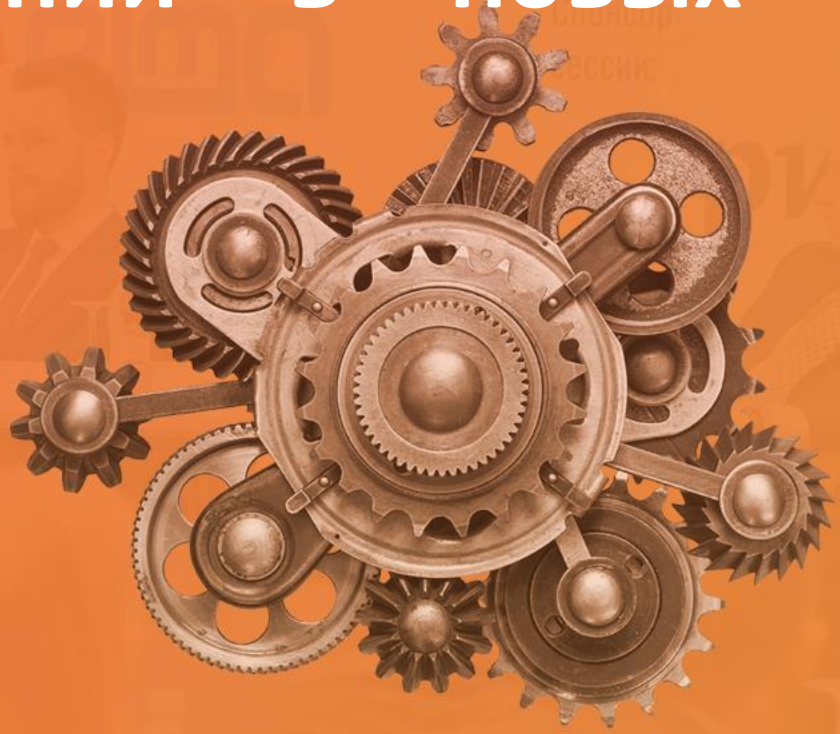
Трансформация ИТ в географически распределенной компании в новых рыночных реалиях

CNews FORUM Кейсы
Опыт ИТ-лидеров



Дмитрий Пшиченко
Директор по информационным технологиям,
Highland Gold Mining

Структурирование ИТ-ландшафта

В качестве первого шага необходимо провести структурирование и актуализацию информации об используемых в компании информационных технологиях:

- ✓ Платформы прикладного программного обеспечения.
- ✓ Программное обеспечение рабочих мест пользователей (АРМ).
- ✓ Оборудование рабочих мест пользователей (АРМ).
- ✓ Системное программное обеспечение (в т.ч. серверное).
- ✓ Вычислительная инфраструктура и СХД.
- ✓ Телекоммуникационная инфраструктура.
- ✓ Оргтехника.

Формирование рисков для компонентов ИТ-ландшафта

Далее необходимо сформировать перечень рисков, связанных с санкциями. Для рисков можно вводить числовые коэффициенты значимости.

Примеры некоторых рисков перечислены ниже:

- Ограничения (запрет) на использование импортных технологий со стороны регуляторов РФ.
- Блокировка зарубежного ПО и оборудования со стороны вендора.
- Запрет на расширение объёма лицензирования.
- Запрет на ввоз технологий в РФ (санкции).
- Прекращение технической поддержки.
- Кража информации.
- Прекращение официальных поставок в РФ.

Оценка рисков для компонентов ИТ-ландшафта

Шаг 1. Проводим качественную оценку угроз для компонентов ИТ-ландшафта (например, «Отсутствует», «Низкая», «Средняя», «Высокая») с присвоением числовых значений [0;3].

Шаг 2. Оцениваем вероятность риска:

- отсутствует [0] - для РФ или свободно распространяемого программного обеспечения.
- низкая [1] – производители из стран, не присоединившихся к санкциям и входящих в политические и экономические блоки с РФ.
- средняя [2] – производители из стран, не присоединившихся к санкциям, но не входящих в политические и экономические блоки с РФ.
- высокая [3] – производители из стран, присоединившихся к санкциям (США, Страны ЕС и др.).

Шаг 3. Оценка рисков для компонентов будет являться произведение угрозы для данного компонента и вероятности риска для данного компонента (max = 9).

Шаг 4. Выбор стратегий реагирования на риски:

- Отказ от дальнейшего развития (фиксация версии).
- Замена поддерживающей организации на российскую.
- Переход на российский аналог.
- Использование аналога из другой страны.
- Локальная сертификация с участием вендора.
- Разработка собственного решения.
- Выкуп прав для самостоятельного развития.

