Приветственное слово

Сергей Кирюшин

Главный редактор Учебника 4CIO,
член Совета Клуба 4CIO

Уважаемые коллеги!

Вашему вниманию предлагается специальная версия Учебника 4CIO, выпущенная к XII Конгрессу «Подмосковные вечера».

В неё вошли новые главы, написанные в 2018 году, а также несколько обновленных глав первой версии Учебника, которые не были опубликованы в прошлогодней версии, выпущенной к XI Конгрессу.

К работе над Учебником неизменно привлекаются высокопрофессиональные CIO и известные эксперты рынка.

Работа продолжается, в ближайшее время будет подготовлена к выпуску печатная версия Учебника 3.0, и мы будем очень рады новым авторам и новым идеям — присоединяйтесь к нам!

Алексей Кравченко

Директор управляющего офиса
Клуба ИТ-директоров 4CIO

Мы ведём проект «Учебник 4CIO» с 2010 года. За это время много что изменилось в жизни и в ИТ, а вместе с этим — и в версиях Учебника. Неизменным остаётся одно — желание опытных CIO делиться с товарищами своими знаниями и опытом. При этом, авторы делают это на безвозмездной основе, что укрепляет основную идею нашего сообщества: готовность делиться.

Я хочу выразить огромную благодарность всему авторскому коллективу, а также всем поименно за такой вклад в продолжение развития проекта. Хочу также поблагодарить и всю административную команду — редакторов, корректоров, дизайнеров, верстальщиков.

Мы все большие молодцы, и вот очередной выпуск Учебника перед Вами, дорогие читатели. Читайте, учитесь на опыте других, принимайте участие в развитии проекта, мы всегда рады новым идеям и новым авторам!

Александр Селютин

Выпускающий редактор
Учебника 4CIO

Уважаемые начинающие CIO!

Жизнь не стоит на месте. И уж тем более, на месте не стоят технологии и подходы к реализации ИТ-задач... Автоматизация... Информатизация... Цифровизация... Не за горами, видимо, квантизация...

Однако, устремляясь вперёд, не стоит отбрасывать всё, что помогало (и работало) раньше.

Поэтому в редакцию Учебника 4CIO ПВ-2018 вошли как описания инструментов, которые уже давно зарекомендовали себя и успешно применяются много лет, так и тех, которые только сейчас входят в профессиональную деятельность CIO. Или уже CDO? Уверен, предложенный материал заинтересует и тех, и других!

А я от коллектива авторов хочу пожелать Вам успехов в профессиональной деятельности! В добрый путь!

Оглавление

Часть 1

Введение

Глава 1.1

От CIO — к CDO

Евгений Борисов

Цифровая экономика и цифровая трансформация

Мир быстро вошёл в новую эру – эру цифровой экономики. Мы видим проявления новой цифровой экономики во всех аспектах жизни: Интернет доходит в самые дальние уголки страны, датчики и сенсоры интегрируются не только в дорогое промышленное оборудование, но и в бытовые приборы, мебель, одежду, предметы интерьера, автомобили. Более того, все эти приборы и устройства начинают взаимодействовать между собой на основе протоколов Интернета вещей без участия человека. Появляющиеся технологические платформы убирают посредников между производителем и потребителем продукта или услуги, а накапливающиеся объёмы данных позволяют предсказывать поведение машин и людей. Дети с рождения становятся пользователями компьютеров, смартфонов, планшетов и часто не представляют свою жизнь без социальных сетей. Весь мир у них находится на кончиках пальцев, любая потребность быстро реализуется нажатием на экран девайса в любом месте и в любое время. В 2017 году количество представителей нового поколения Z (родившиеся после 1995 года) составило 27% населения земли. По статистике сайта internships.com, к 2020 году поколение Z составит уже 40% покупательской аудитории мира.

В утверждённой в России «Стратегии развития информационного общества РФ на 2017-2030 годы» дано следующее определение цифровой экономики: «Цифровая экономика – это хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объёмов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг».

Объём цифровой экономики по состоянию на начало 2018 года в мире составил 3 трилли-

она долларов США, что эквивалентно 30% от индекса S&P500 или равно валовому внутреннему продукту (ВВП) Великобритании. Цифровая экономика, появившись всего около 20 лет назад, продолжает набирать обороты, а проникновение технологий во все аспекты нашей жизни стирает грань между понятием «экономика» и понятием «цифровая экономика». Согласно разработанной ФРИИ (Фонд развития интернет-инициатив, официальный сайт iidf.ru) при участии Центра макроэкономического анализа и краткосрочного моделирования и других партнёров «Стратегии развития экосистемы цифрового предпринимательства», экономика России в 2018-2030 годах будет генерировать опережающий спрос на продукцию ИКТ отрасли, доходя до 30 трлн рублей в год к 2030 году, отвечая на который доля ИКТ сектора в ВВП вырастет с 2,6% в 2016 году до 5,4 % к 2030. По оценкам McKinsey, доля цифровой экономики в ВВП России по состоянию на 2017 год составляет 3,9%, но опережает ВВП в темпах роста. Так, с 2011 по 2015 годы ВВП России вырос на 7%, тогда как цифровая экономика прибавила 59% или 1,2 трлн руб.

В 2017 году в России принята государственная программа «Цифровая экономика», в ней поставлены цели и прописан большой набор мер по созданию условий для цифровой трансформации экономики: в части нормативного регулирования, развития инфраструктур связи, безопасности, научных заделов и кадрового обеспечения. Это условия и, своего рода, основа, на которой могут разворачивать свои проекты крупные корпорации, органы власти, малые инновационные технологические предприниматели, образовательные учреждения и другие участники рынка.

В соответствии с программой развития цифровой экономики, к 2025 году 97% российских домохозяйств должны иметь широкополосный доступ в интернет. Во всех городах с населением от 1 млн человек должны быть развёрнуты сети 5G. Планируется также, что до 2025 года в России появятся десять предприятий в сфере высоких технологий и столько же цифровых платформ для основных отраслей экономики, а вузы будут выпускать более 100 тыс. специалистов в сфере IT в год.

Цели Программы «Цифровая экономика Российской Федерации:

1. Создание экосистемы цифровой экономики Российской Федерации, в которой данные в цифровой форме являются ключевым фактором производства во всех сферах социально-экономической деятельности и в которой обеспечено эффективное взаимодействие, включая трансграничное, бизнеса, научно-образовательного сообщества, государства и граждан.

2. Создание необходимых и достаточных условий институционального и инфраструктурного характера, устранение имеющихся препятствий и ограничений для создания и (или) развития высокотехнологических бизнесов и недопущение появления новых препятствий и ограничений как в традиционных отраслях экономики, так и в новых отраслях и высокотехнологичных рынках.

3. Повышение конкурентоспособности на глобальном рынке как отдельных отраслей экономики Российской Федерации, так и экономики в целом.

Традиционные, или назовём их «аналоговые», компании, которые не адаптировались под работу в новых условиях цифровой экономики, имеют шанс не только стать жертвами так называемого disruption со стороны технологических стартапов, но и просто могут оказаться в ситуации, когда не смогут найти новых сотрудников, предпочитающих работу

в модных цифровых компаниях. По прогнозу президента компании Cisco Systems Джона Чэмберса, в течение 10 лет исчезнут 40% компаний, которые мы видим сегодня, при этом 70% существующих компаний попытаются трансформироваться под новые условия цифровой экономики, но лишь у 30% из них это получится.

В соответствии с ежегодным опросом Deloitte, проведённом среди директоров по маркетингу крупнейших корпораций, 87% компаний ожидают, что их бизнес столкнётся с disruption со стороны технологических стартапов. При этом 30% компаний верят, что они обладают необходимыми навыками и качествами, чтобы перейти на цифровую бизнес-модель.

В мире уже немало примеров корпораций, которые, не смогли перестроиться и потеряли рынок – Lockbuster, Blackberry, Nokia, Motorola, MySpace, Friendster, Kodak. Ну и огромное количество обратных примеров, когда небольшие стартапы за несколько лет выросли в огромные корпорации и потеснили бывших лидеров в рейтинге по капитализации рынка – Apple, Alphabet (Google), Microsoft, Amazon, Facebook. Всего 24% компаний из Fortune 500, которые были на рынке 25 лет назад все ещё сохраняют свои позиции в рейтинге (Рис. 1.1.1). Цитируя отчёт McKinsey&Company «Инновации в России – неисчерпаемый источник роста»: «В современной реальности инновации нужны бизнесу не только для ускорения темпов развития, укрепления лидерства и отрыва от конкурентов, но и для своевременной защиты от ущерба для отрасли в случае внедрения радикальных инноваций, делающих экономически нецелесообразными целые направления бизнеса».

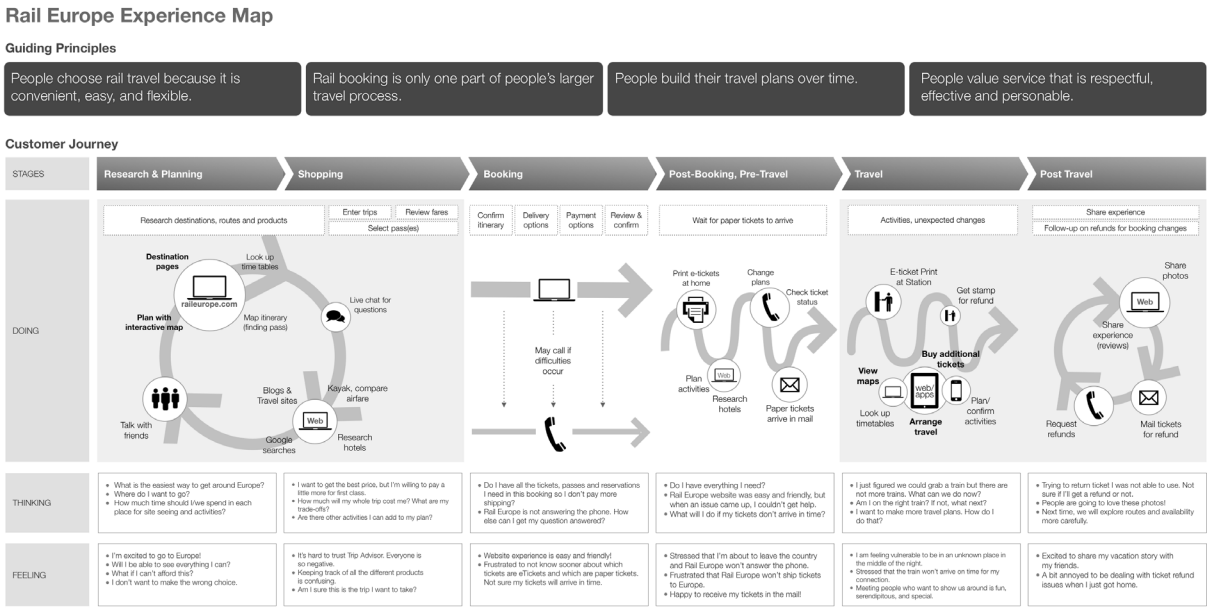
Возможность резкой потери доли рынка, изменение паттернов потребления у нового поколения и рост его численности, возрастающий спрос на цифровые продукты и услуги, появление новых бизнес-моделей – эти и другие факторы сделали цифровую трансформацию задачей №1 на повестке дня компаний, образовательных учреждений и органов власти. По отчёту IDC, мировые затраты на цифровую трансформацию в 2017 году уже достигли 1,3 триллиона долларов США. Прогнозы показывают, что затраты продолжают расти и удвоятся в ближайшие 3 года. Если говорить про Россию, Президент Владимир Путин 7 мая 2018 года поручил Правительству увеличить долю расходов на реализацию программы цифровой экономики как минимум в 3 раза к 2025 году.

Задача цифровой трансформации – подготовить компанию, орган власти, образовательное учреждение, город, страну к работе в условиях цифровой экономики. Хотя в основе определения цифровой экономики – данные и работа с ними, цифровая трансформация – это не только про технологии и их внедрение, это комплексная трансформация компании,

Рис. 1.1.1. *Top Five Companies by Market Cap (1980-2017). Source: Bloomberg.*

1980	1990	2000	2010	2017
IBM	NTT	Microsoft	ExxonMobil	Apple Inc.
AT&T	Bank of Tokyo-Mitsubishi	General Electric	PetroChina	Alphabet (Google)
Exxon	Industrial Bank of Japan	NTT DoCoMo	Apple Inc.	Microsoft
Standard Oil	Sumitomo Mitsui Banking	Cisco Systems	BHP Billiton	Amazon.com
Schlumberger	Toyota Motors	Walmart	Microsoft	Facebook

Рис. 1.1.2. *Пример карты customer journey.*



которая позволит ей быстро адаптироваться к новым условиям.

Формально можно выделить следующие блоки, входящие во фреймворк цифровой трансформации: «сотрудники», «клиенты», «продукты», «процессы», «бизнес-модели», «партнёрская экосистема», «технологии» и «инфраструктура». Задача цифровой трансформации подразумевает использование новых инструментов применительно ко всем «блокам».

Например, если говорить только о блоке «клиенты», то можно выделить следующие входящие в него разделы и инструменты:

1. Понимание клиента: построение карт customer journey (пример на Рис. 1.1.2) для определения поведения клиента, что он думает и чувствует на каждом из этапов, какие неудобства он испытывает и где наиболее оптимально можно было бы предложить ему решение компании, сбор данных о клиенте в социальных сетях и в сети Интернет, построение постоянной и полноценной коммуникации с клиентом на основе этих данных, построение карт потребностей клиента, проведение customer development.

2. Персонализация предложения для клиента: разработка персонализированного предложения в зависимости от поведения клиента, часто в режиме онлайн, создание ценностного предложения исходя из потребностей и болей клиента, подготовка предложений на основе данных и с учётом вышеописанного в пункте «Понимание клиента»

3. Прямой доступ к клиенту: современная экономика характеризуется упрощением и спрямлением коммуникации, поэтому очень важно обеспечить прямой доступ к своим клиентам без участия посредников, обеспечить омниканальность этой коммуникации: поддержка через сайт и социальные сети, YouTube, чаты, пользовательские приложения, онлайн-сообщества, обеспечить настройку и получение обратной связи по всем этим каналам.

4. Реакция в режиме онлайн: реакция на от-

зывы или запросы клиентов в режиме онлайн и, конечно, 24x7, во всех каналах общения, т.к. клиент хочет покупать в то время и в том месте, где ему это удобно.

5. Возможность самообслуживания: возможность самообслуживания клиентов в удобное время и в удобном месте. В Китае, например, есть вендинговые автоматы для покупки автомобиля – отличный пример реализации этого принципа на практике.

Цифровая трансформация и CIO

Цифровой трансформации можно посвятить отдельный учебник. Почему мы так подробно разбираем задачи цифровой трансформации? Только лишь для того, чтобы показать, что это важный и сложный процесс. По сути, такой масштаб изменений в организации – это задача генерального директора. Так почему бы генеральному директору не взять эту задачу на себя? Возможно, что вопрос загрузки руководителя общими операционными вопросами, возможно вопрос психологии, т.к. эта роль требует некого творческого профайла (см. ниже), а, возможно, есть и другие факторы. Но в большинстве случаев мы видим, что задача цифровой трансформации как за рубежом, так и в России всё же делегируется.

Встаёт вопрос, кому правильно делегировать задачу цифровой трансформации. Первое, что приходит в голову – это делегировать CIO. В голове у среднестатического российского генерального директора по состоянию на лето 2018 года, цифровая трансформация – это про информационные технологии. Ровно так и происходит, например, в США, но немного по другим мотивам. Объясняется это тем, что там исторически CIO занимался не только поддержкой ИТ-инфраструктуры, но и стратегией развития компании. Поэтому, когда пришло время цифровой трансформации, эта задача органически была делегирована CIO.

В России же CIO исторически занимались поддержкой и развитием ИТ. Поэтому, когда встал вопрос трансформации компаний или органов власти, то пришло решение о создании новой руководящей позиции – Chief Digital Officer. Их назначают в компаниях, органах власти, образовательных учреждениях. Позиция CDO впервые возникла в 2009 году. Основная задача – реализация цифровой трансформации. McKinsey в 2015 году чётко назвал Chief Digital Officer – «***Transformer in Chief***».

Появление позиции CDO

Впервые термин CDO был упомянут в 2009 году в США. CDO также называют CDIO – Chief Digital Information Officer.

Спрос на позицию впервые возник в B2C сегментах таких отраслей, как финансы и ритейл, а далее нарастал как снежный ком. По опросу, проведённому KPMG (одна из крупнейших в мире сетей, оказывающих профессиональные услуги, и одна из аудиторских компаний Большой четвёрки наряду с Deloitte, Ernst & Young и PwC. Международная штаб-квартира расположена в Амстелвене, Нидерланды) и Harvey Nash среди почти 4,5 тысяч CIO средних и больших корпораций в 86 странах ввели позицию CDO, более 25% компаний ввели позицию CDO. По оценкам McKinsey, количество CDO удвоилось в период с 2013 по 2014 год и спрос продолжает расти.

По статистике CDO Club роль CDO настолько важна для корпораций, что эти люди часто впоследствии занимают должность генерального директора. Так, в 2012 году три участника клуба получили повышение на позицию генерального директора, а в 2015 году – уже 16.

По определению из Википедии:

> ***Chief Digital Officer*** *– это лицо, которое помогает компании, органу власти или городу осуществлять рост за счёт превращения традиционного «аналогового» бизнеса в цифровой с использованием потенциала современных онлайн технологий и данных, иногда курирует процессы в цифровых направлениях, например, мобильные приложения, социальные сети.*

Как мы видим из классического определения, есть несколько важных аспектов. Во-первых, основная задача CDO – это осуществление роста. Если говорить про органы власти, то более уместным будет говорить про эффективность. Эта функция по сути близка к развитию бизнеса, продажам, маркетингу. Часто на позицию CDO назначаются люди именно из этих функций. Во-вторых, рост должен осуществляться в основном за счёт использования современных онлайн технологий и данных. Это означает, что CDO должен быть хорошо знаком с технологиями, возможно иметь некий технический бэкграунд.

По статистике Gartner, руководители на позиции CDO меняются каждые 2-3 года. Эта печальная статистика объясняется тем, что ключевые показатели эффективности (англ. Key Performance Indicators, KPI) CDO привязаны к финансовым показателям компании, и руководители на этой позиции должны показывать прирост выручки компании или сокращение расходов за счёт применения цифровых технологий. Например, в рамках форума «Иннопром-2017», компанией МТС была озвучена цифра в 10 млрд рублей дополнительной выручки за счёт цифровых технологий. Это достаточно серьёзные показатели, которые часто сложно достигнуть без соответствующего опыта в продажах и маркетинге на стабилизированном рынке. При этом, с CDO не снимаются задачи по цифровой трансформации организации, которые мы кратко описали выше. А это задачи, которые включают в себя не только продажи, но и трансформацию кадров, процессов, инфраструктуры, подходов к работе, культуры и многого другого, что нельзя напрямую измерить в цифрах выручки или издержек.

До апреля 2019 года CDO должны быть назначены во всех государственных корпорациях в России, а также в основных министерствах, а Минэкономразвития России даже выпустил рекомендации по полномочиям для нового типа руководителей. Для решения задачи эта роль наделяется соответствующими полномочиями и бюджетом. Кстати, ровно из-за того, что в США CIO – это всегда была стратегическая позиция в компании, по исследованию KPMG, количество CDO в США растёт не так быстро, как в России или Европе.

Фактически, CDO берут на себя задачу генерального директора или даже во многом владельца компании. Они должны быть харизматичными, смелыми, исполнительными, ответственными, творческими лидерами, чтобы трансформировать корпорацию или орган власти (во многом сломать их старые устои). По сути, нужны новые предприниматели. Кстати, нужных регламентов просто нет, и их нужно изобретать. Эти люди сами найдут в сети и изучат описания полномочий руководителей по трансформации, описание различных digital transformation frameworks, придумают на этой базе свои подходы к решению стоящих перед ними задач. Это очень важно именно на этом этапе развития, когда нужно фактически запустить «стартапы» внутри корпораций и министерств. Под «стартапами» понимаем новые направления работы, где много что не понятно, и нужно найти

ту самую точку роста, которая даст нужный эффект. Да и работа непосредственно с рынком по модели открытых инноваций организациям пойдёт на пользу и позволит повысить эффективность.

Если посмотреть на статистику сайта payscale.com, то средний годовой заработок CIO в США составляет 154 тысячи долларов, тогда как средняя зарплата CDO составляет 205 тысяч долларов США, с верхней границей, доходящей до 750 тысяч долларов США в год.

По мнению автора данной главы, можно составить идеальный профиль людей, которые должны заниматься цифровой трансформацией. Если кратко, то это, как правило, люди из индустрии, хотя допустим переход из смежных индустрий. Очень важно, чтобы работа велась не только с ноу-хау внутри, чтобы компания не замыкалась внутри себя, но и мониторились внешние инновации, запускались новые партнёрские программы с другими корпорациями. Это люди с опытом управления, пониманием векторов развития отрасли, навыками стратегического планирования, навыками ведения бизнеса, пониманием особенностей работы стартапов и стадий их развития. Не помешает опыт личного предпринимательства – может быть, это даже не опция, а почти «must have». Ну и опыт работы в ИТ или с ИТ, опыт инвестирования в стартапы. А идеальный кандидат – это тот, кто не просто знает или умеет, но уже проводил цифровую трансформацию.

Сейчас на различных мероприятиях часто звучит вопрос о различии позиций CDO и CIO. Если говорить о российской специфике, то CIO – это руководитель, отвечающий за стабильность работы IT систем организации и их развитие. Его КПЭ ориентирован, прежде всего, на стабильность работы инфраструктуры, отсутствие сбоев. Соответственно CIO ориентирован на отсутствие рисков. CDO же ориентирован на риск, на новые инициативы, на развитие бизнеса. Его КПЭ – это выручка, полученная от внедрения новых технологий и цифровой трансформации организации в целом. Он ориентирован на эксперименты, работу с технологическими стартапами, поиск новых бизнес-моделей и диверсификацию бизнеса. Как мы видим из рекомендаций Минэкономразвития – он участвует в управлении бизнесом организации и ориентирован на генерацию новых доходов.

> «Chief Digital Officer станет ***самой захватывающей стратегической позицией*** в организации на долгое время. Скорее всего эту позицию попытается занять CIO».
>
> ***Дэйвид Виллис, вице-президент Gartner***

Подводя итог, нужно отметить что не важно, как будет называться должность этого «Transformer in Chief» в организации: CDO, CIO, CINO или CEO. Важно понимать, что один в поле – не воин, и каждая компания должна найти правильное распределение обязанностей между своими CxO, чтобы быстро начать цифровую трансформацию.

CDO и открытые инновации

Разработка инновационных продуктов и создание ценности через технологии невозможна без стимулирования внутренних инноваций, а также работы с рынком по модели открытых инноваций. Внутренние инновации – это ноу-хау, которые вызревают внутри организации. Открытые инновации – это технологические стартапы, которые разрабо-

тали технологию, продукт или услугу вне периметра организации. Мировая практика показывает, что успешные компании работают сразу по двум из этих направлений.

Один из основных аргументов за работу по модели открытых инноваций – это, конечно, экономические эффекты от внедрения новых технологий, продуктов, сервисов, решений. Работа по модели открытых инноваций, по статистике ФРИИ, может дать корпорации, городу или региону эффект, измеряемый в десятках миллиардов рублей в год. В рамках форума «Иннопром-2018» Министр Промышленности и Торговли РФ Денис Валентинович Мантуров приводил примеры цифровой трансформации российских компаний. Так в «Вертолётах России» внедрение цифрового двойника дало эффект 20% экономии ресурсов. Или, если говорить про госсектор, внедрение технологии стартапа eldis24.ru в сфере ЖКХ для Новгородской области позволило сократить расходы бюджета на оплату коммунальных услуг для социальных объектов с 1,5 млрд рублей до 675 млн рублей в год. Также организация получает дополнительные нефинансовые выгоды, в том числе новые продукты или услуги, новые бизнес-модели, повышение конкурентоспособности, выходы на новые рынки, доступ к новым технологиям, доступ к новым партнёрствам.

Задача по работе с открытыми инновациями формально попадает в рамку цифровой трансформации корпорации или органа власти в блок «технологии». Корпорации, которые приняли решение о цифровой трансформации, достаточно быстро начинают работу по модели открытых инноваций и включаются в работу с технологическими стартапами. Процесс работы можно условно разбить на несколько этапов: поиск, скоринг, пилотирование, анализ результатов, масштабирование.

Каждый из этапов имеет свои особенности. Например, если говорить про поиск стартапов, то на сегодня в России можно выделить несколько основных «воронок», в основном все они формируются институтами развития – ФРИИ, Сколково, РВК. Но появляется и большое количество частных инкубаторов, акселераторов, ИТ-парков. Часто корпорации на этом этапе могут столкнутся с отсутствием предложений, особенно если речь идёт не о «сквозных» цифровых технологиях, а об отраслевых решениях, о наукоемких отраслях, в частности, о медицине или энергетике. Основная проблема – это, с одной стороны, отсутствие спроса от отрасли, а с другой – отсутствие так называемых «collaborative spaces», то есть площадок для превращения идей в прототипы с непосредственным участием корпораций.

Если говорить про этап скоринга, то он подразумевает не просто оценку применимости продукта или услуги к корпорации, но также распаковку решения стартапа до технологии и оценку применимости технологии к процессам или продуктам организации.

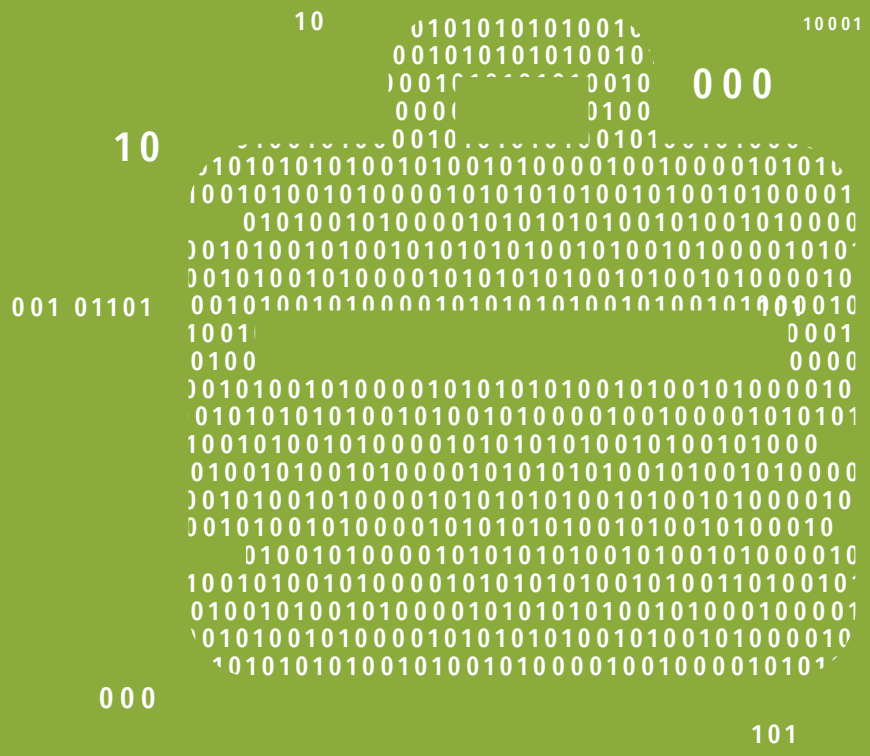
На этапе пилотирования решения производится оценка предполагаемого эффекта от внедрения, переупаковка решения под задачи организации, подготовка дорожной карты проекта.

По результатам проводится анализ, и может быть принято решение о масштабировании. Также корпорация может принять решение об инвестировании в стартап или его покупке. С учётом Поручения Президента России В.В. Путина о создании госкорпорациями корпоративных венчурных фондов – это уже не кажется чем-то сверхъестественным. Очень важно, что пилотный проект может закончиться неудачно. На то он и пилотный,

что мы проверяем достижимость заявленного эффекта, продукт, сервис, команду. Поэтому очень важно прописывать «право на ошибку», выделять отдельную строку бюджета на проведение тестов.

С появлением эффекта от запуска проектов, корпорации из различных отраслей начинают активно работать по модели открытых инноваций, начинают создавать «тягу» на рынке и стимулировать появление нужных им технологий. Задача CDO, если он взял на себя функции руководителя по цифровой трансформации в рамках этой деятельности – осуществлять работу по развитию внутренних инноваций, а также по поиску и интеграции открытых инноваций в процессы или продукты организации. Также под его начало попадает курирование работы корпоративного венчурного фонда и оркестрация всех подразделений, которые вовлечены в цифровую трансформацию: кадры, юристы, бухгалтерия, производство и др.

Существенное повышение эффективности различных видов производства, как это отмечено в «Стратегии развития информационного общества РФ на 2017-2030 годы», невозможно достичь традиционным путём, уже существующими подходами: вместо этого требуется включение организации в работу по модели открытых инноваций. На момент написания данной статьи формальной статистики по работе корпораций или органов власти с инновациями в России нет, можно лишь ссылаться на косвенные данные. Так, например, корпорации, с которыми ФРИИ начинал работать в 2015 году, существенно продвинулись по сравнению с другими компаниями на рынке. Они готовы платить стартапам за пилотные проекты, готовы давать авансирование, рассматривать «сырые» технологии, а не только прототипы или продукты. Сегодня в активную работу включились практически все индустрии: медиа, операторы связи, финансы, страхование, медицина, сельское хозяйство, ритейл. Постепенно начинают включаться в гонку транспортная индустрия, промышленность и энергетика.



Часть 2

ИТ-деятельность

Глава 2.1

Стратегическое планирование ИТ

Павел Алфёров

Константин Зимин

ИТ-стратегия необходима. Она нужна руководителям компании, чтобы определить текущую ситуацию в ИТ и наметить цель, а также контролировать движение к этой цели. ИТ-стратегия нужна руководителям компании, чтобы сделать деятельность ИТ прозрачной и максимально уменьшить непонимание: куда и как развивается ИТ. Она нужна руководителям подразделений компании (и другим заинтересованным менеджерам), чтобы знать, что происходит в сфере ИТ, и тем самым наладить эффективное взаимодействие. ИТ-стратегия экономит нервы и время менеджеров, потому что появляется понимание: почему принимаются те или иные решения. ИТ-стратегия нужна CIO, чтобы:

- чётко понимать свои цели и задачи в компании;
- зафиксировать ограничения и возможности, которые у него есть по достижению поставленных перед ним целей;
- иметь возможность принимать тактические решения;
- показывать своим ИТ-специалистам, куда нужно идти, и мотивировать команду.

ИТ-стратегия нужна сотрудникам ИТ службы, чтобы понимать цели и конечный результат своей работы.

Определения и подходы

Понятие «***стратегия***» — достаточно общее, и не всегда понимается одинаково. Стратегию можно рассматривать как некоторую рамку, которая очерчивает границы будущих целей,

> Скажите, пожалуйста, куда мне отсюда идти? — спросила Алиса.
> А куда ты хочешь попасть? — ответил Кот.
> Мне все равно... — сказала Алиса.
> Тогда всё равно, куда идти, — заметил Кот.
>
> ***Льюис Кэрролл «Приключения Алисы в стране чудес»***

и тем самым определяет решения, которые должны приниматься.

Очевидно, что стратегия должна содержать видение будущего и набор целей. Однако, из определения видно, что видение или цели являются необходимыми, но не достаточными атрибутами стратегии. С целью может быть связано множество путей её достижения. Стратегия накладывает ограничения на способы достижения целей. Основа эффективной стратегии: те, кто отвечает за реализацию цели, должны видеть ограниченный набор способов её достижения, понимать, что является наиболее важной очередной задачей. «Миссии» и «ценности» стратегиями не являются. Они могут быть частью стратегии, даже определять её «стиль», но стратегия ими ограничиваться не может.

> ИТ-стратегия формулирует чёткую миссию, видение и цели, создаёт варианты для достижения этих целей и определяет план их достижения.
>
> ***Gartner***

Кроме того, стратегия должна определять план достижения целей. Она должна показывать, как компания будет меняться на пути к поставленным целям. В этой части стратегия сопрягается с тактикой. В отличие от стратегии, тактика — это уже конкретные решения и пути, которые направлены на достижение целей. На это надо обратить внимание, поскольку в российской практике под стратегией часто понимается именно тактика — конкретный проектный план развития. Но стратегия — это не набор проектов. Такой проектный план развития может быть частью стратегии, однако в качестве дополнительного, а не основного её содержания. Более того, эксперты Gartner рекомендуют вопросы планирования развития ИТ систем разделять на два раздельных документа — «ИТ-стратегия» и «План реализации проектов».

Целью ИТ стратегии является предоставление правильных и нужных технологий и прикладных систем в правильном месте, в правильное время и на необходимом уровне соотношения цены, качества и объёмов. В общем случае, ИТ-стратегия должна:

- фиксировать то, что бизнес ожидает от ИТ;
- определять систему приоритетов в области ИТ;
- определять направления развития ИТ в компании;
- определять границы развития ИТ в компании;
- быть комплексной и обеспечивать единую основу для всех проектов и инициатив компании в области ИТ.

Надо сказать, что понимание ИТ-стратегии со временем меняется. Следуя за ускоряющейся динамикой развития компаний, ИТ-стратегия сейчас приняла формализованную и более динамичную форму. При этом, рекомендованный горизонт планирования сократился с 5-7 до 1-2 лет. Более того, по рекомендациям Gartner, проработанность и детализация ИТ-стратегии может быть различной: на первый год максимальная, на второй — меньше, и так далее.

Очевидно, что ИТ-стратегия должна основываться на бизнес стратегии (или даже быть её частью). ИТ-стратегия должна:

- опираться на основополагающие бизнес-ценности и принципы;
- поддерживать существующую бизнес-стратегию и отвечать её целям и видению;
- координировать стратегическое видение ИТ с реалиями бизнеса;
- обеспечивать возможность для развития бизнеса.

Логическая взаимосвязь элементов бизнес-стратегии и элементов ИТ-стратегии в представлении Gartner показана на Рис. 2.1.1. Важно отметить, что не только ИТ-стратегия

Рис. 2.1.1. *Связь элементов бизнес и ИТ-стратегии (Gartner).*

зависит от бизнес-стратегии, но и наоборот. То есть, существует обратная связь, когда ограничения ИТ-стратегии могут влиять на бизнес-стратегию. Понимание наличия этой обратной связи особенно важно в ситуации, когда сильный бизнес-лидер, за счёт своей харизмы, «продавливает» недостаточно взвешенное и обдуманное решение в области развития компании. В таких случаях влияние ограничений ИТ на бизнес может стать значительным.

В соответствии со стандартом COBIT, общая последовательность шагов при разработке ИТ стратегии показана на Рис. 2.1.2. На основе бизнес-стратегии определяются те бизнес-цели, которые связаны с ИТ (бизнес-цели для ИТ). Далее из них определяются цели работы ИТ-службы, на основе которых, в свою очередь, строится целевая корпоративная архитектура ИТ. Итогом всей этой работы должно стать создание системы сбалансированных показателей ИТ, которая позволяет контролировать эффективность работы ИТ.

Одна из самых больших трудностей при разработке ИТ-стратегии — трансляция целей бизнеса в ИТ-цели.

Транслировать цели бизнеса в цели ИТ можно различными способами, стандартов здесь не существует. Один из наиболее последовательных вариантов предлагает методология COBIT. В приложении 1 к COBIT приведе-

Рис. 2.1.2. *Общая последовательность шагов при разработке ИТ-стратегии (COBIT).*

ны типовые и наиболее распространённые примеры связи бизнес-целей, ИТ-целей и ИТ-процессов. На основе сбалансированной системы показателей (BSC) описаны стандартные бизнес-цели, которых, в общем-то, немного (в COBIT приведено 28 наиболее распространённых бизнес-целей). Им сопоставлены соответствующие ИТ-цели (в COBIT приведено 17 наиболее распространённых ИТ-целей). И отдельная таблица показывает, какие ИТ-процессы необходимо развивать, чтобы достигнуть определённых ИТ-целей.

Что делать, если бизнес-стратегии не существует?

Допустим, у компании есть бизнес-цель «Оптимизация затрат на оказание услуг». Согласно методологии COBIT, ей соответствуют три ИТ-цели (Рис. 2.1.3):

- «Приобретать и поддерживать стандартизированную унифицированную ИТ-инфраструктуру».
- «Установить взаимовыгодные отношения с поставщиками».
- «Оптимизировать затраты на ИТ».

Достижение этих ИТ-целей, в свою очередь, зависит от нескольких ИТ-процессов.

При соотнесении типичных бизнес-целей с целями ИТ можно опираться на COBIT. Только не стоит забывать, что сами авторы COBIT не позиционировали приведенный им набор бизнес и ИТ-целей как полный и исчерпывающий, а лишь как возможный и наиболее вероятный. Поэтому не стоит автоматически следовать COBIT — опирайтесь на свой опыт и здравый смысл.

Ситуация, когда бизнес-стратегия либо не определена вообще, либо не документирована, либо недоступна для разработчиков ИТ-стратегии, не так уж редка. Но, пусть и не записанная на бумаге, в головах руководителей компании она в любом случае есть, и если правильно поставить вопрос, то её вполне можно оттуда извлечь.

