БИЗНЕС ЗАВЕРБОВАЛ ИИ-АГЕНТОВ

В РОССИИ КОМПАНИИ ВСЕ АКТИВНЕЕ ВСТРАИВАЮТ АВТОНОМНЫЕ ИИ-АГЕНТЫ В БИЗНЕС-ПРОЦЕССЫ — НО РЕЧЬ ИДЕТ НЕ О ГОТОВЫХ «КОРОБОЧНЫХ» РЕШЕНИЯХ, А О КАСТОМНЫХ СИСТЕМАХ И ПЛАТФОРМАХ, АДАПТИРОВАННЫХ ПОД КОРПОРАТИВНЫЕ КОНТУРЫ. ПО ДАННЫМ КОМПАНИИ «ЯКОВ И ПАРТНЕРЫ», РЫНОК ФОРМИРУЕТСЯ ВОКРУГ ВНУТРЕННИХ РАЗРАБОТОК И СПЕЦИАЛИЗИРОВАННЫХ ИНСТРУМЕНТОВ, А ПОЛЬЗА ОТ ИИ-АГЕНТОВ ПРОЯВЛЯЕТСЯ ТАМ, ГДЕ ЗАДАЧИ ФОРМАЛИЗУЕМЫ, РЕЗУЛЬТАТ ИЗМЕРИМ, А КОНТРОЛЬ ОСТАЕТСЯ ЗА ЧЕЛОВЕКОМ. АЛЕКСАНДР КРЫЛОВ

В России рынок готовых ИИ-агентов пока окончательно не сформировался, об этом идет речь в исследовании консалтингового агентства «Яков и партнеры» (бывшей российской «дочки» McKinsey & Company). Отечественные платформы для сборки агентов, адаптированных к корпоративным процессам (Yandex AI Studio, Agent Platform, MWS AI Agents Platform, GigaChat Enterprise), занимают большую часть рынка, но на нем нет готовых ИИ-агентов, которых можно купить как самостоятельное решение. Полноценные ИИ-агенты возникают как внутренние решения компаний, при этом аналитики отмечают, что применяемые компаниями ИИ-агенты обеспечивают точечную автоматизацию, выполняя работу с определенными инструментами, но не обладают такими возможностями, как планирование, память и автономное завершение задач.

ОЩУТИМЫЙ ЭФФЕКТ Собеседники Guide из различных отраслей подтверждают, что внедрение ИИ-агентов в бизнес-процессы приносит ощутимый экономический эффект. При этом полная автономия таких инструментов пока остается недостижимой — контроль за их работой сохраняется за человеком.

«Для ИТ-компании ключевой процесс — разработка ПО, именно здесь ИИ-агенты показали наибольшую эффективность. Задачи в этом процессе хорошо формализуются и быстро верифицируются: код либо компилируется и проходит тесты, либо нет. Там, где результат работы агента проверяется за минуты, автономный ИИ дает максимальную пользу при минимальном риске»,— рассказывает президент ГК «СофтБаланс» Владимир Каменецкий, добавляя, что программисты используют ИИ-агенты при написании кода, поиске ошибок, рефакторинге, подготовке сценариев тестирования, при этом скорость разработки увеличилась в среднем до пяти раз.

Заместитель генерального директора по внедрению и эксплуатации компании «Базис» Денис Романов отмечает, что ИИ-агент собственной разработки «Цифровой техлид» используется в техподдержке и эксплуатации ИТ-инфраструктуры. → 10



ЕВГЕНИЙ ПАВЛЕНКО

В РЕКРУТИНГЕ ИИ-АГЕНТ МОЖЕТ САМОСТОЯТЕЛЬНО ИСКАТЬ КАНДИДАТОВ ПО НЕСКОЛЬКИМ ИСТОЧНИКАМ И АНАЛИЗИРОВАТЬ РЕЗЮМЕ

ВЗЛОМАТЬ МОЖНО, ПРОДАТЬ СЛОЖНО

**КОНСТАНТИН РОДИН,
ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ПО РАЗВИТИЮ БИЗНЕСА «АЙТИ БАСТИОН»**



«АЙТИ БАСТИОН»

Рынок малого и среднего бизнеса остается неприступным для ИБ-компаний и интеграторов не первый год. Интерес понятен: компаний много, потенциал для защиты есть, а продажи пока не соответствуют ожиданиям. По этому поводу в отрасли уже существует объяснение: заказчику незнакомы риски и денег у него недостаточно. Но что предлагается рынку? Система, рассчитанная на отдельную службу безопасности, предполагает вместе с приобретением лицензии еще и наличие компетенций для ее обслуживания. Можно снизить цену вдвое, но второй системный администратор в штате не появится, а на первом — бухгалтерия, серверы и рабочие места.