№	Перечень компонентов	Риск	Стратегии
1	Платформа ПО российского производства	0	
2	СУБД производства США, используемая в ERP	9	1. Отказ от дальнейшего использования (фиксация версии) И 2. Выкуп прав для самостоятельного развития ИЛИ 3. Переход на аналог (российский или из другой страны вне санкций).
3	Серверная операционная система производства США, используемая в ERP	9	1. Отказ от дальнейшего развития (фиксация версии) И 2. Переход на аналог (российский или из другой страны вне санкций).

Направления снижения рисков при импортозамещении в в географически распределенной компании в условиях санкционных рисков

1. Выбрать 2-3 вендора оборудования в целях снижения рисков «загрузки» производства российского оборудования и срыва сроков поставов по заказам.
2. Выбрать 2-3 производителей ПО в связи с различными недостатками функционала российского ПО для возможности оценки в «боевых» условиях с учетом требований пользователей, особенностей ИТ инфраструктуры и прикладного ПО (облачные решения\локальные\совместимость и пр.).
3. По ряду ПО (CAD, PLM, PDM, геологическое моделирование) отсутствуют прямые аналоги, что требует подбора решений из нескольких российских программных продуктов, либо разработку\доработку ПО под заказ.
4. Дефицит ИТ персонала и риски потери ключевого персонала в регионах снижаются за счет создания Центров ИТ компетенций в крупных городах (Москва\С-Петербург\Хабаровск и пр.).
5. Сборка АРМ и ноутбуков на заказ для снижения стоимости, сроков поставок и получения гарантии на комплектующие.
6. Закрытие выхода в интернет для ИТ систем и АРМ в целях снижения рисков обновлений, тестирование обновлений в отдельном контуре.
7. Формирование ЗИП оборудования в региональных ключевых точках для исключения риска выхода из строя эксплуатируемого зарубежного оборудования.
8. Переход на российских телеком провайдеров в части спутниковых и обычных каналов связи.
9. Автономная система вместе с блоком собственных IP-адресов для любой организации, имеющей крупную ИТ-инфраструктуру для обеспечения отказоустойчивого доступа к своим ресурсам из сети, а также самостоятельного определения политики маршрутизации.
10. Модернизация и повышение отказоустойчивости собственных ЦОД, РЦОД, либо аренда мощностей у коммерческих ЦОД для обеспечения отказоустойчивости в долгосрочном плане (2-5 лет).

Препятствия к импортозамещению ПО и оборудования

1. Финансы.

ИТ бюджеты ограничены, поэтому, закупив единожды дорогой софт, не все готовы инвестировать в его обновление.

2. Отсутствие по ряду категорий конкурентных отечественных аналогов ПО. Вследствие этого для замены проверенных временем и зарекомендовавшего себя западного ПО должны быть достаточно весомые аргументы.

3. Длительные сроки замены ПО. Сложно взять и заменить ПО, которое создавалось и внедрялось годами. Существующие сложные ИТ-системы и комплексные решения «вросли» в инфраструктуру компаний. Она усложнялась и совершенствовалась долгое время, а для импортозамещения нужно менять практически все.

Риски технологической зависимости в цифровой экономике

ЦЕНТР КОМПЕТЕНЦИЙ ПО ИМПОРТОЗАМЕЩЕНИЮ В СФЕРЕ ИКТ

- С ростом цифровизации возникает риск полной технологической зависимости.
- Помимо рисков безопасности, возникают риски потери компетенций и отставания в технологиях.
- Импортозамещение снижает уровень зависимости и развивает внутренний рынок.

Основная опасность технологического отставания России лежит в области ПО, а не «железа».

Разработка долгосрочной стратегии (концепции) импортозамещения

Совершенствование правил и требований к закупкам, технических и технологических стандартов

Формирование перечня иностранного ПО, подлежащего замене

Уточнение используемых решений при необходимости модернизации ПО

Модернизация прикладного ПО для обеспечения совместимости с отечественным ПО

Тестирование, апробация, пилотное внедрение отечественного ПО, заключение договоров

Формирование предложений по совершенствованию ПО

Разработка плана реагирования на случай введения ограничений или запрета на закупки

**** Фото и рисунки предоставлены ТАСС***

Спасибо за внимание!

Вопросы?

Пшиченко Дмитрий Викторович

E-mail: dmitry@pshychenko.com

Моб. +7-916-669-62-99 (WhatsUp, Telegram)

Канал «CIO» в телеграмм: t.me/CIOCDO

Личный телеграмм (писать сюда): **@DVIPS**