Для этих целей необходимо провести интервьюирование ключевых руководителей компании. При этом, в ходе интервью предлагаем не упустить следующие вопросы:

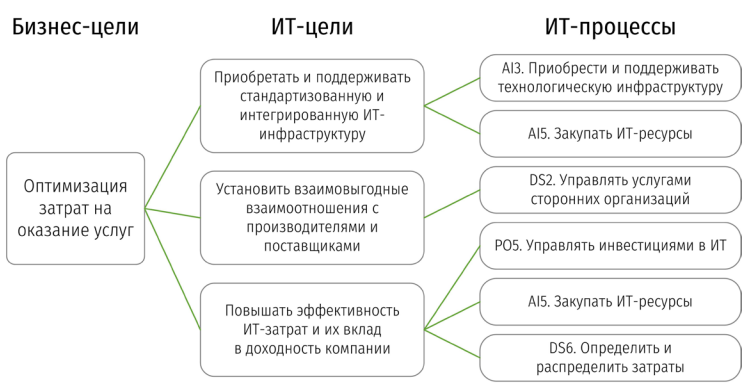
1. Желательный горизонт планирования ИТ-стратегии. Зависит от горизонта бизнес-стратегии. Чем более широким является временной горизонт, тем в большей степени стратегические аспекты должны найти отражение в архитектуре ИТ.

2. Планируемые изменения в продуктах и услугах, которые поставляет компания. Показатели/цели, которые при этом планируется достичь.

3. Планируемые изменения в бизнес-процессах и системе управления. Насколько жёстко организация планирует придерживаться принятых методов работы? Или, наоборот, насколько она хочет/готова изменять модели ведения бизнеса, а значит, соответствующие бизнес-процессы и приложения.

4. Планируемые изменение географии бизнеса. Распределение производственных объектов, клиентов и партнёров и планы по их изменению имеют непосред-

Рис. 2.1.3. *Пример связи бизнес-целей, ИТ-целей и ИТ-процессов (COBIT).*



ственное влияние на развёртывание инфраструктуры и представление ИТ-сервисов.

5. Подходы к интеграции с партнёрами и клиентами. Существует ли тенденция к интеграции с клиентами и поставщиками? Планируется ли передача каких-либо функций в аутсорсинг? Желание рассматривать внешние организации как активных участников своих бизнес-процессов обычно значительно повышает требования в области интеграции.

6. Финансирование ИТ. Финансовые методы и подходы к оценке функционирования подразделений, прежде всего ИТ.

Структура ИТ-стратегии

Описание ИТ-стратегии целесообразно формировать в виде документа, ориентированного, прежде всего, на бизнес-пользователей. Использование технических терминов и аббревиатур должно быть сведено до минимума, насколько это возможно.

Основными разделами (главами) ИТ-стратегии должны быть:

1. Описание текущей ситуации «как есть» (AS-IS).

2. Варианты целевого состояния ИТ (варианты TO-BE). Известный историк Бэзил Лиддел Гарт, написавший знаковую книгу «Стратегия непрямых действий», утверждал, что нельзя идти напролом, необходимо найти и использовать обходные пути достижения цели, они всегда есть. По его словам, план без вариантов подобен дереву без ветвей и, соответственно, ни к чему хорошему не приведёт. Любая стратегия при разработке должна учитывать наличие вариантов развития каждого из указанных направлений.

3. Лучший вариант, целевое состояние ИТ (TO-BE). Он выявляется путём анализа применимости всех вариантов, и на нём строится основная ИТ-стратегия. Остальные варианты сохраняются для объяснения причин выбора текущего пути, а также на случай, если что-то пойдёт не так, как предполагалось, и потребуется корректировка пути развития. Эти варианты надо хранить и периодически их пересматривать.

4. План инициатив (проектов), показывающий пути движения от AS-IS — к TO-BE. Часто именно его называют ИТ-стратегией, но очевидно, что это слишком упрощённый подход.

5. Набор KPI — индикаторов движения к цели и достижения результата; показатели того, насколько мы продвинулись от AS-IS к TO-BE. По мнению авторов Учебника, ИТ-стратегия, претендующая на комплексность и полноту, — в первом и в третьем (также, возможно, во втором) из вышеуказанных разделов — должна быть описана по пяти нижеследующим уровням (Рис. 2.1.4):

- информация и информационные потоки;
- приложения;

Рис. 2.1.4. *Пять уровней и пять разрезов ИТ-стратегии.*

	AS IS	Варианты To BE	Выбранный To BE	План проектов	KPI
Информация					
Приложения					
Инфраструктура					
ИТ-процессы					
Люди / Оргструктура					

инфраструктура;
- ИТ-процессы;
- сотрудники и оргструктура.

Заметим, что в отличие от указанного выше подхода, Gartner рекомендует проанализировать деятельность в области ИТ по четырём областям. Эти области охватывают отношения бизнеса и ИТ, технологии, а также организационные вопросы.

Процесс создания ИТ-стратегии

Согласно Gartner, процесс построения ИТ-стратегии содержит 8 шагов (Рис. 2.1.5):

1. Согласование понимания требований бизнеса к ИТ (понимание направлений развития бизнеса).

2. Определение направления развития ИТ (высокоуровневое описание).

3. Анализ текущего состояния ИТ и оценка вариантов реализаций целевой ИТ-архитектуры с учётом существующих ограничений, накладываемых имеющейся инфраструктурой ИТ.

4. Разработка стратегии развития и изменения приложений и целевого плана ИТ-архитектуры.

5. Разработка целевой модели предоставления ИТ-услуг.

6. Формирование стратегии развития процессов и операций управления ИТ-ресурсами. Определение стратегии и задач по развитию необходимых кадровых ИТ-ресурсов.

7. Разработка подхода и плана миграции к целевому состоянию ИТ.

8. Подготовка документа с описанием стратегии ИТ и представление результатов для обсуждения в компании.

Советы по разработке ИТ-стратегии

1. Понимание роли ИТ в компании. У компаний различная оргструктура, культура и принципы управления, объём бизнеса и маржинальность, а также различная зависимость от ИТ, поэтому нельзя одну и ту же стратегию применять к разным компаниям.

2. Максимально тесная привязка ИТ-стратегии не только к стратегии бизнеса, но и к запросам ключевых бизнес-подразделений. CIO должен находить компромиссные варианты развития ИТ, учитывающие данные за-

Рис. 2.1.5. *Восемь шагов создания ИТ-стратегии (Gartner).*

просы.

3. Связь с финансами. В ИТ-стратегию должны включаться вопросы финансирования, хотя бы на общем уровне. Иначе ИТ-стратегия рискует превратиться в декларацию, не поддержанную реальными ресурсами.

4. Связь с нефинансовыми ресурсами, прежде всего, человеческими. ИТ-стратегия должна включать в себя стратегию в области ИТ-персонала и сорсинга.

5. ИТ-стратегию надо оцифровывать. В стратегию необходимо включить некоторые KPI, по которым можно отслеживать степень приближения к целевому состоянию ИТ.

6. Реализация ИТ-стратегии. В стратегии должно быть описано, как минимум, в общих чертах, как мы предполагаем реализовать целевое состояние ИТ. План реализации является неотъемлемой частью хорошо сделанной ИТ-стратегии. С другой стороны— этот план не должен быть слишком детализирован, в противном случае мы переходим от стратегии к тактике.

7. CIO не стоит «брать на себя слишком много» и пытаться самому формулировать бизнес-стратегию. Такая инициатива может быть неудачной из-за недостаточного учёта политических аспектов.

8. Периодический пересмотр ИТ-стратегии. Раз в год-два (в зависимости от специфики бизнеса компании) необходимо пересматривать принятую ИТ-стратегию, — для отражения изменений, происходящих в компании и на рынке.

Проблемы разработки ИТ-стратегии

Создание ИТ-стратегии сопряжено с определёнными проблемами и трудностями. Основные из них следующие:

1. Разработка стратегии — это «политика». Не просто принимать объективные решения в условиях высокой степени «политической» неопределённости. Всегда есть риск «поддаться на уговоры» наиболее харизматичного «спонсора» и политического тяжеловеса в компании, вместо использования профессиональных подходов. Поэтому есть риск, что разработка ИТ-стратегии станет политическим ритуалом. Это приводит к тому, что в ряде случаев руководители ИТ боятся разрабатывать стратегию.

2. Перетягивание «одеяла» на себя. Вместе с тем, слишком большая активность CIO при разработке ИТ-стратегии может вызвать вопросы, особенно в ситуации, когда бизнес-стратегия не сформулирована достаточно чётко и требуются дополнительные беседы с топ-менеджерами. В результате, у руководства организации может создаться впечатление, что ИТ-служба пытается подменить бизнес-планирование.

3. Создание ИТ-стратегии — процесс сложный и затратный. Выработка стратегии требует от руководителей максимума гибкости и коммуникабельности. Достижение согласия даже по таким простым вещам, как термины, может вызывать сложности. Сотрудникам компании, в том числе и CIO, может не хватать теоретических знаний и опыта в создании стратегических документов. С другой стороны, следует избегать чрезмерных и неконтролируемых затрат времени на проведение консультаций и достижение взаимопонимания. Не стоит забывать и о стоимости консультантов — разработчиков ИТ-стратегии.

4. Разработка стратегии — это дополнительная нагрузка. Процесс разработки стратегии ИТ воспринимается как нежелательная нагрузка, поскольку не является частью ежедневных обязанностей большинства участников этого процесса. Вовлечение руководителей в процесс планирования — непростая

задача: у них всегда мало времени на планирование.

5. Создание ИТ-стратегии может потребовать много времени. В крупных организациях для разработки стратегии ИТ может потребоваться более полугода. Отнюдь не все компании в текущей динамичной бизнес-среде могут позволить себе ждать столько времени. Кроме того, возможно, что часть факторов, на основе которых отбирались проекты для включения в стратегический план, потеряют свою актуальность.

6. Чрезмерная детализация или, наоборот, слишком общие и расплывчатые формулировки ИТ-стратегии. CIO необходимо найти ту оптимальную детализацию планов развития ИТ, которая устроила бы бизнес.

7. Стратегия не должна быть статическим документом. Характерный «период полураспада» большинства стратегических планов в области ИТ составляет от 6 месяцев до года. А, значит, важен не столько сам стратегический план, сколько построение процесса обновления стратегии ИТ.

8. Планирование и практическая реализация слабо связаны друг с другом. К сожалению, очень часто разработанная ИТ-стратегия становится лишь «пыльным документом» на полке, а не руководством к действию. А при этом CIO придётся отвечать за отсутствие результатов...

Возможные варианты представления стратегии развития ИТ

Разработанная ИТ-стратегия может иметь несколько представлений. ИТ-стратегия может быть оформлена в трёх вариантах.

1. Полное описание ИТ-стратегии. Оно может занимать 50-100 страниц. Полный вариант ИТ-стратегии хорош своей детализацией. К сожалению, такой вариант ИТ-стратегии не в состоянии прочитать руководство компании. Как его утверждать? Тем не менее, написание такого варианта необходимо для детальной проработки всех вопросов, относящихся к ИТ-стратегии.

2. Резюме ИТ-стратегии для бизнеса. Это средний по объёму вариант описания ИТ-стратегии, он может состоять из 15-30 страниц. Этот вариант предназначен, прежде всего, для прочтения руководителями компании и её подразделений. Именно такой вариант и утверждается руководством компании. Однако, ограничиться только таким вариантом представления ИТ-стратегии не получится — полный вариант необходим.

3. Минимальный вариант ИТ-стратегии. Это одна или несколько страниц с основными выводами — перечень стратегических ИТ-проектов и пр. Такой вариант может быть полезен для принятия текущих решений в области ИТ, как средство быстро освежить в памяти руководителей основные направления действующей ИТ-стратегии, может быть выполнен в виде слайд-презентации.

Глава 2.2

Корпоративное управление ИТ

Михаил Потоцкий

Павел Алфёров

Корпоративное управление ИТ (или корпоративное руководство) является очень важной и одновременно достаточно новой областью знаний. Важность обусловлена тем, что корпоративное управление в значительной степени определяет законы и правила, по которым далее работает управленческая команда.

Корпоративное управление ИТ определяет ту среду, в которой далее действует руководитель ИТ. Более того, эта среда выходит за рамки только лишь законов и правил и включает стиль руководства и принятия решений, порядок контроля исполнения, способы поощрения и принуждения к исполнению решений, в случае необходимости, и т.д. Корпоративное управление смыкается с внутренней культурой и стилем лидерства, который использует руководитель ИТ в своей работе.

В то же время, корпоративное управление имеет свои подходы и практики. Мы рассмотрим наиболее важные аспекты корпоративного управления ИТ, используемые в современных организациях, а читатель имеет полную свободу применить их в сочетании с тем стилем лидерства, который он считает наиболее подходящим для своей работы.

Эта глава Учебника будет полезна, как в случае, если в компании корпоративное управление ИТ находится на самом начальном уровне, так и в случае, если корпоративное управление в компании уже начинает складываться как система.

В английском языке используется термин ***IT Governance***, перевод которого на русский язык не устоялся. Наиболее часто встречающиеся варианты: «корпоративное управление ИТ», «стратегическое управление ИТ», «руководство ИТ» и «корпоративное руководство ИТ».

В любом случае, перевод должен отделять понятие «governance» от «management» (управление). В Учебнике будет использоваться перевод «***корпоративное управление ИТ***».

Определения и подходы

Корпоративное управление ИТ является одной из новых областей знаний. Безусловно, ряд входящих в него направлений (управление рисками, управление финансами) известны уже давно, и для них разработаны уже достаточно эффективные подходы. Однако, объединение всех этих направлений в единую систему даёт новое качество управления, что и позволяет говорить об этом как о новой области знания.

Приведём несколько определений корпоративного управления (стратегического управления, руководства).

> ***Стратегическое управление ИТ (governance of IT)*** *— система, при помощи которой осуществляется управление и контроль настоящим и будущим использованием ИТ.* ***(ISO 38500:2017)***

Другими словами, корпоративное управление позволяет развивать ИТ максимально полезным для компании образом. Корпоративное управление ИТ определяет нормы, по которым происходит постановка целей и задач для ИТ подразделений, принятие решений относительно ИТ, выделение ресурсов и контроль получаемых результатов. Важно отметить, что под информационными технологиями в мире понимаются не только информационно-технологические средства (оборудование и ПО), но и работа ИТ-персонала, а также управление со стороны руководства ИТ-службы, позволяющее максимальным образом реализовать потенциал информационных технологий.

Кратко корпоративное управление ИТ можно определить, как ответ на вопрос: «***Кто принимает решения в области ИТ и как?***» Этот вопрос можно разделить на три части:

1. Какие решения должны приниматься относительно ИТ?

2. Кем должны приниматься эти решения?

3. Каким образом они должны приниматься?

Приведём ещё одно определение корпоративного управления ИТ:

> ***Руководство ИТ на предприятии*** *— точка зрения на руководство, при которой обеспечивается использование информационных и связанных с информацией технологий для поддержки и реализации стратегии предприятия и достижение задач, стоящих перед предприятием. Также руководство включает в себя функциональное руководство ИТ, например, обеспечение эффективного и рационального использования возможностей ИТ. Предприятия, которые достигли успеха, смогли признать, что совет директоров и исполнительные директора обязаны относиться к ИТ, как к любой другой значимой части бизнеса. Совет директоров и управленцы — как в бизнесе, так и в ИТ — должны совместно работать над тем, чтобы ИТ были частью общего подхода к руководству и управлению предприятием.* ***(COBIT 5)***

Определение подчёркивает, что область корпоративного управления ИТ шире, чем ответственность ИТ-руководителя, но в очень большой степени зависит от него и от его способностей организовать взаимоотношения с руководством компании. Заметьте, что вопрос лидерства поставлен на одно из первых мест в определении корпоративного управления COBIT и CIO — это тот руководитель, от которого руководство компании ожидает лидерства в вопросах ИТ.

Однако, надо понимать, что лидерство — это двунаправленный процесс. С одной стороны, это умение сформировать видение, получить поддержку руководства и вести коллектив к поставленным целям. С другой стороны — это инициативы в области ИТ, которые во многих случаях являются важными и ресурсоёмкими для компании и должны быть скоординированы внутри организации. Можно без преувеличения сказать, что во всех российских компаниях, которые успешно используют возможности ИТ, есть ясное и чёткое лидерство в вопросах ИТ, должным образом согласованное с руководством компании.

И ещё одно определение:

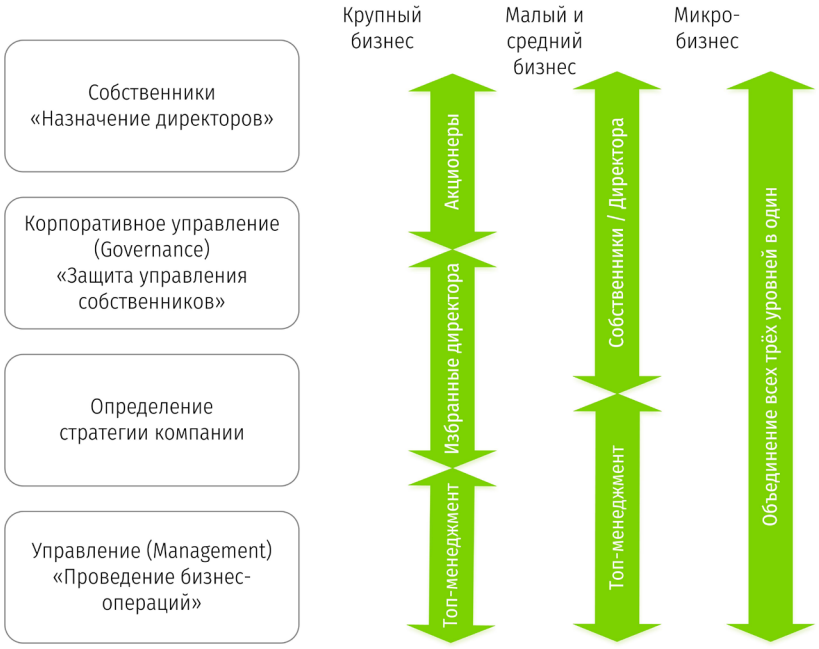
> ***Корпоративное управление ИТ*** *— это набор процессов, которые обеспечивают результативное (effective) и эффективное (efficient) использование ИТ и позволяют организации достигать своих бизнес-целей.* ***(Gartner Group)***

Необходимо обратить внимание, что результатом корпоративного управления является скорее именно «использование ИТ», нежели менеджмент ИТ. То есть, корпоративное управление является той системой, принятой в организации, которая обеспечивает постановку целей и задач для ИТ и контроль их исполнения. В этом — главное отличие корпоративного управления (governance) от управления (management). На Рис. 2.2.1 показаны три уровня управления компанией и место корпоративного управления. Корпоративное управление находится над оперативным управлением бизнесом, его осуществляют другие субъекты и преследует иные цели. В то же время, корпоративное управление определяет и взаимоотношения внутри ИТ-службы, так как определённые механизмы принятия решений, утверждённые высшим руководством компании, должны реализовываться внутри ИТ-департамента.

Это важный вопрос, поэтому остановимся на нём подробнее. Контроль — это слишком ёмкое понятие, и для его конкретизации имеет смысл разделять постановку целей и их исполнение. Когда мы используем понятие «контроль» по отношению к исполнению поставленных целей (чем занимается коллектив менеджеров), то «контроль» подразумевает мониторинг ситуации, сравнение её с желаемым состоянием и применение по результатам корректирующих воздействий. Когда же мы говорим о корпоративном управлении, то есть о постановке целей и задач для ИТ, то на этом уровне вмешательство в оперативную работу ИТ обычно уже меньше — ставится цель и контролируется её достижение, а также оценивается общая способность коллектива осуществлять достижение целей. Такое разделение горизонтов целеуказания и целеисполнения, как и уровней управления компанией (акционеры — совет директоров — менеджмент) является принципиально важным для понимания того, что же такое корпоративное управление.

При этом, не нужно уменьшать роль менеджмента ИТ-подразделений компании, который выполняет функции оперативного управления, подконтрольные корпоративному управлению. Ответственностью менеджмента является непосредственное управление ИТ-подразделениями компании, направленное на достижение поставленных ИТ-целей и, в конечном итоге, — на достижение совместной итоговой цели — обеспечение результативного и эффективного использования ИТ в компании.

Рис. 2.2.1. *Три уровня управления компанией и место корпоративного управления.*



Практика построения корпоративного управления

На практике становление корпоративного управления компанией в целом, и корпоративного управления ИТ в частности, происходит постепенно и зависит от:

- бизнес-целей компании;
- корпоративного стиля руководства;
- бизнес-среды компании;
- других факторов.

Со временем руководство компании и руководство ИТ-подразделения приходят к желанию совершенствования наиболее общих методов управления, которыми являются методы постановки целей и осуществления контроля выполнения задач. Появляются коллективные органы управления, которыми в части ИТ являются Комитет по управлению ИТ (IT Steering Committee), Комитет по управлению ИТ-проектами (IT Project Committee) и т.д. Так складывается новая система управления.

Разная скорость роста и разная зрелость компаний привела к тому, что существующая практика корпоративного управления ИТ в российских компаниях существенно отличается. Есть компании, в которых высшее руководство продолжает сохранять за собой право принятия значительного количества решений относительно ИТ. Есть компании, в которых руководитель ИТ-службы фактически единолично принимает все необходимые решения. Есть компании, в которых решения принимаются коллегиально в рамках специальных органов управления. Во многих случаях выбор схемы связан с уровнем доверия к менеджменту ИТ-службы со стороны высшего руководства компании. При этом, правильная система корпоративного управления ИТ значительно способствует росту доверия со стороны высшего руководства.

Существуют структурированные подходы к созданию систем принятия решений в области ИТ. Однако, на практике становление корпоративного управления ИТ начинается с формирования правил и распределения функций по принятию ИТ-решений и организации ключевых комитетов, связанных с ИТ. В целом количество и задачи комитетов, связанных с ИТ, определяются практикой управления конкретных организаций и уже существующими в компании коллегиальными органами управления (например, наличием «Комитета по инвестициям»).

Однако, создание Комитета по ИТ — это только первый шаг. В определении Gartner Group, которое мы приводили выше, делается акцент на том, что корпоративное управление ИТ — это именно набор процессов, а не только ряд комитетов по управлению ИТ. Процессы, организующие подготовку, обсуждение, принятие решений в области ИТ и контроль их исполнения, которые используют специализированные ИТ комитеты и корпоративные органы управления, составляют корпоративное управление.

Согласно ITIL, такой комитет несёт ответственность за выбор направлений развития, политик и стратегий развития ИТ и оказания ИТ-услуг. Функции управляющего комитета по ИТ—поддерживать партнёрство между ИТ и бизнесом. Комитет должен собираться на встречи регулярно и постоянно проводить обзор бизнес- и ИТ-стратегий, рассматривать вопросы проектирования, планирования, портфеля услуг, архитектуры и политик, чтобы убедиться в том, что все они соответствуют друг другу. Это должно обеспечить единое и комплексное видение развития ИТ в компании. Темы обсуждений на Комитете по ИТ могут включать:

- обзор планов бизнеса и ИТ, определение изменений в процессах создания, улучшения и совершенствования ИТ-обслуживания;

- оценка стратегий бизнеса и ИТ, обсуждение изменений в бизнес-стратегии и предполагаемых изменений в ИТ-стратегии;
- планирование потребления ИТ-услуг, определение изменений потребностей в краткосрочной и долгосрочной перспективе;
- приоритизация и утверждение проектов;
- оценка хода проектов для достижения уверенности, что ожидаемые бизнес-выгоды будут реализованы в соответствии заданиями на проект, и для контроля графика проектов;
- аутсорсинг, определение потребностей и возможных сценариев сорсинговых стратегий;
- непрерывность бизнеса и ИТ-услуг, обеспечение соответствия стратегий непрерывности бизнеса и непрерывности ИТ-услуг;
- политики и стандарты, обеспечение соответствия политик и стандартов в области ИТ корпоративным целям и финансовой стратегии.

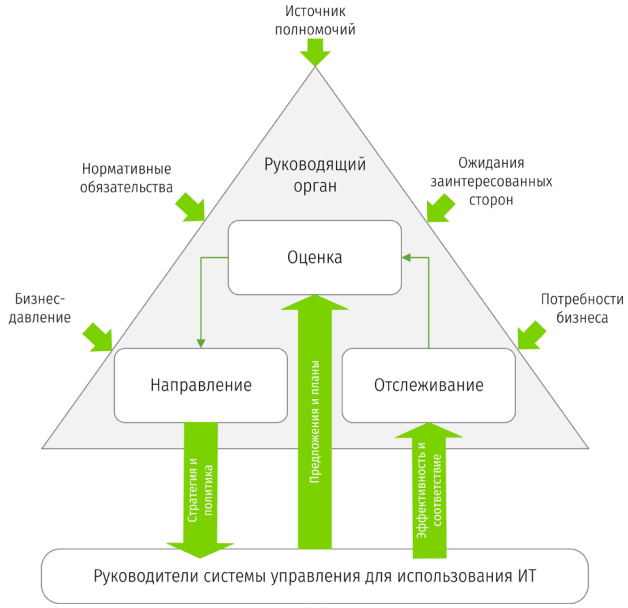
Подходы и методы

Далее мы кратко опишем два наиболее известных свода знаний по построению системы корпоративного управления ИТ: стандарт ISO 38500:2017 и COBIT.

Стандарт ISO 38500:2107

Международный стандарт ISO 38500:2017 даёт общую высокоуровневую модель корпоративного управления ИТ (Рис. 2.2.2).

Рис. 2.2.2. *Модель корпоративного управления (ISO 38500:2017).*



Стандарт ISO 38500:2017 определяет, что высшему руководящему органу компании следует осуществлять корпоративное управление ИТ через решение трёх основных задач:

- ***Оценка***. Оценка текущего и будущего использования ИТ;
- ***Направление***. Направление подготовки и внедрения стратегий и политик, чтобы гарантировать соответствие ИТ целям бизнеса;
- ***Отслеживание***. Мониторинг результативности (performance) использования ИТ и соответствия принятым политикам в области ИТ.

В рамках первой задачи — ***оценки использования ИТ*** — стандарт обращает внимание на необходимость непрерывного выполнения данной задачи в соответствии с изменяющимися рыночными условиями.

При решении второй задачи — ***руководства направлениями подготовки и реализации планов и политик использования ИТ*** — высшему руководящему органу компании следует распределить ответственность, осуществлять общее руководство разработкой и реализацией планов и политик компании в области ИТ. При этом, высшему руководяще-

му органу компании следует поддерживать культуру должного корпоративного управления ИТ через требования к менеджменту о своевременном предоставлении информации, соответствии принятым направлениям использования ИТ. Кроме того, планы и политики ИТ должны соответствовать шести принципам корпоративного управления ИТ:

- ***принцип ответственности*** — сотрудники и коллективы компании понимают и принимают на себя ответственность, связанную с вопросами ИТ;
- ***принцип стратегии*** — бизнес-стратегия компании принимает во внимание текущие и будущие возможности ИТ, стратегические планы в части ИТ удовлетворяют потребностям бизнес-стратегии компании;
- ***принцип приобретения (закупок)*** — закупки в области ИТ производятся, исходя из реально необходимых потребностей, на основе соответствующего анализа с ясной и понятной схемой принятия решений; при этом, должен осуществляться баланс между полезностью, возможностями, стоимостью и рисками в краткосрочной и долгосрочной перспективах;
- ***принцип эффективности*** — корпоративные ИТ отвечают целям организации, предоставляя ИТ-сервисы должного качества для удовлетворения текущих и будущих бизнес-потребностей;
- ***принцип соответствия требованиям*** — корпоративные ИТ соответствует всем нормам требований и законов, политики и правила четко определены и введены в действие;
- ***принцип норм человеческого поведения*** — корпоративные политики и нормы в области ИТ демонстрируют уважение к общечеловеческим нормам, включая потребности всех участников производственных и бизнес-процессов компании.

При решении третьей задачи — ***отслеживания*** — высшему руководящему органу компании следует осуществлять мониторинг результативности использования ИТ средств с целью постоянной уверенности в том, что ИТ используется в соответствии с бизнес-целями компании.

Стандарт ISO 38500:2017 отмечает, что, хотя определённые полномочия на выполнение непосредственных действий в области корпоративного управления ИТ могут быть делегированы ИТ-менеджменту компании, общая ответственность за эффективное использование ИТ в организации должна оставаться за высшим руководящим органом.

Кроме того, ценность стандарта ISO 38500:2017 заключается в выделении двух уровней — уровня постановки и уровня исполнения задач. В рамках стандарта не делается каких-либо замечаний о совмещении или разделении этих уровней. На практике, в компаниях происходит постепенное разделение этих уровней с ростом значимости ИТ-организации.

COBIT 5

В то время как стандарт ISO 38500:2017 определяет общие принципы организации корпоративного управления ИТ для практического использования, также интерес представляет подход, получивший название COBIT (Control Objectives for Information and related Technology, «Цели контроля для информационных и смежных технологий»), на момент написания этой книги выпущенный в версии 5.

Он был создан Международной ассоциацией аудита и контроля за информационными системами (ISACA) в 1996 году именно как средство аудита информационных систем. Но поскольку контролировать проще то, что стандартизировано, со временем методология аудита превратилась в рекомендованный ассоциацией набор лучших практик.

COBIT предлагает общий взгляд на вопросы ценности ИТ для компании, определяет целевую модель процессов и де-факто является стандартом аудита ИТ-деятельности. В итоге, на сегодняшний день COBIT позволяет организовать системный мониторинг работы ИТ службы, соотнесённый с целями и задачами бизнеса. Этот стандарт используется ведущими мировыми аудиторскими и консалтинговыми компаниями в части вопросов, касающихся ИТ.

Структура материалов COBIT 5

В настоящее время COBIT 5 представляет собой набор из ряда публикаций, созданный организациями ISACA и ITGI (Рис. 2.2.3).

Рис. 2.2.3. *Состав COBIT 5.*

Семейство COBIT 5 включает следующие публикации:

1. COBIT 5 (бизнес-модель).

2. Своды рекомендаций по факторам влияния, которые детально описывают каждый из них, а именно:

- COBIT 5: Процессная модель;
- COBIT 5: Enabling Information;
- Прочие своды знаний по факторам влияния (см. на сайте isaca.org/cobit).

3. Рекомендации COBIT 5 для профессионалов, а именно:

- COBIT 5: Внедрение;
- COBIT 5 for Information Security;
- COBIT 5 for Assurance;
- COBIT 5 for Risk;
- Прочие рекомендации для профессионалов (см. isaca.org/cobit).

4. Онлайн-среда для совместной работы, которая призвана способствовать наиболее эффективному использованию COBIT 5.

COBIT 5, так же, как и ISO 38500:2017, чётко разделяет руководство и управление ИТ (Рис. 2.2.4).

COBIT 5 не предписывает, но рекомендует внедрение процессов руководства и управления на предприятии в представленных на рисунке 3 областях охвата. Предприятие может организовывать процессы так, как считает нужным, с единственным условием: должны быть охвачены все задачи руководства и управления. На малых предприятиях процессов может быть немного, а в крупных и сложных организациях может существовать несколько процессов, выполняющих одну задачу.

В методологию COBIT 5 входит эталонная модель процессов (Рис. 2.2.5), в которой подробно описаны процессы руководства и управления. В модель включены все

Рис. 2.2.4. *Ключевые области руководства и управления (COBIT 5).*

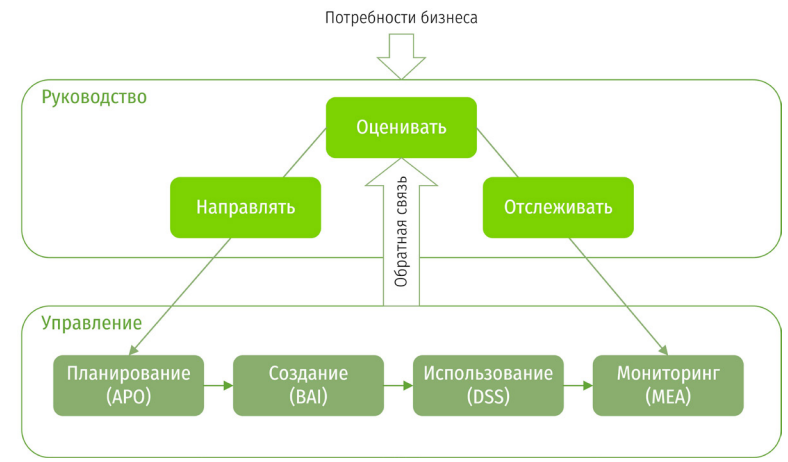
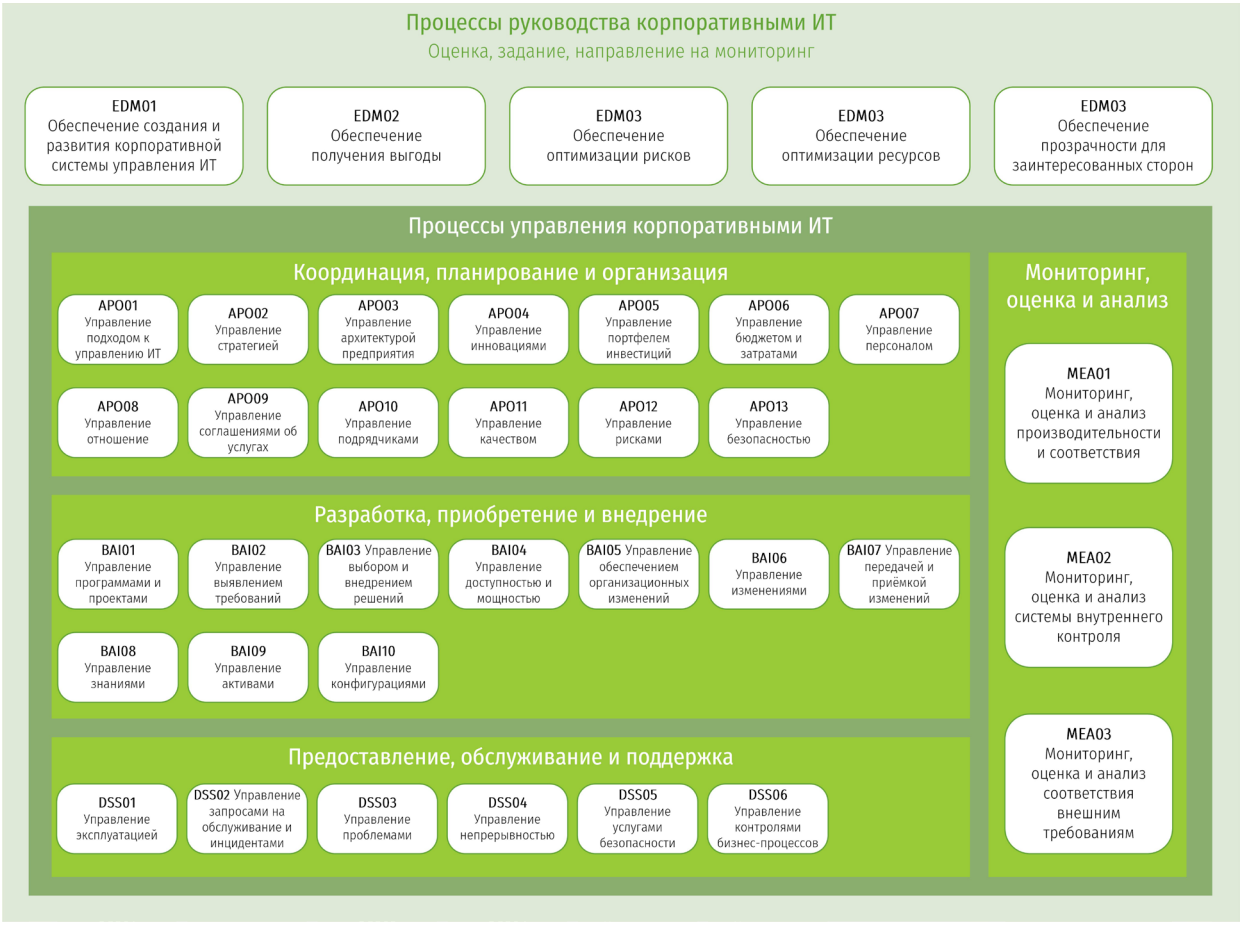


Рис. 2.2.5. *Эталонная модель процессов COBIT 5.*



связанные с ИТ процессы, обычно существующие на предприятии, что создаёт единый понятийный аппарат, общий для ИТ- и бизнес-менеджеров. Предложенная модель является полной и подробной, однако она не единственно возможная. Каждое предприятие определяет свой набор процессов, принимая во внимание контекст, в котором работает.

COBIT 5 также предоставляет рекомендации по внедрению, модели каскада целей бизнеса и ИТ, факторы влияния и множество других материалов, которые могут быть полезны при практическом внедрении подхода.

Организация контроля ИТ-деятельности

В этом разделе мы поговорим об одном из важнейших, и в то же время сложном элементе корпоративного управления — контроле ИТ-деятельности. По мере роста своего подразделения, CIO становится всё в большей степени постановщиком задачи, нежели непосредственным управляющим тех или иных процессов. В таких случаях, если ИТ-руководитель делегирует кому-либо из своих подчинённых или во внешнюю компанию задачи по управлению соответствующими процессами, организация контроля становится особо важной задачей. Одним из таких случаев является наличие филиалов, когда,

даже имея технические средства удалённого мониторинга ИТ-инфраструктуры, необходимо обладать определённой уверенностью, что ИТ-персонал в филиалах действует согласно принятым нормам и правилам.

