Умная автоматизация в интересах кибербезопасности

Анжело Невес
Эксперт, 20192365@academia.uatlantica.pt

Вирджиния Араухо
Профессор, varaujo@uatlantica.pt

Кафедра информационных систем, Университет Атлантика (Department of Information Systems, Atlântica University Institut), 2730–208 Barcarena, Lisbon, Portugal

Аннотация

В экосистеме интеллектуальной автоматизации, или роботизации процессов, особое место занимают практика и подходы к созданию и эксплуатации систем обеспечения информационной защиты, необходимых любой организации. Большая безопасность расширяет возможности повышения качества и эффективности деятельности и прибыльности предприятия. Наиболее перспективными для организаций, пользующихся гибкими методами разработки программного обеспечения (ПО), в настоящее время представляются принципы и передовой опыт культуры «Разработка, Безопасность, Эксплуатация» (Development, Security, Operations — DevSecOps). В эпоху цифровизации софтверные компании все сильнее нуждаются в методах комплексного использования различных навыков и компетенций — от анализа и внедрения до дальнейшего совершенствования программных продуктов. Информационная безопасность выступает важнейшим аспектом всего жизненного цикла продукта, обеспечивающим такие фундаментальные характеристики, как конфиденциальность, надежность и доступность систем роботизированной автоматизации, от которых зависят репутация и бизнес компании.

Не забывая о потребностях клиентов, создание ПО требует внедрения более гибких методов, которые позволяют разработчикам обеспечить пользовательскую ценность при моделировании ПО на протяжении всего жизненного цикла продуктов, а также соответствие требований, планов и результатов интересам клиентов. В статье представлены подходы к постоянному совершенствованию интеллектуальных платформ автоматизации в крупных международных организациях. Кроме того, рассмотрены барьеры для применения методологии DevSecOps при создании программной оболочки для систем роботизированной автоматизации.

Ключевые слова: роботизированная автоматизация процессов; управление бизнес-процессами; DevSecOps; интеллектуальная автоматизация; кибербезопасность

Цитирование: Neves A., Araújo V. (2023) Smart Automation for Enhancing Cyber-Security. *Foresight and STI Governance*, 17(1), 89–97. DOI: 10.17323/2500-2597.2023.1.89.97

Smart Automation for Enhancing Cyber-Security

Ângelo Neves
Expert, 20192365@academia.uatlantica.pt

Virgínia Araújo
Professor, varaujo@uatlantica.pt

Department of Information Systems, Atlântica University Institut, 2730-208 Barcarena, Lisbon, Portugal

Abstract

In an intelligent automation ecosystem, namely in the context of Robotic Process Automation, there is a need to review the development and operation processes and practices, to combine competences from these two areas with the common good necessary for any organization or security team. It is with security that quality, efficiency, and profitability become possible. The elaboration of guidelines and best practices for the application of a DevSecOps culture is currently essential for Agile software development at any organization. In the digitalization era, teams increasingly need a collaborative method to involve several competencies and capabilities, from analysis to implementation and the evolution of a software product. Information security needs to be an integral part throughout the entire product's lifecycle, as without it, fundamental aspects of confidentiality, integrity, and availability put information and software security at serious risk in the course of business operations.

Without losing focus on customer needs, it is necessary to model software development practices, following more agile methodologies. In this way, teams can model the software throughout its lifecycle, focusing on facilitating the delivery of value to the customer and having greater certainty that requirements, plans, and results are 100% aligned with customer needs. This paper presents an analysis and proposal for the continuous improvement of an intelligent automation platform at a large-scale multinational organization. In parallel, aspects that generate resistance to the implementation of a DevSecOps methodology within the scope of RPA code development is considered.

Keywords: robotic process automation (RPA); business process management; DevSecOps; intelligent automation

Citation: Neves A., Araújo V. (2023) Smart Automation for Enhancing Cyber-Security. *Foresight and STI Governance*, 17(1), 89–97. DOI: 10.17323/2500-2597.2023.1.89.97

Для эффективной реализации бизнес-процессов любой организации приходится выполнять множество административных задач, характеризующихся низким уровнем риска. Многие из таких задач выполняются постоянно и требуют значительных временны*х* затрат. Зачастую при их решении применяются устаревшие подходы, подлежащие оптимизации. Модернизационные усилия все большего числа компаний направлены на минимизацию указанных негативных аспектов для повышения производительности и эффективности работы персонала.

Совещания, административные задачи, переписка и телефонные разговоры отнимают у сотрудников много времени и иногда отвлекают их от основной работы. Это неизбежно и существенно снижает концентрацию их внимания, что сказывается на производительности труда и реализации основных задач организации. Как отмечено в статье, опубликованной сотрудниками Гарвардской школы бизнеса (Harvard Business School), повторяющиеся рутинные операции быстро надоедают и вызывают потребность отвлечься от напряженной работы. Авторы отмечают, что, если работнику приходится выполнять одну и ту же задачу существенно дольше необходимого, он предпочитает затягивать ее выполнение, а не заканчивать как можно быстрее (Brodsky, Amabile, 2018).

