24 октября 2024

Западное ПО в России: так ли страшен черт, как его малюют?

Внедрение иностранного программного обеспечения в России в 2024 году - неочевидный шаг. С одной стороны, качественное ИТ-решение может улучшить производственные процессы и повысить конкурентоспособность компании. С другой стороны, использование международного ИТ-продукта может привести к значительным рискам. Среди них и нарушение работы из-за санкций, зависимость от иностранного поставщика и угрозы, связанные с информационной безопасностью.

Есть случаи, когда использование западного ПО - единственный выбор, и компании приходится идти на риски, чтобы бизнес не останавливался. Давайте рассмотрим, почему компаниям может понадобиться внедрять западное ПО в 2024 году и в каких случаях польза превышает риски.

ЗАЧЕМ КОМПАНИЯМ МОЖЕТ ПОНАДОБИТЬСЯ ВНЕДРЯТЬ ЗАПАДНОЕ ПО В 2024 ГОДУ

Компании могут решиться на внедрение западного ПО после ухода из России иностранных вендоров по нескольким причинам.

Во-первых, иностранные ИТ-решения зачастую обладают более развитой функциональностью и надежностью по сравнению с отечественными аналогами. Например, некоторые аналитические решения, ERP-системы и ряд других продуктов пока не имеют российских альтернатив, которые смогли бы предложить все функции классических западных решений. Это и функции на базе искусственного интеллекта в BI-решениях, и поддержка МСФО для учетных систем, и индустриальные ИТ-продукты, учитывающие требования той или иной отрасли. Особенно трудная ситуация с инжиниринговыми системами CAD/ECAD/CAM/CAE.

Во-вторых, российские компании, работающие на международных рынках, могут быть вынуждены использовать определенное ПО для соответствия стандартам и требованиям своих партнеров и клиентов. Это касается всех решений от систем для ведения международной финансовой отчетности до ERP, которые учитывают тонкости ведения кадрового учета за рубежом.

Кроме того, внедрение иностранных ИТ-решений может быть обусловлено стратегическими планами компании по выходу на новые рынки или повышению эффективности работы. Пока деятельность компании ведется только в России, ей может быть достаточно систем кадрового учета и финансового планирования. Однако при выходе на новый рынок, найме персонала, следовании требованиям нового регулятора, понадобятся ИТ-системы, в которых эта специфика заложена.

КАК ОПРЕДЕЛИТЬ, ПЕРЕВЕСИТ ЛИ ПОЛЬЗА ВНЕДРЕНИЯ ЗАРУБЕЖНОГО ПО РИСКИ

Однако при выборе ИТ-продуктов, разработанных за рубежом, необходимо взвешивать риски.

РИСК 1: САНКЦИИ

В условиях текущей геополитической ситуации внедрение западного ПО может привести к тому, что организация окажется под воздействием санкций. Это будет означать невозможность обновления программного обеспечения, потере технической поддержки и даже отключении системы.

Частично этот риск можно обойти, используя гибридные решения, где ключевые компоненты системы базируются на отечественных разработках, а западное ПО используется только для вспомогательных задач. Таким образом, можно обеспечить независимость от иностранных вендоров критичной для бизнеса ИТ-инфраструктуры и постепенно создавать дорожную карту перевода дополнительных ИТ-компонентов на решения на базе открытого кода или на российское ПО.

РИСК 2: ЗАВИСИМОСТЬ ОТ ИНОСТРАННЫХ ПОСТАВЩИКОВ

Внедрение западного ПО делает компанию зависимой от иностранных поставщиков, что может быть критично в случае изменения политической или экономической ситуации.

Одним из решений может быть использование мультивендорной стратегии, где компания работает сразу с несколькими поставщиками ПО. Также полезно иметь план В, предусматривающий возможность быстрой миграции на отечественные или другие альтернативные решения.

РИСК 3: УГРОЗЫ, СВЯЗАННЫЕ С ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Использование иностранных ИТ-решений несет риск, так как иностранное ПО в некоторых случаях может содержать уязвимости. Самый очевидный вариант - размещение данных российской организации на серверах иностранного вендора за пределами России. В таком случае данные могут быть зашифрованы или слиты, что повлечет за собой потерю репутации и технические вопросы по восстановлению базы.

Для минимизации этого риска необходимо проводить регулярные аудиты безопасности, использовать средства защиты информации и применять лучшие практики по кибербезопасности. Также важно сотрудничать с проверенными поставщиками и использовать только сертифицированное ПО.

За последние два года российские компании реализовали несколько проектов на иностранных ИТ-решениях в области аналитики данных. Во всех этих случаях при выборе платформы проводится тщательный аудит существующей ИТ-инфраструктуры, возможностей самостоятельной поддержки будущей системы, а также функциональные требования того решения, которое ищет компания. В результате обычно совместно с профессиональной компанией-консультантом разрабатывается план по минимизации возможных рисков и создаются аналитические системы на зарубежном ПО, которые помогают компаниям оставаться конкурентоспособными.

Внедрение иностранного ПО в России в 2024 году - это весьма рисковый шаг. Тем не менее в некоторых случаях это может быть необходимо для достижения стратегических целей компании и повышения ее конкурентоспособности. При правильном подходе к управлению рисками и стратегическому планированию компания может успешно использовать западное ПО, минимизируя возможные негативные последствия.