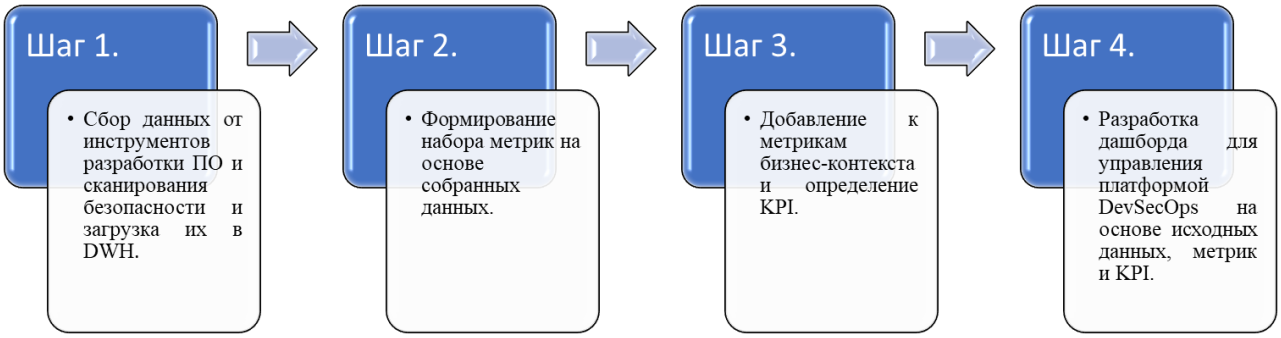

Рисунок 2 – Реализация функционального модуля для консолидации, хранения и анализа собранных данных

Чтобы настроить интеллектуальное управление платформой, нужно скорректировать шаги реализации функциональности дополнительного модуля для работы с данными. Первые три шага, указанные выше, остаются прежними, а на четвертом нужно обработать исходные данные, метрики и KPI с помощью технологий искусственного интеллекта и машинного обучения. После этого можно формировать дашборды для управления платформой DevSecOps на основе обработанных данных, метрик и KPI (рисунок 3) [4].

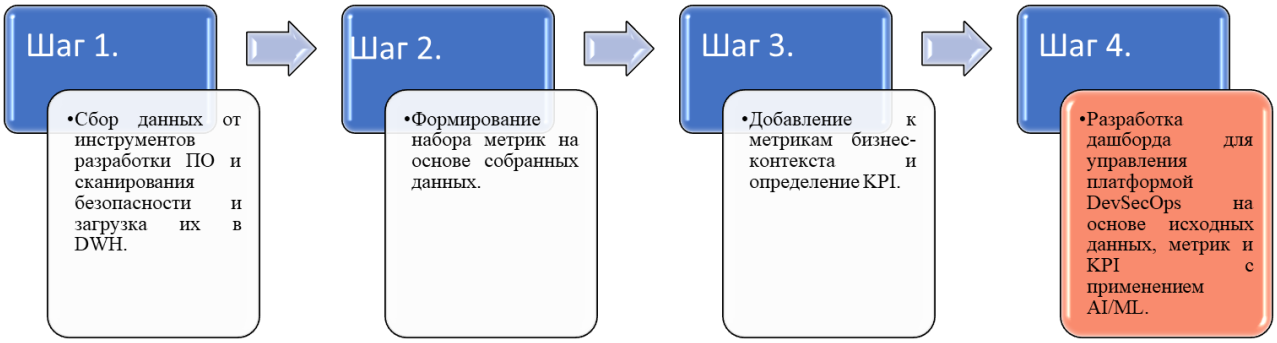

Рисунок 3 – Настройка интеллектуального управления платформой класса ASOC

С точки зрения практики ASOC технологии AI/ML могут улучшить работу оркестрации и корреляции (рисунок 4).

Рассмотрим практическую пользу от применения технологии AI/ML в методологии DevSecOps подробнее [4]:

1. Автоматическая проверка критериев качества ПО. AI в платформах класса ASOC может динамически формировать состав и критерии прохождения каждой точки контроля качества артефактов ПО. Для этого AI использует собранную информацию и данные метрик.

Сформированные искусственным интеллектом точки контроля качества ПО и их критерии позволят решать, готова ли сборка к выходу на следующий этап жизненного цикла ПО. С использованием технологий AI можно продвигать артефакты по DevSecOps-конвейеру в максимально автоматизированном режиме. Решения будут приниматься по итогам сканирования сборки в различных средах – это позволит быстро и непрерывно выпускать релизы.

