Трансформируем IaaS провайдера

Введение

Первое место работы — это то что многие вспоминают с теплотой и ностальгией. Позади ВУЗ и впереди интересная карьера в области информационной безопасности. И особенно хорошо, когда есть выбор!

Перспективный специалист всегда нарасхват и может придирчиво выбирать. Конечно, не стоит питать иллюзий, абсолютное большинство сменят место работы в течение 3-5 лет.
Как же выбрать первое место работы? Многие выбирают крупные и стабильные компании — там отличная социалка, есть бюджеты и вроде бы интересные задачи. Но есть и много минусов, например, в крупной компании все процессы слишком зарегулированы и всегда существует непробиваемая вертикаль руководства.
С другой стороны — в маленькой компании многое даётся проще. Возникла интересная идея или задача — можно в течение пары часов назначить встречу с директором и получить «зелёный свет». Отличный простор для творческой личности! К плюсам также можно отнести меньшее внимание государственных регуляторов и практически полное отсутствие аудитов. По крайней мере, пока малая компания не станет достаточно крупной.
В маленькой компании можно сосредоточиться на решении практических задач, а не написанием бесконечных бумаг. Конечно, есть и много минусов.
Некоторые специалисты предпочтут именно маленькие компании, а ещё лучше — компании друзей.
И наш герой — именно такой. И прямо сейчас он идёт на собеседование в модную кофейню с директором и CIO компании, заинтересованной в нём.
Вы хорошо знакомы с этими людьми — они учились в параллельном потоке на смежной специальности. В общем, всё выглядит как встреча друзей, но все пытаются быть серьёзными.

Знакомство

Итак, компания называется **PPCS**. И в ней работают пока только два сотрудника:

- **Александр Дронов** — директор и сооснователь компании;
- **Звягинцев Павел** — CIO и сооснователь компании.

Вы: ребята, привет! Рад видеть! Ну что, дожили до того, что вы меня собеседуете? Никогда бы не подумал!

Александр Дронов: Привет! Жизнь — непредсказуемая штука. Помнишь, на втором курсе, я подрабатывал системным администратором на кондитерской фабрике? Я им быстро наладил инфраструктуру, но потом просто стало некогда ездить туда на работу. В это время я уже познакомился с будущей женой и ездить туда-сюда на разные концы города стало сложно. Да и что делать на этой фабрике? Пустая трата времени — десяток старых серверов. Но это лишь на первый взгляд. Ребятам из фабрики было тяжело найти мне замену, и тут я подумал...А что если перевести отношения на новый уровень? Может быть оказывать им услуги по договору, вместо того чтобы работать в штате? И взять на себя не только администрирование их софта, но и железо. И тут мы встретились с Пашей у меня дома, заказали пиццу и устроили мозговой штурм...

Звягинцев Павел: Да и тут появляюсь я. Меня вначале удивило, что у Саши получилось договориться на такой формат работы. Похоже на настоящий бизнес — мы можем размещать у себя серверы компаний и администрировать их за деньги. И это можно масштабировать — таких заказчиков можно найти много. ОК, я договорился арендовать небольшой угол в бывшем машинном зале провайдера - после модернизации телефонных АТС, у них появилось много площадей для аренды.
Я взял на себя техническую составляющую — купили недорогой стеллаж для серверов, поставили ИБП. И вот мы готовы к приему миграции в наше облако!

Александр Дронов: Но тут нельзя забывать про оборудование. Мы смогли получить льготный кредит для малого бизнеса и закупили несколько бывших в употреблении серверов, коммутаторы и маршрутизаторы. Провайдеров Интернет мы провели льготно, на площадке они уже были. И вот — наш PPCS запустился с первым заказчиком. И это та самая фабрика.

Вы: Что такое PPCS?

Александр Дронов: Pied Piper Commodity Service. Крутое название, да?

Вы: Безусловно. Ну что же в итоге? Звучит как небольшая компания с парой сотрудников и с клиентами из малого бизнеса. Для чего вам я?