Поэтому ниже мы кратко опишем практическую методику постановки системы контроля ИТ-деятельности компании. Система контроля ИТ-деятельности может и должна дать CIO уверенность в надёжной и качественной работе ИТ- подразделения.

Перед этим необходимо сделать важное замечание. Приведём пример целей контроля по организации управления службой технической поддержки и инцидентами.

- ***Служба технической поддержки***. Наличие службы технической поддержки, являющейся зоной взаимодействия пользователей и ИТ, призванной регистрировать, распределять и анализировать все обращения, докладывать об инцидентах, требованиях оказания услуг и запросах на информацию. Налаженный мониторинг и процедуры разрешения инцидентов, основанные на принятых уровнях обслуживания в соответствии с соглашением об уровне обслуживания (SLA), которые дают возможность классифицировать и расставлять приоритеты в отношении всех инцидентов, запросов о поддержке или об информации.
- ***Регистрация запросов***. Наличие функции и системы, позволяющих учитывать и отслеживать обращения, инциденты, запросы о поддержке или об информации. Наличие тесной связи с процессами управления инцидентами, управления проблемами, управления изменениями, управления мощностями и управления доступностью. Классификация инцидентов в соответствии с корпоративными и сервисными приоритетами. Информирование пользователей о текущем статусе своих запросов.
- ***Разрешение инцидентов***. Наличие процедур службы поддержки, предусматривающих управляемое разрешение инцидентов, которые не могут быть ликвидированы незамедлительно. Разрешение инцидентов в пределах, установленных SLA.
- ***Закрытие инцидента***. Наличие процедур оперативного мониторинга по окончательному разрешению запросов пользователей. Фиксация механизма решения инцидента и подтверждение отсутствие претензий пользователя после разрешения инцидента.
- ***Отчётность и анализ тенденций***. Наличие учёта работы службы поддержки и времени ответа службы поддержки на запросы, чтобы руководство имело возможность оценить е` эффективность.

Контроль, конечно, не может осуществляться только «по событиям», когда каждое задание (поручение) подчинённому фиксируется, и затем проверяется его исполнение. Такое возможно только по важным проектам и перечню особо критически важных заданий. Современные подходы к организации системы контроля позволяют осуществлять контроль непрямыми методами:

- периодический анализ нормативно-методического обеспечения деятельности ИТ-подразделения;
- анализ знаний сотрудниками этой документации;
- автоматизированная система организации ИТ-деятельности;
- сбор документальных доказательств о действиях сотрудников согласно нормативно-методическим документам и т.д.

На базе такого подхода в компании создаётся система контроля ИТ. На практике данную систему можно формировать в четыре этапа.

Этап 1. Где мы осуществляем контроль?

На этом этапе определяются области контроля и те группы процессов, которые мы собираемся контролировать. Очевидно, что отражённые в модели COBIT 37 процессов в разные моменты времени имеют разную ак-

туальность для компании. Поэтому, в первую очередь, необходимо определить перечень наиболее важных областей (групп процессов).

Во многих случаях компании начинают внедрение структурированного процессного управления и контроль с области «эксплуатации и сопровождения», с последующим постепенным распространением на другие области. Хотя, во всех без исключения компаниях ведётся в той или иной степени деятельность во всех четырёх областях, но именно эксплуатация и сопровождение в первую очередь требуют чёткой процессной организации работ для минимизации рисков, связанных с отказами в работе ИТ-систем.

Этап 2. Что контролируем?

На этом этапе определяются цели ИТ-контроля для выбранных на предыдущем этапе ИТ-процессов. Цели контроля должны быть чётко зафиксированы; причём, именно по степени их достижения, а точнее, по степени отклонения от их достижения, будут определяться итоговые ИТ-риски в компании. Необходимая основа для формулирования целей контроля содержится в COBIT — там приведены цели контроля для каждого из ИТ-процессов. В качестве примера ниже приведены цели контроля для процесса «Управление запросами на обслуживание и инцидентами» (Manage Service Requests and Incidents, DSS02) из COBIT. По результатам разработки первых двух уровней методики должна сложиться картина, связывающая цели контроля и конечные бизнес-цели компании.

Этап 3. Как контролируем?

На этом этапе определяются критерии и показатели, по которым происходит контроль, то есть условия, которые должны быть выполнены, чтобы можно было сделать вывод о достижении определённой цели контроля. Значительное количество критериев также содержится в COBIT. Например, для процесса «Управление запросами на обслуживание и инцидентами» COBIT предлагает оценивать результаты с помощью следующих показателей:

- доля пользователей, удовлетворённых службой поддержки «первой линии»;
- доля инцидентов, разрешённых в течение согласованного/приемлемого срока;
- доля запросов, оставшихся без ответа.

На этом же уровне определяются и эталоны для оценки степени продвижения к заданной цели. Здесь можно опираться на модели зрелости процессов, приведённые в COBIT.

Этап 4. Как собираем данные?

Этот этап завершает формирование методики контроля созданием списка контрольных вопросов, позволяющих выполнить наблюдения, произвести опросы и собрать необходимые свидетельства выполнения заданных критериев.

В итоге, двигаясь по данным уровням «сверху — вниз», CIO определяет необходимую методику проверки. После этого движением «снизу — вверх» производится контроль ИТ-деятельности через получение ответов на обозначенные вопросы и сбор свидетельств, выяснение степени выполнения критериев и, соответственно, достижения целей контроля. Результатом работы становится выяснение уровня зрелости процессов в ИТ-подразделении компании.

Отдельным этапом контроля может стать интерпретация результатов. Несмотря на общеизвестность модели зрелости процессов, изложение результатов в этих терминах для бизнес-руководителей может оказаться недостаточно понятным. В то же время, прямое следствие уровня зрелости ИТ-процессов — уровень существующих рисков, связанных с ИТ-деятельностью — является категорией, гораздо более ясной руководству компании. В итоге, сложившаяся по результатам проведения контрольной проверки картина состояния ИТ-деятельности и уровня существующих ИТ-рисков может стать основным контрольным инструментом программы улучшения, разработанной по результатам проведения проверки.

Глава 2.3

ИТ в холдинговых структурах

Роберт Киракосян

Классификация холдингов

В этой главе мы опишем те особенности управления ИТ, которые связаны со сложной организационной структурой холдингов. Существует несколько типов и классификаций холдинговых структур. Для CIO важны три разреза.

1. В зависимости от видов работ и функций, которые выполняет головная компания, различают:

- ***чистый (финансовый) холдинг***, в котором головная компания не ведёт никакой производственной деятельности, а выполняет только контрольно-управленческие и финансовые функции;
- ***смешанный (операционный) холдинг***, в котором головная компания ведёт хозяйственную деятельность, производит продукцию, оказывает услуги, но одновременно выполняет и управленческие функции по отношению к дочерним предприятиям.

2. С точки зрения производственной взаимосвязи компаний, выделяют:

- ***интегрированный (или вертикально интегрированный) холдинг***, в котором предприятия связаны технологической цепочкой (данный тип холдингов получил широкое распространение в нефтегазовом комплексе, где под руководством головной компании объединены предприятия по добыче, транспортировке, переработке и сбыту продукции);
- ***конгломератный холдинг***, который объединяет разнородные предприятия, не связанные технологическим процессом, и каждое из дочерних предприятий ведёт свой бизнес, не зависящий от других «дочек».

3. В зависимости от степени взаимного влияния предприятий, различают:

- ***классический холдинг***, в котором головная компания контролирует дочерние предприятия в силу своего преобладающего участия в их уставном капитале, а дочерние предприятия, как правило, не

владеют акциями головной компании;

- ***перекрёстный холдинг***, при котором предприятия владеют контрольными пакетами акций друг друга.

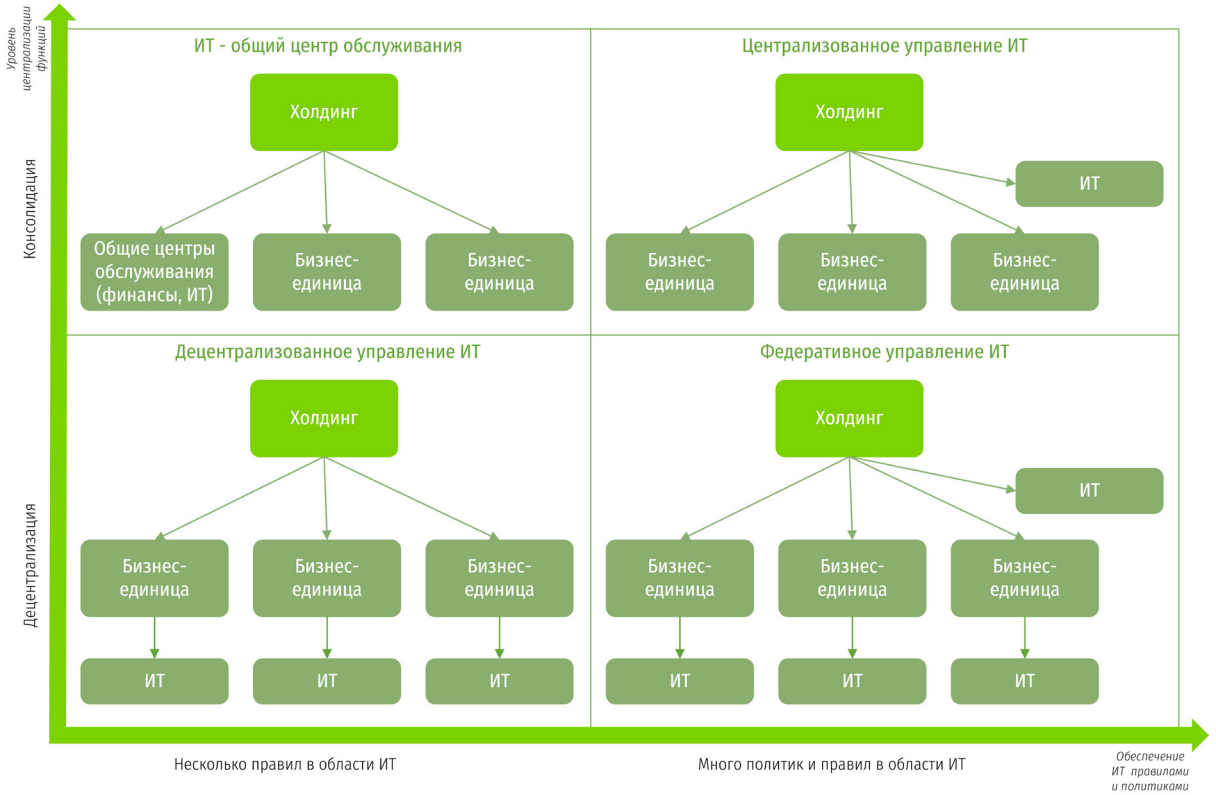
В зависимости от типа холдинга, возможности централизации процессов управления, в том числе и ИТ, принципиально различны. Например, в случае чистого (финансового) холдинга, контроль операционной деятельности дочерних компаний минимален. И в этом случае в головной компании холдинга необходим лишь минимальный набор ИТ-систем, например, класса BI, ECM, бюджетирования и т.п. А в случае смешанного (операционного) холдинга весь холдинг фактически развивается как единое предприятие — и тут необходимы совсем другие, комплексные/интегрированные ИТ-решения. Существует и масса «промежуточных» вариантов организации ИТ, зависящих как от типа холдинга, так и от конкретных бизнес-процессов, динамики рынка, законодательных требований и т.д.

Четыре модели управления ИТ в холдингах

В зависимости от уровня централизации/децентрализации функций управления в холдинге, а также от объёма политик и правил, используемых при управлении ИТ, можно выделить четыре модели управления ИТ в холдинге (Рис. 2.3.1).

1. Централизованное управление.
2. Децентрализованное управление.
3. Общие центры обслуживания.
4. Федеративное управление.

Рис. 2.3.1. *Четыре модели управления ИТ в холдингах.*



Централизованное управление

Общую тенденцию, которая явно наблюдается в крупных компаниях и холдингах, можно описать так: «все что можно централизовать — надо централизовать». Преимущества централизации очевидны.

При централизованном управлении вся дирекция по ИТ и основная ИТ-инфраструктура располагается в корпоративном центре. В бизнес-единицах холдинга остаётся только очень небольшое количество ИТ-сотрудников, которые обеспечивают выполнение некоторых элементарных функций, таких как установка новых рабочих мест из «образов», подготовленных в корпоративном центре, обслуживание оргтехники — принтеров, факсов, телефонов и пр. Эта форма управления ИТ подразумевает максимальную и практически полную стандартизацию всех элементов ИТ-инфаструктуры, процессов, а также услуг в рамках всех предприятий холдинга. Это позволяет легко управлять и контролировать ИТ-бюджет и избегать проведения неконтролируемых закупок и активностей на местах.

С другой стороны, у этой формы есть и недостатки, важнейший из них — отсутствие гибкости и фокусировки, необходимой различным компаниям холдинга. Централизованные компании испытывают серьёзную нехватку гибкости в удовлетворении потребностей своих бизнес-единиц, порождая неэффективные бюрократизированные бизнес-процессы. В случае с холдингом, компании которого работают в различных отраслях, централизованная форма управления зачастую становится неэффективной.

Децентрализованное управление

Это модель максимальной децентрализации управления, когда каждая из компаний холдинга имеет свою ИТ-службу и практически не взаимодействует с остальными компаниями холдинга. Такие формы управления встречается в модели чистого (финансового) и конгломератного холдинга (объединяющего разнородные предприятия, не связанные технологическим процессом). Централизации в этом случае могут подвергаться лишь несколько функций. Как правило, даже в этом случае корпоративный центр проводит утверждение и контроль бюджетов на уровне годовых бюджетов, а также, возможно, устанавливает стандарты на некоторое оборудование. Все остальные функции ИТ самостоятельно выполняются в компаниях холдинга, включая закупку всего компьютерного и телекоммуникационного оборудования, выбор и внедрение информационных систем и т.д.

Однако, практика показывает, что децентрализация функций приводит к высокой стоимости обслуживающих ИТ-структур, а также ряду дополнительных проблем (дублирование функций, разрозненность информации и т.д.).

Общие центры компетенции

При любой модели управления, связанной с той или иной степенью централизации, важной формой управления ИТ является создание специальных центров компетенции по различным ИТ-направлениям, которые централизованно выполняют ряд функций для всех предприятий холдинга. В каком-то смысле такие центры компетенции являются «предтечей» создания выделенного общего центра обслуживания, и их создание влечет за собой те же преимущества, что и общие центры обслуживания, только в меньших масштабах. Примеры функций, которые могут охватываться центрами компетенции:

- внедрение и обслуживание каналов связи и магистральных маршрутизаторов, систем унифицированных коммуникаций, служб каталогов и т.д.;
- первая линия Service Desk;
- обслуживание и развитие ERP-системы;
- информационная безопасность;
- обслуживание ЦОД.

Общий центр обслуживания

Организация общих центров обслуживания — современное направление развития холдингов и крупных компаний. Две стратегии построения компании (централизация и децентрализация) находятся на разных полюсах шкалы «эффективность/кастомизация и гибкость». В результате золотая середина — создание общих центров обслуживания бизнеса, которым свойственна эффективность и, одновременно, гибкость услуг.

Целесообразность создания общих центров обслуживания зависит от совокупности огромного количества внутренних и внешних факторов. Несмотря на положительную в целом мировую практику, к сожалению, не существует однозначного ответа на вопрос об их эффективности в российских условиях. Основные цели создания общих центров обслуживания, как правило, следующие:

- оптимизация затрат холдинга в целом;
- совершенствование системы управления качеством;
- унификация и сокращение бизнес-процессов в рамках единой структуры;
- повышение управляемости холдинга.

Общие центры обслуживания бизнеса уменьшают стоимость часто используемых операций за счёт их консолидации и унификации. Компания, создав обособленный центр обслуживания, значительно уменьшает избыточные операции и повышает эффективность и уровень услуг внутренним потребителям. В случае, когда бизнес-единицы холдинга достаточно близки по бизнесу, формам организации и принципам управления, выделение ИТ в специализированный общий центр обслуживания представляется достаточно эффективным решением. В остальных случаях, это решение требует дополнительного анализа.

Тема выделения общего центра обслуживания в значительной степени пересекаются с темой аутсорсинга.

Федеративное управление

В большинстве холдингов используется лишь частично централизованное управление ИТ. Это связано со сложностью производственных процессов на предприятиях, наличием большого количества унаследованных систем, «дороговизной» персонала в местах расположения центральных компаний холдинга. Такая форма управления, сочетающая централизацию и децентрализацию, носит название федеративной.

В этом случае дирекция по ИТ в корпоративном центре берёт на себя только часть функций, при этом оставляя достаточную свободу ИТ-службам компаний холдинга. Важнейшие функции, которые должна брать на себя центральная дирекция по ИТ корпоративного центра, следующие:

- разработка стратегии и тактики развития ИТ в холдинге;
- согласование портфеля ИТ-проектов холдинга, контроль выполнения ключевых для всех компаний холдинга проектов;
- согласование и контроль ИТ-бюджетов всех дочерних компаний холдинга на ежемесячной или ежеквартальной основе;
- выработка и контроль соблюдения стандартов на всё основное серверное, телекоммуникационное и офисное оборудование;
- выбор ключевых поставщиков оборудования и корпоративных лицензий на ПО.

Каждая из компаний холдинга, при этом, имеет свою ИТ-службу и часто свой ЦОД. ИТ-службам каждой из компаний должны быть переданы все нецентрализованные функции, например, внедрение и обслуживание корпоративных информационных и аналитических систем, закупка компьютеров и офисного оборудования и т.д. Как правило, в случае федеративной формы управления создаётся консультационный орган по ИТ — Совет по информационным технологиям. Совет по информационным технологиям возглавляется CIO холдинга, и в него входят все CIO дочерних компаний. В зависимости от типа холдинга, функции Совета различны.

Глава 2.4

Управление персоналом

Дмитрий Иншаков

Зачем CIO компетенции ИТ-менеджера?

Несмотря на стремительное развитие информационных технологий, они по-прежнему не могут успешно работать без людей — ИТ-персонала, который администрирует, поддерживает, модернизирует и т. д. информационные системы и ИТ-сервисы в компании. Несмотря на то, что требования к уровню профессиональной квалификации сотрудников в целом растёт, согласно мировой статистике, основной источник проблем и ошибок в ИТ-системах – это люди, «человеческий фактор». Таким образом, необходимое условие успешной работы ИТ-департамента — эффективное управление персоналом. Но для CIO это нередко оказывается сложнее, чем управлять бизнес-системами и ИТ-инфраструктурой. Чтобы привлечь и удержать в штате наиболее опытных и талантливых специалистов, а также их мотивировать на достижение высоких результатов, требуется продуманная кадровая политика в ИТ-подразделениях и действенные методы работы с персоналом.

Кадровая работа с ИТ-специалистами имеет целый ряд особенностей. Работники по кадрам признают, что ИТ-сотрудники – люди особенные. А значит, и их оценка, и мотивация, и развитие – это отдельная нетривиальная работа. Чтобы работать с айтишниками и успешно противостоять «кадровому голоду», от которого страдают практически все организации, необходимо тесное сотрудничество кадровой службы и ИТ-руководителей. Хорошей практикой может быть выделение в кадровой службе одного или нескольких сотрудников (в зависимости от размера компании), предоставляющих сервисы ИТ-отделу. Речь идёт как о найме (когда важно, чтобы рекрутёр хотя бы в общих чертах понимал специализацию и задачи различных ИТ-специалистов и руководителей), так и о помощи в оценке, развитии, материальной и нематериальной мотивации сотрудников отдела.

Структура ИТ-департамента

Структура большинства ИТ-департаментов на сегодняшний день является иерархической. Существуют различные принципы формирования оргструктуры ИТ-департамента. Она может формироваться по:

- территориальному признаку;
- проектному признаку;
- функциональному признаку (компетенциям).

Авторы Учебника считают, что наиболее эффективно формирование структуры по функциональному признаку, так как это создаёт возможности для развития компетенций, позволяет унифицировать процессы и используемые технологии в ИТ-департаменте. А уже в рамках функционального деления может проводиться деление по территориальному признаку, если это необходимо. Но старайтесь избегать создания в крупных офисах компании мини ИТ-отделов с собственной иерархией, поскольку это обычно приводит к дублированию систем и сервисов, проблемам с общей ИТ-архитектурой, стретегией и т.д. В рамках каждого функционального подразделения очень важно создать качественный набор требуемых вам компетенций ИТ-специалистов. Хорошей практикой является создание центров компетенций, когда, например, все программисты находятся в одном офисе и активно делятся опытом и знаниями между собой.

> «Заберите у меня мои деньги, заводы, станки и фабрики, но оставьте мне моих людей и вскоре мы создадим заводы лучше прежних. Оставьте мне мои фабрики, но заберите моих людей — и скоро полы заводов зарастут травой.»
>
> ***Генри Форд***

Экспертиза – это комплексное понятие, которое включает в себя не только наличие квалифицированных и опытных ИТ-специалистов, но и грамотные процессы по организации их работы, а также требует формирования слаженной команды.

В непосредственном подчинении у CIO, как правило, находятся руководители следующих ИТ-подразделений:

- проектный офис,
- группа разработки бизнес-приложений,
- группа поддержки бизнес-систем,
- служба поддержки пользователей,
- служба системного администрирования и ИТ-инфраструктуры,
- служба информационной безопасности (но более правильным будет, для обеспечения независимости от ИТ-руководства, вынести её за пределы ИТ-отдела – с подчинением руководителю, ответственному за управление рисками/безопасностью или за операционное управление компанией).

При этом, оптимальным количеством прямых подчинённых на любом уровне, по мнению авторов, является пять-семь человек. В этом случае возможно уделять достаточно времени не только непосредственно управлению подчинёнными, но также их развитию и обучению.

Количество подразделений внутри ИТ-департамента может сильно отличаться в зависимости от размеров компании, но всегда следует стараться не смешивать между собой команды, отвечающие за разработку и внедрение систем, с командами, которые занимаются их поддержкой и эксплуатацией.

Оценка ИТ-персонала. Уникальность ИТ-специалистов

Каждая компания так или иначе оценивает результаты работы своих сотрудников и их потенциал для дальнейшего развития. В зависимости от целей, которые ставятся при оценке, выбирается соответствующий метод. Давайте рассмотрим четыре наиболее распространенных из них:

1. Оценка результатов достижения целей и показателей (чаще всего – годовая, реже – на ежеквартальной или ежемесячной основе);

2. Оценка профессиональных качеств (аттестация);

3. Оценка потенциала сотрудника или оценка по компетенциям (assessment/ ассессмент);

4. Экспертная оценка по компетенциям, например, по методу «360 градусов».

Оценка результатов достижения годовых целей и показателей (annual performance review) является важнейшей составляющей «управления по целям» (management by objective). При этом, активно используются ключевые показатели эффективности (КПЭ/KPI – key performance indicators), о которых мы более подробно будем говорить ниже. Как правило, это не только оценка результатов достижения целей показателей за прошедший год, но и определение целей сотрудника на следующий год на основании декомпозированных стратегических целей компании, а также определение потребностей сотрудника в обучении. Такой подход позволяет опираться в оценке работы сотрудника на объективные показатели, а не только на личное мнение непосредственного руководителя. Чаще всего проводится менеджерской командой отдела, либо непосредственным руководителем. Результаты такой оценки используются в системе мотивации (как основание для премирования), для рекомендаций по внутренней ротации, являются предпосылками для обсуждения изменения заработной платы.

> Говоря о команде ИТ-департамента следует отметить, что поддержание командного духа в коллективе — одна из важнейших задач CIO, серьёзно влияющая на эффективность ИТ в компании.
>
> Здесь важно правильно поддерживать баланс между новичками и опытными сотрудниками, молодыми и пожилыми, мужчинами и женщинами и т.д.
>
> Вопрос формирования команды ИТ-специалистов заслуживает отдельного обстоятельного обсуждения и, возможно, получит своё развитие в следующих версиях Учебника.
>
> Пока скажем лишь о том, что для команды важно иметь общую цель, харизматичного лидера, общие принципы управления, традиции, удобные средства совместной работы и коммуникации.
>
> Формирование команды начинается с подбора сотрудников, которые «впишутся» в общую команду – для этого CIO прибегают в том числе к таким методам, как личное финальное собеседование отобранных кандидатов на вакансии в ИТ-отделе, и/или групповое собеседование кандидата с несколькими ключевыми сотрудниками команды, в которую он приходит. Но не забывайте, что групповое интервью может быть стрессом для кандидата.

Аттестация – это оценка профессиональных качеств, знаний и навыков сотрудника на соответствие занимаемой им должности. Форма проведения аттестации регламентируется Трудовым Кодексом РФ (ТК РФ). Результатом, как правило, является заключение аттестационной комиссии, в котором указывается соответствие или несоответствие занимаемой должности. Также по результатам аттестации возможно изменение заработной платы, выплата бонусов. Но аттестация может явиться и

причиной увольнения сотрудника или его перевода на другую должность.

Ассессмент – это определение степени владения наиболее важными компетенциями, а также определение потенциала сотрудников. Основывается на специально разработанном профиле компетенций компании. Зачастую, он проводится с привлечением внешних экспертов в области оценки персонала. Нередко частью ассессмента являются бизнес-игры, в которых сотруднику приходится проявлять себя через решение управленческих задач, далеко выходящих за пределы его полномочий в обычной работе. Частым сценарием является то, что сотрудника в ходе игры ставят на место его непосредственного руководителя (или руководителя ИТ-подразделения, в котором он работает), и дают для решения проблемы соответствующего уровня. Результатом ассессмента должно являться выявление сильных и слабых сторон сотрудника, получение «обратной связи», составление планов обучения, оценка и планирование человеческих ресурсов компании. Формат проведения не регламентируется ТК РФ, а определяется только внутренними нормативными документами. По результатам оценки нельзя проводить административные изменения, результаты носят рекомендательный характер. Тем не менее, их вполне можно использовать, к примеру, для выявления «кадрового резерва» — будущих руководителей. Также попутным дополнительным результатом такой бизнес-игры может явиться свежий взгляд на известные проблемы и задачи отдела.

Добавим, что в аттестации и ассессменте могут оказаться весьма полезны профессиональные стандарты в области ИТ (см. врезку ниже).

Профессиональные стандарты

Марина Аншина

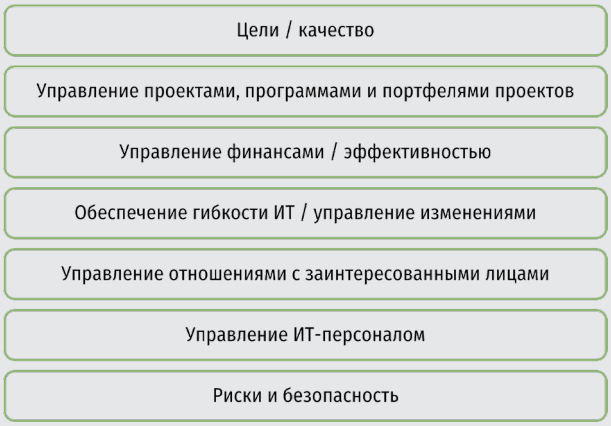
В статье 195.1 Трудового кодекса Российской Федерации профессиональный стандарт определяется как «*характеристика квалификации, необходимой работнику для осуществления определённого вида профессиональной деятельности*». В свою очередь, согласно указанной статье, квалификация работника – «*это уровень знаний, умений, профессиональных навыков и опыта работы работника*».

Такой подход к профессиональной деятельности является общим для большинства стран и, несомненно, представляет собой шаг вперёд по сравнению с оценкой профессионалов только по знаниям.

В России работу по созданию профстандартов в области ИТ возглавила АПКИТ – Ассоциация предприятий компьютерных и информационных технологий. В мае 2013 года прошло собрание членов АПКИТ, на котором были распределены задачи по разработке профстандартов. Работу над профстандартом «Менеджер по информационным технологиям» возглавил СОДИТ (Союз ИТ-Директоров России).

При выборе и описании квалификационных уровней профстандарта «Менеджер по ИТ» члены рабочей группы учитывали опыт международных профессиональных стандартов, прежде всего EQF и e-CF.

Рис. 2.4.1. *Архитектура профстандарта «Менеджер по ИТ».*



Кроме международного опыта при разработке профстандарта рабочая группа постаралась применить системный подход, разработав архитектуру профстандарта, приведённую на Рис. 2.4.1.

По шаблону Минтруда, каждый профстандарт должен начинаться с описания основной цели профессиональной деятельности. Для менеджера по ИТ она была определена следующим образом: «Управление предоставлением, использованием и развитием информационных технологий (ИТ)».

Всего Минтруд определил 9 уровней квалификаций, из которых для Менеджера по ИТ были выбраны уровни 6-9. В Табл. 2.4.1 приведён список уровней квалификации и их трудовых функций, сформированных на основании архитектуры стандарта, приведённой на Рис. 2.4.1.

В соответствии с методическими рекомендациями и шаблоном Минтруда, уровням квалификаций даются наименования, которые называются обобщённые трудовые функции.

Для каждой обобщённой трудовой функции описываются возможные наименования должностей, требования к образованию и обучению, требования к опыту практической работы и особые условия допуска к работе. Для всех обобщённых трудовых функций необходимо высшее образование в объёме магистратуры или специалитета и опыт работы от одного года для 6-ого уровня квалификации до 7 лет для 9-ого. Трудовые функции представляют собой группу действий, которые должен выполнять менеджер по ИТ соответствующего уровня квалификации. Затем для каждой обобщённой трудовой функции для каждой трудовой функции прописываются конкретные трудовые действия, которые должен выполнять менеджер по ИТ.

В Табл. 2.4.2 приведён список утверждённых и разрабатываемых профстандартов в области ИТ. Кроме того, профессиональные стандарты становятся основой для созданий образовательных стандартов, что даст возможность готовить специалистов, востребованных на рынке труда.

Табл. 2.4.1. *Уровни квалификации и их трудовые функции профстандарта «Менеджер по ИТ».*

Наименование обобщённой трудовой функции	Уровень квалификации	Наименование трудовых функций
Управление ресурсами ИТ	6	Управление качеством ресурсов ИТ Управление ИТ-инфраструктурой Управление расходами на ИТ Управление изменениями ресурсов ИТ Управление отношениями с поставщиками и потребителями ресурсов ИТ Управление персоналом, обслуживающим ресурсы ИТ Управление информационной безопасностью ресурсов ИТ

Наименование обобщённой трудовой функции	Уровень квалификации	Наименование трудовых функций
Управление сервисами ИТ	7	Управление договорами об уровне предоставления сервисов ИТ (SLA) Управление ИТ-проектами Управление моделью предоставления сервисов ИТ Управление изменениями сервисов ИТ Управление отношениями с пользователями и поставщиками сервисов ИТ Управление персоналом, осуществляющим предоставление сервисов ИТ Управление непрерывностью сервисов ИТ
Управление информационной средой	8	Управление стратегией ИТ Управление программами и портфелями ИТ-проектов Управление формированием и внедрением системы показателей оценки эффективности ИТ Управление изменениями информационной среды Управление отношениями с поставщиками и потребителями информации Управление персоналом, обслуживающим и развивающим информационную среду Управление рисками ИТ
Управление ИТ-инновациями	9	Управление формированием вклада ИТ в создание и реализацию инновационной стратегии Управление выявлением и внедрением ИТ-инноваций Управление оценкой эффективности ИТ-инноваций Управление знаниями с помощью ИТ Управление взаимоотношениями с заинтересованными лицами Управление персоналом, обеспечивающим инновации ИТ Управление рисками инновационного отставания в ИТ

Табл. 2.4.2. *Профессиональные стандарты области ИТ, принятые и разрабатываемые.*

Профессиональные стандарты	Актуальная версия	Код в реестре
Администратор баз данных	5.140917 Утверждён Приказом Минтруда России №647н от 17.09.2014	06.011

Профессиональные стандарты	Актуальная версия	Код в реестре
Архитектор программного обеспечения	5.140411 Утверждён Приказом Минтруда России №228н от 11.04.2014	06.003
Менеджер по информационным технологиям	5.141013 Утверждён Приказом Минтруда России №716н от 13.10.2014	06.014
Менеджер продуктов в области информационных технологий	5.141120 Утверждён Приказом Минтруда России №915н от 20.11.2014	06.012
Программист	5.131118 Утверждён Приказом Минтруда России №679н от 18.11.2013	06.001
Разработчик Web и мультимедийных приложений	5.160824 Утверждён Приказом Минтруда России № 44н от 18.01.2017	06.035
Руководитель проектов в области информационных технологий	5.141118 Утверждён Приказом Минтруда России №893н от 18.11.2014	06.016
Руководитель разработки программного обеспечения	5.140917 Утверждён Приказом Минтруда России №645н от 17.09.2014	06.017
Системный аналитик	5.141028 Утверждён Приказом Минтруда России № 809н от 28.10.2014	06.022
Специалист по большим данным	5.170106	-
Специалист по интеграции прикладных решений	5.170106	-
Специалист по интернет-маркетингу	5.170604	-
Специалист по информационным ресурсам	5.140908 Утверждён Приказом Минтруда России №629н от 8.09.2014	06.013
Специалист по информационным системам	5.141118 Утверждён Приказом Минтруда России №896н от 18.11.2014	06.015
Специалист по тестированию в области информационных технологий	5.131214 Утверждён Приказом Минтруда России №225н от 11.04.2014	06.004
Специалист по управлению данными и инфообъектами	-	-
Технический писатель (Специалист по технической документации в области ИТ)	5.140908 Утверждён Приказом Минтруда России №612н от 8.09.2014	06.019

Экспертная оценка по компетенциям несколько похожа на ассессмент, поскольку также проводится на основе специально разработанного профиля компетенций. Может проводиться по методу «360 градусов», когда компетенции сотрудника оценивают «со всех сторон» — коллеги, подчиненные, руководители и клиенты. Результатом должно явиться определение динамики развития компетенций сотрудника за год, определение потребности в дальнейшем обучении. Итоги оценки и план развития обычно обсуждаются с непосредственным руководителем одновременно с оценкой результатов деятельности за год. При этом, потенциал сотрудника не оценивается. Формат проведения не регламентируется ТК РФ, определяется только внутренними нормативными документами. По результатам экспертной оценки нельзя проводить административные изменения, результаты носят рекомендательный характер, учитываются при составлении планов на обучение, выдвижении в кадровый резерв.

Давайте сравним упомянутые четыре метода оценки. Как правило, оценить результаты работы, а также профессиональные качества ИТ-персонала – это не самая сложная задача. Во-первых, это могут сделать ИТ-менеджеры самой компании (оценивая достижения целей и другие результаты работы, проводя беседы с сотрудником и его коллегами, чтобы понять, какой ценой достигнут результат), во-вторых, сотрудников можно направить на сертификационные экзамены по их специализации (но помните, что этим вы также можете поднять их стоимость на рынке труда). Оценить потенциал гораздо сложнее. Ассессмент, пожалуй, наиболее эффективный (хотя и не дешёвый) метод, который позволяет решить эту задачу — понять, как и куда сотрудник может развиваться дальше, например, оценить возможности специалиста как потенциального менеджера; раскрыть сильные и слабые стороны. На практике ассессмент может состоять из двух этапов: первый — блок письменных тестов, второй — упражнения (бизнес-игра и индивидуальная презентация). По итогам эксперты должны оценить каждого участника по компетенциям.

Ассессмент, проведённый в рамках всей компании, даёт возможность посмотреть и проанализировать личные и обобщенные психологические портреты специалистов и руководителей отдельных подразделений, сравнить их со «средним» профилем. В одной из крупных российских компаний за два года ассессмент прошло около шестисот сотрудников, в том числе около сотни сотрудников ИТ подразделения (подробнее: «IT-персонал: оценка, мотивация и развитие». Дмитрий Иншаков и Анна Иншакова, Intelligent Enterprise, №1 2007). При этом, были выявлены следующие обобщенные психологические качества ИТ-специалистов, которые отличают их от специалистов других подразделений:

- независимы и самостоятельны, предпочитают минимальный контроль;
- уверены, что отличаются от других отделов и к ним необходимо «особое» отношение;
- как правило, имеют высокий уровень ответственности и лояльности;
- предпочитают предсказуемость переменам (в первую очередь, здесь имееются в виду перемены в управлении, организационной структуре и т.п., при этом к новым версиям программного обеспечения или «железа» сотрудники обычно гораздо более благосклонны);
- заинтересованы во мнении окружающих и хотят выглядеть в их глазах в лучшем свете;
- коммуникативные навыки – ниже, чем в среднем по компании (но в последние годы ситуация в ИТ с точки зрения развития этих навыков заметно улучшилась);
- склонны к интеллектуальному труду, анализу сложных технических вопросов, освоению новых технологий.

Стоит заметить, что не только ИТ-специали-

сты считают, что они отличаются от других отделов, но и представители других отделов часто воспринимают ИТ-специалистов как людей, занимающихся чем-то не очень понятным и говорящих на своём особом языке. Поэтому одну из задач CIO авторы видят в том, чтобы «навести мосты» между ИТ-подразделением и другими отделами компании. С одной стороны, «презентовать» стратегию и проекты ИТ для других отделов, помочь эффективно использовать уже имеющиеся в компании ИТ-системы и сервисы. С другой стороны, научить ИТ-персонал быть ближе к задачам бизнеса и избегать сложных технических терминов в общении с пользователями, принимать во внимание бизнес-приоритеты, цикличность бизнеса конкретной компании и т.д.