Злоумышленнику тем временем достаточно одной доступной уязвимости. Открытый удаленный доступ и слабые пароли для захвата серверов 1С и почт небольших компаний ищут автоматические сканеры — без всякого предварительного интереса к конкретной компании. Для вымогательства достаточно того, что атакуемая компания не сможет нормально работать без зашифрованных данных. В 2025 году первоначальные требования за расшифровку для МСБ составляли от 240 тыс. до 4 млн рублей. Пока предприниматель и вендор не могут договориться о цене и условиях защиты, расходы появляются там, где не ждали.

Из вышеописанного очевидно: потребность в защите определенно есть. Чтобы выяснить, почему она не вырастает в покупку, мы заказали исследование спроса на PAM (англ. Privileged Access Management — «контроль привилегированного доступа») в малом и среднем бизнесе. Из интервью с собственниками предприятий складывается знакомая многим ситуация: внешний специалист подключился, провел работы, а что именно он сделал — остается загадкой, особенно если что-то пошло не так. Саму же PAM-систему участники исследования нередко относили к инструментам корпораций, а некоторые и вовсе не были знакомы с этим классом решений. Возможно, именно восприятие является главным препятствием к покупке — насколько хорошо мы объяснили необходимость продукта, прежде чем объявлять клиента неготовым к нему?

Для бизнеса важнее, сможет ли он завтра восстановиться после сбоя и продолжить работу в штатном режиме. На языке разработчика тот же разговор часто может превращаться в перечисление преимуществ системы, и чем длиннее список — тем, кажется, убедительнее цена. Только заказчик еще не понял, для чего ему весь этот набор. Участники исследования просят быстрое развертывание, простое управление и готовые сценарии эксплуатации. А пока разработчики пытаются обосновать достоинства функций, которые потребителю не особо нужны, предприниматели выстраивают защиту, как умеют: вручную собирают журналы событий, поручают администратору следить за подрядчиками в неурочное время. Ограничения у такого подхода есть, но он уже вошел в рутину и часть задач закрывает. Поэтому конкурент разработчиков — уже принятое в компаниях решение обходиться без специализированных технологий. И для его пересмотра мало критиковать существующую защиту, нужно объяснить, как события могут развиваться во время или после инцидента — возможно, получится быстрее установить его причину, снимется часть ручной работы с администратора или же инцидента в принципе удастся избежать.

Небольшой компании нужна возможность взять под контроль доступ подрядчиков к важным серверам по посильной цене и без длительного освоения. Расширять возможности системы бизнес сможет уже по мере необходимости. Не менее существенен выбор модели обслуживания системы. Конечно, можно администрировать ее самостоятельно, но если свободных рук нет, то, возможно, будет разумнее передать согласованные задачи провайдеру по подписке и вовсе не брать систему «на баланс». При этом подписка не должна оставлять заказчика с теми же обязанностями, от которых он рассчитывал избавиться. При любом варианте PAM дополняет базовые меры защиты, включая резервное копирование и обновления.

Большой потенциал рынка не превратится в выручку лишь потому, что атаки продолжаются. Можно еще несколько лет убеждать предпринимателей потратиться, подкрепляя каждую презентацию новой историей взлома. Но это значит, что мы снова требуем от заказчика измениться, ничего при этом не меняя в собственном подходе. Формировать культуру безопасности придется и через собственную работу: объяснять без профессионального высокомерия, показывать настройку на понятной задаче и сопровождать заказчика в освоении системы. А прежде — признать, что отказ от продукта не обязательно означает отказ от защиты как таковой.