DOI 10.37882/2223-2966.2023.06.17

ПРОБЛЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОБОТИЗИРОВАННЫХ СИСТЕМ: ПРОГРАММНЫЕ РОБОТЫ

THE PROBLEM OF INFORMATION SECURITY OF ROBOTIC SYSTEMS: SOFTWARE ROBOTS

G. Ivanov
A. Kamenskikh
A. Yuzhakov

Summary: Robotic process automation (RPA), based on the use of software robots, has proven to be one of the most sought-after technologies that has emerged in recent years and is used in automated systems to perform tasks of a programmatic nature in many industries, such as banking or manufacturing. As any new technology, RPA has a number of potential cybersecurity vulnerabilities that arise due to fundamental logical errors in the applied approach, or errors caused by human actions in the stages of implementation, configuration and operation of the technology. It is important to have a complete understanding of the relevant vulnerabilities and associated risks before integrating RPA into an enterprise automated system. The primary asset that RPA operates with is sensitive enterprise information. Data leakage and theft are two major threats. The widespread use of RPA technology in information security-sensitive sectors makes protecting RPA from cyberattacks an important challenge. Nevertheless, this topic has not yet been sufficiently studied in the academic environment and existing solutions have mainly focused on describing some threats. This article describes the technology RPA, formulates the problem of information security and the analysis of major threats to RPA, then proposed a solution by developing an ontology taking into account the specifics of.

Keywords: information security, automated system, robotic process automation, software robots, robotic system.

Иванов Глеб Олегович
Аспирант, Пермский национальный исследовательский политехнический университет
gleb_molodoi5@mail.ru
Каменских Антон Николаевич
Доцент, Пермский национальный исследовательский политехнический университет
antoshkinoinfo@yandex.ru
Южаков Александр Анатольевич
Пермский национальный исследовательский политехнический университет
uz@at.pstu.ru

Аннотация. Роботизированная автоматизация процессов (RPA), основанная на использовании программных роботов, оказалась одной из наиболее востребованных технологий, появившихся в последние годы и используемых в автоматизированных системах для выполнения задач программного характера во многих отраслях, например, в банковском или производственном сегменте. Как и любая новая технология, RPA имеет ряд потенциальных уязвимостей в области кибербезопасности, возникающих ввиду наличия фундаментальных логических ошибок в применяемом подходе, либо ошибок, порождаемых действиями человека на этапах внедрения, настройки и эксплуатации технологии. Важно иметь полное представление о соответствующих уязвимостях и связанных с ними рисками до интеграции RPA в автоматизированную систему предприятия. Основным активом, которым оперирует RPA, является конфиденциальная информация предприятия. Утечка и кража данных — две главные угрозы. Широкое применение технологии RPA в секторах, чувствительных к обеспечению информационной безопасности, делает защиту RPA от кибератак важной задачей. Тем не менее, эта тема еще недостаточно изучена в научной среде и существующие решения в основном сосредоточены на описании некоторых угроз. В данной статье проводится описание технологии RPA, формулируется проблема обеспечение информационной безопасности и проводится анализ основных угроз RPA, после чего предлагается решение по средствам разработки онтологии с учетом специфики RPA.

Ключевые слова: информационная безопасность, автоматизированная система, роботизированная автоматизация процессов, программные роботы, робототехническая система.

Введение

Роботизированная автоматизация процессов — это семейство технологий автоматизации бизнес-процессов, основанных на использовании программных роботов и искусственного интеллекта. Программный робот воспроизводит действия человека, взаимодействуя с интерфейсами информационных систем. Сценарий его поведения программируется разработчиком на основе наблюдения за реальным пользователем, выполняющим задачу с помощью различных программных инструментов. Предполагается, что внедрение роботов RPA в скором времени позволит освободить значительную часть ресурсов предприятий, занятых рутинной обработкой информации. Использование этой технологии позволяет сократить количество сотрудников, выполняющих низкопрофильную или цикличную работу, тем самым увеличивая скорость выполнения бизнес-процессов, снижая стоимость работы компании, позволяя выполнять бизнес-процессы в любое время суток, уменьшая количество человеческих ошибок. Цель данной статьи заключается в подтверждение проблемы

обеспечения информационной безопасности и поиска ее решения для успешного внедрения RPA на практике.