Для многих ИТ-специалистов имеет большое значение хорошее мнение окружающих, им важно иметь авторитет, и ради этого они готовы работать и работать. Поэтому ИТ-руководителям можно порекомендовать чаще хвалить своих подчинённых — это обычно стимулирует их к дальнейшим «подвигам». Также выделяется высокая толерантность (терпимость), наверное, поэтому ИТ-специалисты бывают неприхотливы к офисным помещениям (но не характеристикам компьютера, на котором работают) и «странностям» коллег, которых другие терпеть не могут. Безусловно, одной из отличительных черт является склонность к интеллектуальному труду и работе с абстрактными проблемами, поэтому не бойтесь давать подчинённым сложные задачи и достаточную самостоятельность в поиске вариантов их решения. Кроме этого, стоит отметить невысокую коммуникабельность и эмпатию (способность понимать других людей и сопереживать с ними), часто сопровождающиеся отсутствием стремления к лидерству. Поэтому к коммуникабельным сотрудникам ИТ, обладающим лидерскими навыками, стоит присмотреться, уделить особое внимание их дальнейшему развитию и карьерным перспективам.

Проблемы подбора ИТ-специалистов и ИТ-менеджеров

Стоимость подбора ИТ-специалиста через рекрутинговые агентства обычно составляет 20-25% от годовой заработной платы, а это существенная сумма. Хорошего, знающего ИТ-специалиста всегда сложно было найти, однако в последнее время рынок труда многих городов стал ещё сложнее и «беднее» на высококлассных специалистов. Сейчас в ИТ скорее «рынок кандидатов», чем «рынок работодателей». Доходит до того, что сильные кандидаты одновременно получают несколь предложений о работе, из которых неторопясь выбирают лучшее для них. Также бывают случаи, когда «тестовое задание» получает не только кандидат, но и будущие коллеги, работающие у потенциального работодателя.

К основным проблемам подбора ИТ-персонала можно отнести следующие:

- из-за демографической ситуации на рынке труда появляется меньше новых специалистов;
- быстро развивающийся рынок, появление новых крупных игроков приводит к тому, что спрос на ИТ-персонал превышает предложение;
- завышенные ожидания по размеру заработной платы, подогреваемые отдельными компаниями с большими бюджетами и высокой зависимостью от ИТ;
- HR-эксперты считают, что не-ИТ-компании (например, производственные) изначально менее привлекательны для некоторых ИТ-специалистов;
- гибкость и хитрость некоторых ИТ-компаний – студенты старших курсов начинают работать в ИТ-компаниях на неполную занятость и затем остаются в них, а первое знакомство с этими компаниями может

начинаться ещё со школы;

- для ряда ИТ-специалистов (особенно программистов) характерно искать работу через «узкий круг ограниченных лиц», поэтому работодателю сложно их найти;
- спрос на квалифицированный ИТ-персонал обычно превышает предложение, особенно на новые или редкие специальности.

В результате, поиск хорошего специалиста с узкой специализацией может затянуться на несколько месяцев, и во многих случаях компании вынуждены прибегать к помощи агентств по подбору персонала. При этом, поиск будет ещё более затруднён, если компания требует от ИТ-специалиста умения говорить на английском языке. Это обычно необходимо в международных компаниях для общения с коллегами в других странах и для оказания ИТ-поддержки иностранцам, работающим в российском представительстве. Как правило, прочитать техническую документацию на английском для большинства ИТ-сотрудников проблемы не составляет, но с разговорным языком у них дела обстоят гораздо хуже. Этот барьер преодолевает лишь около 20% соискателей.

Если вы не являетесь экспертом в предметной области кандидата, не стоит пытаться оценить его уровень знаний — лучше полагаться на профессиональные сертификаты (особенно, если их несколько), результаты тестов, мнение заслуживающего доверия эксперта в этой предметной области (желательно сотрудника вашей компании). Но если кандидат может и хочет учиться, то профессиональные навыки можно развить достаточно быстро. Слабо обучаемые ИТ-шники встречаются крайне редко. Но личные качества (например, умение общаться с людьми, устойчивость к стрессам, стремление к лидерству) развиваются гораздо медленнее и сложнее, чем технические навыки. Однажды один из авторов, принимая на работу специалиста службы поддержки, отдал предпочтение не «технарям», а кандидату с гуманитарным образованием и минимальным опытом в ИТ (он занимался установкой правовых баз). Зато этот кандидат прекрасно вписывался в команду, на лету схватывал новые знания и умел общаться с любыми собеседниками. Через несколько месяцев он стал лучшим специалистом службы поддержки, а ещё через пару лет — её руководителем.

Возникает вопрос: «Когда же сотрудник начнёт работать на 100%?» Для сотрудников ИТ-департамента этот момент чаще всего наступает примерно через 6 (на рядовых позициях) до 12 месяцев (на руководящих или на имеющих явный годовой цикл позициях) после прихода в новую компанию. Сотрудники, успевшие до этого поработать в нескольких компаниях, обычно адаптируются заметно быстрее, но с другой стороны и риск их дальнейшего перехода к другим работодателям – выше.

Роль KPI в управлении персоналом

По мнению многих экспертов, для долговременного успешного развития компании важно, чтобы были сформулированы и доведены до сотрудников миссия, стратегия и цели компании (краткосрочные, среднесрочные и долгосрочные). С практической точки зрения, это помогает правильно расставить приоритеты в работе с портфелем ИТ-проектов и сформировать штатное расписание на следующий год. Для каждого сотрудника имеет смысл составить и согласовать с его непосредственным руководителем список персональных целей (KPI) на год. Выполнение персональных целей должно систематически контролироваться в течение года (обычно ежеквартально или ежемесячно), а в кон-

це года — проводиться оценка конечного результата. Финансовые бонусы обычно завязаны на выполнение KPI. У сотрудников, работающих на одинаковых должностях (например, у специалистов службы поддержки пользователей), целевые значения KPI имеет смысл делать одинаковыми.

Одним из плюсов системы KPI является то, что она во многом переводит сложные диалоги между подчинённым и руководителем в плоскость цифр, а не эмоциональной личной оценки.

Можно ли выделить какие-либо универсальные KPI, которые можно применять для оценки работы большинства ИТ руководителей, отвечающих за разные направления? По мнению авторов, к ним можно отнести следующие показатели:

- степень удовлетворённости пользователей (внутренних клиентов ИТ-департамента),
- соблюдение соглашений об уровне сервиса (SLA),
- процент успешно выполненных проектов (срок, качество, бюджет),
- количество новых ИТ-сервисов и степень их востребованности в компании.

Конечно же, к ним стоит добавить и финансовые показатели:

1. Отклонение от утверждённого ИТ-бюджета менее чем на X% (имеет смысл только для медленно меняющихся компаний и практически не подходит для стартапов);

2. Возврат на инвестиции (ROI) от ИТ-проектов;

3. Соотношение инвестиционной (больше – лучше) и операционной частей ИТ-бюджета;

4. Расходы на ИТ в расчёте на одного сотрудника компании;

5. ИТ-бюджет в процентах от оборота компании (показатель достаточно популярный, но спорный).

Целевые значения по 3-му, 4-му и 5-му финансовым показателям необходимо выбирать на основе фактических значений KPI других компаний той же индустрии. Так, «хорошее» значение расходов на ИТ для производственной компании не будет таковым для банка, и наоборот.

Для сотрудников службы поддержки в качестве KPI можно выбрать процент своевременно решённых проблем пользователей; процент проблем, решённых непосредственно во время звонка в службу поддержки; количество решённых проблем/запросов и число оказанных консультаций (с учётом их сложности). И, пожалуй, самым интегральным KPI будет степень удовлетворённости пользователей тем, как решались их запросы. Причём, кнопки с выбором оценок (например, в виде смайликов-эмодзи) можно вставить прямо в электронное письмо с уведомлением о выполнении заявки. Из интересных практических идей стоит упомянуть, что в опросах пользователей можно использовать нетипичную шкалу (например, 6-ти или 10-ти балльную) и задавать значение «по умолчанию» на единицу меньше максимальной оценки.

Для некоторых позиций (таких, как программисты) выбор и отслеживание KPI представляет собой весьма нетривиальную задачу.

Выстраивая систему KPI, стоит избегать следующих типичных ошибок:

- несоответствие KPI стратегическим целям компании,
- неверное определение целевых значений и порогов,
- непонимание способов измерений и недостоверность данных,
- непрозрачность и излишнее усложнение KPI с точки зрения сотрудников, качество и количество работы которых мы оцениваем,
- слишком большое количество KPI (это снижает прозрачность и заставляет тратить неоправданно много времени на их измерение и оценку).

Развитие ИТ-персонала. Планирование тренингов

Развитие персонала целесообразно начать с планирования целей. Сначала определяются задачи, которые сотрудник должен решать в течение следующего года. Затем выявляются компетенции, которые необходимо развивать для успешного решения поставленных задач. Идеальной является ситуация, когда компания может предварительно провести оценку персонала, тем самым определив текущий уровень развития менеджерских и технических компетенций; затем сопоставить это с целями и задачами ИТ-департамента на следующий год и только после этого планировать развитие сотрудников. Это совместная работа HR и ИТ-руководителей. Целесообразно составлять годовой план тренингов для каждого сотрудника, и он может включать в себя не только развитие технических навыков, но и такие курсы, как «Управление проектами», «Управление временем», «Основы менеджмента», «Публичные выступления», «Ведение переговоров». На уровне ИТ-департамента в целом, во избежание накладок, нужно согласовать годовой план тренингов с графиками проектов и отпусков.

Не стоит забывать и о возможностях «бесплатного» обучения. Нередко при покупке лицензионного программного обеспечения (например, корпоративных лицензий Microsoft) в качестве бонуса может предлагаться определённый объём «бесплатного» обучения ИТ-специалистов на авторизованных курсах.

Есть и возможности «внутреннего» обучения. И это не только курсы «для своих», которые ведут опытные сотрудники компании. Например, если у предприятия несколько офисов, то можно проводить внутреннюю ротацию с целью приобретения нового опыта и знаний. Например, на несколько недель поменять местами специалистов службы поддержки двух офисов. Это также позволяет сотрудникам «встряхнуться», зарядиться новыми для них идеями и подходами, ближе познакомиться с коллегами, что помогает в дальнейшем взаимодействии на большом расстоянии.

Сегодня ряд экспертов считают, что традиционное обучение «в классе» даёт лишь 10% вклада в развитие сотрудников, ещё 20% — помощь руководителя, в том числе диалог и обмен практическим опытом. Так откуда же взять оставшиеся 70%? Это применение и закрепление полученных знаний на практике, в т.ч. в ходе новых проектов, работы в смежных, но незнакомых областях и т.д. Не стоит об этом забывать! Ведь бывает так, что после успешного, на первый взгляд, обучения сотрудника, стиль и методы его работы практически не меняются, а содержание тренинга достаточно быстро стирается из памяти. Если сотрудник не показал прогресса после обучения, то это повод побеседовать с ним и сделать вывод, почему так произошло. Есть ли для этого объективные причины (например, слабый преподаватель/тренер) или у сотрудника просто нет стимула к обучению? Следует помнить об этом при планировании тренингов на следующий год.

Компетенции как источник устойчивого развития

Рустем Валиев

при поддержке ССК Консалинг

Современный высококвалифицированный сотрудник востребован на рынке не как источник физической силы, а как источник знаний, компетенций, как производитель интеллектуального труда. Обладание сотрудниками необходимыми компетенциями и их эффективное использование в функциональной деятельности, особенно в сфере быстроразвивающихся информационных (а ныне и цифровых) технологий, становятся фундаментом для обеспечения инновационной деятельности и, как результат, источником долгосрочного устойчивого развития.

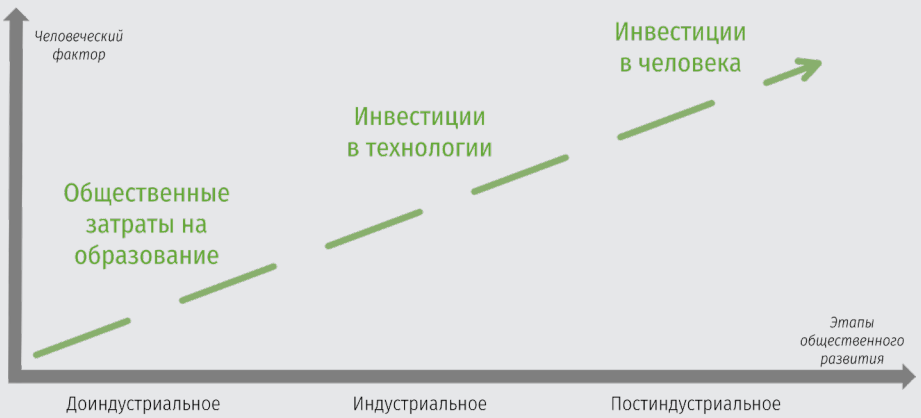
Ф. Махлуп доказывал, что в информационной экономике хозяйственная деятельность – это, главным образом, производство и применение информации и знания с целью сделать все другие формы производства более эффективными и тем самым создать больше материального богатства. Лимитирующий фактор здесь – наличие необходимых знаний . Известный специалист по управлению человеческими ресурсами Д. Ульрих утверждал: «обеспечение интеллектуального потенциала означает ускоренное распространение идей и информации внутри фирмы».

Компетенцию сотрудника можно представить как сумму двух составляющих – знания сотрудника и его способности и желания к коммуникациям с другими сотрудниками, направленным на выполнение функциональных обязанностей в полном объёме. При этом, использование баз знаний (порталов знаний), как внешнего источника структурированной и неструктурированной информации, позволяет существенно улучшить оба показателя, что даёт синергетический эффект, выражающейся в повышении общего уровня квалификации сотрудника. В общем виде данный подход можно представить в виде следующей формулы, где «знания» и «коммуникации» представлены в виде функции от параметра «База знаний»:

Компетенция = Знания (Базы знаний) + Коммуникации (Базы знаний)

Следует особо подчеркнуть, что анализ и контроль компетенции сотрудников позволяет компании эффективно строить краткосрочные (оперативные) и долгосрочные (стратегические) планы. При этом, текущая компетенция сотрудников используется для составления краткосрочных планов. Так, руководители могут прогнозировать результаты своей деятельности с использованием имеющихся ресурсов. В данном случае цель опосредована ресурсами. Для долгосрочных стратегических задач руководители компании действуют от обратного, т.е. прогнозируют необходимые ресурсы с требуемым уровнем квалификации. Требуемые ресурсы опосредованы стратегическими задачами компании.

Рис. 2.4.2. *Роль человеческого фактора на различных этапах общественного развития..*



Примечение редакции: *Подробно тема управления компетенциями будет раскрыта в следующей версии Учебника.*

Удержание сотрудников в компании. Мотивация материальная и нематериальная

Современные концепции управления ИТ-персоналом во многом основаны на понимании мотивационных установок сотрудников, умении их формировать и направлять в соответствии с задачами, стоящими перед организацией. Уход ценного специалиста из компании вызывает реальные потери и затраты, которые складываются из многих, не всегда заметных с первого взгляда, составляющих. Это затраты на подбор сотрудника (прямые расходы, а также время, потраченное работниками HR службы и руководителями ИТ-департамента, задействованными в процессе подбора), стоимость «простоя», так как успеть подобрать и пригласить нового человека в течение двух недель практически нереально. Также не стоит забывать, что в период испытательного (адаптационного) срока отдача от нового сотрудника редко составляет более 50%. Кроме того, из компании чаще уходят ценные сотрудники, которые востребованы на рынке и на замену которым иногда приходится брать не одного, а «полтора», а то и двух новых человек.

Как говорят некоторые руководители: «Незаменимых людей не бывает, просто некоторых можно заменить двумя-тремя». Чтобы минимизировать риски при уходе ИТ-специалистов из компании, CIO имеет смысл «резервировать» все ключевые функции в ИТ-департаменте. Например, системный администратор может выполнять основные процедуры, за которые отвечает администратор почтовой системы. Это также пригодится, если сотрудник болеет или уходит в отпуск. Хорошо, если у каждого ИТ-руководителя также есть заместитель/преемник, — тогда не придётся ломать голову, кем заменить его на время отпуска или в случае ухода из компании. Заметим, что найти и «вырастить» преемника – это задача, которая обычно занимает от нескольких месяцев до нескольких лет.

Во многих случаях оказывается дешевле вкладывать силы и деньги в мотивацию и удержание сотрудников, вместо того чтобы тратить их на подбор новых. Но не стоит воспринимать эти слова как призыв удерживать в компании всех сотрудников любой ценой. Не стоит забывать об эффекте «профессионального выгорания» — бывают ситуации, когда сотруднику действительно необходимо

Как удержать ИТ-специалистов?

- Убедитесь, что заработная плата соответствует среднерыночной стоимости специалистов с аналогичной квалификацией (или превышает её, если ваши требования или интенсивность работы выше средней по рынку).
- Минимизируйте контроль за ежедневной работой над проектами и задачами, контролируйте только промежуточные результаты.
- Помните про ориентацию на мнение окружающих — хвалите, но только «за дело»!
- Давайте новые интересные проекты тем, кто этого сам хочет.
- Предоставляйте возможности для (само) обучения, тестирования новых программ и оборудования.
- Рассмотрите возможности работы из дома (например, 1-2 раза в неделю) или по свободному графику для успешных специалистов.

сменить компанию, коллектив, заняться решением других задач. Очень важно понять, какова причина возможного ухода работника, и принять решение, что с этим делать. Если непосредственному руководителю или CIO сложно самостоятельно провести такую беседу, можно подключать HR-специалистов. В этом случае также будет проще разрабатывать и применять план удержания сотрудника или его индивидуальный карьерный план.

Точно так же, как и для сотрудников любых других отделов, мотивация ИТ-персонала разделяется на материальную и нематериальную составляющие. Материальная мотивация может быть постоянной и переменной. Изменение «постоянной» мотивации, т. е. размера заработной платы, «работает» не так долго, как может показаться, — по некоторым исследованиям, всего около двух-трёх месяцев (после этого сотрудник привыкает к новой цифре). С другой стороны, отсутствие роста заработной платы или планов по её изменению — серьёзный демотивирующий фактор. В случае, если уровень заработной платы заметно ниже среднего по рынку, серьёзно увеличивается риск, что сотрудник уйдёт в другую компанию. Лояльность и преданность сотрудников — не бесконечная величина. Поэтому размер заработной платы должен пересматриваться (в идеале — именно пересматриваться, а не «автоматически увеличиваться на X процентов») как минимум один раз в год. Сотрудник должен знать, что если он стал решать новые, более сложные задачи, увеличилась его зона ответственности, то компания обязательно это оценит. Должна быть и обратная составляющая: если сотрудник не покажет хороших результатов, то повышения заработной платы не будет.

Упорядочить процесс повышения заработной платы многим компаниям помогает система «грейдов» («уровней») сотрудников. К каждому грейду обычно привязаны как диапазон заработной платы, так и определённый уровень компетенций и знаний. Для перехода на следующий грейд сотрудник обычно должен своей работой подтвердить, что существенную часть времени он уже работает на этом уровне, а у компании должна быть бизнес-причина на такое продвижение.

Переменная часть (премии, бонусы и т. п.) должна быть связана с управлением по целям и выполнением KPI. Хорошие результаты дают также разовые премии и персональные надбавки, отмечающие особый вклад сотрудника в ключевые проекты, решение сложных задач или проблем.

Если же говорить о нематериальной составляющей, то для многих ИТ-специалистов важным нематериальным фактором мотивации является сама работа, если она интересна и «интеллектуальна». Для многих сотрудников имеет значение, когда они понимают, как их работа связана с общими задачами департамента и компании в целом. Положительным фактором является возможность быть в курсе ключевых событий в компании и в ИТ-департаменте, участвовать в обсуждении важнейших ИТ-проектов и технических решений, иметь возможность получать поддержку от руководителей, задать вопросы и напрямую общаться с CIO.

В некоторых компаниях хорошо себя зарекомендовали внутренние конкурсы типа «Лучший ИТ-специалист месяца (года)». Сама идея не нова и происходит из извест-

ной всем «доски почёта», но практика показывает, что она вполне работоспособна. Более трудоёмким, но более точным может быть выбор лучшего сотрудника по «методу 360 градусов», когда человека оценивают со всех сторон — руководитель, коллеги, подчинённые, клиенты/пользователи. Оценки могут выставляться по нескольким критериям: участие в проектах, ориентация на клиента, вклад в работу всей команды, личные достижения и т. д. Ещё один альтернативный вариант — опираться в выборе лучшего специалиста исключительно на сравнительные показатели выполнения KPI.

Весьма желательно, чтобы у специалистов оставалась определённая свобода в выборе технических решений для достижения поставленных целей (естественно, в рамках принятых в компании ИТ-стандартов). Делегирование полномочий (например, управление отдельными проектами), командная работа и личный пример руководителя также можно отнести к мотивирующим факторам.

Что демотивирует ИТ-персонал?

- Неуважительное отношение.
- Тотальный контроль.
- Частая отмена или изменение поставленных задач.
- Работа, не имеющая отношения к ИТ.
- Большое количество рутинных операций.
- Выполнение работы за пользователей.
- Отрицательные примеры «боссов».

Как уже отмечалось выше, для ИТ-специалистов важен профессиональный рост, поэтому полезно предоставлять им возможность самообучения, тестирования новых программ и оборудования.

В силу специфики работы, ИТ-специалистам нередко приходится работать поздно вечером и в выходные. Поэтому они рассчитывают на то, что если основные ИТ-сервисы доступны, то можно прийти на работу и попозже, взять отгул за проведённое на работе воскресенье. Если этого нет, то сотрудник может быть демотивирован.

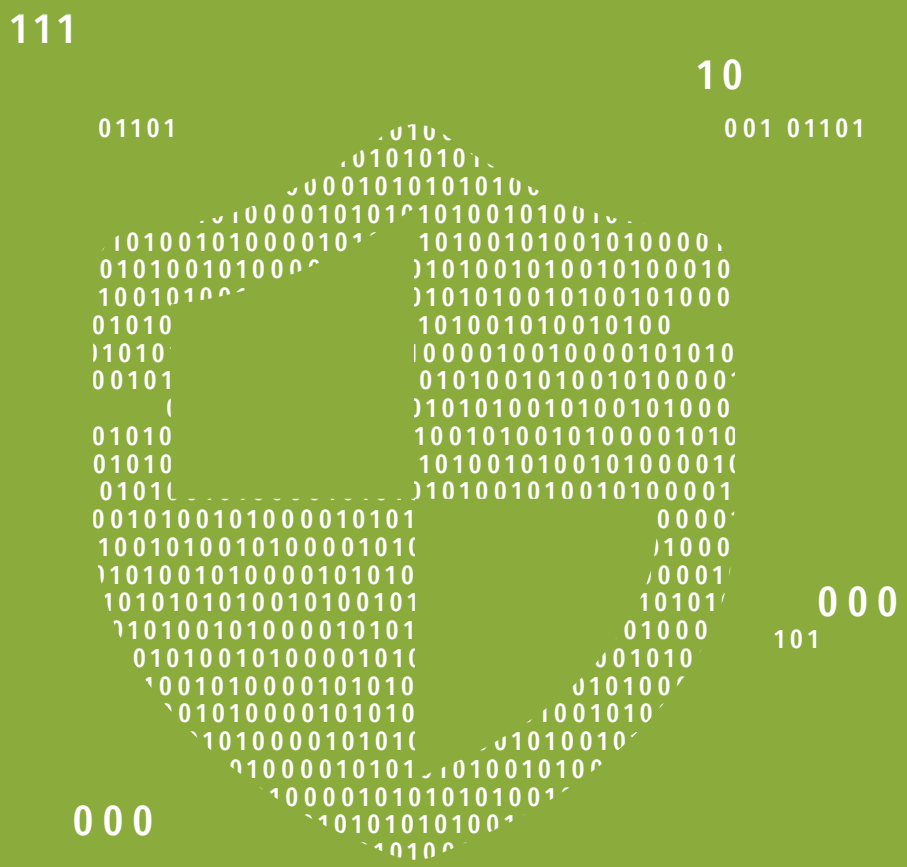
Новые тенденции: виртуальные команды и не только

Рано или поздно новые решения в области ИТ, а также менталитет и требования молодых сотрудников, приходящих работать в компанию, подталкивают CIO и других руководителей к тому, чтобы начать пересматривать саму организацию работы сотрудников. И это далеко не только замена командировок видеоконференциями. Это настоящая «мобильность» сотрудников, которые могут получать доступ к корпоративным системам с различных устройств (вплоть до личного смартфона) не только во время командировок, но и работая из дома; появление «виртуальных» команд и центров компетенций; подключение к корпоративным бизнес системам клиентов и поставщиков компании; создание корпоративных социальных сетей и т.д. Обсудим подробнее некоторых из них.

На сегодняшний день в крупных городах России уже не редкость встретить ИТ-специалистов, которые по несколько дней (а некоторые – недель) не появляются в офисе,

работая из дома. Предоставление возможности работать из дома или по свободному графику могут использоваться как методы поощрения наиболее успешных сотрудников. Но, конечно, есть и «подводные камни». В первую очередь, с формированием сплочённых команд, передачей знаний и практического опыта, контролем работы. Также авторы считают, что не стоит надеяться, что каждый специалист, при переходе с «офисного» на «домашний» режим работы станет более эффективным. Тем более, если и в офисе некоторые сотрудники нуждаются в регулярном контроле (обычно из дома они работают ещё хуже).

Ещё одна тенденция – объединение в «виртуальные» команды экспертов, занимающихся одним и тем же направлением (например, сетевой инфраструктурой или разработкой программного обеспечения), но находящихся в разных городах, а иногда даже в разных странах. Личные встречи хотя бы раз год, видео или аудиоконференции не реже раза в неделю, чёткая постановка целей и распределение работы, регулярная проверка результатов помогают повысить эффективность таких команд.



Часть 3

Информационная безопасность

Алексей
Лукацкий

Глава 3.1

Что такое информационная безопасность?

Как это ни странно, но у каждого, кто отвечает на этот вопрос, будет свой ответ, зависящий от множества факторов — образования, опыта, предыдущих мест работы, текущего руководства и т.п. Даже у регуляторов в области защиты информации (а в чем разница между информационной безопасностью и защитой информацией, не говоря уже о кибербезопасности, мы говорить не будем, так как эта дискуссия сама по себе потянет на целый учебник) нет единства. Согласно определению, написанному в документах ФСТЭК (Федеральной службы по техническому и экспортному контролю — одному из основных регуляторов в области защиты информации в России), защита информации — это обеспечение целостности, доступности и конфиденциальности. Для кого-то это процесс (то есть понятие динамическое), для кого-то — состояние (то есть понятие статическое). У каждого своё понимание и толкование. Поэтому до сих пор на уровне государства не существует чётко определённого термина для информационной безопасности (ИБ), а уж между государствами — тем более (Россия и США с 1998-го года не могут договориться в рамках ООН о том, «как правильно» — «информационная безопасность» или «кибербезопасность»). ФСТЭК, ФСБ, Совет Безопасности, Минкомсвязь — у них есть свои нормативные акты по этим темам, все они используют различные термины, иногда похожие, иногда нет.

На наш взгляд стоит отдать предпочтение следующему определению.

> ***Информационная безопасность*** *— это состояние защищённости интересов заинтересованных лиц (стейкхолдеров предприятия) в информационной сфере, определяющееся совокупностью сбалансированных интересов личности, общества, государства и бизнеса.*

Данный термин мы немного перефразировали, взяв его из предыдущего варианта Доктрины информационной безопасности, утверждённой ещё в 2000-м году. Если посмотреть чуть глубже, то становится понятно, что он очень ёмкий и, в зависимости от того, что мы вкладываем в понятия «стейкхолдер», «информационная сфера» и «интересы», картина информационной безопасности у нас будет меняться: она станет либо очень узкой, либо, наоборот, достаточно широкой. Если по-

смотреть на понятие ***стейкхолдер***, то у каждого из нас эти стейкхолдеры разные. У традиционного безопасника стейкхолдер — это он сам и регуляторы по защите информации (ФСТЭК, ФСБ, Банк России, Минкомсвязь и другие), т.е., в этом случае безопасность нужна ради безопасности. Соответственно, классический безопасник далеко не всегда смотрит за пределы этих стейкхолдеров и именно отсюда и проистекают многие конфликты с ИТ, с бизнесом, с пользователями. Пользователи считают безопасников дармоедами, которые ничего не делают, только читают чужую почту и блокируют выход в социальные сети. Мнение достаточно распространённое, и нельзя сказать, правильное оно или нет, просто оно исходит из того, что у разных лиц, которые думают о безопасности, разное понимание того, для кого должен работать безопасник, и что он должен делать.

Разумеется, если мы расширяем круг стейкхолдеров и учитываем, что безопасность должна учитывать интересы бизнеса, а если компания публичная, то и интересы акционеров, а ещё и клиентов, партнёров и т.д., то и спектр мероприятий по ИБ, и их приоритет будут меняться. Мы в последнюю очередь будем смотреть на нормативные документы (а в ИБ их на пару порядков больше, чем в ИТ), а в первую очередь — на выполнение требований бизнеса и соответствие целям его развития, в том числе и в контексте информационной безопасности.

Второе важное понятие из определения информационной безопасности — ***информационная сфера***. Это тоже очень ёмкое понятие. Кто-то его ограничивает только информацией — и тогда понятие информационной безопасности скукливается до термина «защита информации». В этом случае нас уже не волнует ни доступность информационных систем, ни субъекты, которые имеют доступ к этой информации и к информационным системам, её обрабатывающим. А это неправильно. Лучше постараться посмотреть шире и рассматривать «информационную сферу» как совокупность информации, информационной инфраструктуры (информационных систем), в которой эта информация передаётся и обрабатывается, и субъектов, которые имеют доступ к этой информации или информационным системам. Тем самым, мы сразу начнём учитывать в понятии ИБ, например, атаки «отказ в обслуживании», которые никак не влияют на информацию, а направлены на выведение из строя только информационных систем. А социальный инжиниринг? Он направлен не на информацию (хотя она является конечной точкой для злоумышленника), а на пользователя, как на самое слабое звено. Если мы убираем человека из обеспечения информационной безопасности, мы тем самым оставляем огромную дыру в системе защиты. А если мы добавляем его туда, то у нас сразу включаются в процесс ИБ и моменты, связанные с повышением осведомлённости в области безопасности, обучение, тренинги, подписание документов о неразглашении конфиденциальной информации или о неиспользовании, например, компьютеров в личных целях, и т.д.

Наконец, третий элемент определения ИБ — ***интересы***. Очевидно, что если у нас разные стейкхолдеры, то и интересы у них будут разными. Если для безопасника важно обеспечить конфиденциальность, целостность и доступность (именно это написано в нормативных документах регуляторов), то для юристов важнее обеспечить соответствие каким-то нормативным актам и документам, необязательно ведомственным приказам, а, в первую очередь, документам высокого уровня, например, федеральным законам или международным договорам. Юристов интересует защита от преследования за нарушение каких-то нормативных актов (тех же договоров, в которых могут быть разделы о конфиденциальности или о качестве обслуживания). Далее — пользователи. Это тоже стейкхолдеры, как ни странно. Их не волнует ни целостность, ни доступность

в явной форме, они таких терминов даже не знают. Их волнует бесперебойный Интернет, комфорт работы (чтобы по 20 раз на дню не спрашивали логин и пароль для доступа к информационной системе и не заставляли запоминать пароли на 20 символов в случайной комбинации), да ещё и тайна переписки.

И, как следствие, коль скоро у нас разная информационная безопасность, то и угрозы будут разными. Есть угрозы традиционные — вирусы, атаки «отказ в обслуживании», утечки информации, несанкционированный доступ, нарушения работоспособности приложений, кража ключей электронной подписи и так далее. А есть вещи нетрадиционные — например, приход регулятора с проверкой или уголовное преследование за отсутствие лицензии на деятельность в области шифрования, или изъятие незаконно ввезённого оборудования (например, маршрутизатор с поддержкой IPSec для организации межофисной VPN), или лишение свободы за несоблюдение правил эксплуатации критической информационной инфраструктуры.

Таким образом, в зависимости от толкования термина «информационная безопасность» (по тексту мы будем использовать также термины «кибербезопасность» и «защита информации» как синонимы «информационной безопасности») и от того, кто является нашим стейкхолдером (для кого мы работаем), у нас существенно меняется сфера деятельности и набор мероприятий (да и технологий тоже), которые будут относиться к ИБ.

Кейс: когда безопасность борется с угрозами, но мешает бизнесу

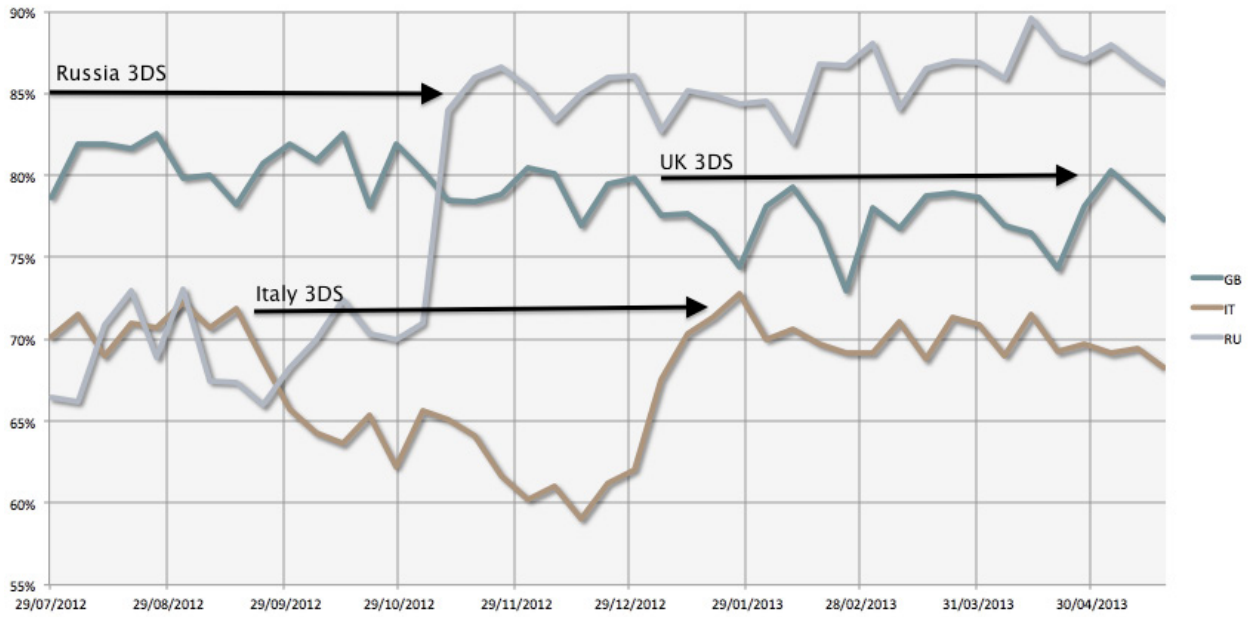
В качестве примера давайте посмотрим на систему защиты финансовых транзакций по платёжным картам 3D Secure, используемой как Visa, так и Master Card. Мы все регулярно сталкиваемся с ней, совершая покупки в Интернете. Считается, что эта технология призвана защитить от мошеннических операций, и это верно. Но значит ли это, что применять её надо всегда и везде? Например, приложение «Парковки Москвы» от Электронной Москвы не использует 3D Secure. И Аэрофлот при покупке билетов — тоже. А ещё AppStore, Amazon, «Одноклассники» и куча других ресурсов. Значит ли это, что эти компании не беспокоятся о своей безопасности? Ни в коем случае. Просто бизнес важнее.

Посмотрите на статистику социальной сети Badoo (Рис. 3.1.1). В России 3D Secure была включена принудительно с самого начала. После её отключения число успешных платежей выросло на 20%! В Италии включение 3D Secure привело к падению объёма платежей на 10-15%. В США включение 3D Secure привело к тому, что пользователи Badoo перестали платить вообще, а в Южной Африке число успешных платежей после отключения 3D Secure привело к положительной динамике.

Это очень хороший пример того, как технология безопасности, которая призвана помогать бизнесу, может ему мешать. Разумеется, данные Badoo не означают, что 3D Secure плоха и не нужна. Совсем нет. Просто надо чётко осознавать место и область применения 3D Secure (как и любой иной технологии). Необходимо проводить соответствующие исследования, чтобы иметь на руках цифры, помогающие принять нужное решение. Например, на конференции «Payment Security» в 2016-м году, на круглом столе, посвящённом дилемме «Удобство или безопасность» представитель Сбербанка привёл интересные цифры. Оказывается, число опротестований платежей в «Парковки Москвы» составляет всего несколько... десятков рублей за 3 года работы сервиса. Несколько десяткой рублей! И зачем при таких цифрах внедрять 3D Secure?

В случае с Аэрофлотом ситуация схожая. Зачем там 3D Secure? Есть ли там мошенничества при продаже билетов? Ведь все равно билет будет выписан на конкретного человека

Рис. 3.1.1. *Статистика Badoo по использованию 3D Secure.*



с паспортными данными, позволяющими его идентифицировать. Да и этот покупатель физически придёт на рейс, и его можно задержать, если он мошенник. Видимо, в Аэрофлоте посчитали объём мошенничества и конверсию (то есть соотношение числа покупателей билетов с числом посетителей сайта Аэрофлота или с числом тех, кто билеты забронировал) и оказалось, что снижение конверсии от включения 3D Secure приводит к бóльшим потерям, чем мошенничество при отключенной 3D Secure.