Автоматизированные точки контроля качества могут включать проверку различных практик AST. Их конфигурация способна динамически изменяться – это зависит от стадии конвейера ИБ. Таким образом, можно

установить точки контроля в CI/CD-пайплайнах, настроить их критерии и управлять с помощью этого инструмента качеством ПО.

2. CI/CD-пайплайн как код. Для масштабной реализации DevSecOps подход к управлению CI/CD-пайплайнами как к коду дает очевидные преимущества. Компании, применяющие такую концепцию, получают механизм для улучшения процессов развертывания, запуска, управления и отслеживания статуса своего ПО. Современные решения класса ASOC позволяют строить конвейеры ИБ "из коробки" нажатием одной кнопки. С помощью технологий AI/ML можно автоматически обнаруживать компоненты ПО и создавать для них CI/CD-пайплайны с точно определенными критериями качества.

Рисунок 4 – Направления, подлежащие улучшению при использовании технологии AI/ML

AI может инвентаризировать артефакты ПО, в автоматическом режиме создавать сквозные конвейеры и заранее встраивать в них вызовы инструментов ИБ на основе контекста и ряда параметров разрабатываемого продукта. Технологии AI также способны динамически определять порядок и количество контрольных точек качества ПО в каждом конвейере CI/CD. Этот подход помогает ускорить выпуск продуктов, поскольку весь процесс, от первого коммита в ветке до выхода финального релиза, тщательно контролируется.

3. Технология AVC как часть процесса разработки ПО. Технологии AI/ML дают возможность построить механизм корреляции проблем безопасности AVC (Application Vulnerability Correlation) на основе данных, полученных из инструментов тестирования безопасности. Процесс корреляции включает в себя ML-модель, которая может автоматически отфильтровывать ложноположительные срабатывания, выявлять дубликаты и однотипные проблемы ИБ и группировать их в единый дефект ИБ.

Этот механизм значительно сокращает время, необходимое на устранение проблем безопасности. Таким образом, команда может сосредоточиться на крайне важных уязвимостях и нарастить скорость распознавания угроз в разрабатываемом ПО.

4. Автоматизированное руководство по устранению уязвимостей. Среди обнаруживаемых проблем всегда встречаются типовые уязвимости, в том числе критические, которые можно устранить несложными способами. Технология AVC находит и приоритизирует дефекты ИБ, а также автоматически предоставляет рекомендации по устранению проблем.

Платформы ASOC умеют собирать данные об уязвимостях из различных сканеров безопасности с помощью практик тестирования – SAST, SCA, DAST и т.д. Если внедрить технологии AVC и предоставить им подробные стандарты и детальные рекомендации по безопасному кодированию для каждого языка программирования, то это позволит технологиям формировать шаблоны защищенного кода, настроенные под особенности реализации DevSecOps в компании.

5. Управление соответствием требованиям ИБ. При разработке ПО одним из важных аспектов является соответствие индустриальным стандартам ИБ и требованиям регуляторов. Процесс управления требованиями можно полностью автоматизировать в рамках жизненного цикла продуктов – это значительно облегчит выполнение задач в компании.

Автоматические проверки на соответствие требованиям и стандартам должны гарантировать, что все критерии соблюдены и ПО можно выпускать в промышленную эксплуатацию. В рамках платформ класса ASOC технологи AI/ML позволяют организовать непрерывный мониторинг соответствия на основе статуса точек контроля качества ПО с возможностями предиктивного анализа. По итогам мониторинга команда будет получать заключение о соответствии разрабатываемого ПО необходимым требованиям.

Заключение

Таким образом, современные решения в области проектирования ИС, такие как платформы класса ASOC с применением технологий искусственного интеллекта и машинного обучения, позволяют значительно повысить эффективность всех процессов и сократить жизненный цикл разработки ПО.