Оценка рынка

В настоящее время RPA продолжает развиваться на рынке автоматизированных систем. Значительный толчок получили отечественные производители, в результате ухода крупнейших зарубежных вендоров. Согласно последнему прогнозу ООО «ИБА»: «К 2024 году доля российских RPA по количеству клиентов на российском рынке составит более 90 %, хотя в 2021 она была менее 10 %».

Ожидается, что объем мирового рынка роботизированной автоматизации процессов вырастет с 10,01 млрд долларов в 2022 году до 43,52 млрд долларов к 2029 году при темпах роста 23,4 %.

На сегодняшний день на рынке RPA-платформ в России представлено как несколько зрелых и проверенных временем решений от опытных разработчиков, так и около десятка новых продуктов. Такое количество новых игроков на рынке является типичным признаком стадии быстрого роста. Хотя количество российских RPA-платформ уже достаточно велико, все они имеют свои отличия, что можно отнести к их индивидуальной специфике и особенностям разработки. Одним из интересных прогнозов является мнение экспертов, которые предполагают, что к 2024 году список ведущих RPA-компаний может пополниться новыми игроками, такими как Sber RPA или Атом.Рита. [1]

Принцип работы RPA

Общая концепция функционирования программного робота представлена на рисунке 1. Обычно робота можно рассматривать как зацикленную последовательность шагов, каждый из которых выполняет определенную программу, используя результаты предыдущих шагов и генерируя данные для следующих. В процессе работы роботы могут генерировать отчеты, использовать файловую систему локального компьютера, взаимодействовать с внешними операционными системами и другими ресурсами (почтовые серверы, серверы баз данных, интернет-сервисы, облачные системы и т.д.). [2]

Весь программный код, выполняемый внутри робота, можно разделить на три группы программ: встроенный, стандартный (утилиты) и определяемый пользователем. Эти программы используют ресурсы локальной операционной системы (файловую систему, оперативную память, процессорное время). Локальный компьютер взаимодействует с внешними операционными системами. Встроенные программы обычно являются частью приложения, которое обозначается как RPA-исполнитель. Основная цель приложения RPA-исполнителя — запуск и остановка робота. Стандартные программы предоставляются как часть программного обеспечения робота и предназначены для выполнения базовых действий: распознавание текста, отправка и получение электронной почты, заполнение шаблонов, форм, и так далее. Пользовательские программы используются, если функциональность встроенного и стандартного программно-