Аналогичная ситуация с конверсией и для других сайтов с большим числом клиентов и покупок по картам — Amazon или AppStore. Снижение числа успешных платежей на 20% — это огромные деньги в масштабах этих компаний, которые они не готовы терять. Тем более, что существуют и другие способы защиты от мошенничества, без 3D Secure. Например, по имеющимся у нас данным, в платёжной системе ASSIST работает своя антифрод-система, которая снижает число мошеннических операций без снижения конверсии и без 3D Secure (по данным ASSIST процент успешных платежей при использовании 3D Secure ниже на 15-20%, чем без этой технологии). Badoo тоже разработала свою антифрод-систему, чтобы не ухудшать бизнес-показатели.

Ещё один пример, когда ИБ мешает бизнесу, — это различные проверки, которые раздражают пользователей сайтов электронной коммерции. Чем больше кликов и операций (например, CAPTCHA) заставляют сделать пользователя (даже с благой целью повышения защищённости и защиты от мошенничества), тем ниже конверсия и число успешных оплат. Аналогичная ситуация со временем загрузки страницы — чем дольше грузится сайт из-за тех же проверок безопасности, тем ниже лояльность пользователя, выше их отток и ниже конверсия (если сайт что-то продаёт).

Поэтому приходится подолгу ждать отображения контента. На других же сайтах долгая загрузка приводит к потерям. Допустим, сайт продаёт в день на 100 тысяч рублей. Всего одна секунда задержки загрузки страницы из-за проверки Web Application Firewall (WAF) или

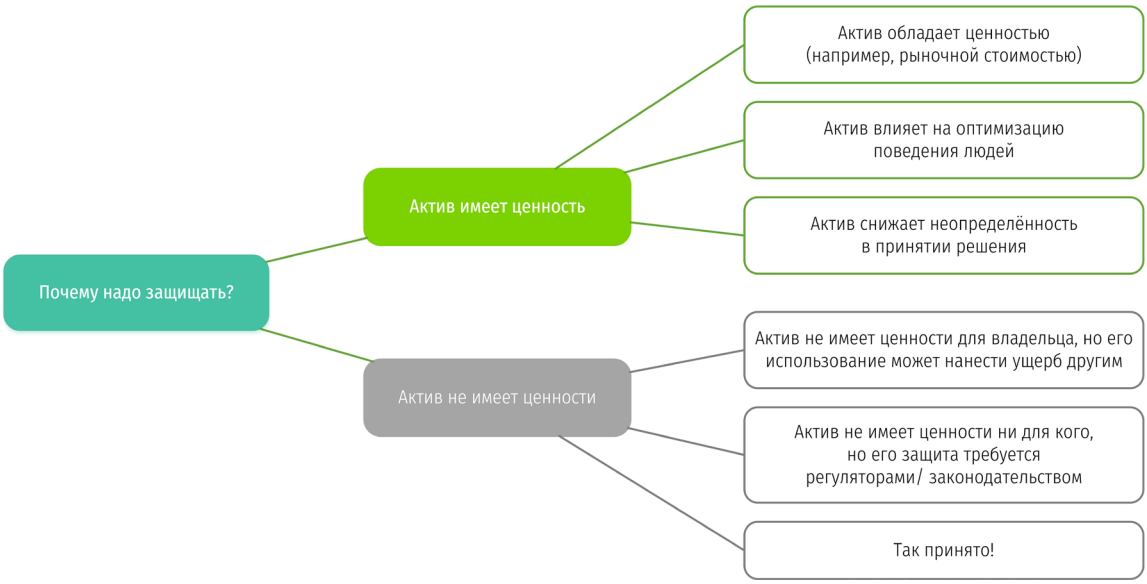
встроенными в сайт модулями проверки вводимых в поля форм значений приводит к годовым потерям в 2,5 миллиона рублей. 1 секунда = 2,5 миллиона рублей! А если это не 100 тысяч рублей, а столько же тысяч долларов? Потери составят уже 2,5 миллиона долларов! По статистике, односекундная задержка в загрузке странице приводит к снижению конверсии на 7%, то есть к прямым потерям.

Понятно, что на конверсию влияет не только и не столько безопасность, сколько множество других параметров — дизайн страницы, навигация, контент, юзабилити, отсутствие персонализации, отсутствие призыва к действию и т.п. Но и ИБ тоже вносит свой вклад в общие потери, которые нужно учитывать и, не отказываясь от безопасности, предлагать альтернативные варианты. Как это было сделано в случае с Badoo или ASSIST. В противном случае, говорить о вкладе ИБ в бизнес не приходится, и лучше эту тему вообще не ставить на повестку дня — получится только хуже. Кто в такой ситуации будет положительно относиться к безопасности, которая по старинке думает только о себе, то есть, в лучшем случае, о борьбе с угрозами, а в худшем — о выполнении требований какого-либо нормативного акта, который выпущен непонятно зачем?

Драйверы информационной безопасности

Что движет сегодня информационной безопасностью? Принято считать, что безопасность борется с опасностями, то есть с угрозами (Рис. 3.1.2). И именно злоумышленники и их методы заставляют компании инвестировать в различные технологии и решения. Но, увы, это не совсем не так. Так обычно на ИБ смотрят люди, в хорошем смысле далёкие от того, что в России понимают под информационной безопасностью. Те же ИТ-директора часто воспринимают ИБ (если эта функция попадает в их поле деятельности) именно как борьбу с угрозами — вредоносным ПО, DDoS-атаками, кражей баз данных и т.п. Однако это однобокий взгляд, который ведёт в тупик. И чтобы понять, что же движет кибербезопасностью в России (и регуляторов, и потребителей, и поставщиков продуктов и услуг), необходимо провести краткий экскурс в историю ИБ в России.

Рис. 3.1.2. *Шесть причин для защиты информационных активов.*



Глава 3.2

Краткая история ИБ в России

История информационной безопасности в России ведёт своё начало с древнейших времён, но в более-менее управляемое русло она вошла со времена Ивана Грозного, когда российское государство начало активную внешнеполитическую деятельность. Потом Россия вошла во времена регулярной дипломатической переписки, постоянных войн и конфликтов... Незаметно царская Россия столкнулась с революционерами, и после Октябрьского переворота, когда была особенно высока потребность в защите революционных интересов в информационной сфере, при ВЧК был создан 8-й Спецотдел (в Красной Армии были свои органы защиты информации), который и можно считать прародителем отечественной отрасли информационной безопасности. Правда, тогда, в начале XX-го века, ни о каких компьютерах и речи не было, и вся защита ограничивалась только обеспечением конфиденциальности информации, т.е. её шифрованием. Именно с шифрования начиналась история защиты информации в Российской империи (да и не только в ней), и очень длительное время только ею и ограничивалась... пока не пришло время первых вычислительных машин.

Эпоха ФАПСИ и Гостехкомиссии

Конец 80-х годов и начало 90-х бывшая главная спецслужба страны вступает в не самое лучшее своё время — её лихорадит, она постоянно переименовывается, её покидают сотрудники, оседающие в коммерческом секторе, который растёт очень активно и семимильными шагами движется в ногу с прогрессом. А прогресс неумолим — появляются первые компьютеры. При этом службы безопасности фирм и кооперативов новых русских возглавляют «бывшие» сотрудники КГБ, привнесшие в коммерческую сферу весь свой богатый опыт защиты тайн; правда, на этот раз применительно к коммерческим секретам. Пожалуй, с этого времени можно отсчитывать начало коммерческого сегмента отрасли информационной безопасности. Хотя задачи перед ней стояли, схожие с областью государственных секретов — обеспечение конфиденциальности и защиты от прослушки.

В конце 80-х годов значительно расширились задачи и возможности КГБ и Гостехкомиссии по своим основным направлениям деятельности в области ИБ — шифрование (включая и спецсвязь) и ПДИТР (электронную разведку я специально оставляю в стороне). 91-92-й годы можно назвать переломными в области формирования концепции обеспечения информационной безопасности в стране на долгие годы.

В 1990-м году парламентская комиссия, созданная по распоряжению Президента Ельцина и возглавляемая академиком

Рыжовым Ю.А. впервые ввела в обиход термин «информационная безопасность». Эта комиссия, работавшая 40 дней, разрабатывала Концепцию национальной безопасности, а также иерархию основополагающих документов, на которые должны были опираться все нормативные акты по безопасности. Из интервью Рыжова Ю.А. на Радио Свободы в январе 2003-го года: *«Я выступал как председатель Комиссии Верховного совета СССР по разработке концепции национальной безопасности и говорил, что нам, в первую очередь, нужно обеспечить следующую иерархию безопасности: безопасность и права личности, потом общества и потом государства при условии, что оно обязано служить людям и обеспечивать две эти первые безопасности. Это была первая парадигма, которая ставила всё с головы на ноги, потому что предыдущие столетия эта парадигма была иная: живёт государство — и оно является главным»*. В июне 2011 года Юрий Рыжов в интервью журналу «Эхо России» так писал про период работы своей комиссии: *«Я примерно с 90-го года заболел проблемой национальной безопасности моей страны. Когда-то с согласия Горбачёва, а потом по его поручению я возглавлял комиссию Верховного Совета по разработке Концепции национальной безопасности. Мы хотели перевернуть парадигму советскую и Победоносцева — обер-прокурора Синода, который в период «подморозки» Александра III провозгласил православие, самодержавие и народность... а у нас было сказано: государство, общество, а только потом — человек. Мы старались перевернуть эту парадигму в обратном направлении: главное — безопасность личности, второе — общества, третье — государства, и лишь в том случае, если оно обеспечивает две первых. За последние 20 лет, с тех пор, как я увлёкся этой безнадёжной задачей, всё вернулось. Только вместо Победоносцева некий Сурков теперь выступает»*.

Если бы тогда идеи Рыжова были приняты, кто знает, как бы сейчас развивалась отрасль ИБ в России. Хотя, попытки переломить ситуацию нашими регуляторами (как минимум ФСТЭК) предпринимались. Но безуспешно. Сама комиссия Юрия Рыжова была закрыта Язовым и Крючковым, позже прославившимися в рамках ГКЧП. Примечательна цитата председателя КГБ Крючкова: *«Всё хорошо, всё разумно, но концепция комиссии Рыжова — это для будущего, а нам нужно работать здесь и сейчас. Поэтому следует принять срочно нашу концепцию»*. С этой концепцией мы все знакомы. На первом месте находится безопасность государства, затем идёт безопасность общества и только потом безопасность личности.

Отказавшись от идеи академика Рыжова, наши спецслужбы продолжают развивать эту концепцию. Создаётся Федеральное агентство правительственной связи и информации, до 2003-го года ставшее основным стопором всех инициатив, связанных с так называемой гражданской криптографией. В 92-м году появляются первые руководящие документы Гостехкомиссии, устанавливающие требования к защите средств вычислительной техники и автоматизированных систем. Часть документов и множество идей, появившихся в то время, действует и до сих пор, продолжая уже устаревший, но все-таки никем не отменённый курс в области информационной безопасности.

Эпохи глобализации и первых отечественных ИБ-стартапов

Середина и конец 90-х годов вспоминается активным использованием Интернет (хотя первые попытки подключения к Всемирной Сети были, безусловно, и раньше). В это время в Россию начинают приходить первые иностранные компании, являющиеся признанными мировыми игроками на рынке информационной безопасности. На этом рынке начинают появляться и отечественные компании, которые сейчас модно называть стартапами. В то время ключевой задачей для любого производителя было выпустить

продукт, соответствующий руководящим документам ФСТЭК, получить сертификат соответствия. К сожалению, такой подход у большинства российских ИБ-компаний остаётся превалирующим и до сих пор.

Российские ИБ-предприятия ориентировались на государственный сектор, имея в своём портфолио достаточно небольшой спектр продуктов (1-3, не более), преимущественно в сфере защиты персональных компьютеров (СЗИ от НСД), локальных сетей Novell и каналов связи (шифраторы X.25, IPX/SPX, TCP/IP). В это же время западные компании активно осваивали сегмент Интернет-безопасности, предлагая российским потребителям межсетевые экраны, системы предотвращения вторжений, сканеры безопасности и т.п. И только антивирусная индустрия стояла немного особняком:— два игрока — «Диалог-Наука» (продвигавшая Aidstest, Dr.Web и ряд других, уже местами подзабытых антивирусных продуктов) и «Лаборатория Касперского» (сначала являющаяся подразделением НТЦ КАМИ) активно конкурировали с иностранными антивирусами от компаний Norton, Dr.Solomon и др.

А вот регуляторы в это время были не очень активны. ФАПСИ, по сути, монополизировало рынок средств шифрования и не пускало туда посторонних (эта тенденция сохраняется до сих пор, только преемником ФАПСИ стал 8-й Центр ФСБ). А Гостехкомиссия продолжала спокойно заниматься темой ПДИТР и, при этом, редко выпускала новые руководящие документы. В 2003-м году Президент Путин упразднил ФАПСИ, разделив его функции между Министерством обороны, ФСБ и ФСО. В 2004-м году прекратила своё существования и Гостехкомиссия, превратившись по решению Президента в Федеральную службу по техническому и экспортному контролю (ФСТЭК).

Эпоха персональных данных и отраслевых стандартов

В 2007-м году началась новая эпоха в российской отрасли защиты информации. Отечественные депутаты решили не отставать от всего прогрессивного человечества и приняли новый закон «О персональных данных», задавший определённый вектор в развитии информационной безопасности. Сначала этому закону никто не придал большого значения, и только в 2008-м году, после выхода «четверокнижия» ФСТЭК и методических документов ФСБ по защите персональных данных, отрасль очнулась ото сна и стала активно привязывать всё, что в ней делалось, к теме персональных данных. Шутка ли, требования по защите информации впервые стали обязательными для всех юридических лиц и индивидуальных предпринимателей в России. А это, без малого, пять миллионов потенциальных потребителей продукции и услуг в области защиты информации.

На фоне законодательства о персональных данных стала активно развиваться и тема отраслевых стандартов. И, хотя законодательной базы под ней не было, это не помешало Банку России, НАУФОР, НАПФ и ряду других ведомств, госкорпораций и монополий выпускать свои «отраслевые» требования по обеспечению информационной безопасности.

Несмотря на то, что ФСТЭК редко выпускала новые и, что самое важное, актуальные документы, защищать свои информационные активы как-то было нужно.

Эпоха растерянности ибшников и ФСТЭК v2.0

Поговорим о двух важных событиях, которыми ознаменовался собой 2012-й год, и которые станут началом очередного витка развития отечественной отрасли ИБ.

Первое событие произошло там, где этого уже никто не ждал, — во ФСТЭК. Произошедшие в руководстве этого госоргана организационные изменения привели к тому, что он впервые за последние лет 15-20 вновь стал поднимать упавшее знамя методолога

в области защиты информации. Новые документы по персональным данным и государственным информационным системам, планы по изменению системы сертификации, планы по новым руководящим документам с требованиями к средствам защиты, активное привлечение отраслевых экспертов и потребителей к совместной разработке и экспертизе проектов нормативных документов... Всё это позволяет надеяться, что у нас, наконец-то, появится аналог американского NIST, выпускающего различные методические (а местами и обязательные) документы по широкому спектру вопросов, не мешающие, а помогающие российским организациям защищать свои информационные активы.

А вот второе событие сложно отнести к разряду положительных. Речь идёт о «потерянности» безопасников, многие из которых обучались, воспитывались и росли в непростые 90-е и 2000-е годы. Парадигма стала меняться. Бизнес уже не устраивает старый подход к защите информации — любыми средствами и без учёта потребностей бизнеса. Последний начинает требовать от безопасников считать деньги, говорить на языке бизнеса, оценивать эффективность своей работы... А многие ли безопасники готовы к этому? Многие ли знают, как перестроиться под новые требования своих работодателей? Многие ли сумеют преодолеть этот кризис?.. Схожие вопросы, только на несколько лет раньше, стали задаваться и ИТ-директорам.

Час быка прошёл?..

Из краткого экскурса в историю и раздела, посвящённого термину «информационная безопасность», можно сделать один простой вывод — у ИБ всего три драйвера, каждый из которых имеет свою область применения, свои плюсы и минусы.

Самый ***первый драйвер*** — страх. Не зря у иностранцев даже есть специальный термин — FUD (fear, uncertainty and doubt), то есть страх, неопределённость и сомнения. Страх стать жертвой хакеров очень сильно двигает отрасль вперёд и заставляет генеральных директоров спрашивать своих подчинённых, всё ли сделано, чтобы не попасть на первые страницы газет в рубрику «Их взломали хакеры». Этот драйвер универсален для любой страны мира и поэтому он так популярен — достаточно перевести на русский язык иностранные страшилки, и вот у нас на руках готовое обоснование для приобретения нужных продуктов и технологий.

Второй драйвер, чуть менее популярный и не такой универсальный, как страх, — это регуляторика или соответствие требованиям, как внешним, так и внутренним (в бизнес-литературе часто используют термин «compliance»). Поскольку нормативные акты отличаются не только от страны к стране, но и от отрасли к отрасли, то в данном случае сложно говорить об унификации этого драйвера. Отсюда и его заслуженное второе место в списке. Руководство многих компаний боится быть наказанным (можно было бы даже отнести этот драйвер к страху, но природа его иная) за несоблюдение множества защитных технических и организационных мер (мы их рассмотрим дальше). Особенно сильно масла в огонь подлил закон «О безопасности критической информационной инфраструктуры», который установил уголовную ответственность за несоблюдение мер защиты критических инфраструктур — до 10 лет лишения свободы. Это пусть и верные драйверы, но могут сыграть злую шутку с их апологетами, особенно если страхи не оправдаются (вспомните притчу про мальчика, кричавшего «Волки, волки!»).

Последний в списке, но не последний по важности, ***третий драйвер*** — это бизнес-требования. Вообще, он должен быть первым и единственным, но увы, только сейчас многие специалисты стали задумываться над таким простым и сложным одновременно вопросом: «Зачем ИБ бизнесу?». Именно ответ на него помогает правильно преподнести ИБ менеджменту предприятия, получить нужные инвестиции и поддержку, и не играть на страхах руководства.

Глава 3.3

ИБ — это путь, а не точка назначения

А давайте сразу использовать третий драйвер, если он такой правильный? Закономерный вопрос, но, увы, перейти к нему, не использовав первые два, нельзя. Такая попытка будет обречена на неуспех в абсолютном большинстве случаев. И чтобы понять это, надо вспомнить путь, который проходят многие специалисты, а позже руководители, ответственные за ИБ на своих предприятиях (это может быть и ИТ-директор).

Начинали все как обычные специалисты, занимающиеся ***защитой инфраструктуры*** — установкой антивирусов, настройкой межсетевые экранов. Зачем? Ну так было принято. Об этом говорилось в лучших мировых практиках — COBIT, ITIL, ISO 27001/2 и т.п.

Позже стала преобладать ***compliance***-составляющая, и безопасники стали уделять больше времени соблюдению различных нормативных актов — закону о персональных данных, СТР-К, стандарту Банка России.

Наконец, в условиях катастрофического изменения ландшафта угроз мы пришли к тому, что безопасник должен ориентироваться именно на них в своей деятельности. Многие директора по безопасности сегодня находятся именно здесь. С ИТ-директорами путь мог чуть отличаться — местами менялись второй и третий пункты маршрута, но суть оставалась прежней. В обоих случаях акцент делался на ***борьбе с угрозами*** и на выполнении требований различных нормативных актов.

Но мы прекрасно понимаем, что это ещё не конец пути. В условиях роста угроз, роста нормативных требований, роста числа используемых технологий, мы встанем перед вопросами: *«Чему уделить больше внимания? На что потратить имеющиеся не безмерные ресурсы? Что надо сделать в первую очередь, а чем можно пренебречь, приняв риски?»* И тут мы понимаем, что нам придётся вернуться к теме, которая была популярна в России ещё несколько лет назад, но потом тихо сошла на нет — к ***управлению рисками***. Именно они позволят приоритизировать усилия в области информационной безопасности и не пытаться охватить всё, что свалится на плечи ИТ-руководителя, ответственного и за вопросы ИБ.

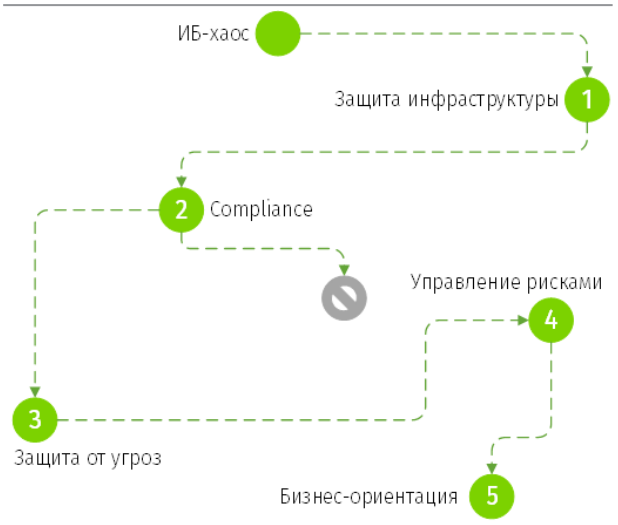
Но и это ещё не финальная точка назначения. А как быть с бизнесом? Пока мы говорили о выполнении задач, к бизнесу имеющих опосредованное отношение. Борьба с угрозами — это хорошо, но у бизнеса, как правило, есть более серьёзные проблемы, чем вирусы или утечки данных. Выполнение требований регуляторов и нормативных актов... А если штраф за их неисполнение равен десяти-двадцати тысячам рублей (именно таково большинство административных наказаний в области ИБ)? А если у регуляторов нет полномочий прийти с проверками (на-

пример, в части проверки технических мер защиты персональных данных у коммерческих компаний)? Есть ли смысл заниматься тогда соответствием требованиям, если риск наказания невелик, а то и вовсе равен нулю? Финальной точкой пути современного ИТ-директора, отвечающего за ИБ (по крайней мере, так как это видится сейчас), будет именно ***бизнес-ориентация*** в своей деятельности.

Схематически этот путь из пяти шагов к безопасности представлен на схеме (Рис. 3.3.1).

Давайте попробуем вместе пройти по этим пяти шагам и выделить ключевые задачи на каждом из них.

Рис. 3.3.1. *Путь директора, отвечающего за ИБ.*



Шаг №1. Защита инфраструктуры

В наши дни для достижения приемлемого уровня безопасности уже недостаточно развернуть точечные продукты на периметре корпоративной или ведомственной сети. Сложность и изощрённость современных угроз требует внедрения совместно работающих интеллектуальных механизмов безопасности во все элементы распределённой инфраструктуры. С учётом этих соображений, новая архитектура безопасности современного предприятия как никогда нуждается во внедрении подхода глубокой многоуровневой защиты (Defense in Depth или «эшелонированная оборона»), согласно которому множество уровней защиты распределены по стратегически важным элементам по всей сети и действуют в рамках унифицированной стратегии. Информация о событиях и состоянии систем согласованно используется различными элементами системы информационной безопасности, что позволяет обеспечить более надёжный контроль состояния ИТ-инфраструктуры, а ответные действия координируются в рамках общей стратегии управления.

В такой архитектуре предусмотрен модульный принцип построения системы информационной безопасности, что позволяет ускорить развёртывание и способствует внедрению новых решений и технологий по мере развития потребностей бизнеса. Такая модульность расширяет срок использования имеющегося оборудования и обеспечивает защиту произведённых капитальных вложений. В то же время архитектура предусматривает набор инструментальных средств, упрощающих повседневную эксплуатацию и обеспечивающих снижение совокупных эксплуатационных расходов.

Данная концепция позволяет создать систему информационной безопасности, ориентированную на обеспечение доступности сети и сервисов, а также ***поддержание непрерывности бизнеса*** (этим термином обозначается создание систем профилактики и восстановления деловой активности при борьбе с потенциальными угрозами для компании). Угрозы безопасности характеризуются высокой динамикой, и предлагаемая концепция предусматривает способы выявления текущих направлений угроз, а также отслеживания новых и развивающихся угроз за счёт

следования лучшим практическим рекомендациям и использования комплексных решений.

Но начинать надо не с внедрения защитных мер, а с внедрения политик безопасности, разработанных по результатам анализа угроз и рисков и согласованных с бизнес-целями и задачами. Критически важным фактором для достижения успеха бизнеса является создание таких политик безопасности, которые не только не препятствуют, а, напротив, способствуют достижению организацией поставленных бизнес-целей и плановых показателей. Поэтому разработка политик должна начинаться с чёткого определения бизнес-целей и задач. После определения этих целей необходимо выявить возможные угрозы для выделенных целей и задач. В Табл. 3.3.1 представлены некоторые типовые примеры бизнес-целей и задач, а также связанные с ними возможные угрозы. Следует иметь в виду, что цели, задачи и возможные угрозы могут сильно меняться в зависимости от организации и среды, данный перечень приводится только в качестве примера.

Табл. 3.3.1. *Бизнес-цели, задачи и возможные угрозы.*

Бизнес-цели и задачи	Возможные угрозы
Получение прибыли	· Кража средств со счетов клиентов и самой организации. · Снижение числа финансовых транзакций из-за недоступности банковских сервисов. · Потеря клиентов или снижение их лояльности.
Оптимизация издержек	· Рост затрат на операционные расходы, связанные с расследованием инцидентов ИБ и восстановлением работоспособности организации после кибератаки или действия инсайдера. · Неэффективные эксплуатация и управление инфраструктурой организации.
Рост лояльности клиентов	· Утечка коммерческой тайны и персональных данных (списки клиентов, условия их обслуживания). · Недоступность сервисов. · Негативные отзывы в СМИ и ущерб имиджу и репутации организации. · Устаревшие технологии.
Повышение эффективности внутренних процессов	· Снижение продуктивности работников. · Устаревшие технологии. · Неэффективные эксплуатация и управление инфраструктурой организации. · Сговоры среди сотрудников.
Географическая экспансия	· Несоблюдение нормативных требований. · Срыв сроков выхода на новые рынки. · Недоступность сервисов. · Утечка коммерческой тайны (планы развития). · Потеря клиентов или снижение их лояльности.
Предоставление качественных продуктов	· Недоступность сервисов.
Формирование образа надёжного и инновационного предприятия	· Недоступность сервисов. · Негативные отзывы в СМИ и ущерб имиджу и репутации организации. · Устаревшие технологии. · Утечка конфиденциальной информации (списки клиентов, условия их обслуживания, планы развития).
Соответствие нормативным требованиям	· Приостановление деятельности или отзыв лицензии на осуществление определённого вида деятельности. · Штрафы и иски со стороны регулирующих органов (например, Банка России).
Рост лояльности работников	· Устаревшие технологии. · Утечка персональных данных сотрудников. · Негативные отзывы в СМИ и ущерб имиджу и репутации организации. · Снижение продуктивности работников.

После определения бизнес-целей и задач и проведения анализа угроз необходимо выполнить более глубокий анализ угроз и рисков, чтобы определить важность ресурсов, имеющихся в среде, проанализировать возможные риски и угрозы безопасности для этих ресурсов, а также оценить возможное воздействие нарушений безопасности на бизнес. Таким образом, будет сформировано представление об усилиях, необходимых для защиты каждого ресурса. Мы прекрасно понимаем, что, хотя обычный аквариум с функциями мониторинга через Интернет или IoT-термометр могут стать точкой входа в корпоративную сеть (такие истории известны), применять к ним точно такие же подходы, что и к защите центра обработки

Рис. 3.3.2. *IoT-устройство как интересная мишень для хакеров.*

данных, нецелесообразно (Рис. 3.3.2).

Результатом этих шагов является создание политик безопасности и формулирование принципов, которыми определяется приемлемое и безопасное использование каждого сервиса, устройства и системы в рамках ИТ-инфраструктуры организации. В свою очередь, политики безопасности определяют процессы и процедуры, необходимые для достижения бизнес-целей и выполнения задач. Совокупность процессов и процедур определяет функции по обеспечению безопасности.

Результат, обеспечиваемый внедрением политик безопасности, полностью зависит от того, насколько они улучшают контроль и управление. Другими словами, безопасность можно представить как функцию контроля и управления. Без контроля невозможно управление, а без управления нет безопасности. Таким образом, описываемая в данной главе концепция ориентирована главным образом на повышение уровня контроля и управления, которые являются основными факторами успешного обеспечения безопасности — независимо от масштаба инфраструктуры и стоящих перед ней задач.

В рамках концепции определены шесть мер обеспечения безопасности, которые обеспечивают выполнение политик безопасности и расширяют возможности контроля и управления (Табл. 3.3.2). На уровне контроля реализуется три меры — «идентификация», «мониторинг» и «выявление аномалий». Уровень управления повышается с помощью также трёх мер — «повышение устойчивости», «сегментация и изоляция» и «контроль и обеспечение выполнения политик».

В контексте архитектуры безопасности описываемая концепция используется при создании каждого сегмента сети. Результатом следования этому подходу является идентификация технологий и лучших типовых практических рекомендаций для выполнения каждой из шести ключевых мер, которые наиболее подходят для данной среды. Таким образом, многочисленные технологии и функции используются в масштабе всей сети и обеспечивают контроль сетевых операций, реализуют сетевую политику и направлены на разрешение проблем, связанных с обработкой аномального трафика. Элементы сетевой инфраструктуры, такие как маршрутизаторы и коммутаторы, точки беспроводного доступа и сервера, используются в качестве средств всеобъемлющего упреждающего мониторинга и обеспечения выполнения политики.

Хотя по мере роста бизнеса и его требований большинство инфраструктур развивается, предлагаемая концепция защиты инфра-

Табл. 3.3.2. *Меры обеспечения безопасности инфраструктуры.*

Контроль	Идентификация	Идентификация и классификация пользователей, сервисов, трафика и оконечных устройств.
	Мониторинг	Мониторинг производительности, поведения, шаблонов использования, событий и соответствия политике.
	Выявление аномалий	Сбор, анализ и выявление взаимозависимостей событий в масштабе системы.
Управление	Повышение устойчивости	Повышение устойчивости оконечных устройств, сервисов, приложений и инфраструктуры.
	Изоляция и сегментация	Изоляция пользователей, систем и сервисов для сдерживания и защиты.
	Обеспечение выполнения политик	Обеспечение выполнения политики разграничения доступа, политик безопасности и противодействие угрозам безопасности.

структуры использует ***открытый модульный подход*** — совокупности небольших независимых блоков (модулей), структура и поведение которых подчиняются определённым правилам. Данный подход имеет два основных преимущества: во-первых, он описывает архитектуру с точки зрения защиты взаимодействия отдельных модулей/сегментов сети, а во-вторых, позволяет проектировщику оценивать защищённость каждого модуля по отдельности, а не только всей системы в целом. Защищённый дизайн каждого модуля можно описать и реализовать по отдельности, а оценить в рамках всей системы (это реализация принципа «не есть слона целиком» помогает и при поэтапном бюджетировании вопросов ИБ). Хотя многие инфраструктуры нельзя чётко разграничить на отдельные модули, такой подход даёт ориентиры при внедрении в сети функций защиты.

Семь модулей / зон корпоративной инфраструктуры

Практически любую инфраструктуру можно представить в виде набора взаимодействующих между собой модулей, которых можно выделить всего семь, в отдельных организациях их может быть и меньше (Рис. 3.3.3):

1. Промышленный модуль. Данный модуль присутствует на предприятиях, имеющих либо производственные мощности (например, машиностроение, ТЭК, металлургия и т.п.), либо осуществляющих те или иные критические процессы (например, процессинг в банке и т.п.)

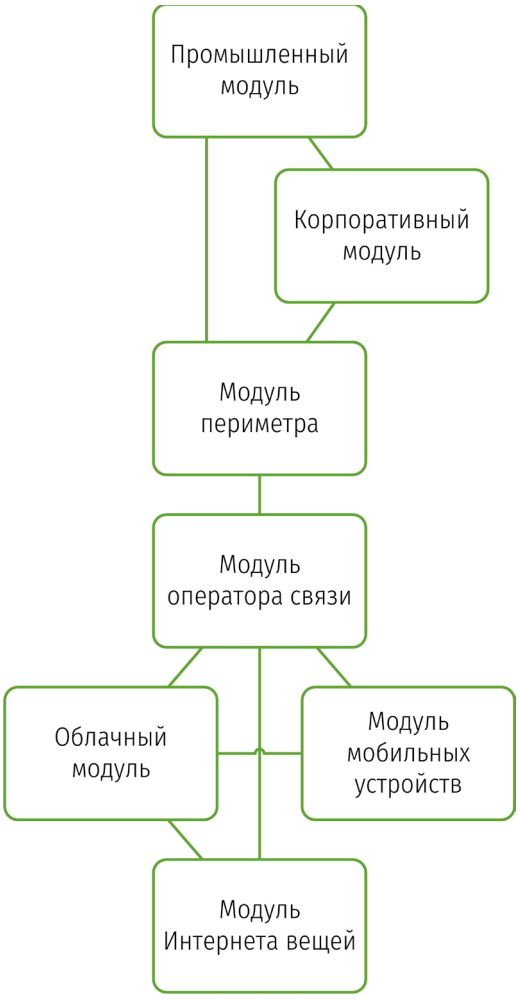
2. Корпоративный модуль. Данный модуль представляет устройства конечных пользователей и обслуживающую их инфраструктуру, может включать в себя до 80% всех устройств компании.

3. Модуль периметра. Данный модуль обеспечивает взаимодействие корпоративной или ведомственной сети с внешним миром.

4. Модуль оператора связи. Данный модуль, хотя и не принадлежит предприятию, но включается в общую схему, т.к. некоторые угрозы (например, DDoS) могут быть отражены только путём взаимодействия с операторами связи.

5. Модуль облачных вычислений. Данный модуль подразумевает не только использование и, как следствие, обеспечение безопасности облачной инфраструктуры, которая принадлежит третьему лицу (или даже нескольким лицам в разных юрисдикциях), но и контроль так называемых «теневых облаков», то есть использование сотрудниками неразрешённых в организации облачных сервисов, которые могут приводить к потере

Рис. 3.3.3. *Модули корпоративной инфраструктуры.*



контроля над корпоративными данными.

6. Модуль мобильных устройств. Данный модуль отвечает за работу с различными мобильными устройствами, принадлежащими как компании, так и самим сотрудникам, которые могут хранить на них ценную корпоративную информацию, но при этом находиться за пределами периметра организации, что представляет особую опасность.

7. Модуль Интернета вещей. Принтеры, СКУД, видеокамеры, термостаты и освещение, контролируемые через Интернет, паллеты с RFID-метками, автомобили с GPS/ГЛОНАСС-трекингом и т.д. — все эти объекты попадают именно в этот модуль с особыми требованиями к безопасности.

Каждый модуль представляет собой не только определённую функциональную зону, но и отличается набором актуальных угроз и защитных мер.

Кейс: защита периметра

Периметр есть у любой организации (даже у той, которая считает, что у неё нет периметра, и она физически изолирована от Интернет). Подключенный к глобальной сети, он является элементом сетевой инфраструктуры, который агрегирует каналы глобальной сети, соединяющие географически удалённые отделения, дирекции и дочерние предприятия с центральным офисом. Задача глобальной сети состоит в том, чтобы предоставить пользователям, находящимся в филиалах, такие же сетевые сервисы, что и пользователям, находящимся в центральном офисе. Что может угрожать периметру в такой трактовке? Основная пятёрка угроз будет выглядеть следующим образом:

- ***Отказ в обслуживании***. Аппаратные и программные сбои. DDoS-атаки, направленные на сервисы и инфраструктуру.
- ***Раскрытие и изменение данных***. Подмена IP-адресов отправителя, атаки типа «человек посередине» на данные, передаваемые по сети.
- ***Злоупотребление сетевыми сервисами***. Злоупотребление клиентами файлообменных сетей и систем мгновенного обмена сообщениями, просмотр ресурсов, не соответствующих требованиям политики организации, доступ к запрещённому контенту из филиалов.
- ***Нарушения качества предоставляемого сервиса***.
- ***Распространение вредоносного ПО***. Ботнеты, вредоносные программы, вирусы, программы-вымогатели, APT.

Отсюда вытекают и ключевые задачи безо-

пасности периметра:

- Повышение уровня защищённости сетевой инфраструктуры.
- Повышение уровня защищённости каждого устройства, входящего в сетевую инфраструктуру, защита сервисов маршрутизации и коммутации, реализация основных принципов сетевой политики.
- Защищённые коммуникации.
- Шифрование трафика, передаваемого по глобальной сети.
- Обнаружение и отражение угроз. Использование различных видов сетевой телеметрии и интеграция системы предотвращения вторжений в головной сегмент корпоративной сети.
- Мониторинг сети. Поддержка основных операций по обеспечению безопасности за счёт внедрения сетевой телеметрии и инструментальных средств обнаружения аномалий и выявления взаимозависимостей.

Данные задачи, будучи наложенными на описанные выше меры безопасности, дают нам следующую картину (Табл. 3.3.3).

