Работа ИБ-вендоров в условиях жёстких санкций

Пресс-конференция РУССОФТ "Российская IT-индустрия: влияние санкций и тенденции развития"

25.03.2022

Сергей Груздев
ген. директор
"Аладдин Р.Д."

Наш опыт корпоративной войны

- То, что сейчас происходит со страной, против нас (Аладдин) было применено в 2012 г.
  - Тогда мы работали с израильской компанией по схеме VAD (Value Added Distribution) - "железо" покупали у них, а прошивки (ПО) переделывали, добавляли в них российскую криптографию и сертифицировали
  - После покупки нашего технологического партнёра американцами (SafeNet, потом Gemalto), ситуация коренным образом изменилась и закончилась "войной" - нам остановили поставки, на всех конференциях от них звучало "Aladdin must die!"
  - Причина? Мы отказались "сдавать" им контакты наших клиентов и вычистили из их продуктов появившиеся там и ставшие нам известные "закладки"
  - Война шла 3 года (активно), потом еще 2
- Процесс замещения зарубежных средств нашими собственными занял
  - Быстро - за 9 мес. - выпустили первую версию, 2.5 года - нормальный полноценный продукт, способный полностью заместить импортный
  - Полностью - 5 лет (отвоевали свои позиции на 70%)
- Потери
  - 40% персонала (перекупили, моральное давление, нервы - "все пропало, сейчас у Аладдина отберут бизнес"...)
  - 50% рынка за 3 года
    - Многие заказчики предпочли остаться на старом импортном продукте и продолжить покупать его у американцев - с закладками! Нам не очень поверили...
    - Многие партнеры (~50%) перевели наших клиентов на продукты конкурента
- Смогли выйти на прежний уровень - через 6 лет

Готовность к импортозамещению - когда всё началось?

- Американцы давно готовились к столкновению
  - ✓ **11.09.2001 - разделило мир на ДО и ПОСЛЕ**
    - Америка развязала себе руки под флагом проактивной борьбы с терроризмом
    - Запустили программы смещения неугодных правительств и получение новых колоний
  - 10 лет, с **2012** г.
    - Cloud Act и PPD-20 (Б. Обама)
    - Закладка в объекты КИИ России "**кибербомб**"
    - Отработка **информационной составляющей ведения гибридных войн** под чужим флагом
    - Отработка технологии "управление толпой"
    - Обязанность всех американских вендоров собирать и передавать в ЦРУ, АНБ, ФБР "**телеметрии**"
    - Запрет на **раскрытие исходных кодов**
    - Право США наносить **кибердары** по любой стране без санкции ООН
    - Ответом на кибернападение на США м.б. **военный удар**
  - 2018 - Трамп - **переход от "Мягкой силы" к "Миру через силу"**
    - Силовое разрешение любых противоречий и угроз доминированию Америки
    - "**Сделаем Америку снова велико**й" - как?
    - В 1971 г. Президент Никсон отвязал доллар от золота и привязал его к нефти - нефть - мировая кровеносная система, кто контролирует продажу нефти, тот контролирует всю мировую экономику
    - За это время ситуация в мире сильно изменилась… Как сегодня можно держать весь мир за горло?
  - ✓ **Сегодня это полупроводники - без них ничего не ездит, не летает, не работает, экономика любой страны просто встанет**
    - Контроль за производством полупроводников - вот новая цель Америки, ради которой и затеян весь этот очередной передел мира