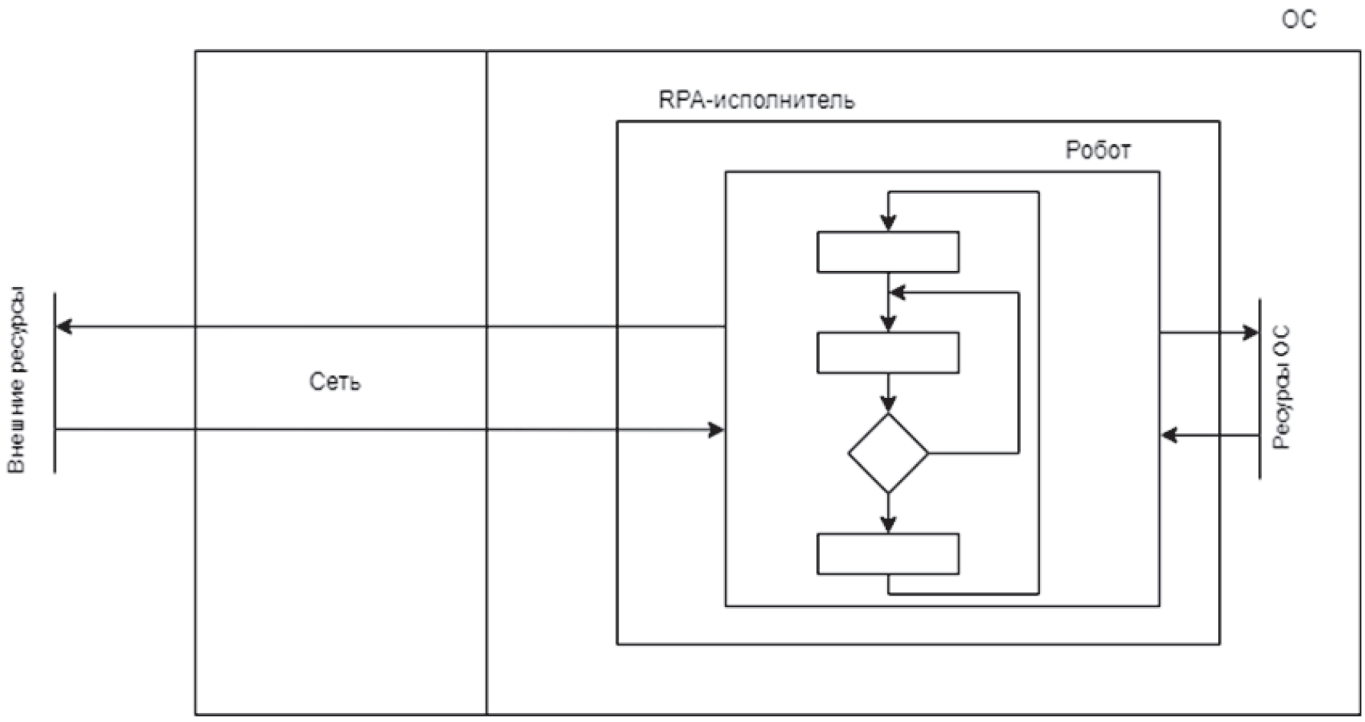

Рис. 1. Архитектура приложения RPA

го обеспечения не соответствуют поставленным перед роботом задачам. Разработка таких программ основывается на стандартах и интерфейсах (API), описанных в документации к системам RPA. Пользовательский код, подобно утилитам, функционирует как часть цикла выполнения робота. [3]

Как правило, роботизировать можно только линейные процессы, в которых есть ограничения принятия решений, присутствует вариативность, а алгоритмы взаимодействия робота с окружающей средой являются строго детерминированными. Хотя ограничения, связанные с примитивностью и применимостью к линейным отлаженным процессам, можно рассматривать как заложенные в основу RPA, порождаемые ими риски информационной безопасности должны быть все равно снижены.

Проблема обеспечения информационной безопасности

Управление рисками безопасности является одним из приоритетных вопросом при реализации решений RPA, поскольку информация имеет крайне высокую ценность в сегодняшнем устройстве общества. Значительное количество рисков информационной безопасности в решениях RPA объясняются большим числом взаимодействующих компонентов и каналов, использующих различные протоколы связи (в том числе открытые каналы связи) для передачи конфиденциальных или аутентификационных данных, которые могут иметь известные недостатки в защите. Это создает многочисленные возможности для злоумышленника реализовать такие известные атаки как: сниффинг, «человек посередине», спуфинг и другие.