Звягинцев Павел: Мы не такие уж и маленькие теперь. Впрочем, всё по порядку. Пока ты учился и классно проводил свободное время, мы упорно работали.
Опыт первого клиента нам сильно помог дальше. Мы поставили пару «Микротиков» — один у нас, другой на фабрике — и начали миграцию. Постепенно перетащили все 20 серверов — что-то мы виртуализовали, что-то обновили от совсем уж старого софта, в общем за полгода управились. Дополнительно, настроили им резервное копирование и также стали

продавать как услугу с ежемесячной платой. Заказчику понравилось! В итоге, сарафанное радио также сыграло свою роль.

Александр Дронов: Давай теперь я продолжу. Итак, к нам пришли еще пара клиентов. Но это уж совсем микробизнес — ребята из бизнес-центра рядом с фабрикой. Это недорогой бизнес-центр, и арендаторам нужны совсем базовые услуги — где-то резервное копирование у нас, где-то небольшие сервисы нужно поднять. Платят они немного, но все же это тоже клиенты, и их довольно много. Но с ними и проблем много! Конечно, никаких айтишников у них нет, и они постоянно ловят вирусы, становятся жертвами DDoS-атак и прочих неприятностей.
Один раз даже столкнулись с тем что их всех разом зашифровали — кто-то скачал зловред, и он распространился по всем организациям. В основном целью зловреда были базы 1С. Кое-как уладили, что-то удалось восстановить, а что-то нет. В общем, пришлось немного поработать бесплатно.

Вы — да уж, проблемные клиенты. Чтобы с этим жить, нужны специалисты и бюджеты. Судя по всему, у них нет бюджетов на безопасность.

Звягинцев Павел: Конечно нет. Те, у кого есть, это, к сожалению, не наши клиенты, по крайней мере, сейчас. Но это еще не конец истории.

Александр Дронов: Как обычно, знакомства решают! Итак, хотелось масштабировать бизнес до нормального облачного провайдера с крутыми оркестраторами, серверами с GPU и прочими атрибутами. А для этого нужны нормальные клиенты. Итак, мы стали их искать. Полгода не удавалось, но мне улыбнулась удача!
Итак, нашелся солидный заказчик. Знаешь такую платежную систему — МРТ?

Вы: Слышал, Международный расчетный терминал. В последнее время, в связи с санкциями, они хорошо растут.

Александр Дронов: Да, точно, растут. И у них есть задача — DR-сайт. Проще говоря, это резервная площадка МРТ, которая будет включаться при недоступности их основных ЦОД. И мы договорились, что будем это организовывать!

Вы: Вау, звучит, конечно, круто. Но, ребята, тут есть много нюансов и подводных камней.

Звягинцев Павел: Понимаем. Какие ты видишь тут риски?

Вы: у платежных систем довольно серьезные требования к доступности и безопасности. И есть регуляторы, проверяющие эти требования. Судя по

вашему рассказу, с бюджетами у вас довольно плохо. Вы уверены, что сможете работать с таким заказчиком на должном уровне?

Александр Дронов: Думаю, ты нам поможешь.

Вы: Спасибо, не думал получить предложение прямо на собеседовании. Но если серьезно — придется много вкладывать в покупку лицензий и разного дорогого оборудования. Здесь микротиками и серверами с Авито не обойтись.

Александр Дронов: Да. И самое главное — МРТ понимает ситуацию и готовы делать инвестиции в наш PPCS. В дальнейшем они рассчитывают, что мы будем отлично выполнять и задачи МРТ, и привлекать клиентов как солидный облачный провайдер.

Вы: звучит, как будто вы сорвали джекпот. И деньги на игрушки, и развитие бизнеса. Саша наверное планирует новую Теслу купить.

Александр Дронов: Хотелось бы, но всё не так просто. Все инвестиции должны согласовываться с Департаментом информационной безопасности МРТ. Боюсь, они Теслу не согласуют. Но на хорошие дела денег дадут. Но вот наша основная проблема — мы не можем с ними разговаривать на одном языке. Павел их вообще не понимает, а ты не прогуливал занятия.

Вы: теперь понятно. Вы готовы меня нанимать? Обсудим условия?

Александр Дронов: Конечно! Готовы прямо сейчас, но есть нюансы.

Вы: как обычно...Выкладывай.