Роботизированная автоматизация процессов (Robotic Process Automation, RPA) предполагает применение машин для осуществления задач, ранее выполнявшихся людьми. Речь идет не о любых операциях, а о повторяющихся и не требующих критического мышления. Ведущие мировые гиганты, такие как Bosch, Siemens, Caterpillar и др., постоянно предлагают инновационные решения по оптимизации своих процессов. Основные направления автоматизации — инвентаризация запасов продукции, перемещение грузов по производственным помещениям и складам с оптимизацией логистики, мониторинг техники безопасности, управление документооборотом и многое другое (Lu et al., 2020). Внедрение новых технологий расширяет возможности бизнеса по ускорению производственного цикла, минимизации роли человеческого фактора, повышению производительности и качества продукции (Quazi et al., 2022).

Однако, чем выше степень автоматизации, тем выше риски для кибербезопасности и угрозы функционированию организаций. Принцип активного обеспечения безопасности клиентов предполагает предотвращение утечек данных или кибератак, а не реагирование на них. Грамотное использование подхода «Разработка, Безопасность, Эксплуатация» (Development, Security, Operations — DevSecOps) с самого начала жизненного цикла ПО позволяет снизить соответствующие издержки, поскольку они учитываются на каждом этапе создания продукта. Подобный подход применим и к RPA, где информационная безопасность требуется на всех платформах, а также при выполнении любых мероприятий по планированию, проектированию, конструированию, тестированию, практическому внедрению и дальнейшему развитию систем с акцентом на защиту и конфиденциальность данных и аутентификацию пользователей. Функциональные системы контроля позволяют ограничить доступ к приложениям в зависимости от функций конкретного пользователя.

Более эффективный контроль и управление деятельностью за счет возможностей RPA, методов DevSecOps и автоматизации проверки кода существенно повышают качество ПО и позволяют заметно снизить число внештатных ситуаций в ходе эксплуатации этих систем.

Роботизированная автоматизация процессов

Технология RPA представляет собой инструмент разработки ПО, который упрощает создание, внедрение и управление роботами, имитирующими взаимодействие человека с другим ПО и цифровыми системами. Такие роботы выполняют заданную последовательность операций без участия людей, сокращая объем ручного труда и позволяя организациям гибко и экономично автоматизировать свои бизнес-процессы. RPA обеспечивает интеграцию интерфейсов прикладного программирования и других технологий автоматизации, включая искусственный интеллект, модели машинного обучения, когнитивные сервисы (такие, как чат-боты, обработка естественного языка и оптическое распознавание символов).

Автоматизируя повторяющиеся операции, технология RPA дает сотрудникам возможность сосредоточиться на более специализированных и важных задачах. Для организаций RPA выступает потенциальным инструментом рационализации бизнес-процессов, снижения затрат на персонал и минимизации ошибок, вызванных человеческим фактором. Благодаря этому удается сократить число сбоев критических процессов, повысить прибыль и качество обслуживания, а значит, и удовлетворенность клиентов.

RPA служит эффективным и продуктивным решением многих задач. В частности, одной из наиболее трудоемких операций остается обработка счетов. Счета-фактуры поступают по разным каналам, после чего комплектуются с заказами, а для их оплаты зачастую необходимо согласие нескольких сотрудников. RPA предлагает механизм автоматической отправки счетов на утверждение нужному сотруднику, повышая эффективность проведения платежей. Аналогичным образом можно автоматизировать процесс проверки заказов для утверждения оплаты на базе контрольных списков.

Системы RPA находят применение в банковском и производственном секторах, страховании, здравоохранении, хайтеке и сфере услуг (например, телекоммуникационных либо энергетических) для выставления и оплаты счетов или ведения бухгалтерии. Банковский, финансовый, страховой сектора и здравоохранение располагают значительным потенциалом по внедрению RPA в механизмы активации карт, выявлению мошенничества, обработке заявлений на возмещение убытков, развитию бизнеса, автоматизации отчетности и координации работы различных систем (Madakam et al., 2019).

DevOps и DevSecOps

Современные подходы к разработке ПО опираются на гибкие методы, которые, в отличие от последовательного подхода Waterfall, предполагают постоянное совершенствование. Если группы разработчиков действуют разрозненно, не учитывая вопросов эксплуатации и безопасности создаваемых продуктов, у пользователей могут возникнуть проблемы, что скажется на финансовой или производственной эффективности бизнеса[1].

Под информационной безопасностью понимаются инструменты и методы проектирования и разработки устойчивого к кибератакам ПО для максимально раннего их предотвращения, выявления и реагирования на потенциальные угрозы. Ранее вопросами безопасности ПО, как правило, начинали заниматься лишь по завершении его разработки с помощью сотрудников специальных подразделений кибербезопасности, которые не участвовали в более ранних стадиях жизненного цикла продукта. Такой разрозненный подход замедляет создание ПО и устранение его уязвимостей. Работа всех вовлеченных в эти процессы специалистов осложняется трудностями в выявлении проблем с безопасностью в контексте производственной среды (Koskinen, 2019).