Наиболее острой проблемой является обеспечение того, чтобы конфиденциальные данные не использовались не по назначению через привилегии, выданные программным роботам или тем, кто занимается их разработкой и настройкой. Вопрос безопасности данных можно разделить на две очень взаимосвязанных области, одна из которых — безопасность самих данных, а другая — безопасность доступа к ним. Объединяя эти области с принципом «минимальных привилегий», мы сможем гарантировать, что данные, к которым робот получает доступ, останутся конфиденциальными. Более того, эти роботы имеют повышенные права на выполнение задач и доступ к паролям, поэтому, должна быть надлежащим образом реализовано модель управления доступом, подобно тем, что применяются для управления учетными записями пользователей. [4]

Систематический подход по снижению рисков в любой области предполагает, что масштабная оценка рисков должна проводиться чтобы определить возможные уязвимости и потенциальный ущерб от их использования, а также получить представление о том, что могло привести к возникновению этих событий. Риски должны быть приняты во внимание независимо от того, находится ли источник этих рисков под контролем организации или нет. Обычно оценка включает в себя идентификацию активов, идентификацию угроз, идентификацию средств контроля и мер защиты, идентификацию уязвимостей (не только в программном или аппаратном обеспечении), которые могут быть использованы существующими угрозами, и идентификацию последствий реализации угроз. Поскольку этот процесс должен проводиться регулярно и при каждом новом развертывании RPA, необходим инструмент, который мог бы помочь в выполнении всех этих этапов оценки. Традиционно используются контрольные списки угроз и уязвимостей, но этот подход обладает серьезными недостатками, поскольку набор активов, их безопасность и уязвимости могут меняться и отличаться в зависимости от типа организации и поставщика в области программной робототехники, из-за чего большая часть списков может оказать неприменимой. Ввиду новизны направления RPA, в списках также может отсутствовать информация о еще не выявленных уязвимостях.

Анализ основных угроз RPA

Чтобы оценить состоятельность проблемы необходимо провести обзор работ в научной литературе, посвященных угрозам RPA. При рассмотрении основных групп угроз, связанных с RPA, можно выделить следующие типы как наиболее важные:

Уязвимости. Это недостатки в информационной системе, которые позволяют злоумышленникам получить доступ к системе для выполнения запрещенных действий. Большинство систем RPA сегодня используют шифрование данных, что снижает риск возникновения уязвимостей, но они все еще встречаются в некоторых относительно слабо защищенных решениях. Например:

1. Уязвимость безопасности может существовать в среде виртуальной машины, в которой работает бот. Боты Automation Anywhere [5] развернуты на виртуальных машинах Microsoft Windows server 2012 R2, и если в среде виртуальной машины существует уязвимость безопасности, злоумышленник может получить удаленный доступ к виртуальной машине и через нее попасть в защищённый сегмент сети для получения доступа к конфиденциальным данным;
2. Разработчики бота могут запрограммировать его на отправку/получение конфиденциальных данных без шифрования. Эти данные могут быть перехвачены с помощью активного (проведение атаки человек посередине) или пассивного (прослушивание сети) воздействия.

Злоупотребление Интернетом. Это ситуации, в которых происходит нелегитимное распространение данных, связанных с информационной безопасностью компании. Согласно статистике, большинство утечек таких данных происходит из-за того, что пользователи, имеющие учетные записи с расширенным доступом, передают параметры от них кому-то в личных целях. Если у робота есть подключение к интернету, то по аналогии с пользователем, он также может реализовать алгоритм, который приведет к передаче данных учетной записи. Злоумышленники могут использовать привилегии робота для компрометации системы и неправомерного использования информации. Например:

1. Злоумышленник может скомпрометировать учетную запись администратора, используемую ботом. Злоумышленник может использовать учетную запись администратора для получения доступа к конфиденциальным данным;
2. Перед уходом с работы бывший сотрудник может запрограммировать бота на выполнение вредоносного кода или снять с него защиту, предоставив прямой доступ другим злоумышленникам.