Александр Дронов: если ты занимаешься ИБ в PPCS, твою кандидатуру нужно согласовать с инвестором — МРТ. Лично у нас нет бюджетов ни на тебя лично, ни на необходимое железо и софт. Нужно встретиться с куратором из ДЗИ МРТ и представить им твою кандидатуру вместе с планом работ на первый год и твоим видением архитектуры безопасности.

Вы: звучит заманчиво. Но, как обычно, не всё оказалось так просто. Получается, что для найма нужно сделать тестовое задание?

Александр Дронов: Послушай, давай смотреть чуть выше вопроса найма. Сейчас фактически мы сможем круто трансформировать нашу компанию. И мы рассматриваем тебя не просто как наемного работника, но и партнера, с кем сможем дальше выстраивать работу и развивать систему защиты. Фактически, сейчас мы в той ситуации что от безопасника зависит сможем ли мы получить инвестиции.

Вы: хорошо. Давайте подумаем как обосновать и попробуем подготовить презентацию.

Звягинцев Павел: Мы знали что, тебе будет интересно! Итак, давай поговорим о том что есть сейчас.
Кажется, что ты уже понимаешь, как устроен старый PPCS. У нас одна площадка, несколько маленьких маршрутизаторов и серверы с виртуалками. Виртуализация сделана на пиратской Vsphere 7. Глобально, в старом PPCS есть пара десятков виртуальных серверов кондитерской фабрики. А еще есть предельно токсичный сегмент с мелкими клиентами — там около 50 ВМ. Честно говоря, если ДЗИ МРТ это увидит, они не захотят с нами работать. Но мы будем сохранять этих клиентов.
Главная проблема — один клиент может поймать вредонос, и он распространится по сети на остальных. С таким уже сталкивались.
Еще в старом PPCS есть доступ в интернет — каждому клиенту мы выделяем отдельный белый адрес и они просто публикуют свои серверы в интернет.
А с фабрикой у нас есть VPN через «Микротики».
В общем вот, такой старый PPCS. Но есть и новый — и он в проекте.
Что мы уже продумали - поставим три новых стойки в том же помещении, закупим за счет инвестиций МРТ. Для серверов будет виртуализация и SDS от российского производителя. Сеть — высокопроизводительные коммутаторы Yadro.
Будет прямой канал связи с ЦОД МРТ — прямой оптический канал, предоставляет городской провайдер. Так называемая «темная оптика» — полностью и только для нас.
Еще МРТ хотят иметь на площадке PPCS прямой доступ в интернет. Это тоже важное требование и его следует продумать.

Вы: Круто, а может у вас еще схемы есть? Или некогда было?

Звягинцев Павел: Обижаешь, кое-что есть! Но куратор от ДЗИ МРТ ожидает от нас уже проектируемую схему с новым PPCS и правильной безопасностью.

Александр Дронов: Паша, а у нас будет возможность встретиться с куратором ДЗИ МРТ для обсуждения задачи? Хотя бы по видео поговорим.

Звягинцев Павел: Думаю, можно, но там, как обычно начнется давление по срокам и прочие нюансы. Но давай попробуем.

Вы: Отлично. Назначайте встречу на ближайшие дни, я пока попробую проанализировать схемы.

Встреча в кофейне закончилась на позитивном тоне. Кажется, что ребята предлагают интересную и перспективную работу. Для начала карьеры это прекрасно, а может и не для начала.
Уже дома эйфория слегка спала и начались конструктивные мысли. По сути, решение о найме и об инвестициях в облачный провайдер PPCS принимает инвестор, а точнее — куратор от Департамента защиты информации МРТ. Но в случае благоприятного впечатления от презентации планов можно рассчитывать на хорошую зарплату и хорошие бюджеты на проект.

Итак, смотря на схему, Вы смогли идентифицировать большое количество проблем «старого PPCS». Эти проблемы необходимо решать, и хорошо, если их решение впишется в инвестиционный бюджет.

Попробуйте обозначить и кратко объяснить три главные проблемы «старого» PPCS:

Анализ проблем существующей инфраструктуры:

Проблема №1_____
Проблема №2_____
Проблема №3_____

Встреча с сотрудниками ДЗИ МРТ

На следующий день позвонил Александр Дронов.
Александр Дронов: Привет! Как дела? Нам удалось договориться с куратором от ДЗИ МРТ о коротком звонке на полчасика. Он как обычно сильно занят, такой солидный и чопорный. Зовут Морозов Дмитрий Николаевич. Завтра в 14.30, прошу быть чуть заранее.
Вы: Принято! Давай.