Набирающий популярность подход «Разработка и эксплуатация» (Development and Operations, DevOps) предполагает параллельную реализацию указанных процессов на протяжении всего жизненного цикла продукта. Сама по себе эксплуатация продукта после его создания может упростить выявление и устранение потенциальных проблем, но замедлит внедрение, а в сочетании с разработкой обеспечит организациям экономию времени и повышение общей эффективности (Lwakatare et al., 2019; Azad, Hyrynsalmi, 2021). DevOps применяется многими крупными компаниями в сфере электроники, интернет-торговли, доставки и др. (например, Starbucks, Etsy, Apple, Airbnb, Ashley Madison) и государственными органами (ФРС США, NASA и др.) (Plant et al., 2022; Rzig et al., 2022)[2].

DevSecOps представляет собой следующий шаг в развитии модели DevOps, расширяющий его возможности за счет превентивного обеспечения кибербезопасности. Он предполагает эффективную интеграцию тестирования и защиты на протяжении всего жизненного цикла ПО, поскольку вопросы безопасности продукта и инфраструктуры требуют учета с самого начала процесса разработки. В рамках многоуровневого подхода к ее достижению внимание уделяется не только защите данных и приложений, но и всему контексту интеграции, обслуживания и конечной эксплуатации систем (Smolander et al., 2022).

Как и DevOps, методология DevSecOps рассчитана на применение всеми специалистами, участвующими в разработке и внедрении ПО. Принятие культуры информационной и кибербезопасности в сочетании с другими требованиями дает возможность «разделить ответственность» за конкретные технологии и методы и разрабатывать протоколы защиты, обеспечивающие более эффективный контроль и управление рисками и оперативное решение соответствующих проблем.

DevSecOps позволяет быстро и безопасно разрабатывать более качественное ПО на основе единой логики с DevOps. Если обеспечению безопасности уделяется внимание лишь на завершающей стадии разработки, это может снизить эффективность реализующих методологию DevOps организаций. Причина — в том, что без интегрированных систем безопасности возрастает вероятность дублирования операций и необязательных перекомпиляций, увеличивая сроки разработки ПО и ухудшая характеристики конечного кода (Rajpakse et al., 2022).

Метод DevSecOps предполагает разработку и интеграцию модернизированных подходов к обеспечению безопасности, совместимых с DevOps. Эта тактическая триада объединяет разработку, информационную безопасность и эксплуатацию ПО (Myrbakken, Colomo-Palacios, 2017). Ее суть состоит в глубокой интеграции безопасности во все стадии жизненного цикла продукта благодаря серии автоматизированных операций, реализуемых в ходе создания его новых версий. Совокупность отмеченных операций способствует повышению эффективности и продуктивности процесса разработки.

Опытом успешной реализации DevSecOps располагают самые разные компании — Microsoft, Verizon и Pokemon Company, заинтересованные в слаженной коллаборации групп программистов и специалистов по безопасности (Swinhoe, Nadeau, 2019). Так, Verizon создала панель для мониторинга (когда и по чьей вине) возникающих уязвимостей в своих бизнес-приложениях на всех этапах жизненного цикла. Формируемая комплексная картина уязвимостей дает разработчикам практически в режиме реального времени сигналы о рисках, которые эти уязвимости несут для бизнеса, и позволяет им находить способы улучшить свои навыки. На базе DevSecOps Pokemon Company выстроила систему защиты для предотвращения утечек персональных данных пользователей онлайн-игры, что повысило общую корпоративную культуру безопасности.

Наконец, Microsoft создала многоуровневую систему коммуникаций и обмена опытом между разными командами разработчиков. На начальном уровне все сотрудники обучаются стандартам делового поведения, включая вопросы защиты данных. Следующий уровень позволяет добиться более глубокой безопасности для всех сотрудников. Третий предназначен только для инженеров компании, которых в закрытом режиме знакомят с источниками угроз, помогая им сформировать глобальную картину рисков. Персонал компании осваивает принципы, лежащие в основе политики корпоративной безопасности Microsoft, методы и тактики, применяемые хакерами, а также доступные инженерные решения. В конечном счете должна сложиться сеть,

[1] https://threatpost.com/apps-built-better-devsecops-security-silver-bullet/167793/, дата обращения 22.01.2023.

[2] См. также: https://digital.ai/catalyst-blog/9-companies-you-wouldnt-expect-to-be-using-devops/, дата обращения 22.01.2023.

объединяющая коллег и ресурсы, которые можно задействовать в любых проектах для целей безопасности. Чем лучше специалисты службы безопасности и разработчики будут понимать, что делает другая команда, тем более чуткими и готовыми к сотрудничеству они окажутся. Это ведет к снижению числа уязвимостей в финальном продукте и ускоренному их исправлению.