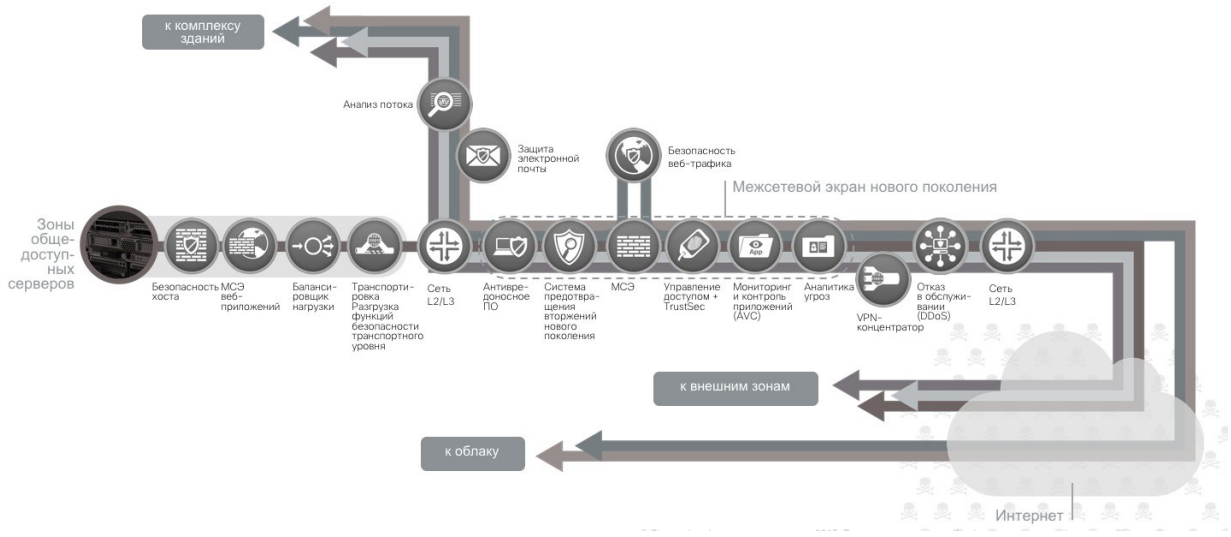
Но периметр — это не только элемент инфраструктуры, агрегирующий глобальные каналы и объединяющий разрозненные точки присутствия предприятия в глобальной сети (Рис. 3.3.4). Это ещё и сетевая инфраструктура, обеспечивающая централизованное соединение с Интернетом и выполняющая функции шлюза для ресурсов Банка при необходимости передачи данных во всемирную сеть. Периметр, подключенный к Интернету, обслуживает множество других модулей, имеющихся в корпоративной сети и за её пределами. Пользователи центрального офиса и филиалов осуществляют доступ в Интернет через периметр, подключенный к Интернету. Мобильные и работающие дома сотрудники могут получать доступ к корпоративным ресурсам и приложениям через периметр, подключенный к Интернету. А ещё периметр обслуживает общедоступные сервисы демилитаризованной зоны и обеспечивает доступ в Интернет для пользователей организации. В этом случае у нас расширяется как модель угроз (например, мы можем опасаться утечек данных или компрометации нашего Web-сайта), так и перечень защитных мер, которые выглядят уже по-другому.

В реальности, модуль периметра (как и любой из семи перечисленных выше модулей) сам состоит из ряда сегментов/зон, предназначенных для решения своих функциональных задач — выход

Табл. 3.3.3. *Меры защиты периметра, подключенного к глобальной сети и Интернету.*

Контроль	Идентификация	Аутентификация VPN. Глубокий анализ пакетов на межсетевом экране. Классификация трафика. Профилирование.
	Мониторинг	Система обнаружения вторжений следующего поколения. Сетевое управление. Отслеживание событий.
	Выявление аномалий	Анализ и выявление взаимозависимостей событий.
Управление	Повышение устойчивости	Базовые средства защиты сети. Резервирование VPN. Резервирование каналов и систем.
	Изоляция и сегментация	Сети VPN. Сети VLAN.
	Обеспечение выполнения политик	Разграничение доступа на межсетевом экране с контролем состояния событий. ACL-списки, функция uRPF, предотвращение IP-спуфинга. Предотвращение вторжений. Применение политики QoS.

Рис. 3.3.4. *Типовые компоненты защиты периметра организации.*

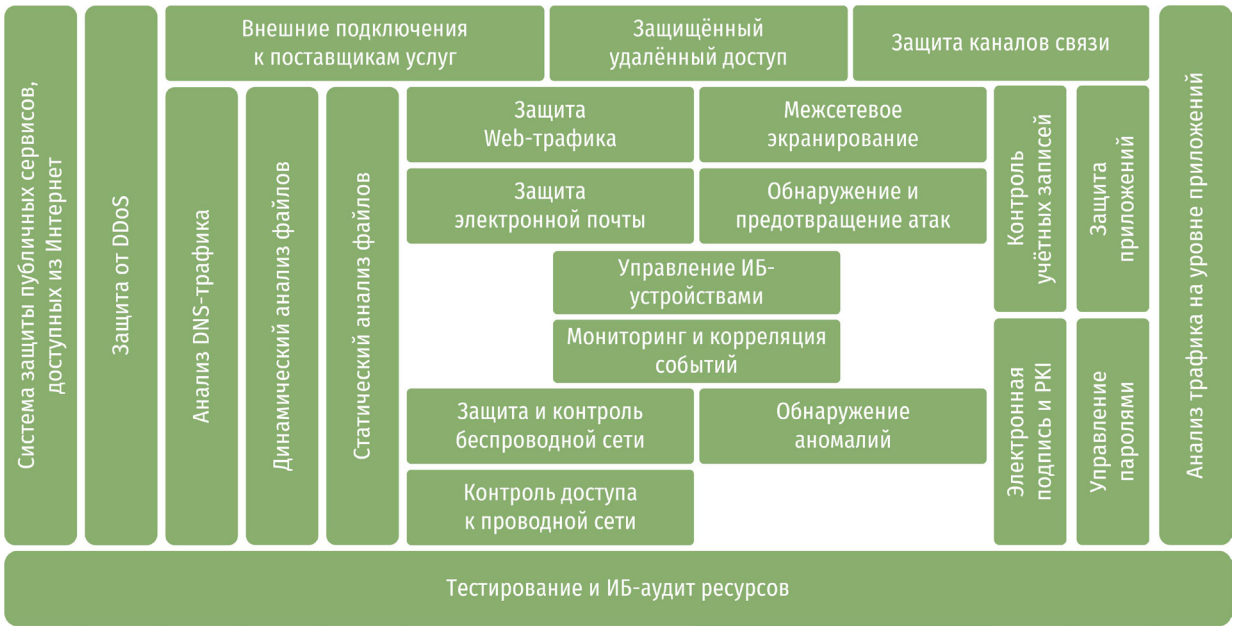


в Интернет, объединение филиалов, удалённый доступ, подключение к облачным сервисам, обеспечение функционирования Интернета вещей, электронная коммерция и т.п. Поэтому и полный перечень защитных мер для точки (или линии?) соединения организации с Интернет будет выглядеть совсем иначе (Табл. 3.3.4, Рис. 3.3.5).

Табл. 3.3.4. *Полный перечень защитных мер периметра.*

Контроль	Идентификация	Глубокий анализ пакетов на межсетевом экране. Аутентификация VPN. Защита web-ресурсов. Фильтрация контента. Защита обмена сообщениями. Анализ приложений. Анализ файлов.
	Мониторинг	Система обнаружения вторжений. Система обнаружения аномалий. Сбор данных о потоках сетевого трафика. Сбор пакетов. Сетевое управление. Защита оконечных и мобильных устройств. Отслеживание событий.
	Выявление аномалий	Анализ и выявление аномалий событий.
Управление	Повышение устойчивости	Базовые средства защиты сети. Резервирование VPN. Резервирование каналов и систем.
	Изоляция и сегментация	Политика доступа на основе пользователей и групп, реализованная на межсетевом экране. Сети VPN. Сети VLAN. Защита оконечных и мобильных устройств.
	Обеспечение выполнения политик	Разграничение доступа на межсетевом экране с контролем состояния соединений. Предотвращение вторжений. Защита оконечных устройств. Фильтрация контента. Защита обмена сообщениями.

Рис. 3.3.5. *Набор мер для защиты периметра, решающего разные задачи организации.*



Шаг №2. Выполнение требований регуляторов

Сегодня существуют сотни различных нормативных актов по безопасности — международных и национальных, отраслевых и локальных (Рис. 3.3.6). Многие из них являются обязательными к применению, некоторые относятся к категории «лучших практик».

Рис. 3.3.6. *Многообразие нормативных требований по ИБ.*

И самое неприятное, что число таких регулятивных требований только растёт (не только в России, но и в мире). Оно и понятно — уровень зависимости мировой экономики и национальной безопасности от информационных технологий и качества информации становится все выше, а, следовательно, государства, международные и отраслевые организации хотят взять это направление под свой неусыпный контроль (Табл. 3.3.5).

Согласно российскому законодательству, обладатель информации или оператор информационной системы ***обязаны*** принимать меры по защите информации, а в ряде случаев делать это так, как установлено законодательством. Сегодня можно выделить шесть основных направлений ИБ, которые регулируются государством и в которых установлены обязательные требования:

1. Защита персональных данных.

2. Защита государственных и муниципальных информационных систем.

3. Защита информации в Национальной платёжной системе и, более широко, в банках и на финансовых рынках.

4. Защита государственной тайны.

5. Безопасность критической информационной инфраструктуры, включая АСУ ТП.

6. Безопасность операторов связи.

На закономерный вопрос, а как же коммерческая, врачебная и другие виды тайн (их в российском праве свыше 60), то к счастью для большинства из них не установлены какие-либо конкретные меры защиты. Это не отменяет необходимости обеспечивать их сохранность, но позволяет их обладателю или лицу, которому поручена их обработка, включая хранение и передачу, самостоятельно выбирать нужные защитные меры, например, в соответствии с международными лучшими практиками (COBIT, ITIL, NIST, ISF, ISO 27001/2 и др.).

Табл. 3.3.5. *Соотнесение распространённых НПА по ИБ с отраслями экономики.*

Отрасль	Основной НПА	Регулятор	Надзор	Наказание
Финансовая организация (банк)	НПА Банка России	Банк России	Прокуратура Банк России Роскомнадзор	КоАП УК (ст.183)
Финансовая организация (НПС)	ФЗ-161 ПП-584 382-П 437-П 552-П	Банк России ФСБ ФСТЭК	Прокуратура Банк России Роскомнадзор ФСТЭК ФСБ	КоАП Приостановление деятельности
Финансовая организация	ФЗ-152	Банк России	Прокуратура Банк России Роскомнадзор	КоАП
Госорган	ФЗ-149	ФСТЭК ФСБ Минкомсвязь	Прокуратура ФСТЭК ФСБ Роскомнадзор Минкомсвязь	КоАП
ТЭК	ФЗ-256 ФЗ БКИИ ФЗ-152 НПА МинЭнерго	Минэнерго ФСБ ФСТЭК ФОИВ по БКИИ	Прокуратура ФСБ Роскомнадзор	КоАП УК
ИП	ФЗ-152		Роскомнадзор Прокуратура	КоАП
ИТ-разработчик	ФЗ-149 ФЗ-128 ПП-549 ПКЗ-2005	ФСТЭК Минкомсвязь ФСБ	ФСТЭК ФСБ	КоАП УК
Сервисная компания	ФЗ-152 ФЗ-128	ФСБ ФСТЭК	Роскомнадзор ФСБ ФСТЭК Прокуратура	КоАП УК

Рис. 3.3.7. *Структура требований по защите ИТ-активов.*

Несмотря на то, что обязательных на уровне федерального законодательства направлений по защите информации всего шесть, существуют и различные другие нормативные акты, которые могут носить характер обязательных. Например, правила международных платёжных систем (PCI DSS и PA DSS), национальные стандарты (да, ГОСТы по ИБ могут быть обязательными в соответствии с законом «О стандартизации в Российской Федерации»), правила фондовых бирж и т.п. (Рис. 3.3.7).

Выбор защитных мер

Каждый из таких нормативно-правовых актов может содержать от нескольких десятков до нескольких сотен требований (например, в SWIFT CSF их 27, в 17-м приказе ФСТЭК уже 113 требований по защите, в PCI DSS 3.0 их 293, в ISO 27002 — почти 300, а в NIST 800-53R4 их уже 721). Как выполнить все это многообразие требований и не забыть про потребности бизнеса и отражение угроз (хотя есть надежда, что, хотя бы, часть нормативных требований поможет бороться с угрозами)? К счастью, нам на помощь приходит итальянский инженер, экономист и социолог Вильфредо Парето, который так сформулировал своё известное правило: «Небольшая доля причин, вкладываемых средств или прилагаемых усилий, отвечает за бóльшую долю результатов, получаемой продукции или заработанного вознаграждения». Его ещё часто называют правило 80/20, хотя на самом деле Парето говорил всего лишь о диспропорции, являющейся неотъемлемым свойством соотношения между причинами и результатами, вкладом и возвратом, усилиями и вознаграждением за них.

В случае с нормотворчеством правило Парето позволяет нам выделить небольшое количество защитных мер, которые позволяют реализовать практически все существующие и будущие нормативные акты по защите информации. Вот этот список:

1. Определение угроз безопасности, анализ уязвимостей и анализ рисков.

2. Предотвращение неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения информации на объекте защиты.

3. Недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено или прекращено функционирование объекта защиты.

4. Применение прошедших в установлен-

ном порядке процедуру оценки соответствия средств защиты информации.

5. Оценка эффективности принимаемых мер по обеспечению безопасности.

6. Обнаружение фактов несанкционированного доступа и принятие мер.

7. Восстановление информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней.

8. Установление правил доступа к информации, а также обеспечением регистрации и учёта всех действий, совершаемых с ней.

9. Контроль за принимаемыми мерами по обеспечению безопасности.

10. Непрерывное взаимодействие с государственной системой обнаружения, предотвращения и ликвидации последствий компьютерных атак (ГосСОПКА).

11. Наличие выделенного ИБ-подразделения или ответственного сотрудника.

12. Обучение и повышение осведомлённости персонала.

Стоит обратить внимание, что мы сознательно ограничиваемся рассмотрением только мер защиты информации, упомянутых в нормативных актах. Обзор иных организационных и технических мер (например, получение согласий на обработку персональных данных, локализация персональных данных, выбор отечественной ИТ-продукции и т.п.) является важным, но выходит за рамки данного раздела.

Что же касается выбора технических мер защиты (надо ли ставить NGFW или можно обойтись встроенным в маршрутизатор межсетевым экраном?), то сегодня, к счастью, большинство нормативных требований (таковы документы ФСТЭК, Банка России, NIST, ISO и т.п.) построены по принципу свободы выбора. Этот принцип последовательно реализуется четырьмя шагами:

1. Выбор базового состава мер.

2. Адаптация выбранного базового набора мер применительно к структурно-функциональным характеристикам ИС, реализуемым ИТ, особенностям функционирования ИС и модели угроз.

3. Уточнение (включает дополнение или исключение).

4. Дополнение адаптированного базового набора мер по обеспечению безопасности дополнительными мерами, установленными иными нормативными актами.

Иными словами, вы самостоятельно выбираете только те защитные меры, которые подходят под вашу задачу, а не пытаетесь реализовать закрытый перечень защитных мер, придуманных регулятором, и вам совершенно не подходящих.

Особняком стоит вопрос о необходимости применения сертифицированных средств защиты информации, но мы его осознанно оставляем за рамками данного учебника, так как в ответе на этот вопрос нет единодушия среди специалистов и юристов. Да и сами нормативные акты в этой сфере постоянно меняются. Уверенно сегодня можно сказать только следующее:

- Государственные и муниципальные информационные системы должны быть защищены только с помощью сертифицированных средств защиты информации и никаких иных вариантов тут не предусмотрено.
- Персональные данные, АСУ ТП и значимые объекты критических информационных инфраструктур могут быть защищены с помощью любых средств защиты информации, в т.ч. и не сертифицированных, но прошедших оценку соответствия в одной из выбранных потребителем форм (например, в форме ввода в эксплуатацию или госконтроля/надзора).

Кейс: защита от фишинга

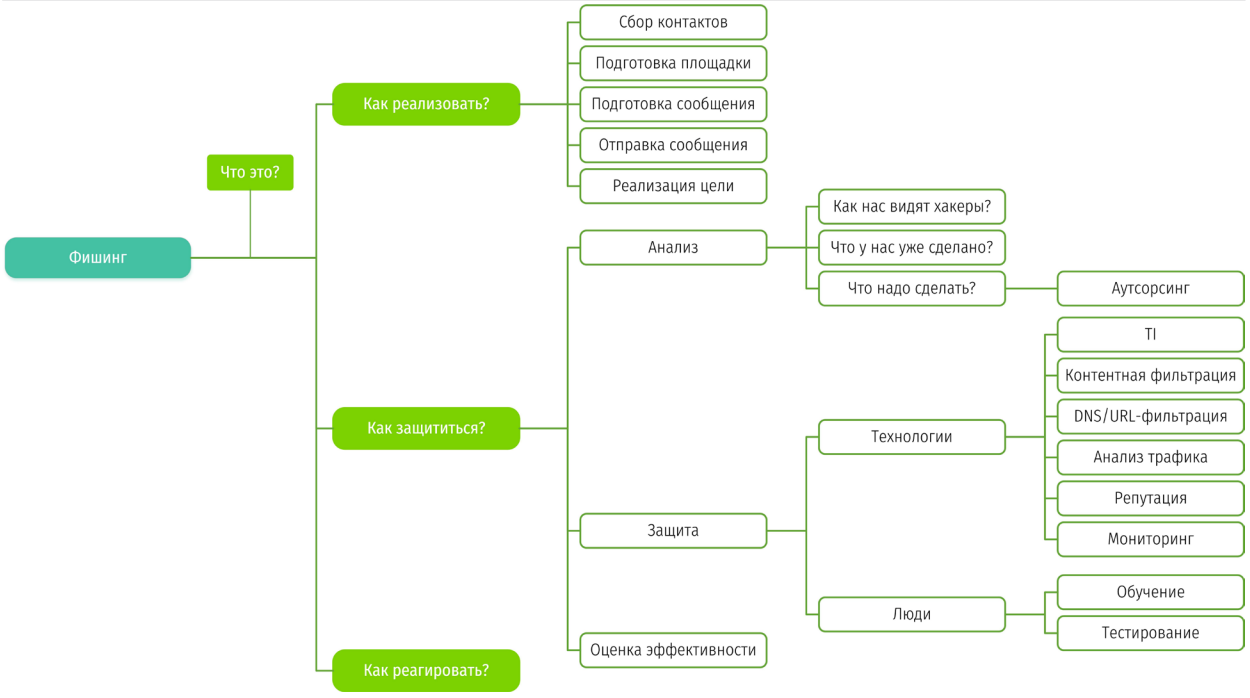
Фишинг сегодня — это одна из самых распространённых угроз, которая затрагивает и домашних пользователей, и малый бизнес, и крупные предприятия. С фишинга часто начинаются и более сложные атаки — заражение компьютеров, перехват управления технологическими процессами, вывод систем из строя и т.п. При этом, фишинг постоянно эволюционирует и поэтому эпизодическими мероприятиями его победить очень сложно. Например, относительно недавно был анонсирован проект Evilginx, демонстрирующий возможность перехвата идентификационных параметров и сессионных cookies для любого Web-сервиса, в том числе и в случае двухфакторной аутентификации.

Не случайно регуляторы в своих нормативных актах упоминают о необходимости борьбы с фишингом, маскируя его расплывчатыми формулировками про контроль поступлений незапрашиваемых электронных сообщений. Но что скрывается за такими формулировками, помещающимися всего на одной строчке? Как правильно читать хотя бы одну защитную меру, посвящённую борьбе с фишингом?

Большинство людей знает, что такое фишинг, но всё-таки, чтобы иметь единую точку отсчёта для дальнейшего повествования, мы считаем нужным дать определение. Фишинг — это отправка фальшивых сообщений через различные сервисы с целью получения доступа к конфиденциальной информации. Обратите внимание — через «различные», а не только через электронную почту. При этом, сейчас в индустрии сложилось определённое разделение различных видов фишинга:

- ***Просто фишинг (phishing)*** — массовая рассылка сообщений, ведущая на фальшивые или заражённые сайты. Также этот термин является общим для всех видов фишинга.
- ***Spear phishing*** — фишинг, сфокусированный на конкретной жертве. По статистике около 90% всех целенаправленных атак

Рис. 3.3.8. *Комплексный взгляд на проблему защиты от фишинга.*



(APT) реализуется именно через этот вид фальшивых сообщений.

- ***Whaling*** — фишинг, сфокусированный против «больших», высокопоставленных лиц (от английского слова «кит»).
- ***Vishing*** — фишинг через IP-телефонию и иные VoIP-сервисы.
- ***Smishing*** — фишинг посредством SMS- и MMS-сервисов.
- Существует также ***сервис рассылки фальшивых сообщений через социальные сети***, но для него названия ещё не придумали.

Видя такое разнообразие методов фишинга, мы понимаем, что серебряной пули нам не найти и одним продуктом проблему не решить. Поэтому нам нужна комплексная система, позволяющая взглянуть на проблему с разных сторон, и найти правильные решения для каждой из них. По сути можно говорить о целом дереве, ветви и листья которого и определяют шаги, необходимые для выстраивания эшелонированной защиты от фишинга (Рис. 3.3.8).

К сожалению, реализация фишинга сегодня не очень сложна и не требует дорогостоящих инструментов. Всё можно сделать с помощью программ, которые свободно скачиваются в Интернет или входят в состав какого-либо дистрибутива, например, Kali Linux. Обычно последовательность действий злоумышленников такова (мы не будем глубоко вдаваться в детали по понятным причинам — важно показать суть данной ветви нашего дерева):

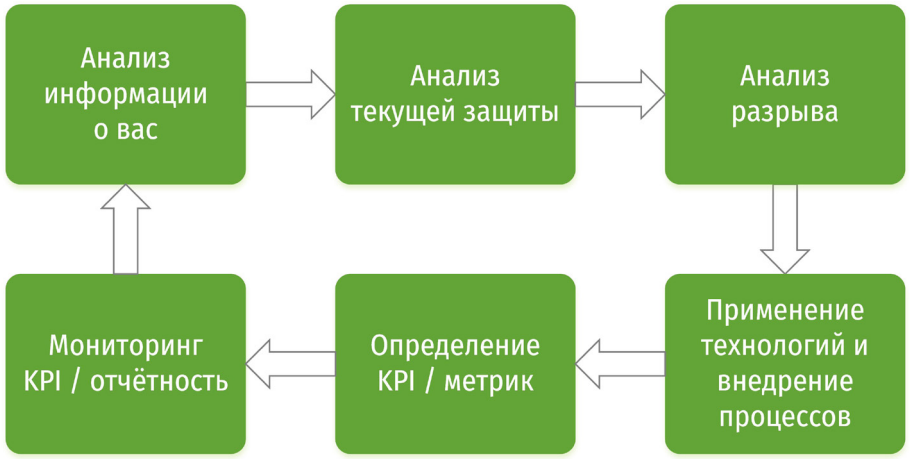
- ***Собрать контакты***. Вы удивитесь, сколь много информация о вас хранится в Интернете и особенно в различных соцсетях — Facebook, LinkedIn и других. Утилиты вроде theHarvester или recon-ng способны выуживать эти данные, составляя таким образом базу для последующих рассылок e-mail или SMS/MMS.
- ***Подготовить площадку для заражения и для рассылки***. На данном этапе злоумышленники создают сайты-клоны или сайты, похожие по своему названию на жертву (sbrrbank.ru вместо sberbank.ru), а также заражают легальные сайты вредоносными программами, размещают на легальных сайтах вредоносную рекламу (через баннерные сети) или просто перенаправляют пользователя на подставной сайт. При этом, клонировать сайт на подставном домене не составляет большого труда — для этого можно использовать как специализированные утилиты типа Social Engineer Toolkit (SET) в составе Kali Linux или онлайн-сервисы, например, Clone Zone.
- ***Подготовить и разослать сообщение*** e-mail / SMS / MMS / VoIP также можно с помощью специализированных программ (тот же SET) или онлайн-инструментов для рассылки рекламы, спама или организации фишинговых рассылок.

Хорошо подготовленное злоумышленниками сообщение приводит к тому, что пользователь-жертва ловится на удочку (отсюда и термин phishing) и дальше злоумышленник выполняет поставленную задачу — получает конфиденциальную информацию (например, логины и пароли), перехватывает управление или выводит системы из строя.

Чтобы защититься от фишинговых атак, мы должны выполнить шесть последовательных шагов, которые на финальном этапе должны нас вновь вернуть в исходное значение и цикл вновь повторится (Рис. 3.3.9):

1. Анализ информации о вас. По сути на этом этапе вы должны поставить себя на место хакера, который будет атаковать вас. Вы должны использовать тот же инструментарий — theHarvester, recon-ng, URLcrazy, CloneZone, HTTrack, SET и другие, но с иной целой — сыграть на опережение и понять, как ваша компания видна с внешней точки зрения и какие угрозы могут быть реализованы против вас.

Рис. 3.3.9. *Последовательность шагов в борьбе с фишингом.*



2. Анализ текущей защиты. Данный этап не является сложным и позволяет вам понять, что у вас есть из защитных мер — встроенных или наложенных, платных или бесплатных, собственных или аутсорсинговых.

3. Анализ разрыва. Поняв, какие угрозы могут быть реализованы против вас, и какая защита имеется в вашем арсенале, вам остаётся выбрать то, чего не хватает вам для нейтрализации выбранных угроз.

4. Применение различных защитных мер — технологических, организационных и юридических. Данный этап мы рассмотрим в деталях дальше.

5. Определение показателей эффективности (метрик) и измерение эффективности. Стремление к чему бы-то ни было требует регулярной оценки достижения поставленных целей, включая и промежуточные результаты. Поэтому вы должны для себя определить показатели эффективности вашей системы защиты от фишинга — процент сотрудников, кликнувших по фишинговым ссылкам, число сотрудников, прошедших тренинги повышения осведомлённости и т.п.

6. Отчётность. Ну и конечно же, вам не обойтись без регулярной отчётности, которая должно предоставляться руководству для оценки статуса программы фишинговой защиты.

При выборе защитных мер, какие бы они не были, перед вами встанет две дилеммы:

- Коммерческие решения или бесплатные?
- Своими силами реализовать защиту или обратиться к услугам аутсорсинговых компаний?

Мы не будем давать ответа на эти вопросы, понимая, что у вас могут быть свои взгляды на них. Выбор в пользу любого из вариантов имеет свои преимущества и недостатки. Например, строительство своей системы означает полный контроль над всеми процессами, гибкость и учёт собственной специфики. При этом, аутсорсинг подразумевает большие компетенции (при правильном выборе партнёра), высвобождение времени и простота внедрения отдельных защитных мер. Как видите, плюсы есть в обоих случаях и решать за вас, по какому из сценариев двигаться, мы не можем.

Обычно защита от фишинга начинается с внедрения средств защиты электронной почты, которые уже включают в себя соответствующие механизмы — SPF, DKIM, DMARC и другие. В Топ-5 соответствующего сегмента рынка, по версии Gartner, сегодня входят следующие игроки: Barracuda Networks, Cisco, Mimecast, Proofpoint и The Email Laundry. Второй линией обороны обычно считаются средства контроля доступа в Интернет — локальные или облачные. Они позволяют блокировать переходы по ссылкам, полученным в почте, SMS или MMS (в последних двух случаях требуется облачное решение — возможно на сторо-

не мобильного оператора или специального поставщика услуг ИБ). Среди лидеров этого сегмента можно назвать Bluecoat, Cisco, Websense и ZScaler.

Но наличие средств мониторинга e-mail и Web-трафика ещё не означает, что вы защищены от фишинга. Он постоянно эволюционирует, и вы должны также на постоянной основе получать информацию о новых адресах, участвующих в фишинге, методах хакеров и т.п. Иными словами, вам нужна информация Threat Intelligence, которая может поставляться в двух вариантах — в виде так называемых фидов (feed) и через API. В первом случае вы получаете небольшие, но частые порции новых источников фишинговых атак. К поставщикам таких регулярно обновляемых сведений можно отнести: Cisco AMP ThreatGrid, Cisco Umbrella, Cyren, FraudWatch, LookingGlass, Netcraft, OpenFish, PhishLabs, PhishMe, PhishTank, SpamCop, Station X, Лаборатория Касперского и др.

В случае с API вы не ждёте информации от поставщика фидов, а сами направляете ему интересующие вас домены, адреса e-mail, URL для проверки.

При выборе технических средств защиты от фишинга стоит обратить внимание на следующие моменты:

- У сотрудников может быть доступ и к личной почте с рабочего ПК (например, через Web-почту). В этом случае вам понадобится защищать и этот вектор атаки.
- Если у сотрудников есть служебные или личные мобильные устройства с доступом к корпоративной почте, то как обеспечивается нейтрализация фишинга на них?
- Фишинг возможен и через соцсети, а значит, необходимо побеспокоиться и о данной угрозе.
- Выбранное вами решение имеет плагины к вашим почтовым клиентам? Это хоть и опционально, но позволяют не только повысить эффективность защиты за счёт получения пропущенных фишинговых писем, но и вовлечь пользователей в процесс защиты, повышая их культуру ИБ.

Но защитой периметра (на уровне e-mail или Web) техническая защита не ограничивается. Мы не должны забывать про оконечные устройства — рабочие станции, лэптопы, планшетные компьютеры и смартфоны. Как защищаются от фишинга и его последствий они? Тут можно посоветовать обратить внимание на средства защиты класса EDR (Endpoint Detection and Response), STAP (Specialized Threat Analysis and Protection) или BDS (Breach Detection System), которые могут блокировать известные и неизвестные угрозы, в т.ч. и реализуемые после посещения фишинговых ресурсов, по их поведению. И, безусловно, нельзя забывать про плагины и расширения к браузерам, которые позволяют в прозрачном режиме блокировать доступ к фишинговым ресурсам.

Много говоря про технические меры, нельзя не сказать про работу с людьми, т.к. именно от них в конечном итоге зависит, нажимать или нет на фишинговые ссылки. Поэтому важнейшим процессом в деле защиты от фишинга является обучение пользователей. В данном вопросе можно обойтись как своими силами, так и используя специализированные обучающие системы. В первом случае внимание пользователей стоит обращать на такие моменты:

- строка адреса в браузере;
- написание домена;
- символ замка (наличие HTTPS);
- сертификат сайта;
- ошибки в тексте;
- просьба внести деньги;
- просьба указать свои идентификационные данные.

Во втором случае ваш выбор должен пасть

на одну из систем обучения и повышения осведомлённости по ИБ (Security Awareness Training System), которые обеспечивают процесс обучения в формате кампании, а не разового события. Эти решения используют различные формы донесения материала, включают напоминания, позволяют измерять и отслеживать результаты по каждому сотруднику, награждая их за определённые достижения. Среди игроков данного рынка можно назвать Wombat Security, PhishMe, MediaPro, SANS, BeOne и др.

Однако помните, в 2016-м году каждый месяц обнаруживалось около 400 тысяч фишинговых сайтов. При такой интенсивности фишинговых угроз поручать только сотрудникам защиту от фишинга и ждать от них высокой эффективности нереалистично. Несовершенство людей делает невозможным распознавание всех фишинговых атак, а обычное человеческое любопытство только ухудшает ситуацию. Поэтому, помимо систем обучения, мы бы рекомендовали воспользоваться фишинговыми симуляторами, которые дополняют процесс обучения и за счёт эмуляции реальных фишинговых кампаний помогают отслеживать тенденции в поведении пользователей. Почти все поставщики SAT-решений предлагают и услуги по фишинговой симуляции, но при их выборе стоит обратить внимание на то, поддерживается ли русский язык. Если нет, а в вашей компании английский не является основным, то, возможно, стоит обратить внимание на отечественных игроков этого сегмента — сервисы phishman.ru или antiphish.ru. А можно развернуть и собственную платформу на базе open source решения под названием getgophish.

В заключение рассмотрения этого кейса нам бы хотелось дать пару рекомендаций в части реагирования на фишинговые атаки, которые полностью предотвратить с помощью описанных выше мер всё-таки не удастся. Например, не стоит забывать про регулярную и внеплановую (при подозрении на фишинговый инцидент) смену паролей. А ещё не стоит забывать про ***разделегирование*** (прекращение существования) фишинговых доменов, чтобы злоумышленники не оставались безнаказанными, и их домены прекращали своё существование. Сегодня правом разделегировать домены обладают: Управление «К» МВД РФ, Генеральная прокуратура, Лаборатория Касперского, Group-IB, РОЦИТ, Лига безопасного интернета, а также RU-CERT, Бизон («дочка» Сбербанка по ИБ), FinCERT (центр реагирования на инциденты Банка России) и регистраторы доменов (по заявлению владельцев).

На сайтах этих организаций (как минимум, некоторых из них) существует соответствующая форма сообщения о фишинговом инциденте.

В финале данного кейса мы бы хотели привести список практичных метрик, которые можно использовать при оценке эффективности системы защиты от фишинга, которая состоит из мер, описанных в данной главе:

- На этапе предотвращения фишинга:
  - процент доставленных фишинговых писем;
  - процент кликнутых фишинговых писем;
  - процент ложных срабатываний.
- На этапе обнаружения фишинга:
  - процент фишинговых писем, о которых сообщили пользователи;
  - время обнаружения (TTD);
  - соотношение ложных обнаружений и необнаружений.
- На этапе реагирования на фишинг:
  - время локализации (TTC);
  - время на устранение (TTR);
  - стоимость инцидента.

Ответственность за неисполнение обязательных мер

За невыполнение обязательных требований по защите информации российским законодательством предусмотрена административная, гражданская, уголовная и дисциплинарная ответственность (Табл. 3.3.6). Правда, надо отметить, что правоприменительная практика в этой области практически отсутствует.

Табл. 3.3.6. *Нормативные акты и виды ответственности за их нарушение.*

НПА	Объект защиты	Статус	Обязательность	Ответственность	Оценка соответствия
ISO 270xx	Все активы	Международный стандарт	Рекомендация	Нет	Сертификация (внешний аудит)
СТО БР	БТ, КТ, ПДн	Отраслевой стандарт	Рекомендация	Нет	Внешний аудит, самооценка
ГОСТ 57580.1	БТ, КТ, ПДн	Национальный стандарт	Обязательный при условии включения ссылок на него в нормативные акты Банка России	Возможно: штраф, предписание об устранении, приостановление оказания операционных услуг и т.д.	Внешний аудит Проверка ЦБ
ФЗ-152	ПДн	Закон и подзаконные акты	Обязательный	Штраф	Не установлена
PCI DSS	БТ, ПДн	Международный стандарт	Обязательный (де-факто)	Штраф, отключение от VisaNet, запрет запуска новых услуг на базе платёжных карт	Внешний аудит, сканирование, самооценка
ФЗ-161	Данные о денежных переводах и другая информация	Закон и подзаконные акты	Обязательный	Штраф, предписание об устранении, приостановление оказания операционных услуг и т.д.	Внешний аудит Проверка ЦБ
Положения ЦБ	Информация, процессы	Нормативные акты регулятора	Обязательные	Предписания об устранении (де-юре)	Внешний аудит Проверка
ФЗ-149	Информация, системы	Закон и подзаконные акты	Обязательный	Штраф, предписание об устранении	Аттестация Проверки ФСТЭК/ФСБ
ФЗ-187	Объекты КИИ	Закон и подзаконные акты	Обязательный	Штраф, дисквалификация, лишение свободы	Проверки ФСТЭК

Шаг №3. Отражение угроз

Задавались ли вы простым вопросом — кто вас атакует или может атаковать в киберпространстве? Хакеры-одиночки? Организованные киберпреступные группировки? Кибертеррористы? А может быть, вы представляете интерес для спецслужб иностранного государства? От ответа на этот, казалось бы, простой вопрос, будет зависеть набор мероприятий по обеспечению вашей кибербезопасности (Рис. 3.3.10). Очевидно, что возможности хакера-одиночки, случайно наткнувшегося на вас в Интернете, разительно будут отличаться от того, что может использовать против вас спецслужба Китая, Германии, Израиля или США.

Концепция активной обороны

Мы должны учитывать изменяющийся ландшафт киберугроз и новые требования нормативных актов, число которых активно растёт. Но как правильно выстраивать линию своей обороны? Пытаться съесть слона целиком и закупить средств защиты на многие десятки и сотни миллионов рублей? Или всё-таки есть стратегия поэтапной реализации защитных мер? Как это не удивительно, но она есть, и имя ей «концепция активной обороны». Она состоит из пяти последовательно реализуемых сценариев, позволяющих наращивать защитный потенциал, в зависимости от задач стороны защиты и разработанной модели угроз, о которой мы уже говорили ранее (Рис. 3.3.11).