Итак, на следующий день произошел конструктивный диалог.

Александр Дронов: коллеги, добрый день! Дмитрий Николаевич, рад сообщить, что в нашей команде пополнение — теперь у нас есть эксперт по информационной безопасности и он хотел бы обсудить с Вами ключевые для ДЗИ МРТ требования.

Дмитрий Николаевич Морозов : коллеги, здравствуйте! Честно говоря странно что в команде появился безопасник только сейчас. На этой встрече я уже рассчитывал увидеть проект презентации для согласования. Мы его вообще дождемся?

Знакомая ситуация со времен учебы в универе. Как обычно, все курсовые работы начинают делаться около дедлайна. Оказывается, и в работе так. Кто бы мог подумать?

Саша же использовал тоже знакомый прием:

Александр Дронов: Дмитрий Николаевич, мы буквально заканчиваем презентацию и решили усилить нашу команду для финальных корректировок.

Конечно, за презентацию еще никто не брался.

Дмитрий Николаевич Морозов: хорошо. Давайте обсудим какие вопросы.

Вы: Дмитрий Николаевич, давайте попробуем уточнить требования. Я уже детально ознакомился со схемами PPCS, обсудили с CIO технические вопросы. Хотелось бы финально уточнить требования по безопасности.

Дмитрий Николаевич Морозов: ничего себе, вы обсуждали с CIO вопросы шкафов и каналов связи? Ну что ж, это круто.

Конечно, Морозов отлично разбирается в людях и понимает, что PPCS — всего лишь небольшая команда энтузиастов, получивших хороший проект. Но в маленьких командах энтузиастов много преимуществ — в первую очередь, мотивация. Но их нужно научить работать.

Дмитрий Николаевич Морозов : хорошо, коллеги. Надеюсь что в последний раз попытаюсь сформировать требования.

Итак, у нас резервная площадка на вашей инфраструктуре. Мы не собираемся на этой площадке хранить и обрабатывать платежные данные, по крайней мере в обозримой перспективе. Но персональные данные наших сотрудников там будут, поэтому требования 152-ФЗ будут в полный рост, и мы ожидаем от вас принятия технических мер.

С документационными требованиями мы согласны взять на себя.

Особое внимание обратите внимание на сетевую безопасность. У нас будет прямой канал, но нужно предусмотреть криптографическую защиту.
На площадке мы ожидаем интернет для некоторых сервисов. Нужно сделать доступ безопасным, архитектуру решения ожидаем от вас.

Вы: Разумно. Что-то еще?

Дмитрий Николаевич Морозов: Физическая безопасность оборудования, выделенного под нас. Мы понимаем, что PPCS будет развиваться как облачный провайдер и туда могут приходить самые разные клиенты. В том числе приходить в ЦОД.
Наше оборудование должно иметь физическую защиту. Продумайте что для физической защиты можно сделать и включите в презентацию.

Важно: если есть какие-то требования, которые мы можем закрыть для площадки средствами МРТ, — предлагайте. Например, отдельную SIEM систему ставить точно не нужно, возможно подключить к нашему. Ну и всё в этом духе.

Александр Дронов: Дмитрий Николаевич, спасибо за уточнение. В ближайшее время постараемся представить презентацию для обсуждения. И сразу же хотелось обсудить закрытие вакансии специалиста ИБ. И условия, конечно.

Дмитрий Николаевич Морозов : хорошо. Коллеги, я напоминаю о необходимости строго следовать срокам проекта. У нас есть практика — мы включаем в договоры с подрядчиками штрафные санкции за нарушение сроков. Пока этого у нас нет, но в дальнейшем можно получить штраф.

Итак, разговор закончился.

И сразу сформировался пул вопросов, требующих решения:

1. За нами (PPCS) — все технические вопросы по соответствию 152-ФЗ. Нужно дополнить схему техническими решениями и быть готовым к разным сложным вопросам. Хорошо, что коллеги из МРТ готовы помочь с бумагами.
2. Техника все еще не доработана. Неясно, как подключить офис МРТ через имеющийся канал связи и предоставить интернет. Нужно это продумать и нанести на схему нужное оборудование для решения этой задачи.
3. Звучал тезис про физическую защиту. Вполне логично, что оборудование, где хранятся данные МРТ, нужно защитить от несанкционированного доступа. Но как это сделать?