По мере появления новых типов кибератак защита среды разработки, непрерывной интеграции и внедрения (Continuous Integration and Continuous Delivery/Continuous Deployment, CI/CD) приобретает все большее значение. С самой ранней стадии разработки и на протяжении всего жизненного цикла продукта внимания требуют вопросы безопасности создаваемого кода, применения передовых методов защиты и быстрого реагирования на уязвимости.

Интеграция метода DevSecOps в платформу RPA: анализ конкретной ситуации

Применительно к бизнес-процессам термин RPA часто понимается как настройка ПО для выполнения операций, ранее осуществлявшихся людьми, в частности ввода данных из различных источников (электронной почты, таблиц и т. п.) в информационные системы (например, планирования ресурсов предприятия (ERP) и управления отношениями с клиентами (CRM)) (Lacity et al., 2015).

Корпоративные принципы Deloitte предусматривают, что с точки зрения рентабельности инвестиций структура процесса важнее, чем применяемая технология. В докладе компании описывается опыт некоего банка по внедрению RPA, в ходе которого был создан новый процесс обработки 1.5 млн заявок в год при помощи 85 роботов для выполнения 13 процедур. Достигнутая производительность эквивалентна 230 постоянным сотрудникам, а затраты на нее составили примерно 30% от зарплаты, которую пришлось бы платить людям (Schatsky et al., 2016).

Компания Siemens Global Business Services ведет разработку цифровых решений для оптимизации бизнес-процессов и расширяет практику оказания цифровых услуг с добавленной стоимостью. В 2017 г. было принято решение создать первую глобальную платформу RPA для поддержки различных корпоративных сервисов. Поставщиком технологии была выбрана компания Blue Prism — первый, один из наиболее авторитетных и зрелых брендов, удерживающий лидерство на рынке технологий RPA. Blue Prism входит в число 15 крупнейших поставщиков комплексных решений, способных поддерживать интеллектуальные автоматизированные экосистемы или общекорпоративные системы RPA для крупного бизнеса[3]. Они обеспечивают мощную поддержку автоматизации бэк-офиса, поэтому лучше подходят для промышленных предприятий и организаций здравоохранения (Khan, 2020).

По сравнению с актуальными на тот момент предложениями конкурентов Blue Prism выделялась централизованным подходом к менеджменту, упрощающим внедрение автономных роботов (полностью автоматизированных систем выполнения операций). Кроме того, продукты Blue Prism соответствовали обязательным требованиям Siemens в области финансов и безопасности, что позволило интегрировать их в систему внутренней отчетности (Internal Control Over Financial Reporting, ICFR). Тем самым Blue Prism отвечала главному критерию выбора технологических партнеров Siemens. ICFR регламентирует политику контроля и процедуры оценки рисков, обеспечивающих разумную уверенность в надежности финансовой отчетности компании, как того требует Закон Сарбейнса-Оксли (Sarbanes-Oxley Act, SOX) о раскрытии корпоративной финансовой информации.

Платформа RPA рассматривается нами как инструмент интеграции методологии DevOps с корпоративными требованиями безопасности. Централизованная платформа RPA Blue Prism, разработанная Siemens как сервис коллективного пользования, предлагает поддержку управления бизнес-процессами. Она позволяет автоматизировать повторяющиеся, рутинные, формализованные операции на базе структурированного ввода данных. Платформа интегрирована с другими технологиями, обеспечивая сквозную автоматизацию, и учитывает характеристики среды разработки, тестирования и производства. В каждом случае в расчет принимается логическое и физическое разделение сред. В производственной среде также обеспечивается физическое разделение данных.

ПО Blue Prism выполняет фиксированный алгоритм на базе технологии Runtime Client. Этот программный робот способен аутентифицироваться в целевых приложениях в зашифрованном формате и взаимодействовать с ними через графический пользовательский интерфейс (GUI), в том числе считывать или вводить данные в поля GUI, взаимодействовать с такими его элементами, как кнопки или ползунковые переключатели, и т. д. — в точности как пользователь-человек. Автоматизированный процесс может работать с несколькими целевыми приложениями. Поскольку для этого роботу нужна учетная запись и соответствующие права в целевой системе, реализовано разделение функций по принципу распределения ответственности (критические для процесса функции делятся между несколькими работниками или подразделениями организации). В подобном случае после аутентификации в системе (например, SAP) один и тот же пользователь не сможет и зарегистрировать заказ и утвердить его.

Диаграммы автоматизированных процессов представляют собой схемы бизнес-процессов, которые фактически служат компьютерными программами. В них применяются основные концепции программирования, а последовательность операций представлена в виде блок-схем. По сути, это визуализация рабочих про-

[3] https://www.gartner.com/en/documents/4016876, дата обращения 22.01.2023.