Сбой системы. Аппаратный или программный сбой может привести к прекращению функционирования системы. Время простоя чаще всего связано с человеческим фактором (ошибки сотрудников), состоянием оборудования, ошибками на сервере и проблемами взаимодействия между программными решениями. Сбой в сети может нарушить работу робота, как и другого программного решения, и привести к снижению производительности. Перебои в работе системы или даже ее полное отключение может быть вызвано в результате слишком быстрого последовательного выполнения действий роботом при наличии ограничения системных ресурсов. Например:

1. Использование неоптимизированных методов программирования могут привести к тому, что бот будет потреблять все системные ресурсы виртуальной машины, в результате чего, виртуальная машина не будет реагировать на запросы и, следовательно, не сможет выполнять какую-либо работу;
2. В системе могут проводится технические работы, незапланированные обновления или обслуживание сети, что может привести к потере данных работа и вызвать у него сбой в цикличной работе.

Разглашение конфиденциальной информации. В отношении RPA этот риск заключается в возможности преднамеренного или случайного неправильного обучения робота, при котором данные попадут в интернет или к сторонним пользователям. Например:

1. Разработчик бота может по ошибке запрограммировать бота на загрузку строго конфиденциальных данных, таких как информация о кредитных картах, в базу данных, доступ к которой открыт для любого пользователя в сети Интернет;
2. Разработчик бота может использовать свой технический аккаунт для кражи интеллектуальной собственности.

Далее, приведем основные выявленные первопричины рассмотренных нами угроз RPA:

1. Информация раскрыта случайно — бот может быть плохо настроен, что приведет к распространению чувствительных данных через Интернет или по другому незащищенному источнику;
2. Отсутствие или уязвимость средств шифрования и контроля доступа;
3. Слабые функции аутентификации;
4. Программные боты RPA требуют привилегированного доступа для выполнения необходимых задач, таких как вход в систему управления взаимоотношениями клиентов или в другие бизнес-системы для чтения, удаления или изменения информации, а также для передачи данных от одного процесса к другому. Необходимость постоянного доступа означает, что привилегированные учетные данные часто применяются и должны храниться непосредственно в сценарии или процессе, основанном на правилах, которым следует бот. Или же сценарий может включать шаг получения учетных данных из небезопасного места, например, из файла конфигурации или базы данных;

Также рассмотрим некоторые рекомендуемых средства контроля безопасности для RPA из технической документации разработчиков: Полные журналы аудита; Интеграция технологий защиты данных; Использование шифрования; Управление доступом на основе ресурсов и ролей; Минимизация площади поверхности атаки; Установка безопасных настроек по умолчанию; Принцип наименьших привилегий; Принцип эшелонирования; Отказоустойчивость; Отсутствие доверия к сервисам; Разделение обязанностей; Избегание защиты без подтверждения; Обеспечение простоты реализации; Правильное устранение проблем безопасности. [6]

Тем не менее, необходимо сказать, что средства контроля могут варьироваться в зависимости от платформы RPA и не существует универсального подхода для их применения. Для успешного проектирования программного робота, минимизации рисков, обеспечения безопасности робота и соответствия принятым в отрасли стандартам необходимо разработать модели и методы защиты, которые позволят достичь безопасности RPA сравнить их с перечнем критериев идентификации рисков в действующих методологиях.

Предлагаемое решение

Для решения проблемы предлагается разработать онтологию безопасности RPA. Онтология — это система-

тизированное описание всех терминов определенной предметной области, их свойств и отношений между ними. Она использует термины и их отношения для составления словарей тематической области, а также правил комбинирования для определения возможностей расширения словаря [7]. Онтология обеспечивает лучшую коммуникацию, возможность повторного использования и организацию знаний, уменьшая неоднозначность языка и структурируя передаваемые данные. [8]

Однако онтологии безопасности в области RPA найдены не были, а в существующих онтологиях безопасности отсутствуют функции, связанные с RPA.