Первый сценарий подразумевает правильную архитектуру, то есть базис для системы защиты. И речь идёт не об архитектуре безопасности, а об ИТ-архитектуре предприятия, правильном применении уже имеющихся элементов информатизации. Сюда попадает сегментирование, управление цепочками поставок оборудования и запчастей, поддержка, устранение уязвимостей, управление патчами и обновлениями, контроль привилегированных пользователей и т.п. Т.е. и к защите-то это даже не всегда относится — это именно основа, задающая тон всем последующим сценариям. Обратите внимание, что это наименее затратный, но при этом наиболее эффективный защитный сценарий, который задействует встроенные механизмы ИБ на уровне сетевой инфраструктуры (сегментирование, 802.1x или Port Security, VLAN

Рис. 3.3.10. *Не все нарушители одинаковы.*

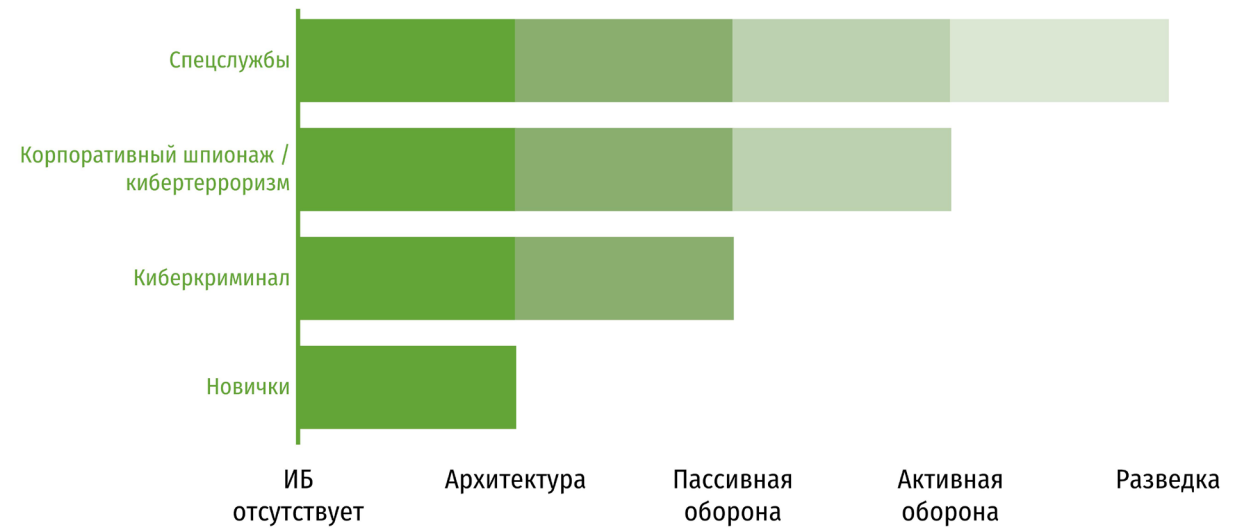
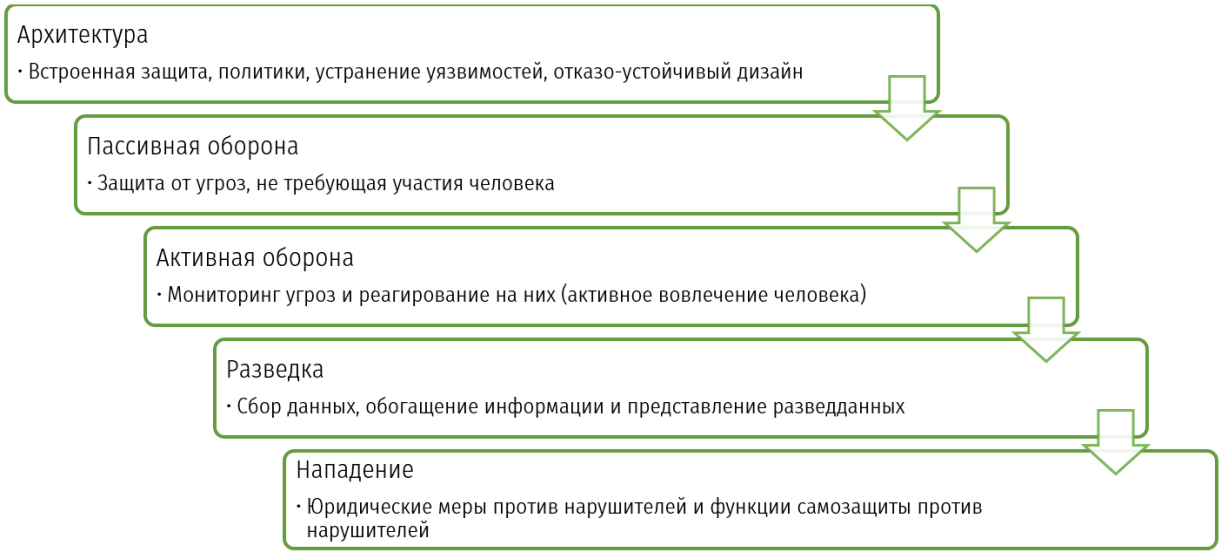


Рис. 3.3.11. *Пять этапов/сценариев концепции активной обороны.*



и т.п.), уровне СУБД, операционных систем и приложений, отвечающих за управление ИТ-процессами.

Второй сценарий начинает использовать традиционные средства защиты, но в пассивном режиме. Пассивной защита называется потому, что не требует, ну или почти не требует, постоянного участия человека в процессе защиты. По сути, речь идёт об установке различных средств защиты, которые работают в соответствии с заданными, зачастую статическими политиками, в автоматическом режиме. К числу таких средств защиты относятся межсетевые экраны, системы обнаружения атак, антивирусы, системы контроля доступа (NAC), системы защиты оконечных устройств. К сожалению, многие предприятия на этом этапе и останавливаются, считая, что установка средств защиты — это всё, что нужно для отражения современных атак и действий внутренних нарушителей. Но это не так.

Третий сценарий подразумевает активное вовлечение человека в процесс защиты. Как это ни странно, но до этого участие homo sapiens сводилось к минимуму. В первом сценарии система защищала себя посредством правильно выстроенной архитектуры. Во втором сценарии мы добавили навесные решения по безопасности. И только сейчас мы обратились к человеческим рукам и интеллекту, которые должны поднять безопасность на более высокий уровень. Именно в этом сценарии начинается проведение тестов на проникновение, позволяющих понять слабые места защищаемой системы, внедрение решений по мониторингу аномальной активности, систем управления журналами регистрации событий и другого инструментария для аналитики и управления инцидентами, который подразумевает непрерывное участие высококвалифицированного персонала, способного обнаруживать то, что пропускается традиционными средствами сетевой безопасности. Сюда же относится анализ и поиск вредоносного кода (не путать с детектированием, которое реализуется антивирусами). Иными словами, к инструментам второго уровня добавляется глубокая аналитика и активное вовлечение человека в процесс принятия решений в области безопасности.

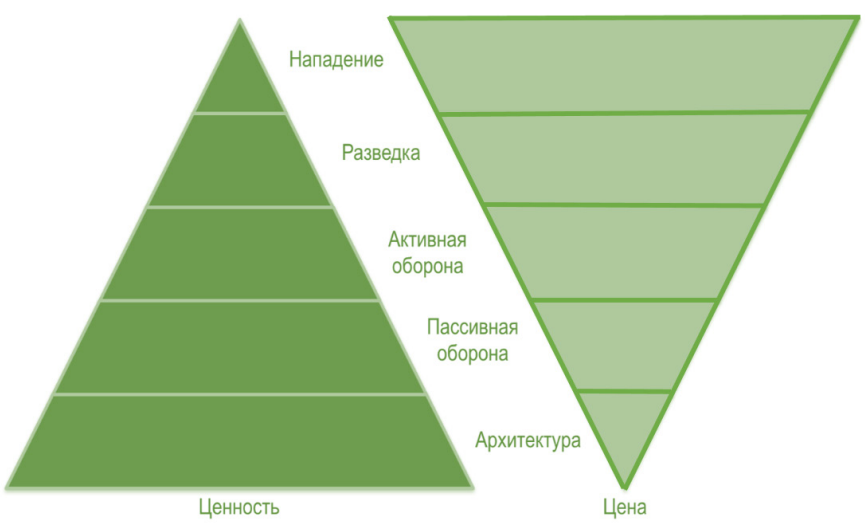
Четвёртый сценарий (хотя грань между 3-и м 4-м достаточно условна) подразумевает высший пилотаж — выстраивание процессов Threat Intelligence и Threat Hunting, в рамках которого разрозненные следы несанкционированной активности, обнаруженные на предыдущем этапе, аккумулируются в индикаторах компрометации (IoC), в бюллетенях и отчётах об угрозах, в формализованном описании угроз, которые можно распространять для широкой общественности или только внутри своей отрасли, группы компаний или предприятия, в том числе и в рамках специально созданных центров распределения информации об угрозах (ISAC, CERT, CSIRT), включая и государственную систему обнаружения, предотвращения и ликвидации последствий компьютерных атак (ГосСОПКА), которую создала Федеральная служба безопасности и подключение к которой является обязательной для всех субъектов, владеющих критической информационной инфраструктурой.

Пятый сценарий отражает получающий всё большее распространение сдвиг от оборонительной тактики к наступательной, что немного противоречит смыслу термина «защита информации», не подразумевающему нападения на своего противника. Обычно на этом этапе идентифицируются не просто атаки, а уже сами атакующие, против которых затем реализуются различные действия — возбуждение уголовного преследования, перехват управления командными серверами вредоносных программ (C&C), разделегирование вредоносных доменов и т.п. Этот сценарий нечасто встречается в жизни и применяется скорее на государственном уровне или монополистами, имеющими соответствующие возможности и ресурсы не только для собственной защиты, но и для нападения на атакующих.

Очевидно, что чем дальше мы продвигаемся по концепции активной обороны, тем больше ресурсов (временных, людских, финансовых) нам требуется. При этом, уровень оборонительных возможностей будет возрастать непропорционально сделанным затратам (Рис. 3.3.12).

Надо ли всем стремиться реализовывать самый последний, или хотя бы предпоследний сценарий обеспечения ИБ на своём предприятии? К счастью, нет. Многие организации, закрепившись на втором уровне, так на нём и остаются, не сталкиваясь с потребностью идти дальше. Им не нужны никакие SOC, CSIRT и другие аналитические подразделения. Им не нужны посменно работающие группы аналитиков и специалистов, реагирующих на инциденты. Их устраивает автоматическая защита, даруемая межсетевыми экранами, системами обнаружения вторжений и антивирусами. А всё почему? Да

Рис. 3.3.12. *Зависимость ценности и цены ИБ от этапа концепции активной обороны.*



потому, что они не сталкиваются с угрозами, требующими серьёзной аналитики и присутствия человека. Иными словами, они борются с традиционными нарушителями, не относящимися к иностранным спецслужбам или кибертеррористам. Поэтому сегодня сценарий пассивной ИБ — это как раз удел большинства предприятий, не сталкивающихся с APT и целенаправленными угрозами. Зачем им тогда тратить деньги на избыточный и редко используемый на практике сервис?

Зрелость российских предприятий в части внедрения концепции «активной обороны» разнится в зависимости от того, о каком из семи модулей корпоративной инфраструктуры, упомянутых выше, мы говорим. По нашим оценкам до 60% российских предприятий сегодня реализуют, в той или иной степени детальности, первый архитектурный сценарий (при этом, что парадоксально, в своих офисных/корпоративных сегментах такие организации, вполне возможно, реализуют уже третий, а то и четвёртый сценарии концепции активной обороны). Ещё 30% осуществляют переход ко второму сценарию, внедряя специализированные, но все ещё пассивные средства защиты в промышленных сегментах или облачных средах. И только единицы начинают присматривать для своих промышленных, IoT-, облачных, мобильных модулей третий и четвёртый описанные сценарии. Однако, рост числа публичных примеров атак, появление всё большего числа примеров специализированного промышленного вредоносного кода (Stuxnet, BlackEnergy, Havex, Crash Override) и ужесточение ответственности за несоблюдение мер защиты критических информационных инфраструктур может изменить эти пропорции в самое ближайшее время.

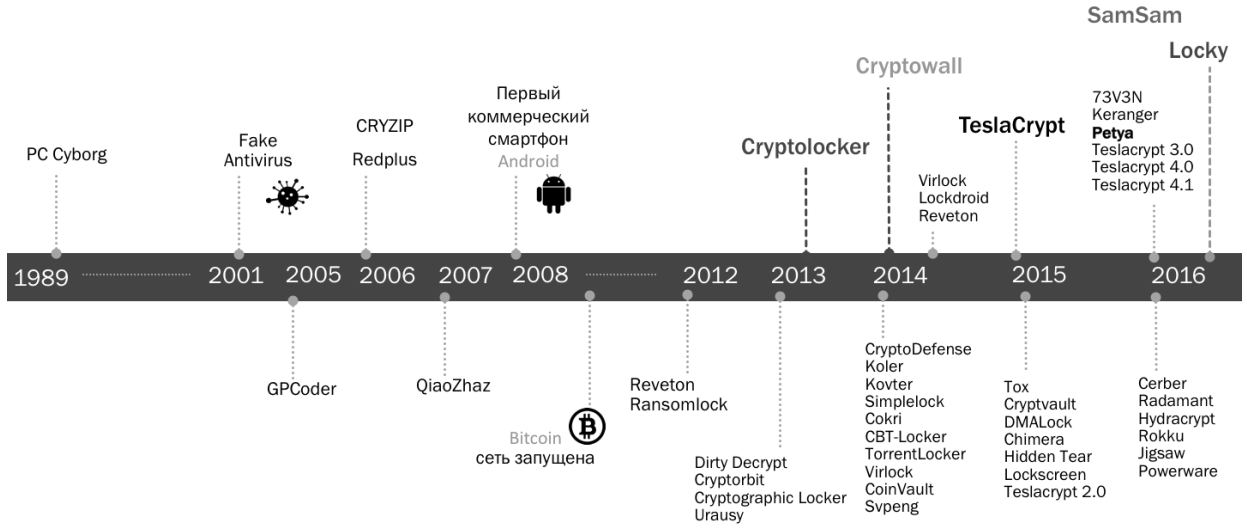
К угрозам ИБ, которые ведут к рискам, мешающим достижению бизнес-целей, можно отнести:

- Вредоносное ПО, в том числе и программы-вымогатели;
- Целенаправленные угрозы (APT);
- Атаки «Отказ в обслуживании» (DoS, Denial of Service), в том числе распределённые (DDoS, Distributed DoS) на инфраструктуру;
- Несанкционированный доступ;
- Потеря контроля;
- Превышение привилегий;
- Несанкционированное изменение информации (подмена реквизитов платёжных поручений, контрагентов и т.п.);
- Фишинг;
- Утечки информации;
- Спам;
- Появление посторонних и фальшивых устройств в инфраструктуре, в т.ч. в беспроводных;
- Потери/кражи мобильных устройств;
- Разведка;
- Использование уязвимостей;
- Перехват данных.

Кейс: защита от программ-вымогателей

Встречается ли ИТ-специалист, который ни разу не сталкивался с криптолокерами или программами-вымогателями (ransomware), при том, что именно эта угроза сегодня считается одной из самых опасных в теневой индустрии киберпреступников? На мероприятиях по ИТ- или кибербезопасности, на которых все мы часто бываем, задавая этот вопрос, мы всегда видим лес рук. Кто-то даже в перерывах и кулуарах делится своими историями и говорит, что тоже сталкивался, но постеснялся поднимать руку со всеми. Это действительно бич современного предприятия, который приносит преступникам колоссальную прибыль — более 1 млрд долларов в год. И это не смотря на то, что сама по себе угроза вымогательства со стороны вредоносного ПО не является чем-то новым. Первые примеры известны ещё с конца 80-х годов (Рис. 3.3.13).

Рис. 3.3.13. *Эволюция вымогательского ПО.*



Но именно сегодня стечение несколько обстоятельств привело к тому, что криптолокеры стали самым доходным видом вредоносных программ:

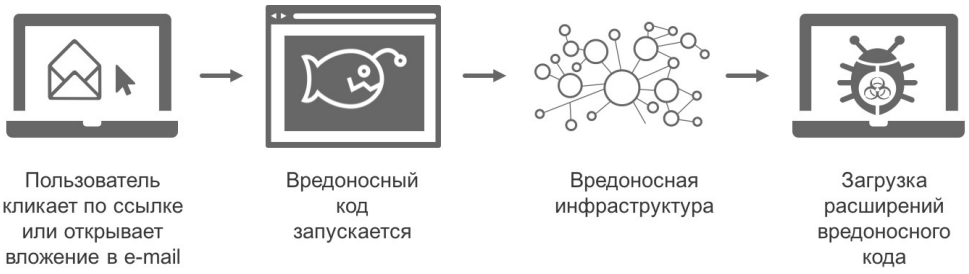
- лёгкое и эффективное шифрование на пользовательских компьютерах;
- популярность эксплойт-китов, осуществляющих заражение компьютеров;
- фишинг, заставляющий пользователей посещать вредоносные сайты или открывать вредоносные вложения;
- готовность платить выкуп шантажистам.

Пользователи и организации, ставшие жертвой программ-вымогателей, находятся в незавидном положении — приходится верить кибершантажисту. На первый взгляд, простейшим (и единственным) решением проблемы является уплата выкупа, однако в этой ситуации важно понимать, что никаких гарантий последующей расшифровки и восстановления файлов не существует. Ошибки в ранних версиях некоторых программ-вымогателей приводили к полной утрате файлов даже в случае уплаты выкупа. Однако, авторы криптолокеров тоже не стоят на месте и постоянно модифицируют и свои творения, и свою тактику. Например, при повторном заражении (а таких случаев немало) тем же самым вымогательским ПО его авторами запрашивалась меньшая сумма выкупа — своего рода «скидка для постоянных клиентов». Также встречается и противоположный подход: сумма выкупа увеличивается, если при первой атаке пользователь не торопится платить злоумышленнику. При этом, злоумышленники даже могут устанавливать крайние сроки (таймеры), по истечении которых увеличивается сумма выкупа или безвозвратно уничтожаются ключи шифрования.

Как осуществляется заражение криптолокером (Рис. 3.3.14)? Основными векторами кибершантажистов являются электронная почта и вредоносная реклама. Однако некоторые организаторы атак пользуются уязвимостями сетей и серверов в сети Интернет.

Невысокая квалификация пользователей приводит часто к тому, что они, не задумываясь, кликают на приходящих им почтовых сообщениях, содержащих либо уже вредоносные вложения, либо ссылки на сайт с таким вредоносным вложением. При этом, в эксплойт-китах, благодаря которым програм-

Рис. 3.3.14. *Типовая цепочка заражения вымогательским ПО.*



мы-вымогатели превратились в столь серьёзную угрозу, по-прежнему эффективно используются уязвимости Adobe Flash (Рис. 3.3.15). Например, недавний анализ популярного эксплойт-кита Nuclear силами аналитиков по безопасности Cisco показал, что на технологию Flash приходится 80% успешных попыток проникновения в систему. И даже несмотря на то, что сама Adobe постепенно сворачивает поддержку и развитие Flash, этот канал распространения будет ещё долго очень популярным — ведь он по умолчанию включён во многие браузеры (исключая платформу Apple iOS).

Рекламные сети невольно (или намеренно) также начинают играют всё большую роль в распространении вредоносной рекламы и таким образом способствуют формированию новой бизнес-модели для хакеров, которую можно назвать «вредоносная реклама как услуга». Организаторы атак покупают рекламные места на популярных веб-сайтах с хорошей репутацией, чтобы разместить на них вредоносную рекламу. Приобретая законные рекламные места, преступники получают возможность распространять угрозы посредством самых разных, никак не связанных между собой веб-сайтов. Реклама отображается в течение короткого времени, которого почти всегда недостаточно для выявления угрозы. Рекламные сети используют различные виды таргетирования, например, по типу и версии браузера, что облегчает преступникам задачу организации адресных атак в отношении конкретных категорий пользователей, включая отбор, например, по языковому признаку.

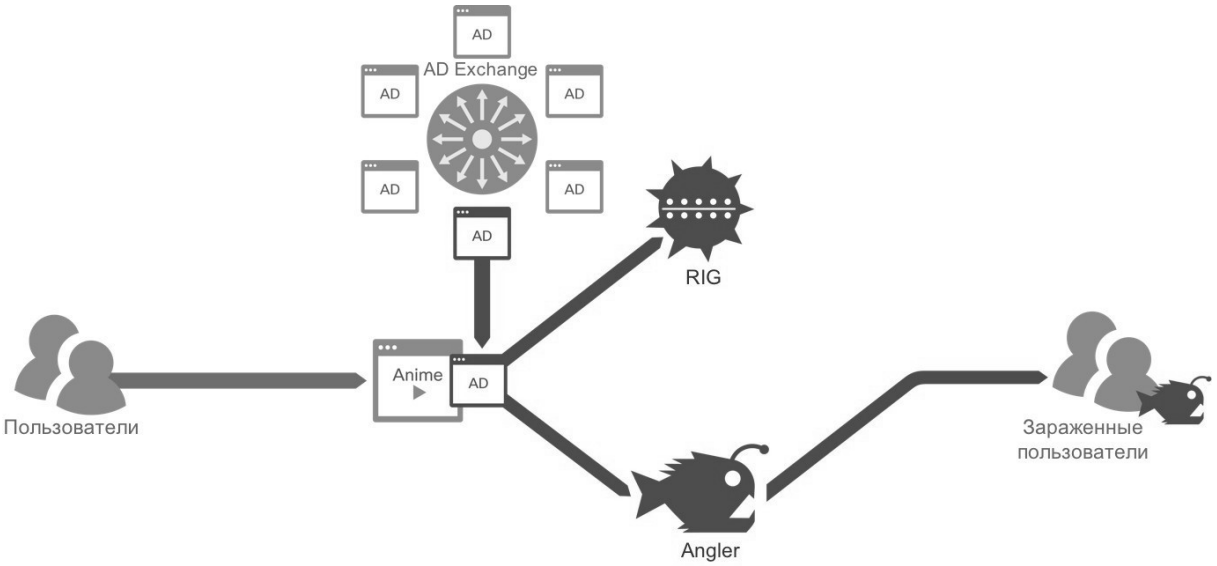
При этом, рекламные места приобретаются для показа рекламы, непосредственно инфицирующей компьютеры, или же для переадресации пользователей на страницу с заражёнными файлами. Нередко имеет место многократная переадресация. Иногда заражение происходит в фоновом режиме без прямого взаимодействия пользователя с вредоносным рекламным содержимым, что ещё больше усложняет процесс защиты.

Разумной и недорогой ответной мерой для борьбы с распространением критоплокеров через рекламные баннеры на сайтах становятся средства блокировки рекламы или блокировки скриптов в веб-страницах. Они приобретают особую актуальность в связи с появлением разнообразных видов атак, при которых заражение системы и загрузка вредоносно-

Рис. 3.3.15. *Использование Adobe Flash различными семействами криптолокеров.*

Уязвимости	Nuclear	Magnitude	Angler	Neutrino	RIG
Flash CVE-2015-7645	✓	✓	✓	✓	✓
CVE-2015-8446			✓		
CVE-2015-8651	✓		✓	✓	
CVE-2016-1019	✓	✓			
CVE-2016-1001			✓		
CVE-2016-4117	✓	✓	✓		
Silverlight CVE-2016-0034			✓		✓

Рис. 3.3.16. *Схема действия вредоносной рекламы, через которую происходит заражение программами-вымогателями.*



го ПО происходят без прямого участия пользователя. Однако, некоторые крупные поставщики онлайн-контента требуют от своих посетителей отключить подобную блокировку, поскольку значительная часть прибыли этих компаний непосредственно связана с Интернет-рекламой. И пользователи, как и специалисты по безопасности, стоят перед дилеммой — отключить рекламу при доступе к тем или иным сайтам или блокировать эти сайты, если они отказываются отображать информацию пользователю, использующему блокировщик.

Кстати, ***почему пользователи платят выкуп***? Всё очень просто. Злоумышленники, которые распространяют программы-вымогатели, проводят свои собственные маркетинговые исследования, чтобы определить идеальную цену для выбранной целевой аудитории (в разных странах эти суммы обычно разные). Взятая на вооружение идея состоит в том, что требуемая сумма не должна быть неподъёмной для жертвы и уж тем более не должна побудить пользователя обратиться к органам правопорядка. В итоге, требуемый выкуп больше похож на раздражающий платёж. Пользователи платят. На Западе средняя сумма выкупа составляет 300-500 долларов. У нас это значение доходит до 5-10 тысяч рублей, что сопоставимо со стоимостью расшифровки данных, в которую оценивают свои работы некоторые антивирусные компании. Недавно было обнаружено несколько кампаний, разработанных и запущенных с целью заражения определённых групп пользователей, в частности, любителей онлайн-игр. Некоторые разработчики вымогательского ПО также создали варианты криптолокеров на таких необычных языках, как исландский, чтобы убедиться, что пользователи в регионах, где преимущественно используется тот или иной язык, не игнорировали сообщение программы-вымогателя. Всё направлено на то, чтобы повысить эффективность работы программ-вымогателей и получать баснословные доходы (до нескольких десятков миллионов долларов на одно семейство вымогательского ПО).

А почему же тогда злоумышленников никто не ловит, если известно, кому надо заплатить выкуп? Почти все транзакции, связанные с программами-вымогателями,

выполняются через анонимную сеть Tor. Осуществляя платежи, злоумышленники полагаются на криптовалюту биткойн, что позволяет сохранить анонимность пользователей, и поэтому органам правопорядка труднее отслеживать транзакции. Биткойн допускает разделение на дробные части, поэтому даже один биткойн можно распределить между всеми участниками атаки, т.е. расплатиться со всеми сторонами удобным и абсолютно анонимным способом. А чтобы поддерживать хорошую репутацию на рынке, которая заключается в возможности выполнить своё обещание предоставить доступ к зашифрованным файлам после оплаты, многие операторы программ-вымогателей организовали работу офиса поддержки заказчиков, по сути копируя деятельность рынка ПО, но со знаком минус.

На что ещё можно обратить внимание, анализируя последние семейства вымогательского ПО? К инновациям, которые быстро становятся нормой, можно отнести:

- Маркировку уже зашифрованных систем (чтобы не тратить усилия на уже занятый плацдарм).
- Индивидуальное шифрование для каждой цели с возможностью выбора каталогов и типов файлов.
- Устойчивость управления и контроля, в т.ч. полное отсутствие инфраструктуры контроля и управления, не позволяющее обнаружить и перехватить управление вредоносной кампанией.
- Использование уже заражённых компьютеров. Некоторые авторы вредоносного ПО, понимая, что в той или иной системе может присутствовать и другая «инфекция», пытаются использовать её для распространения собственного вредоносного ПО.
- Самораспространение. Самораспространяющееся вредоносное ПО — далеко не новая технология. По этому же принципу создаются «черви» и бот-сети, которые существуют уже не одно десятилетие. Однако, в криптолокерах она пока не применялась, и только сейчас к ней начинают присматриваться владельцы теневого рынка.
- Анализируя инновации в области программ-вымогателей, можно заключить, что авторы новой волны вымогательского ПО склонны применять модульную архитектуру, которая встречается во многих известных пакетах с открытым исходным кодом, предназначенных для проверки защищённости систем. Такой подход даёт возможность наделить «продукт» нужным набором функций. Это увеличивает эффективность и позволяет менять тактику в случае, если тот или иной вид активности был обнаружен или не приносит результатов.
- Репликация на все доступные накопители и распространение через файлы автозапуска и USB-накопители большой ёмкости.

Ещё одной интересной и пугающей тенденцией стало применение в вымогательском ПО протокола DNS, без которого невозможен современный Интернет и который обычно разрешён на всех периметровых средствах защиты (Табл. 3.3.7). Проведённый анализ вредоносного ПО показал, что 91,3% вредоносного ПО использует службу доменных имён (DNS) одним из трёх следующих способов:

- перехват управления системой;
- извлечение и утечка данных;
- перенаправление трафика.

При этом, DNS —является слепым пятном для многих специалистов по ИТ и информационной безопасности — его мониторят всего 32% компаний.

Мы плавно подошли к вопросу о том, как бороться с программами-вымогателями. Увы,

Табл. 3.3.7. *Использование протокола DNS в разных семействах шифровальщиков.*

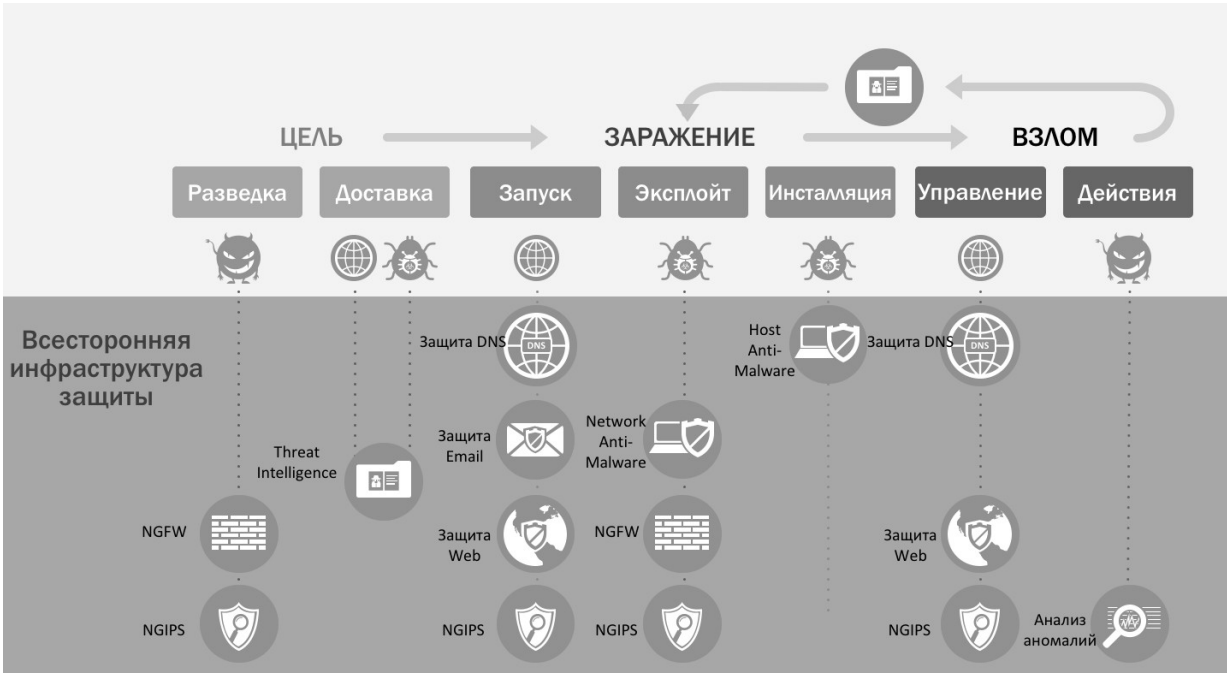
Имя программы-вымогателя	Использование DNS	Использование IP	Отсутствие серверов управления C&C	Применение TOR	Канал оплаты
Locky	Да	Да			DNS
SamSam			Да		DNS (TOR)
TeslaCrypt	Да				DNS
CryptoWall	Да				DNS
TorrentLocker	Да				DNS
PadCrypt	Да				DNS (TOR)
CTB-Locker	Да			Да	DNS
FAKBEN	Да				DNS (TOR)
PayCrypt	Да				DNS
KeyRanger	Да			Да	DNS

одного продукта или решения в этой области не существует. Как показывает данный кейс, злоумышленники очень заинтересованы в том, чтобы и дальше продолжать «стричь купоны» с этой очень доходной категории вредоносного ПО, поэтому они будут продолжать и дальше активно вкладываться в развитие своего детища. Создатели и распространители программ-вымогателей нанимают и финансируют целые группы профессиональных разработчиков для поддержания прибыльности своего преступного бизнеса. Они находят и применяют все новые методы, например, такие, как обнаружение «песочниц», чтобы скрыть своё присутствие в сетях и компьютерах своих жертв. Постоянная модификация и работа на опережение приводит нас к мысли, что для нейтрализации этой угрозы требуется комплексный подход, учитывающий различные этапы жизненного цикла программы-вымогателя и различные вектора их проникновения.

Обратите внимание, на Рис. 3.3.17 мы видим, что бороться с вымогательским ПО нам помогают не только и не столько антивирусы, которые обычно имеют дело с уже попавшим на компьютером вымогателем, да ещё и успевшим заразить жертву. Да-да, антивирусы далеко не всегда сразу обнаруживают и предотвращают заражение, часто просто не видя специально разработанное для обхода антивируса вредоносное ПО. Мы должны сначала выстроить «стену» вокруг пользовательских компьютеров с применением традиционных, но по-прежнему эффективных средств обнаружения и предотвращения угроз, а также межсетевых экранов и защитных Интернет-шлюзов, блокирующих доступ к известным вредоносным сайтам.

Мы не должны забывать про мониторинг всех каналов, которые используют программы-вымогатели для своего проникновения в жертву, подгрузки новых модулей и организации оплаты выкупа. Это e-mail, DNS, HTTP, HTTPS, Tor. Ни в коем случае не стоит упускать из виду мониторинг Netflow (или IPFIX, sFlow, jFlow и т.п.), который присутствует на сетевом оборудовании, и по анализу которого можно составить представление об аномалиях в сети, в т.ч. и о действии вымогательского ПО, которое обошло все остальные защитные преграды. И только потом вступают в игру антивирусы и иные средства защиты, устанавливаемые на персональных компью-

Рис. 3.3.17. *Набор технологий для борьбы с современными программами-вымогателями.*



терах. Они нужны тогда, когда все остальные технологии защиты не справились со своей задачей и пропустили криптолокер, достигший своей жертвы. Правда, на классические антивирусы в этом случае полагаться не стоит — пора присматриваться к решениям класса EDR (Endpoint Detection & Response), которые в своей работе применяют сразу несколько равноправных технологий, включая динамический анализ (песочница), анализ потоков, анализ поведения и т.п.

Но... даже в случае успешного заражения не стоит опускать руки. Вспомните о такой простой, но эффективной мере борьбы с зашифрованными файлами, как резервное копирование. Если у вас есть бэкап ваших данных, так ли важно, успешно сработал криптолокер или нет? Вы можете легко вернуть систему в предатакованное состояние, восстановив данные из резервной копии (главное, чтобы они там тоже не были в зашифрованном виде). Важно извлечь уроки из заражения и не дать злоумышленникам повторить свой путь внутри вашей сети.

Понятно, что такой набор защитных технологий — это недешёвое удовольствие, и не каждая компания готова сразу потратить немалую часть своего ИТ/ИБ-бюджета на борьбу с этой важной, но не единственной угрозой. С другой стороны, вы же защищаетесь не в чистом поле, и какие-то средства защиты у вас уже есть, в т.ч. и встроенные в сетевое оборудование, сервера, системное и прикладное ПО. Но если бы нас спросили: назовите две технологии, которые должны быть реализованы для наибольшей эффективности в борьбе с программами-вымогателями, мы бы ответили — защите e-mail и мониторинг DNS. Они позволят нейтрализовать до 90-95% всех проблем с криптолокерами в настоящее время.

Можно предположить, что программы-вымогатели следующего поколения будут ещё более устойчивыми к анализу и методам противодействия им; при этом также возрастёт эффективность тактик проникновения

криптолокеров в системы своих жертв. Поэтому для организаций и пользователей важно уже сейчас подготовиться к очередному витку гонки вооружений, в т.ч. и создав резервные копии критически важных данных. Без этого битва с вымогательским ПО, приносящим своим владельцам миллиарды, будет все время проигрываться.

Кейс: безопасность маршрутизаторов

Маршрутизаторы контролируют доступ из любой сети к любой сети. Они «рекламируют» сети и определяют тех, кто может получать к ним доступ. Поэтому потенциально маршрутизатор — это «лучший друг хакера». Безопасность маршрутизаторов является критически важным элементом любой системы сетевой безопасности, которым так часто пренебрегают. Основной функцией маршрутизаторов является предоставление доступа, и поэтому маршрутизаторы нужно обязательно защищать, чтобы исключить возможность прямого взлома. Но делаете ли вы это?

В последнее время достоянием гласности становится очень много историй о заражении маршрутизаторов с последующим перехватом и перенаправлением (по сути кражей) интересующего злоумышленников трафика. Как это происходит? Можно выделить четыре основных сценария захвата управления над устройством (в порядке распространённости):

- ***Удалённый доступ***. Многие администраторы забывают (или оставляют «на потом») поменять заданные по умолчанию пароли, отключить доступ извне к интерфейсам управления, заблокировать внешний доступ к маршрутизатору через SNMP, Telnet, SSH.
- ***Использование уязвимостей***. По статистике компании Cisco, среднее время неустранения уязвимостей в сетевом оборудовании составляет... около 5 лет. Это происходит из-за классического «айтишного» принципа «работает — не трогай» и сложностей, которые возникают при обновлении ПО сетевого оборудования, у которого часто нет резервной замены, и останов которого может привести к нарушению тех или иных процессов предприятия. Поэтому уязвимости сетевого оборудования не устраняются годами, чем и пользуются злоумышленники.
- ***Заражённые прошивки***. Снятие оборудования с поддержки и отказ его заменять на новые модели, нежелание оплачивать сервисные контракты, включающие обновление прошивок сетевого оборудования, новый функционал, который официально ещё не поддерживается производителем — вот три основных причины, по которым ИТ-специалисты скачивают прошивки для своего сетевого оборудования с недоверенных Интернет-сайтов, которые часто «заражены» незапланированной и, зачастую, вредоносной функциональностью.
- ***Включение в цепочку поставок***. Это достаточно редкая, но, всё-таки, уже встречавшаяся причина, которая приводила к тому, что злоумышленники не взламывали сетевое оборудование своей жертвы через Интернет одним из трёх вышеупомянутых способов, а действовали гораздо хитрее. Они включались в процедуру закупки маршрутизаторов и, предложив самую низкую цену, выигрывали тендеры и поставляли заказчикам изначально заражённые сетевые устройства. Выступая в качестве «доверенных поставщиков», злоумышленники получали контроль над всей инфраструктурой организации.