Текущая ситуация, связанная с уходом мировых гигантов-поставщиков подобных решений и курс на импортозамещение заставил российские компании искать альтернативные варианты среди отечественных поставщиков или ориентироваться на продукты с открытым кодом. Последнее необходимо делать с большой осторожностью, так как можно наткнуться на «подводные камни» с точки зрения обеспечения безопасности. Среди российских аналогов можно выделить компанию Swordfish Security, которая занимается проблематикой построения процессов разработки защищенного ПО. В конце 2022 г. собственную ASOC-платформу безопасной разработки и управления процессами DevSecOps разработала компания «МТС». Дочерняя компания ПАО «Сбербанк» Sber AI анонсировала в 2021 году первое зарегистрированное в России ПО, написанное искусственным интеллектом. Нейросеть ruGPT-3, обученная специалистами Sber AI, самостоятельно написала компьютерную программу на C++ и Java. Очевидно, что в ближайшем будущем возможности применения искусственного интеллекта в проектировании информационных систем будут расширяться. В фазе инновационного тригера цикла Хайпа компании Гартнер сегодня находятся такие технологии как Machine learning Code generation и Generative Design. При благоприятном развитии событий эти технологии через 5-10 лет (по прогнозам аналитиков Гартнер) смогут предлагать готовый код программы графического интерфейса, контента и кода уровня презентации для цифровых продуктов, основываясь либо на описаниях на естественном языке, либо на частичных фрагментах кода.

Однако необходимо понимать, что сегодня человечество имеет дело со «слабым» искусственным интеллектом. Технологические возможности современного искусственного интеллекта позволяют выполнять либо одну простейшую задачу, либо функцию помощника. Поэтому разработчикам ПО не стоит опасаться, что в ближайшем будущем их полностью заменит нейросеть. Однако определённые изменения с точки зрения навыков и требований к подобного рода специалистам определенно стоит ожидать. Но эта общая тенденция касаемая сегодня, пожалуй, любой профессии.

Список литературы

1. Цифровой бизнес и сквозные цифровые технологии: теория и практика. Часть 1 [Электронный ресурс]: учебное пособие / Стариковская Н.А., Стариковский А.И., Кущ М.В. — М.: МИРЭА – Российский технологический университет, 2022. — 1 электрон. опт. диск (CD-ROM) Режим доступа: https://library.mirea.ru/share/54337/ (Дата обращения 08.01.2023).
2. Воронская С.Е. Как ИИ помогает писать софт. Обзор одной из самых перспективных технологий будущего // 24.09.2021.
3. TAdviser - [Электронный ресурс]. Режим доступа: https://clck.ru/XzFgvДмитрий Шилов. Что такое метод DevSecOps и почему бизнесу надо внедрять его в разработку //14.10.2022. РБК Тренды- [Электронный ресурс]. Режим доступа: https://trends.rbc.ru/trends/industry/634929a99a794746a42b114c (Дата обращения 09.01.2023).
4. Юрий Шабалин. Технологии искусственного интеллекта и машинного обучения в DevSecOps-платформах класса ASOC // Электронный журнал «Информационная безопасность», №5, 2022. Режим доступа: https://www.itsec.ru/articles/tekhnologii-iskusstvennogo-intellekta-i-mashinnogo-obucheniya-v-devsecops-platformah-klassa-asoc (Дата обращения 09.01.2023).

References

1. Digital business and end-to-end digital technologies: theory and practice. Part 1 [Electronic resource]: textbook / Starikovskaya N.A., Starikovsky A.I., Kushch M.V. — M.: MIREA – Russian Technological University, 2022. — 1 electron. opt. disk (CD-ROM) Access mode: https://library.mirea.ru/share/54337 / (Accessed 08.01.2023).
2. Voronskaya S.E. How AI helps to write software. Overview of one of the most promising technologies of the future // 24.09.2021. TAdviser - [Electronic resource]. Access mode: https://clck.ru/XzFgv 023).
3. Dmitry Shilov. What is the DevSecOps method and why business needs to implement it in development //14.10.2022. RBC Trends- [Electronic resource]. Access mode: https://trends.rbc.ru/trends/industry/634929a99a794746a42b114c (Accessed 09.01.2023).
4. Yuri Shabalin. Artificial intelligence and machine learning technologies in DevSecOps platforms of the ASOC class // Electronic journal "Information Security", No. 5, 2022. Access mode: https://www.itsec.ru/articles/tekhnologii-iskusstvennogo-intellekta-i-mashinnogo-obucheniya-v-devsecops-platformah-klassa-asoc (Accessed 09.01.2023).