Разговор с сотрудником департамента развития бизнеса

На следующий день раздался звонок Александра:

Александр Дронов: привет! Как поживает наша презентация? Мне снова звонили из МРТ, просили поскорее назначить встречу. Кстати, ты умеешь завязывать галстук? Последний раз на выпускной мне завязывал отец.

Вы: Мы должны будем пойти в офис МРТ? Там есть дресс-код?
Александр Дронов: Конечно, всё должно быть в лучшем виде. Ну, вы технари, можете чуть ослабить требования. А менеджеру нужно выглядеть строго.

Вы: Нелегко, конечно, быть руководителем. Итак, встреча с Морозовым?

Александр Дронов: Если бы только с ним! Будет целый инвестиционный комитет, где будут разные специалисты, обсуждать наш проект и просматривать с разных сторон — нужно соблюсти интересы и ИБ и ИТ, и бизнеса. В общем, всё сложно.

Вы: И к чему мне готовиться?

Александр Дронов: Давай устроим краткий созвон с еще одним сотрудником МРТ. Это Юлия Вессель. Она из департамента развития бизнеса и введет тебя в курс дела.

Через короткое время снова на видеоконференции.

Александр Дронов: Юлия, добрый день! Хочу представить нашего специалиста по информационной безопасности. Он сейчас работает над презентацией для инвестиционного совета МРТ.

Оказывается, будет целый инвестиционный совет. Очень похоже на защиту дипломной работы, а я надеялся, что навсегда прошел этот этап.

Разговор продолжился:

Юлия Вессель: очень приятно, я — Юлия. Проектный директор в департаменте развития. Насколько я понимаю, у вас простой проект, но если вы впервые на комитете, то лучше знать некоторые моменты.

Александр Дронов: Юлия, здорово, что Вы с нами. Что бы мы делали...

Юлия Вессель: Коллеги, на комитете нужно показать презентацию. Там будут и технари, и представители бизнеса. Пока мы не ожидаем от вас подробного

бизнес-плана, но понимание того, как будет развиваться ваш бизнес просто необходимо. Расчёты окупаемости инвестиций и прочие скучные вещи я помогу вам сделать на следующих этапах. Но пока вы должны понимать, мы не должны быть единственным вашим заказчиком, хотя, и возможно, ключевым. Постарайтесь в презентации отразить ответы на следующие вопросы:

- какие услуги на рынке вы будете предлагать на рынке;
- опишите компанию, являющуюся вашим потенциальным клиентом;
- в случае успеха, как вы будете масштабироваться?
- какие риски, помимо рисков ИБ вы можете назвать для бизнеса и кратко опишите, что с ними делать.

Пожалуй, это всё. Имейте в виду, это лишь первая встреча и вам придется еще долго править презентацию и проект, перед тем как сможете получить первую часть инвестиций. Но, уверена, вы справитесь.

Вы: спасибо, Юлия. Мы дополним презентацию и попробуем пройти этот нелёгкий путь.

Юлия Вессель: Это лишь первый проект, он всегда самый сложный. Дальше будет тоже сложно, но интересно. Но, всем пока, я должна бежать на новую встречу.

Александр Дронов: Юлия, до скорой встречи! Спасибо.

Итоги

Итак, появилось понимание, как должна выглядеть презентация.

1. Нужно показать инвестиционному комитету то что есть сейчас. Указать что сейчас у нас есть проблемы, но желательно описать их в дипломатичном ключе. У всех есть недостатки, но мы с ними работаем.
2. Нужно представить видение выполнения требований ДЗИ, высказанных Д.Н. Морозовым.
3. Нужно представить видение выполнения требований Юлии Вессель.
4. Подготовиться к неудобным вопросам комиссии.

Хм, и моя зарплата также зависит от результатов комитета. Возможно, стоило как-то иначе начинать карьеру? Но упорство и целеустремленность всегда были с Вами. Попробуем сделать отличный проект.