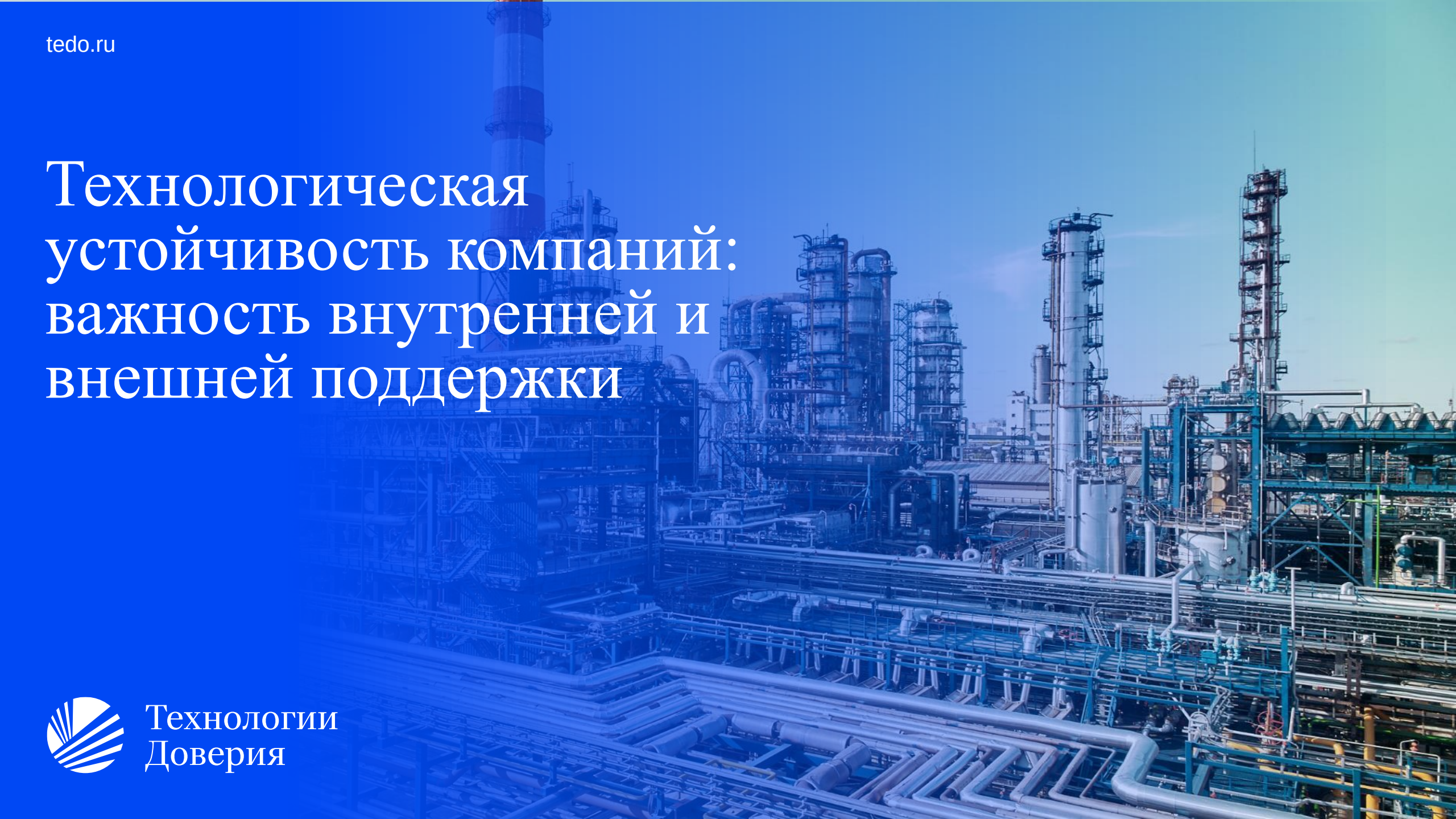
tedo.ru

Технологическая устойчивость компаний: важность внутренней и внешней поддержки



Технологии Доверия

Внешние факторы: Требования регуляторов к технологической устойчивости организаций

Уровни регулирования

Федеральный

Указ Президента РФ № 166 от 30.03.2022 г.

Госкомпаниями и субъектам ФЗ-223 «О закупках товаров, работ, услуг отдельными видами юридических лиц» (в т.ч. организациям электроснабжения), **с 01.01.2025 запрещается использовать иностранное ПО на значимых объектах** критической информационной инфраструктуры

Стратегическим акционерным обществам, системообразующим организациям и субъектам критической информационной инфраструктуры **с 01.01.2025 запрещается использовать средства защиты информации** из недружественных иностранных государств

Постановление Правительства РФ от 20 августа 2022 г. N 1478

Госкомпаниями и субъектам необходимо провести **перекатегорирование объектов КИИ** в связи с обновлением критериев

Постановление Правительства РФ от 20 декабря 2022 г. N 2360*

Госкомпаниями и субъектам необходимо провести **перекатегорирование объектов КИИ** в связи с обновлением критериев

Отраслевой

Отраслевой план Минэнерго РФ от 16 января 2023 г.

Представлен список организационных мероприятий и календарный график по обеспечению готовности заказчиков, согласно которым **к 2027 году должен осуществиться полный переход на российское ПО** на принадлежащих значимых объектах КИИ

Приказ Минцифры России № 21 от 18 января 2023 г.

Утверждены **Методические рекомендации** по переходу на использование российского ПО

*с 21 марта 2023 года необходимо категорировать объекты КИИ, в соответствие с типовым перечнем от Минэнерго

Внешние факторы.