цессов для воспроизведения, анализа, модификации и масштабирования бизнес-задач. Каждый разработчик RPA имеет доступ к среде приложений Blue Prism. Для этого была создана система разделения сред, разграничивающая обязанности в интересах безопасности всей платформы. Именно здесь создаются процессы и объекты, которые затем апробируются в специальной тестовой среде. Автоматизированные процессы и системы внедряются в производство только после успешного прохождения теста на приемлемость для пользователя (User Acceptance Test). Их интеграция осуществляется и контролируется уполномоченным менеджером в рамках системы CI/CD или на индивидуальной основе.

Платформа RPA, разработанная специально для компании Siemens, предназначена для предоставления услуг по автоматизации деятельности различных бизнес-подразделений организации. Спрос на автоматизированные сервисы растет, а технологическая интеграция остается гетерогенной. Каждая автоматизированная операция, выполняемая в рамках системы RPA, реализуется на определенном уровне, что делает отдельного программного робота уникальным с точки зрения как доступа к приложениям, так и места в общем производственном цикле.

Дальнейшее развитие автоматизации RPA на базе концепции «фабрики ПО» может дать преимущества по сравнению с традиционными подходами к разработке. Речь идет прежде всего о совместимости разрабатываемых приложений: фабрика ПО предоставляет пользователям инструменты совместного освоения одних и тех же ресурсов и сходную логику, что требует обмена знаниями и документацией, опоры на общие структуры и соответствующих навыков. Однако в случае автоматизации нескольких процессов в рамках системы RPA подход, который состоит в последовательном применении ранее полученных знаний, может оказаться неэффективным и будет порождать ошибки. Другой аспект связан с качеством: повторное применение ранее написанного кода позволяет сэкономить время и ресурсы на автоматизацию и уделить больше внимания уникальным функциям. Вероятность ошибок в ходе проектирования и кодирования со временем предположительно снижается, но без устойчиво высокого качества разработок трудно добиться надлежащего уровня конечного продукта. Наконец, внимание уделяется повышению производительности, эффективности, совместимости и качества, чтобы проекты реализовывались в кратчайшие сроки и без привлечения дополнительных ресурсов.

Даже после внедрения в производство система требует постоянного мониторинга ее работы. В случае непоправимых ошибок в функционировании робота курирующий его менеджер должен уведомить о сбое разработчика и ответственных за процесс сотрудников организации. При этом собирается и детально проверяется вся необходимая фактическая информация об обстоятельствах и причинах, которые могут быть связаны с работой виртуальных машин, коммуникационными/сетевыми проблемами или, собственно, с автоматизацией. В последнем случае это может быть обусловлено изменениями автоматизируемого приложения или бизнес-процесса, не учтенными при разработке RPA. При крахе на операционном уровне (блок-схема процесса) восстановление потребует вмешательства создателей RPA.

Для коррекции уже задействованного автоматизированного процесса разработчику, как правило, необходим доступ к нему, чтобы отличить реальный процесс от использованного в среде контроля качества. Для решения таких задач и внесения экстренных изменений была создана специальная среда Blue Prism, позволяющая разработчику применять реальные производственные системы для минимизации различий между двумя указанными средами. Например, при обработке счетов-фактур или заказов в SAP среда контроля качества не всегда совпадает с реальной по объему или однородности информации, что затрудняет ее автоматизацию на базе фиктивных данных.

Siemens разрабатывает механизм внесения экстренных изменений в рамках системы обеспечения стабильной работы предприятия, которая позволяет оперативно устранять сбои и восстанавливать работу сервисов для минимизации последствий простоев, вызванных авариями или катастрофами.

В ходе непрерывного процесса интеграции и реализации применяется подход к автоматизации, в рамках которого концепция RPA встраивается в управление производственной цепочкой. Автоматизация RPA сама по себе формирует концепцию цепочки CI/CD, поскольку позволяет управлять разработкой и реализацией новых систем автоматизации в полностью автономном режиме.

Запросы на внесение серьезных изменений должны соответствовать критериям тестирования новых систем автоматизации на приемлемость для пользователя. В документации следует отражать типы или уровни тестов, которые были выполнены для оценки надежности и стабильности кода. Хотя эту процедуру пока не удалось полностью автоматизировать, именно с ее помощью осуществляется контроль качества и условий авторизации для внедрения кода на производстве. Чем больше происходит сбоев, тем чаще приходится выполнять отладку в среде для внесения экстренных изменений и тем больше соответствующих запросов, что удлиняет цепочку реализации CI/CD. В некоторых случаях, например, при незначительных изменениях, проверка и тестирование не выполняются, т. е. системы автоматизации сразу внедряются в производство.

Интеллектуальная автоматизация

Системы RPA, в особенности Blue Prism, позволяют не имеющим отношения к разработке ПО лицам быстро и с небольшими затратами автоматизировать некоторые бизнес-процессы. Последние высоко формализованы (регулируются четкими правилами и требованиями), носят тактический (краткосрочный) характер и реализуются в ИТ-организациях, применяющих сервис-ориентированные архитектуры и инструменты управления (Slaby, 2012).

