IT-системы генерируют новые риски

Специально для «Ведомости»

Сбой в системе бронирования «Аэрофлота», смешавший карты тысяч людей, еще раз показывает, как растет зависимость общества от созданного им же цифрового мира. Эта зависимость стала настолько естественной, что ощущается только в момент непредсказуемых сбоев. Невозможно прогнозировать, когда и в какой части цепочек связей произойдет разрыв и как он повлияет на остальные элементы системы. Граница между человеческим фактором и фактором техники становится все более зыбкой.

Мы только наблюдаем, уже почти безвольно, за технологическими коллапсами, утечками данных, формированием параллельного цифрового мира с его сообществами и платежными системами, который виртуализирует капиталы, собственность, коммуникации. Ряд IT-компаний, призванных создать инструменты киберзащиты от новых угроз, пытаются догнать уходящий поезд, но одновременно готовят отличных профессионалов, чтобы потом эти барьеры обходить.

«Система постоянно усложняется. Одни элементы начинают отставать от других, а сами пользователи ментально не успевают за цифровым авангардом. Больше всех с изменениями опаздывает информационная безопасность, ведь бизнес в конкурентной гонке чаще отдает предпочтение новым технологиям», — отмечает диджитал-предприниматель Олег Грешнев.

Глобальная связь элементов системы создает **«эффект бабочки»:** дефект в одном из звеньев вызывает цепную реакцию, как это и случилось с российским перевозчиком. Решения ищут в том, чтобы увеличивать охват и глубину тестирования софта, внедряя специальные программы, которые проверяют работу других программ, либо дробить процессы на маленькие кусочки, повышая контроль за счет **микросервисной архитектуры.** Но эти меры

удорожают процесс разработки и требуют квалифицированных специалистов, а они в дефиците — на фоне постоянно растущего спроса и отставания системы образования в этой области.

Среди цифровых рисков выделяется группа, связанная с внешними воздействиями. Но, по признанию IT-специалистов, существенно больше проблем с человеческим фактором внутри системы. Вместе с нарастающим кадровым дефицитом растет объем ненадежного кода. Разработчики выстраивают цепочки аутсорсеров, поэтому **уровень компетенции базовых исполнителей практически неизвестен заказчику.** Созданные на начальных этапах ошибки начинают масштабироваться во всем продукте.

Помимо этих двух групп рисков, связанных с человеческим фактором, сейчас приходит третий, наименее управляемый, — **риск самой системы.** Заложенные внутрь ее решения могут при общей подвижности всех элементов давать непредсказуемые эффекты.

Даже Билл Гейтс, называя главные опасности для человечества — новые вирусы, глобальное потепление, биотерроризм, — обходит стороной риск уязвимости всей архитектуры цифрового мира. Такое признание можно было бы рассматривать как подрыв собственной репутации. Но, с другой стороны, это говорит и о том, что Гейтс хорошо понимает: **люди не готовы жертвовать своим комфортом**, пока дело ограничивается застрявшими пассажирами.

Идеального решения в этой ситуации нет. Общество не готово к отказу от делегирования технологиям и искусственному интеллекту все новых функций, да и сам этот отказ, убрав одни риски, тут же вернет прежние, связанные уже с самим человеком. Остается только немного тормозить на поворотах и оставить за людьми функцию этического контроля.

Оригинал статьи