Наш опыт и наши продукты для импортозамещения

- Озаботились этой проблемой с 2012 г. - 10 лет назад
- Что поняли для себя? Какие уроки извлекли из нашей "войны"?
  - Эпоха наложенных средств защиты проходит, нужны **встраиваемые** глубоко интегрированные решения - в железо, в ОС, в экосистему
  - Windows, с её новой концепцией - не для нас!
    - Уход от понятия версии и переход на постоянные обновления, сбор "телеметрии", навязывание бесплатных встроенных средств ИБ - BirLocker и пр., периодические глубокие обновления с отключением всех средств защиты, раздача обновление с локальной обновленной станции (даже в закрытых контурах сети без подключения к сети Интернет и т.д.) - было понятно для чего всё это делается, был лишь один вопрос - когда всё это "рванет"?
    - Переход (импортозамещение) будет долгим и тяжелым, придётся **параллельно** работать в двух системах - Windows и Linux
    - Нужны решения для защиты **главных информационных активов**
      - **Баз данных** (а их всегда оставляют "на потом") - для Postgress, Oracle, MS SQL - импортозаместили встроенные в них американские средства защиты на наши - опровославили (ведь не всегда можно быстро заменить эти СУБД)
      - **Данных на дисках** (системы прозрачного шифрования американцы выкосили с рынка еще в 2009 г.)
    - В первую очередь нужны **инфраструктурные** решения - сделали ставку на них:
      - **Сервер многофакторной аутентификации** (хит сезона - JAS) - сейчас, после блокирования аналогичных зарубежных продуктов, все дружно рванули к нам
      - **Система централизованного управления** средствами ИБ (JMS - сделали версию под Linux, получили сертификат под ГТ до СС)
      - **Центр выпуска и обслуживания сертификатов** для корпоративной PKI (телеком, IoT, сервера, пользователи) - **под Linux** (идёт сертификация под ГТ/СС)
      - Средства **защиты данных от утечки** (прозрачного шифрования) для серверов, ПК, СХД (Windows/Linux - сертификат под ГТ/СС)

✓ **Все они должны входить в экосистему Linux и быть глубоко интегрированы**

Наш опыт и наши продукты для импортозамещения

- Что сделали?
  - Мы отработали технологию сборки ПО из **единых** исходников и для Windows, и для Linux
  - Что это даёт: **нет различий и отставания** версий для Linux, проще переезжать, не надо переучиваться и привыкать к новой системе
  - Все наши продукты способны работать в сложных **гетерогенных** сетях
  - Для управления - единая система **централизованного** управления с единым **хранилищем** (ресурсная база для разных служб каталогов), экономия ИТ-ресурсов на администрирование и автоматизация рутинных операций
  - Прорабатываем включение всех наших продуктов в **репозитории** и экосистемы Linux
  - Что это даёт: **100% совместимость**, в т.ч. с новыми версиями - синхронизацию обновлений
    - Перекрёстное тестирование, сертификаты совместимости
  - **Единая универсальная лицензия для Windows и Linux**-версии продуктов (мягкая миграция) - **экономия бюджетов**
  - Сертификация всех продуктов как **непрерывный процес**с - работает как конвейер (на УД-2 для работы с ГТ)
- Во время пандемии
  - Отработали совместное **решение для безопасной дистанционной работы** сотрудников, позволяющее организовать удалённую работу с ГИС до 1й категории, АСУ ТП, ИСПДн
  - Что это: недорогой терминальный **клиент на USB-токене** LiveOffice для подключения и работы с любого ПК (в т.ч. личного/домашнего) в ИС организации

Исчерпаны ли санкционные возможности?

- Текущие санкции - это вершина айсберга...
- Что у нас делали все эти годы?
  - Следовали навязанным "лучшим практикам"
  - Переносили вычислительные мощности в ЦОДы (и в облака)
    - Его легче грохнуть или вырубить - все данные в одном месте...
    - Все базы - как правило, на СУБД Oracle
  - Подсаживались на сервисную модель (SaaS)
    - Так легче все отрубить одним махом...
  - Переходили на ПО по подписке / в облаке
  - Перенимали "прогресс" - ПО как непрерывный процесс улучшения (постоянные обновления) - отказ от версионности ПО (Windows)
    - Накатив новое обновление можно всё вырубить
    - Раздача обновлений без выхода в Интернет - от обновленной версии
  - Привыкали к сбору "телеметрии" - а что тут такого?
    - Сбор информации о "железе", об установленном ПО
  - Использовали для защиты своей информации (от американцев) американские же (европейские, израильские) СЗИ
    - Сейчас они начинают массово окирпичиваться...

Исчерпаны ли санкционные возможности?

- Где мы храним свои ключи, коды доступа, пароли (в т.ч. от своих банковских счетов), данные платёжных карт (вкл. CVV)
  - В хранилище браузера / Google
  - В "Связке ключей" / Apple
  - В эл. записной книжке смартфона
  - ✓ **Кто-нибудь уже поменял свои пароли и данные карт?**
  - ✓ **Кто-нибудь уже перешел на 2ФА?**
  - ✓ **Что они могут сделать с нашими деньгами?**
- Боюсь, что пока это только цветочки…
  - Тотальная нехватка электроники
  - Блокирование аппаратуры, эл. сервисов и ПО
  - Активация закладок в ПО и в железе (уже видим первые "окирпичивания")
- Нам не впервой - выживем, сделаем своё, окрепнем!