Интеллектуальная платформа автоматизации представляет собой инструмент RPA на базе программных

роботов[4]. Ее ПО разработано в среде Microsoft.Net Framework и совместимо с рядом платформ, в частности IBM Mainframe, Windows, Windows Presentation Foundation (WPF), а также Java и сетью Интернет. Функционал визуального дизайна по принципу «сверху вниз» позволяет этому инструменту представлять материал как на самом общем, так и на максимально конкретном уровне и «перетаскивать» элементы мышью. Таким образом, даже технически неквалифицированные пользователи могут автоматизировать процессы, перемещая компоненты системы мышью в удобном графическом интерфейсе. При этом обеспечиваются соответствие существующей политике безопасности (настраиваемый функционал) и защита данных путем шифрования и «маскировки». Алгоритмы обеспечивают также безопасную передачу и хранение данных и доступ к ним.

С точки зрения контроля доступа указанная технология позволяет ограничивать определенным группам лиц возможности эксплуатации системы, например, предоставлять отдельным пользователям доступ только к конкретным группам роботов, процессов и объектов. Blue Prism поддерживает Стандарты безопасности данных индустрии платежных карт (Payment Card Industry Data Security Standards, PCI-DSS), соответствует требованиям Закона о переносе и подотчетности медицинского страхования (Health Insurance Portability and Accountability Act, HIPAA) и Закона Сарбейнса-Оксли (Sarbanes-Oxley Act, SOX), что задает необходимый уровень защиты и функционала[5].

Предусмотрен также механизм масштабирования на базе централизованного управления. Этот инструмент предназначен для автономной интеллектуальной работы (без взаимодействия с человеком) на всех стадиях автоматизированного процесса с применением модуля управления расписанием («Диспетчерская»), обеспечивающим автозапуск в любое заданное время. Любые процессы можно по мере необходимости автоматизировать и вести централизованный мониторинг их реализации, применяя усовершенствованный инструментарий сбора детальной информации о состоянии робота в режиме реального времени, который дает полное представление о цифровой системе.

Blue Prism также часто используется для масштабного внедрения. В апреле 2015 г. компания Telefónica O2 (принадлежит Telefónica Group) установила более 160 программных роботов Blue Prism, которые обрабатывают 400–500 тыс. транзакций в месяц. Прибыль на инвестиции составляет от 650% до 800% за трехлетний период (Lacity et al., 2015).

Анализ процесса постоянного совершенствования

Siemens GBS стремится повышать качество своих цифровых услуг и разрабатывает механизмы непрерывного совершенствования, чтобы отвечать самым строгим стандартам. Контроль качества позволяет сократить число ошибок или сбоев в ходе предоставления услуг. От RPA ожидается приведение всех автоматизированных систем в соответствие требованиям качества целевых приложений, т. е. систем под управлением роботов. Это не лучшая среда для разработки надежных и качественных процессов, и необходимы другие механизмы достижения данной цели. Автоматизация обеспечения безопасности в рамках цикла разработки указанных систем снижает риск ошибок и некорректного управления, чреватых сбоями в работе систем RPA или атаками на них.

Для повышения качества конечного продукта выполняется анализ кода. В данном случае речь идет о системной проверке кода RPA, написанного другими разработчиками, на наличие ошибок и с применением других критериев качества. В ходе анализа оценивается соответствие кода всем необходимым требованиям. Этот процесс следует планировать и выполнять на ранней стадии разработки. Время здесь имеет решающее значение, поскольку на более поздних этапах (или внепланово) проверка с большей вероятностью приведет к необходимости разработки нового кода, когда роботы уже внедрены в производство и последствия будут более тяжелыми.

Безопасность остается приоритетом на протяжении всего цикла разработки. Вопросы защиты RPA регулируются с помощью специальных средств контроля. Моделирование угроз на этапе дизайна, обучение разработчиков методам безопасного программирования и регулярный анализ кода с привлечением специалистов по безопасности помогут повысить общее качество кода и снизить число потенциальных проблем.

Если не планировать мероприятия по постоянному совершенствованию, риски для стабильности бизнеса возрастают, особенно при активной эксплуатации старых версий ПО, поскольку все системы автоматизации RPA со временем устаревают. Новые технологии появляются на рынке каждую неделю, и Siemens обеспечивает необходимые для поддержания безопасности инфраструктуры обновления, чтобы не оказаться в ситуации исчерпания жизненного цикла ПО. Учитывая столь высокую динамику и инновационную активность, развитие RPA следует воспринимать как непрерывный процесс.

В рамках управления системами роботизированной автоматизации следует регулярно выполнять оценку рисков и аудит процессов RPA. Ответственные сотрудники должны иметь четкое представление о своих обязанностях по обеспечению безопасности, в частности в отношении контроля доступа к роботизированным процессам автоматизации, ведения журналов (логов), мониторинга операций и т. д. Необходимо делегировать полномочия по регулярной оценке информационной безопасности RPA, иметь контрольный список соответствующих требований, структурировать уровни конфиденциальности, надежности и доступности

[4] https://www.blueprism.com/products/intelligent-rpa-automation/, дата обращения 22.01.2023.