Обеспечение санкционной независимости ИТ является **критично** важным фактором для продолжения **функционирования Компании**

РИСКИ:

1. Прекращение поставки оборудования и запасных частей, а также гарантийного ремонта и обслуживания оборудования
2. Прекращение технической поддержки программного обеспечения
3. Невозможность покупки (продления) лицензий на использование программного обеспечения
4. Ужесточение условий лицензионных соглашений
5. Отключение подписок на информационные сервисы
6. Удаленная деактивация оборудования или программного обеспечения вендором
7. Кибератаки на оборудование или программное обеспечение
8. Отказ работы почтовых служб, сбои в системах резервного копирования

ИТ-ПОСЛЕДСТВИЯ

Прекращение эксплуатации ИТ-сервисов

- немедленное
- по истечении срока действия лицензий, подписки, ключей

Деградация уровня сервиса и технической поддержки

- нарастание сбоев и отказов
- увеличение срока устранения поломок
- отсутствие возможности получения новых комплектующих и запчастей
- возрастание случаев каннибализма запчастей

Невозможность дальнейшего развития (модернизации, тиражирования)

ПОСЛЕДСТВИЯ ДЛЯ БИЗНЕСА

- прерывание производственных и управленческих процессов
- падение скорости операций до «ручного» уровня
- дополнительные затраты на выполнение операций
- невозможность использования агрегированных данных
- снижение качества управленческих решений

Внутренние факторы

САНКЦИОННЫЕ РИСКИ:

1. Недостаток компетенций по отечественным продуктам
2. Ограниченность ресурсов на рынке
3. Функциональные ограничения существующих продуктов. Отсутствие полных аналогов западных решений
4. Высокая стоимость отечественных решений
5. Необходимость пересмотра пользовательского опыта
6. Большой объем внутренней разработки

ИТ-ПОСЛЕДСТВИЯ

Деградация оборудования ЦОД

- быстрое устаревание оборудования ЦОД
- увеличение сроков поставки серверного оборудования по причине высокого спроса
- нагрузка на текущие ИТ-процессы компании из-за ежегодного увеличения спроса
- заморозка ИТ-проектов из-за отсутствия ресурсов
- переквалификация персонала на работу с новым оборудованием

Сложность поддержки внутреннего ПО и технической поддержки

- сложность разработки собственных продуктов
- составление гетерогенных решений на OpenSource
- миграция ИТ-систем в сжатые сроки
- низкий уровень автоматизации
- большое количество точек отказов в работе ИТ-сервисов
- поступление на ИТ-рынок не проверенного ПО временем
- отсутствие квалифицированного персонала на ИТ-рынке
- переквалификация внутреннего ИТ-персонала

ПОСЛЕДСТВИЯ ДЛЯ БИЗНЕСА

- дополнительные логистические затраты на поставку оборудования
- отказ от реализации проектов
- дополнительные затраты на переквалификацию сотрудников
- увеличения штата сотрудников
- уменьшение функционала ИТ-сервисов
- снижение качества предоставления ИТ-сервисов

Основные этапы процесса управления импортозамещением

Общий подход при планировании мероприятий по обеспечению устойчивости Бизнеса

Оценка

Выбор

Доп. итерации (при необходимости)

Доп. итерации (при необходимости)

Доп. итерации (при необходимости)

1 Определение и классификация объектов управления

«Чем мы управляем?»

Результаты:

- Формирование исчерпывающего перечня ИТ-активов (бизнес- системы, категории оборудования) по направлению, с учетом организационного охвата
- Предварительное определение категорий[1] ИТ-активов (структуры работ по направлению), по которому будет осуществляться дальнейшее планирование

Инструменты:

- Существующие в Компании реестры ИТ-активов
- Матрица ИЗ[2] в Стратегии ИЗ

2 Определение исчерпывающего набора рисков по каждому типу объектов управления

«Какие риски мы пытаемся предотвратить?»

Результаты:

- Формирование перечня рисков по каждой категории ИТ-активов, из определенных на предыдущем этапе
- Определение возможных последствий от срабатывания рисков для Бизнеса
- Уточненные категории (при необходимости)

Инструменты:

- Реестр рисков по ИТ- продуктам Компании (результат Стратегии ИЗ)

3 Определение мероприятий для управления рисками*

«Как нам управлять имеющимися рисками?»

Результаты:

- Формирование перечня мероприятий по каждому выявленному риску
- Описание каждого из выявленных мероприятий
- Определение способов реализации каждого из мероприятий

Инструменты:

- Типология мероприятий ИЗ (в привязке к рискам)
- Планы действий, определенные в Стратегии ИЗ

4 Ранжирование выявленных мероприятий и формирование планов действий

«Что нам в результате нужно делать?»

Результаты:

- **Оценка «стоимости» реализации мероприятий**
- **Получение от «Бизнеса» приоритетов и согласование «стоимости»**
- Формирование итогового набора необходимых мероприятий
- Формирование планов действий по каждому мероприятию

Инструменты:

- Типология мероприятий
- ИЗ (в привязке к рискам)

1) Категория – группа ИТ-активов для которых характерны одни и те же риски и будут применяться одинаковые подходы к обеспечению устойчивости
2) Импортозамещение

Технологии Доверия

tedo.ru

«Технологии Доверия» (www.tedo.ru) предоставляет аудиторские и консультационные услуги компаниям разных отраслей. В офисах «Технологий Доверия» в Москве, Санкт-Петербурге, Екатеринбурге, Казани, Новосибирске, Ростове-на-Дону, Краснодаре, Воронеже, Владикавказе, Перми и Нижнем Новгороде работают 3 000 специалистов. Мы используем свои знания, богатый опыт и творческий подход для разработки практических советов и решений, открывающих новые перспективы для бизнеса.