Предлагается в основу онтологии RPA включить шесть классов: активы, риски, безопасность, угрозы, уязвимости и контрмеры, определенные как наиболее важные. Она должна обладать возможностью систематически описывать эти специфические классы и расширяться, изучая домен по принципу "сверху вниз". За основу может быть взят стандарт ISO/IEC 27005: 2018, содержащий рекомендации по управлению рисками информационной безопасности, включая телекоммуникационные технологии. Методы, описанные в этом стандарте, следуют общей концепции, указанной в ISO/IEC 27001

Частные задачи для дальнейшего исследования

Решение поставленной проблемы может быть достигнуто путем реализации частных задач, которые позволят реализовать предложенное решение. Планируется выполнить следующие задачи: 1) Определить термины и понятия, относящиеся к информационной безопасности, и установить связи между ними; 2) Создать схему онтологии, включающую все выделенные термины и понятия; 3) Определить классы объектов и связи между ними в рамках онтологии; 4) Определить правила классификации объектов на основе семантики и синтаксиса терминов и понятий; 5) Определить способы формализации знаний об информационной безопасности, включая описание протоколов и алгоритмов.

Перспективы

В дальнейшем предложенная онтология может быть обновлена и использована различными способами, например, как контрольный список для задач управления рисками в решениях RPA и источник информации для экспертной системы или набор данных по конкретной области. Полученная онтология может также использоваться для оптимизации и ускорения моделей машинного обучения, используемых для защиты информации, помогая сузить область поиска решения, тем самым экономя время и ресурсы.

Итоги

Проведенный обзор литературы показал, что широко используемая технология RPA имеет ряд рисков информационной безопасности из-за большого количества взаимодействующих компонентов и каналов, использования различных протоколов связи, и существует необходимость в управлении рисками и их снижении. Для эффективного управления рисками необходим единый источник информации, в котором хранились бы связанные с RPA активы, угрозы и контрмеры, и онтология может рассматриваться как перспективный способ хранения таких данных, но в настоящее время не найдено онтологий, связанных с безопасностью RPA, в связи с чем возникает необходимость в ее разработке, ориентированной на безопасность RPA. Создание онтологии безопасности для RPA позволит быстро определить ключевые моменты обеспечения информационной безопасности при проектировании программного робота, во время его активной работы, позволит оценить степень безопасности робота и определить, какие контрмеры необходимо предпринять для повышения уровня безопасности.

ЛИТЕРАТУРА

1. Яков Шпунт. Избавляйтесь от рутинных задач: рейтинг российских RPA-платформ 2022 // VISION–2022.
2. Schumacher, M. 3. Ontologies. In Security Engineering with Patterns Lecture Notes in Computer Science // Springer: Berlin/Heidelberg, Germany, 2003; Volume 2754.
3. Tsoumas, B.; Dritsas, S.; Gritzalis, D. An Ontology-Based Approach to Information Systems Security Management // In Proceedings of the Third International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security, St. Petersburg, Russia, MMM-ACNS 2005; Springer: Berlin/Heidelberg, Germany, 2005
4. ElectoNeek. Security Concerns in RPA: A 4-Step Guide to Address Them // Режим доступа: https://electroneek.com/blog/security-concerns-in-rpa-4-step-guide-to-address-them/ (дата обращения: 14.04.2023)
5. Microsoft. Azure Policy Built-in Definitions for Azure Virtual Machines // Режим доступа: https://learn.microsoft.com/en-us/azure/virtual-machines/policy-reference (дата обращения: 12.02.2023)
6. Automationanywhere. 10 Best Practices for Secure Bot Design // Режим доступа: https://www.automationanywhere.com/company/blog/learn-rpa/ten-best-practices-for-secure-bot-design (дата обращения: 23.03.2023)
7. Smekhun, Y.A.; Sistemakh, O. Ontologies in the knowledge based systems: Possibilities of their application // Int. Res. J. 2016, 5, 173–175.
8. Hlomani, H.; Stacey, D. Approaches, methods, metrics, measures, and subjectivity in ontology evaluation: A survey. Semant // Web J. 2014, 1, 1–11 // Режим доступа: http://www.semantic-webjournal.net/system/files/swj657.pdf (дата обращения: 14.04.2023)

Журнал «Современная наука: актуальные проблемы теории и практики»