[5] https://www.blueprism.com/resources/white-papers/how-blue-prism-sets-the-standard-for-secure-rpa/, дата обращения 22.01.2023.

(Confidentiality, Integrity, and Availability, CIA) для каждого процесса, чтобы ускорить выявление рисков в аудите внутреннего контроля финансовой отчетности ICFR. CIA включает три основных компонента защиты данных и информации, которые можно использовать при формулировании политики корпоративной безопасности. В случае сбоев в работе платформы RPA специалистам по ИТ и безопасности следует тщательно анализировать журналы операций. Логи автоматизации роботизированных процессов должны храниться в отдельной системе, чтобы обеспечить их сохранность и надежность на случай судебного разбирательства.

В ходе разработки новых систем автоматизации RPA прежде всего требуется достаточный набор критериев безопасности и качества кода. Для стандартизации и масштабирования разработки нужны инструменты автоматизированной проверки кода.

Выводы и дальнейшие направления исследований

Хотя технология RPA активно применяется на практике для поддержки экосистем интеллектуальной автоматизации (или корпоративных RPA-систем), в академической литературе ей уделяется незаслуженно скромное внимание (Syed et al., 2020; Ivancic et al., 2019). Задачей нашего исследования было восполнить этот пробел. Основой исследования послужил анализ масштабного внедрения RPA-сервисов компанией Siemens GBS, которая реализовала интеллектуальную автоматизацию сотен процессов и объектов. Проанализированы ключевые критерии теоретического осмысления и практического применения модели DevOps в области интеллектуальной автоматизации, которые позволили Siemens GBS реализовать методы DevSecOps в системах RPA. Для этого разработчикам на протяжении всего жизненного цикла кода продуктов/систем RPA необходимо использовать гибкие методологии, придерживаться культуры сотрудничества и участвовать в постоянном процессе повышения безопасности.

Программистам и операторам требуются инструменты разработки качественного кода RPA, что позволит сократить время на исправление ошибок и сбоев после практического внедрения роботов RPA (а значит, и время их простоя). Это возможно лишь при эффективной коллаборации обеих команд. Переход от модели независимой разработки к эксплуатационной дает преимущества в обслуживании систем RPA после их внедрения. В случае масштабной интеграции, когда необходима постоянная адаптация или корректировка разработанного кода, эти преимущества могут оказаться критическими.

С учетом несовершенства кода RPA полезными могут оказаться решения по автоматической проверке кода. Их применение и внедрение в систему RPA компании Siemens GBS позволили улучшить качество системы и управление ресурсами. Эти решения могут существенно повысить стабильность платформ RPA, поскольку открывают возможности для разработки более безопасных, надежных и менее трудоемких автоматизированных процессов.

Архитекторам или старшим разработчикам важно иметь возможность тестировать системы управления, поскольку процедуры отладки систем в процессе производства все чаще создают риски для безопасности. При корректировке предстоит учитывать фундаментальные аспекты безопасности не только при работе с готовым кодом, но и на всех стадиях внесения изменений. Например, внедрение кода в производство без адекватного тестирования или устранение ошибок, которые могли возникнуть в ходе разработки, без участия заказчика могут создавать риски для отладки на последующих этапах. Среда тестирования должна во всех деталях воспроизводить потенциальный функционал системы. Если это невозможно, разработчикам следует привлекать к тестированию пользователей (группу эксплуатации).

Платформа RPA будет стабильно работать в производственной среде лишь тогда, когда она удовлетворяет фундаментальным требованиям. Их игнорирование увеличивает риски и делает платформу уязвимой для возможных атак.

Большинство компаний разрабатывают программных роботов RPA в несколько итераций с помощью гибких методологий, которые позволяют повысить потребительскую ценность продукта. Однако системы RPA могут включать разнородные приложения, компоненты и технологии, функционирующие в разных операционных средах. Поскольку автоматизация становится неотъемлемой частью цифровой трансформации, организации все чаще используют технологию RPA, внедрение которой обычно не вызывает проблем, а применение программных роботов снижает эксплуатационные расходы и повышает общую эффективность системы. Фактические затраты на внедрение RPA во многом зависят от масштабируемой мощности платформы и качества разработки роботизированных процессов. Чем оно ниже, тем дороже обслуживание платформы. Сбои программных роботов влекут за собой дополнительные сервисные издержки и снижают ее рентабельность.

Библиография

Azad N., Hyrynsalmi S. (2021) What Are Critical Success Factors of DevOps Projects? A Systematic Literature Review. In: *Software Business. ICSOB 2021 Proceedings* (eds. X. Wang, A. Martini, A. Nguyen-Duc, V. Stray), Heidelberg, Dordrecht, London, New York: Springer. https://doi.org/10.1007/978-3-030-91983-2_17

Brodsky A., Amabile T.M. (2018) The downside of downtime: The prevalence and work pacing consequences of idle time at work. *Journal of Applied Psychology*, 103(5), 496–512. https://doi.org/10.1037/apl0000294.

Ivančić L., Suša-Vugec D., Bosilj-Vukšić V. (2019) Robotic Process Automation: Systematic Literature Review. In: *Business Process Management: Blockchain and Central and Eastern Europe Forum, Vienna, Austria, September 1–6, 2019, Proceedings* (eds. C. Di Ciccio, R. Gabryelczyk, L. García-Bañuelos, T. Hernaus, R. Hull, M. Indihar-Štemberger, A. Kő, M. Staples), Heidelberg, Dordrecht, London, New York: Springer, pp. 280–295..

Khan S. (2020). Comparative Analysis of RPA Tools-Uipath, Automation Anywhere and Blueprism. *International Journal of Computer Science and Mobile Applications*, 8, 1–6. https://doi.org/10.47760/ijcsma.2020.v08i11.001

Koskinen A. (2019) *DevSecOps: Building security into the core of DevOps,* Jyväskylä: University of Jyväskylä. https://jyx.jyu.fi/handle/123456789/67345, дата обращения 17.10.2022.

Lacity M., Willcocks L., Craig A. (2015) Robotic Process Automation at Telefónica O2 (The Outsourcing Unit Working Paper 15/02), London: The London School of Economics and Political Science, дата обращения 21.01.2023.

Lu Y., Xu X., Wang L. (2020) Smart manufacturing process and system automation – A critical review of the standards and envisioned scenarios. *Journal of Manufacturing Systems,* 56, 312–325. https://doi.org/10.1016/j.jmsy.2020.06.010

Lwakatare L.E., Kilamo T., Karvonen T., Sauvola T., Heikkilä V., Itkonen J., Kuvaja P., Mikkonen T., Oivo M., Lassenius C. (2019) DevOps in practice: A multiple case study of five companies. *Information and Software Technology,* 114, 217–230. https://doi.org/10.1016/j.infsof.2019.06.010

Madakam S., Holmukhe R.M., Jaiswal D.K. (2019) The Future Digital Work Force: Robotic Process Automation (RPA). *Journal of Information Systems and Technology Management*, 16(1), 1. https://doi.org/10.4301/S1807-1775201916001

Myrbakken H., Colomo-Palacios R. (2017) DevSecOps: A Multivocal Literature Review. In: *Software Process Improvement and Capability Determination* (eds. A. Mas, A. Mesquida, R.V. O'Connor, T. Rout, A. Dorling), Heidelberg, Dordrecht, London, New York: Springer, pp. 17–29.

Plant O.H., Van Hillegersberg J., Aldea A. (2022) Rethinking IT governance: Designing a framework for mitigating risk and fostering internal control in a DevOps environment. *International Journal of Accounting Information Systems,* 45, 100560. https://doi.org/10.1016/j.accinf.2022.100560

Qazi A.M., Mahmood S.H., Bahl A.H.S., Mohd J., Gopal K. (2022) The impact of smart materials, digital twins (DTs) and Internet of things (IoT) in an industry 4.0 integrated automation industry. *Materials Today: Proceedings,* 62(1), 18-25. https://doi.org/10.1016/j.matpr.2022.01.387

Rajapakse R.N., Zahedi M., Babar A.M., Shenc H. (2022) Challenges and solutions when adopting DevSecOps: A systematic review. Information and Software Technology, 141, 106700. https://doi.org/10.1016/j.infsof.2021.106700

Rzig D.E., Hassan F., Kessentini M. (2022) An empirical study on ML DevOps adoption trends, efforts, and benefits analysis. *Information and Software Technology*, 152, 107037. https://doi.org/10.1016/j.infsof.2022.107037

Schatsky D., Muraskin C., Iyengar K. (2016) *Robotic process automation*: *A path to the cognitive enterprise*, London: Deloitte.

Slaby J.R. (2012) *Cheap, easy-to-develop software robots will eventually supplant many offshore FTEs,* Cambridge (UK): HfS Research, Ltd.

Smolander K., Akbar M.A., Mahmood S., Alsanad A. (2022) Toward successful DevSecOps in software development organizations: A decision-making framework. *Information and Software Technology,* 147, 106894. https://doi.org/10.1016/j.infsof.2022.106894

Swinhoe D., Nadeau M. (2019) 3 DevSecOps success stories. CSO Online, 26.09.2019. https://www.csoonline.com/article/3439737/3-devsecops-success-stories.html, дата обращения 17.11.2022.

Syed R., Suriadi S., Adams M., Bandara W., Leemans S.J., Ouyang C., Ter Hofstede A.H., Van de Weerd I., Wynn M.T., Reijers H. A. (2020). Robotic Process Automation: Contemporary Themes and Challenges. *Computers in Industry,* 115, 103162. https://doi.org/10.1016/j.compind.2019.103162