Что можно противопоставить этой нарождающейся угрозе, которая раньше была присуща только спецслужбам иностранных государств, а сейчас начинает перениматься и обычными киберпреступниками?

Ниже перечислены ключевые области, которые должны рассматриваться при обеспечении безопасности сетевого оборудования:

- Доступ к устройствам, формирующим инфраструктуру.
- Инфраструктура маршрутизации.
- Устойчивость и безотказная работа устройств.
- Сетевая телеметрия.
- Обеспечение соблюдения сетевой политики.

Устройства, формирующие сетевую инфраструктуру, нередко поддерживают большое количество различных механизмов доступа, включая консольные и асинхронные соединения, а также возможности удалённого доступа с использованием протоколов Telnet, rlogin, HTTP и SSH. Некоторые механизмы обычно включены по умолчанию, при этом нередко с ними связаны минимальные меры обеспечения безопасности. Например, платформы на основе программного обеспечения Cisco IOS поставляются с включенными по умолчанию консольным и модемным доступом. По этой причине каждое устройство, формирующее сетевую инфраструктуру, должно быть тщательно проверено и настроено, чтобы обеспечить включение только поддерживаемых механизмов доступа и их надлежащую защиту.

Для обеспечения защиты интерактивного доступа и доступа с целью управления к устройствам, формирующим инфраструктуру, должны применяться следующие основные меры:

- ***Ограничение доступа к устройству***. Ограничение доступных портов, ограничение адресов, с которых разрешено подключение, и разрешённых методов доступа.
- ***Отображение юридического уведомления***. Отображение юридического уведомления, разработанного совместно с юридической службой компании, в начале интерактивного сеанса работы с устройством.
- ***Аутентификация доступа***. Предоставление доступа только пользователям, группам и сервисам, прошедшим процедуру аутентификации.
- ***Ограничение возможностей***. Ограничение действий и представлений только теми, которые разрешены для конкретных пользователей, групп и сервисов.
- ***Обеспечение конфиденциальности данных***. Защита важных данных, хранимых на локальных носителях, от просмотра и копирования. Анализ уязвимости данных, передаваемых по коммуникационным каналам, по отношению к методам перехвата пакетов, взлома сеансов и атакам типа «человек посередине» (MITM).
- ***Регистрация и учёт для всех видов доступа***. Регистрация лиц, осуществляющих доступ к устройству, выполняемых операций и времени их выполнения, в целях аудита.

Система маршрутизации является одной из наиболее значимых составляющих инфраструктуры, которая поддерживает работоспособность сети, и поэтому критически важно принять необходимые меры для её защиты. Существуют различные способы нарушения безопасности системы маршрутизации: от внедрения нелегитимных обновлений маршрутной информации — до DoS-атак, целенаправленно проводимых для нарушения маршрутизации. Атаки могут быть направлены непосредственно на маршрутизаторы, на сеансы обмена маршрутной информацией и (или) на саму маршрутную информацию. Для эффективной защиты уровня маршрутизации в архитектуре безопасности должны использоваться следующие меры:

- ***Ограничение круга систем, использую-***

щих протоколы маршрутизации. Ограничение сеансов маршрутизации только доверенными узлами, проверка происхождения и целостности обновлений маршрутной информации.

- ***Контроль распространения маршрутной информации***. Применение фильтров маршрутизации, чтобы гарантировать распространение только достоверной маршрутной информации. Контроль обмена маршрутной информацией между узлами маршрутизации и между процессами её перераспределения.
- ***Регистрация изменений состояния***. Регистрация изменений состояния сеансов со смежными или соседними узлами.

Маршрутизаторы и коммутаторы могут подвергаться атакам, которые проводятся для снижения доступности сети либо косвенно сказываются на ней. Среди возможных атак — DoS-атаки с использованием неразрешённых и разрешённых протоколов, распределённые DoS-атаки, атаки «шторма» пакетов (flood-атаки), разведка, несанкционированный доступ и другие виды атак.

Для обеспечения устойчивости и безотказной работы маршрутизаторов и коммутаторов в проектах дизайна должны быть предусмотрены следующие практические меры:

- ***Отключение неиспользуемых сервисов***. Отключение сервисов, включённых по умолчанию, которые не требуются для работы.
- ***Ограничение доступа адресным пространством инфраструктуры сети***. Развёртывание списков ACL на периметре сети для защиты инфраструктуры от несанкционированного доступа, DoS-атак и других видов сетевых атак.
- ***Защита уровня управления***. Фильтрация и ограничение трафика, направленного на уровень управления маршрутизаторов и коммутаторов.
- ***Контроль использования памяти коммутаторов, адресуемой по содержимому***. Ограничение списка MAC-адресов, имеющих право отправлять трафик на определённый порт.
- ***Резервирование***. Исключение единственных точек отказа путём резервирования интерфейсов, развёртывания резервных устройств в режиме ожидания и топологической избыточности.

Для успешной эксплуатации и поддержания бесперебойной работы сети важно обеспечить контроль процессов, происходящих в сети, и возможность управлять функционированием сети в любой момент времени. Средства сетевой телеметрии предоставляют развитые и удобные функции обнаружения событий, которые могут использоваться в сочетании со специализированными системами анализа для сбора данных и выявления аномалий регистрируемых событий, в том числе и несанкционированной утечки данных или внешнего управления. В рамках реализации процессов контроля сетевой телеметрии необходимо реализовать следующие защитные меры:

- ***Синхронизация времени***. Внедрение протокола NTP (Network Time Protocol), обеспечивающего синхронизацию отметок даты и времени в журналах регистрации и оповещениях.
- ***Ведение статистики локального трафика устройства***. Использование статистических сведений об общем трафике устройства и трафике для отдельных интерфейсов.
- ***Сбор информации о состоянии системы***. Использование информации о состоянии памяти, ЦП и процессов.
- ***Системный журнал***. Сбор и регистрация информации о состоянии системы, статистике трафика и доступе к устройству.

- ***Регистрация и учёт для всех видов доступа***. Регистрация лиц, осуществляющих доступ к устройству, происходящих событий и времени их выполнения для целей аудита.
- ***Сбор пакетов***. Создание механизмов, позволяющих собирать передаваемые через устройство пакеты, для анализа и статистики.

Обеспечение выполнения основных сетевых политик касается, главным образом, трафика, поступающего в сеть. Этот трафик должен соответствовать сетевой политике, включая диапазон IP-адресов и типы трафика. Аномальные пакеты должны отбрасываться как можно ближе к периметру сети, что позволяет снизить риск их нежелательного воздействия до минимума. В проектах дизайна сетевой инфраструктуры должны быть предусмотрены следующие меры:

- ***Фильтрация на периметре сети***. Обработка трафика, адресованного в пространство инфраструктуры.
- ***Защита от подмены IP-адресов отправителей***. Внедрение фильтрации пакетов и других динамических механизмов для блокирования пакетов с подменёнными IP-адресами отправителей.

Шаг №4. Управление рисками

Четвёртый шаг на пути к понимаю ИБ — это управление рисками. Через этот этап проходят почти все, и почти всегда он заканчивается неудачей. Ведь что такое риск в области информационной безопасности? Это некоторая функция, вычисляемая на основе двух ключевых параметров — вероятности осуществления угрозы и стоимости нанесения ущерба в результате данной угрозы. В ряде источников вместо стоимости ущерба используется стоимость защищаемых информационных активов. Идея оценки рисков в области ИБ достаточно здравая, т.к. позволяет приоритизировать не только риски, грозящие компании, но и меры управления этими рисками, а также оценивать их в понятных бизнесу финансах. Но красивая идея столкнулась с тем, что на практике её очень сложно реализовать. По крайней мере, на сегодняшнем этапе. Почему?

Начнём с вероятности осуществления угрозы? Как её определить? Существует два основных метода:

- сделать вывод на основе собранных своими руками данных;
- воспользоваться собранной кем-то статистикой.

Чтобы заработал первый метод, необходимо потратить не менее двух-трёх лет на составление более-менее репрезентативной выборки. Но и тут не всё просто. Любой математик скажет, что даже такой срок для таких данных не может говорить о репрезентативности. Например, заказчики пока не часто сталкиваются с DDoS-атаками, но это не значит, что мы не должны задумываться о мерах по их отражению. Но дело даже не в этом. Собирать статистику два-три года можно, но зачем? Обычно, эта информация собирается как раз для того, чтобы обосновать выделение денег на средства защиты, которые и собирают эту статистику. Заколдованный круг. Чтобы получить деньги, нам нужны средства защиты, на покупку которых мы эти деньги и просим. И это не говоря про то, что ждать 2-3 года до момента, когда собранная статистика начнёт «работать», мало кто будет.

Второй метод тоже не работоспособен, т.к., во-первых, такой статистики нет, а во-вторых, даже если она появится, то будет отражать «среднюю температуру по больнице». Одними из наиболее часто упоминаемых в среде специалистов статистических дан-

ных является отчёт компании Verizon (отчёт Data Breach Investigations Report компании Verizon в 2013 году включал в себя анализ более 47 тыс. известных инцидентов в области безопасности и 621 подтверждённых случаев утечек данных, содержит в себе очень интересную статистику и показывает тренды, связанные с кибер-безопасностью), который стал неким стандартом де-факто, на который опираются многие производители и интеграторы, запугивая потенциальных клиентов огромными убытками от компьютерных угроз. Однако, при глубоком рассмотрении этого отчёта ситуация становится не такой радужной. Во-первых, этот стандарт ориентирован на опрос только крупных американских корпораций, что, согласитесь, является пусть и интересной, но явно нерепрезентативной выборкой. Да, можно признать, что проблемы американских корпораций могут встречаться и у европейских, и у российских компаний, но... знак равенства всё-таки ставить не совсем корректно. Во-вторых, ориентация на крупный бизнес выводит из под действия данного отчёта операторов связи, малый и средний бизнес, что, конечно, является очень большим упущением авторов отчёта. В-третьих, отчёт не учитывает вертикальной специфики. И если в хорошо компьютеризированной Америке это обоснованно, то, например, в России, где уровень информатизации разных отраслей может различаться на порядки, это уже неправильно. К чему мы приходим?.. Такие отчёты показывают нам «среднюю температуру по больнице», которую нельзя использовать в реальной работе и опираться на эту статистику для прогнозирования ситуации с информационной безопасностью в конкретной компании или организации.

Можно долго ругать американскую статистику, но, к сожалению, надо признать, что другой у нас нет. В России за все годы её информатизации так и не появилось сколь-нибудь значимой и авторитетной статистики. Называть таковой данные о компьютерных преступлениях МВД неправильно по двум причинам. Первая из них аккумулирует всеё, что было сказано выше про отчёт Verizon (отсутствие вертикализации, учёта разных масштабов бизнеса и др.). А вторая заключается в том, что МВД считает не угрозы и не атаки, а «дела», доведённые до суда и, более того, дела по которым преступник был наказан (какой смысл рапортовать о «висяках» и делах, в которых вина задержанного не была доказана). В России пока не стоит ждать появления в обозримом будущем адекватной статистики по компьютерной безопасности, хотя некоторые компании пытаются делать срезы по тем или иным вопросам (хищения у банков и их клиентов, утечки информации и т.п.).

Есть и ряд других методов (сопоставление с аналогичными рисками, использование дерева событий или дерева неисправностей, имитационное моделирование, бинарный метод), но все они либо требуют существенных усилий по измерению, либо отсутствующих исходных данных, либо ограничены очень узким применением. Конечно, у нас остаётся ещё экспертный метод, но это все равно что «пальцем в небо». Способы повышения качества экспертной оценки, хотя бы через простой метод Дельфи, почти не применяются.

Теперь переходим к стоимости информации или ущерба. Кто умеет их считать? Никто. Даже сам заказчик не в состоянии оценить ни стоимость информации, ни стоимость информационных активов, ни стоимость ущерба.

К чему мы пришли? Мы не можем сегодня ***адекватно*** оценивать риски информационной безопасности (чтобы методика оценки давала воспроизводимые результаты на другой группе экспертов). Поэтому не случайно некоторые специалисты на Западе стали говорить о том, что раз мы не можем оцени-

вать риски, то стоит от них отказаться, чтобы не вводить в заблуждение заказчиков. Это не значит, что оценка рисков в ИБ не работает. Просто у неё есть своя область применения и свои ограничения. Например, использовать экспертную оценку для приоритизации своих работ по ИБ вполне логично. Но ждать слишком многого от неё не стоит. И уж не стоит надеяться, что на основе этой экспертной оценки бизнес начнёт выделять финансовые средства на приобретение тех или иных программных и программно-аппаратных средств.

Как было сказано в одной статье больше десяти лет назад: «Анализ рисков, оценка их вероятности и тяжести последствий похожа на посещение игроками Лас-Вегаса — зал общий, а система игры у каждого своя». Оценка рисков как была больше искусством, чем наукой, так и осталась. Если не сказать больше. Оценка рисков ИБ сегодня — это шаманство. Резюме было подведено давно, в международном стандарте ISO 13335, в котором было сказано, что лучшая методика оценки рисков та, которая устраивает все стороны — и того, кто считает риски, и того, кому их демонстрируют. А уж какая она, совсем неважно. Тем более, что рынок сегодня предлагает несколько десятков таких методик — FAIR, ISO, MAGERIT, MEHARI, OCTAVE, ISF IRAM и т.д.

Шаг №5. Бизнес-ориентация

Как-то одиозный глава «Евросети», господин Чичваркин, так высказался об общении со своим ИТ-департаментом: *«С айтишниками я не мог вообще никогда вести переговоры. Мне казалось, что я говорю на русском, а они — на козьем. Надо иметь человека в компании, который переводит с козьего, а нам с этим не везло абсолютно. А переводчика с их стороны практически никогда не бывало»*. Ровно то же, и даже хуже, обычно происходит при общении сотрудников отдела защиты информации (информационной безопасности) со своим руководством. Оно ещё меньше понимает, что делает подразделение, которое вводит множество препон на пути бизнеса, борется с мифическими угрозами и заставляет выполнять «дурацкие законы». Объясняют свои нужды безопасники достаточно банально: «Если мы этого не сделаем, нас взломают» или «Если мы этого не сделаем, нас накажут регуляторы». Но стоит задать встречный вопрос: «И что?» и дискуссия затухает.

Не так часто безопасник может на понятном бизнесу языке объяснить, к чему приведёт та или иная проблема. Например, если вспомнить уязвимость Heartbleed в OpenSSL, то на вопрос: «И в чём её опасность?», часто приходилось видеть обычный copy-past из Википедии:

> ***Heartbleed*** *— ошибка переполнения буфера в криптографическом программном обеспечении OpenSSL, позволяющая несанкционированно читать память на сервере или на клиенте, в том числе для извлечения закрытого ключа сервера.*

На логичный вопрос: *«И что?»* следует обычно недоуменный взгляд, который как бы говорит: *«Ну ты что, совсем ничего не понимаешь? Это же очевидные вещи!»*. Куда как сложнее ответить более понятно для несведущего в информационной безопасности человека: *«Уязвимость Heartbleed была обнаружена в понедельник ночью, и она может иметь негативное воздействие на наши Web-сервера. Эта ошибка позволяет украсть такие приватные данные как имена пользователей, пароли, номера кредитных карт и т.п. Наша команда по безопасности немедленно начала сканировать нашу сеть для оценки потенциального воздействия на неё. В настоящий момент нет*

Рис. 3.3.18. *Три вопроса для понимания связи ИБ и бизнеса.*

никаких признаков того, что нам угрожает этот риск или мы были скомпрометированы ранее».

Бизнес не оперирует понятиями ИТ или информационной безопасности. Бизнес оценивает выгоды и потери от своей деятельности, включая и деятельность по информационной безопасности. Его не интересует жаргонизм и сложные, малопонятные термины, которыми так любят бросаться специалисты по высоким технологиям. Если говорить об инцидентах, то руководство интересует, как инцидент относится к его компании, что произошло, каков ущерб и что было предпринято для устранения последствий и отсутствия повторов в будущем? Если говорить о новых ИБ-проектах, то руководство интересует, как проект относится к его компании, что он даёт, и как этого достичь/получить? И поскольку сам бизнес не будет вникать в то, что делает ИБ, шаг навстречу должны сделать именно те, кто отвечает за ИБ, пытаясь понять, чем они могут помочь своему работодателю. Для этого надо ответить на три вопроса (Рис. 3.3.18), из которых важным является именно первый. Он позволяет затем посмотреть на безопасность с точки зрения именно бизнеса, а не торговли страхом (т.е. борьбы с угрозами) или compliance.

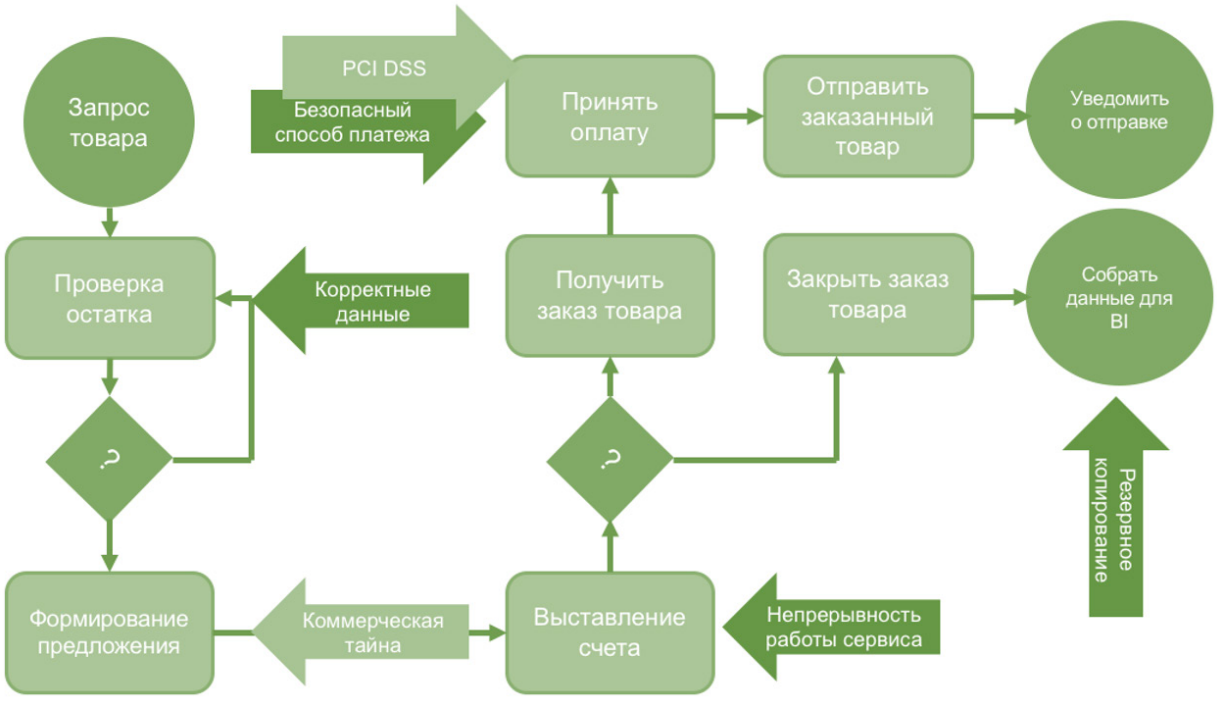
Чем занимается бизнес? Куда он стремится? Какие задачи перед собой ставит? Есть ли в них место информационной безопасности? Дабы не быть голословным и больше не растекаться мыслью по древу давайте посмотрим на три примера, в которых информационная безопасность играет роль, но непривычную, несвязанную с нейтрализацией угроз или выполнением требований какого-либо нормативного акта.

Кейс: заказ товара в Интернет-магазине

Итак, возьмём процесс заказа любого товара в Интернет-магазине (Рис. 3.3.19). На этапе запроса товара перед нами стоит задача обеспечить бесперебойное функционирование системы регистрации заявок и уменьшение времени регистрации. Что может помешать этому? Среди прочего — DDoS-атаки, отсутствие проверки ввода в поля формы заявки на заказ товара, что может привести к утечке номеров кредитных карт или паролей пользователей, а также к заказу товара без реальной оплаты. И бороться с ними нам помогают различные защитные технологии. Обратите внимание — мы «продаём» не средство борьбы от DDoS, а говорим о средстве обеспечения бесперебойного функционирования процесса приёма заявок, так как в противном случае мы эти заявки начинает терять (или обрабатывать меньшее их число), что прямым образом влияет на доходы предприятия. Т.е., вроде и говорим о том же, но позиционируем совершенно по-иному: с точки зрения, понятной бизнесу.

На этапе проверки остатков на складе наша задача — предоставить системе корректные данные. Если данные будут меньше реаль-

Рис. 3.3.19. *Процесс заказа в Интернет-магазине.*



ных, то мы теряем деньги, а если больше, то снижается лояльность клиентов, которых придётся уведомлять о том, что заказанный (и, возможно, уже оплаченный) товар отсутствует. С формированием предложения случай иной. Мы не должны раскрывать детали предложения никому, кроме клиента. Не редки ситуации, когда разные клиенты имеют разные условия обслуживания, разные скидки. Никто не хочет, чтобы об этом узнали другие клиенты. Опять начнётся снижение лояльности, недовольство, уход к конкурентам. И безопасность тут как нельзя кстати; и вновь она нам помогает не бороться с угрозами или выполнять какие-либо законы, а решает вполне конкретную и понятную бизнесу задачу.

Идём дальше. Выставление счёта должно быть не только бесперебойным, в счёте обязательно должны быть указаны правильные реквизиты и сумма, чтобы клиент заплатил ровно столько, сколько нужно, и туда, куда нужно. Никакой подмены реквизитов быть не должно. И вновь решить это можно с помощью технологий ИБ. Наконец, оплата товара должны быть безопасной. И дело не в только требованиях стандарта PCI DSS, но и в том, что клиенты не хотят, чтобы информация об их покупках или их кредитных картах стала достоянием гласности.

А почему нельзя торговать страхом, то есть продвигать борьбу с угрозами? Ведь об угрозах ИБ сегодня слышали все. Утечки, DDoS, программы-вымогатели, APT... Знакомые многим понятия. Что же с ними не так? Почему они плохо «продаются» сегодня? Причин тому две. В непростую экономическую ситуацию перед бизнесом встают в полный рост совершенно иные проблемы, имеющие больший приоритет. Речь идёт о росте кредитных ставок, банкротстве контрагентов, сокращении персонала, изменении курса валюты, кассовом разрыве и других более важных угрозах. Вторая причина связана с тем, что,

приводя статистику об угрозах, мы забываем указать, как она относится к вашей компании и не является ли она «средней температурой по больнице». А если статистика релевантна, то бизнес хочет знать масштаб ущерба от этих угроз, а не просто их перечисление. А считаем ли мы ущерб?

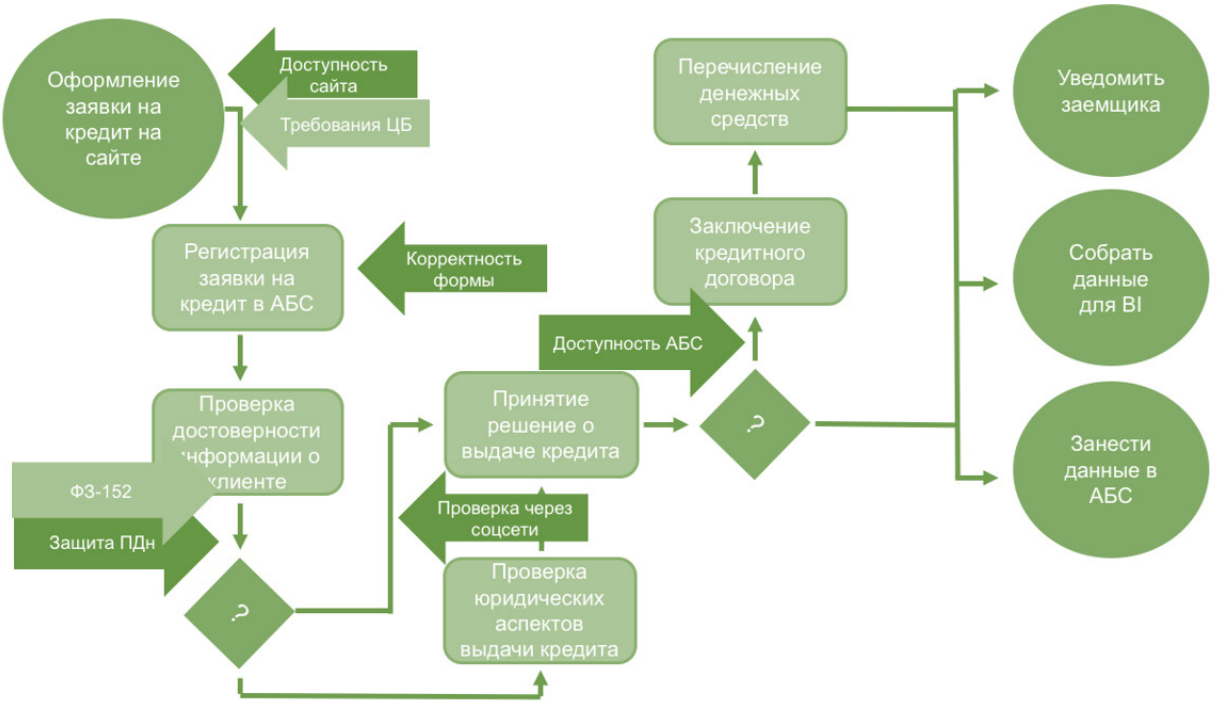
Кейс: оформление заявки на кредит

Рассмотрим второй пример. Оформление заявки на кредит на банковском сайте (Рис. 3.3.20). Обычно, этот процесс интересен безопасникам только в контексте обработки персональных данных в анкете заёмщика, т.е. мы рассматриваем его с точки зрения выполнения требований законодательства (compliance). Но давайте отвлечёмся и посмотрим, как ещё кибербезопасность может помочь в этом деле? Первый шаг совпадает с предыдущим кейсом — регистрация заявки, и мы хотим обеспечить бесперебойность процесса регистрация заявок заёмщиков на получение кредита. В противном случае мы начинаем терять клиентов и их деньги.

Одним из показателей эффективности этапа проверки достоверности информации о заёмщике может служить скорость проверки. Может ли безопасность увеличить этот показатель? Почему бы и нет, если использовать технологии анализа социальных сетей и применять методики OSINT (Open Source INTelligence — разведка по открытым источникам). Они позволяют нам быстро вычислить мошенников или неплательщиков, либо существенно сократить их число, дошедшее до этапа получения денег у банка. Вновь мы видим, что безопасность нам помогает не традиционным путём (нейтрализовывать угрозы или выполнять нормативные требования), а с учётом стоящих перед бизнесом задач — ускорение обработки заявок на выдачу кредитов и снижение числа невозвратных кредитов, выданных мошенникам.

А почему compliance малоинтересен бизнесу? Ведь во всех умных книжках говорится,

Рис. 3.3.20. *Процесс оформления заявки на банковский кредит.*

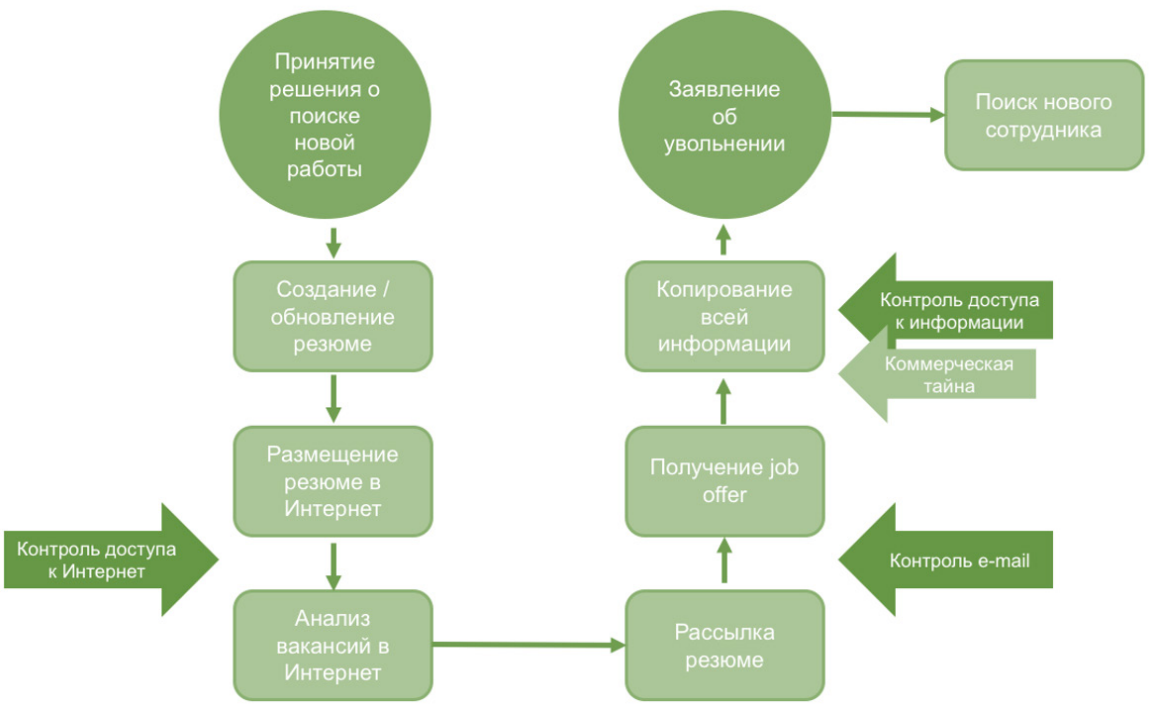


что именно compliance — это епархия генерального директора (или председателя правления). Всё просто. Compliance compliance'у рознь. Одно дело говорить о выполнении требований налогового законодательства и совсем другое — о некоем 21-м приказе ФСТЭК по защите персональных данных. Ведь что мешает бизнесу задать два простых вопроса на требование выделить средства для выполнения того или иного нормативно-правового акта: какова средняя сумма штрафа за невыполнение НПА и сколько наказаний уже было приведено в исполнение (в стране, в регионе, в отрасли)? И окажется, что с точки зрения кибербезопасности, оба этих показателя выглядят смешно, а точнее, практически равны нулю. Да, следуя старой советской поговорке, строгость наших законов компенсируется необязательностью их исполнения. Даже максимальные штрафы по статьям, связанным с невыполнением мер по защите информации, не превышают пары десятков тысяч рублей, а уж про число успешно выигранных по данным статьям дел и вовсе можно пересчитать по пальцам одной руки. В итоге, много болтовни, и полный пшик на практике. Зачем же бизнесу платить за то, за что не наказывают или размер наказания на порядки меньше суммы затрат?

Кейс: снижение ротации кадров

Но обратимся к третьему кейсу. Увольнение сотрудника (Рис. 3.3.21). Как тут может помочь безопасность и может ли? На удивление да. И это, пожалуй, тот хороший пример, который показывает роль ИБ в ситуациях, когда нет ни угроз, ни требований законодательства. Однако увольнение — это всегда проблема для бизнеса. Уволившийся человек не приносит денег, а простаивающая вакансия — это ухудшение KPI для службы управления персоналом. Вот именно о помощи HR мы сейчас и поговорим. Одной из задач хорошего HR является уменьшение времени простаивания вакансий в компании с традиционных для России 2-3 месяцев до нуля. Правда, это только там, где задача HR — удер-

Рис. 3.3.21. *Процесс поиска работы.*



живать персонал (а именно этим должен заниматься HR в компании), а не заниматься только увольнениями и наймом сотрудников. Так вот, в нормальных компаниях HR хочет иметь информацию о том, кто из сотрудников «навострил лыжи» и планирует покинуть «отчий дом». И кто может ему дать такую информацию? Только служба ИБ, которая может с лёгкостью её получить. Ведь нередко люди ищут себе работу не только из дома, и не только с личных мобильных устройств, но и на работе. Они ходят по рекрутинговым сайтам, размещают резюме, читают вакансии. А ещё они рассылают резюме по электронной почте и, реже, получают предложения о новой работе (job offer). И всё это элементарно отслеживается с помощью систем анализа Интернет и e-mail трафика, которые помимо ловли спама и утечек данных, могут и иной контент в информационных потоках выуживать. А с помощью Netflow (сетевой протокол, предназначенный для учёта сетевого трафика, разработанный компанией Cisco Systems; является фактическим промышленным стандартом и поддерживается не только оборудованием Cisco, но и многими другими устройствами) можно увидеть выкачку больших объёмов данных с внутренних серверов предприятия, что часто является признаком готовящегося увольнения, когда сотрудник готов унести все ценное, до чего сможет дотянуться со своего компьютера.

Получив данные сведения, HR может провести воспитательную беседу с готовящимся к увольнению работником и уговорить его остаться или, поняв тщетность своих бесед, начать заранее искать замену. В идеале к моменту подачи заявления об увольнении служба персонала уже находит кандидата на замещение вакантной должности, который выходит в день увольнения своего предшественника или даже заранее, чтобы иметь возможность передать дела. И вновь безопасность смогла учесть интересы бизнеса и улучшить его отдельные показатели.

Мы рассмотрели только три примера, когда информационная безопасность может помочь бизнесу, не продавая ему страх и не пытаясь бороться с ветряными мельницами в виде необязательных нормативных документов. Но на этом вклад ИБ в бизнес не ограничивается. Она может также помочь:

- При географической экспансии;
- Вынести точки продаж «в поля» (ближе к клиенту);
- Создать новый или более дешёвый канал продаж;
- Снизить арендную плату;
- Оптимизировать складские запасы и ускорить вывод продукта на рынок;
- Оптимизировать финансовые показатели (EBITDA, CapEx/OpEx, лизинг, амортизация и пр.);
- Поднять продуктивность сотрудников;
- Уменьшить число командировок и снизить риски путешествий;
- Сократить затраты на Интернет;
- Снизить ИТ-издержки на внутренний helpdesk;
- Повысить лояльность заказчиков;
- Обеспечить стандартизация ИТ-платформы;
- Обнаруживать сговоры и конфликты интересов;
- Снизить простои.

Вот небольшой список того, что бизнес может получить от информационной безопасности при её правильном обосновании, отталкивающемся от целей бизнеса, а не целей самой ИБ, как это нередко бывает. Только в условиях, когда службы ИБ следует за бизнесом, а не вставляет ему палки в колеса, возможно успешное существование этих, часто воспринимаемых как антагонистов, сущностей. Главное — смотреть на ИБ через призму бизнес-задач.

Глава 3.4

Сколько стоит информационная безопасность?

Этот вопрос постоянно возникает на протяжении последних лет двадцати у всех, кто занимается вопросами информационной безопасности. Согласно «2005 CSI/FBI Computer Crime and Security Survey», на информационную безопасность тратится 4,3% от ИТ-бюджета. По данным Gartner, опубликованным в 2004 году, эта цифра составляет 6-9%. А согласно опросу «The Global State of Information Security 2005» от «CIO Magazine», процент достигает уже 13%. Кто же прав? Где взять верные цифры?

Давайте сразу определимся, что вопрос этот поставлен изначально некорректно и исходит из предпосылки, будто информационная безопасность (ИБ) является подмножеством ИТ-задач и входит в компетенцию только ИТ-подразделения. И хотя такое мнение продолжает бытовать среди многих специалистов, на самом деле ИБ — это гораздо более широкая задача, чем защита информационных ресурсов предприятия. Даже если не брать широкое толкование термина «информационная безопасность» из одноименной Доктрины, то все равно специалисты по ИБ занимаются и расследованием инцидентов, и выполнением требований законодательства, и защитой от утечек по техническим каналам, и взаимодействием с регуляторами (ФСТЭК, ФСБ, Роскомнадзор и т. п.), и получением лицензий на деятельность в области защиты информации, и многими другими вопросами, которые не относятся к спектру традиционного восприятия ИТ. Да и с точки зрения подчинённости, информационная безопасность часто вынесена за пределы ИТ-подразделения и имеет если не собственный бюджет, то уж точно дотируется не от ИТ-инвестиций; хотя, безусловно, пересечения есть.

Что влияет на процент?

Почему до сих пор никто не дал однозначного ответа на столь острый вопрос? Дело здесь не только и не столько в двух аспектах, рассмотренных выше. Даже если ограничиться предположением, что мы говорим об ИТ-безопасности, которая входит в ИТ-подразделение, то и в этом случае чёткого ответа не будет. Почему? Ответ придётся разбить на несколько составляющих.

Во-первых, с течением времени классические задачи ИБ начинают перетекать в ИТ и считаться уже ИТ-задачами. Так было с антивирусной защитой, с проектами по идентификации и аутентификации. Так было с проектами по антиспаму и нейтрализации DDoS-атак, с системами защиты мобильных устройств. Сейчас аналогичный сдвиг происходит с другими функциями ИБ. Напри-

мер, приходится регулярно сталкиваться с тем, что внутренним заказчиком межсетевых экранов, систем предотвращения вторжений, систем контроля доступа становятся именно ИТ-департаменты, а не ИБ-подразделения. Для производителя здесь нет никакой разницы; для решения задач заказчика — тоже, а вот для вопроса, вынесенного в заголовок, это имеет громадное значение.

Во-вторых, очень важную роль играет то, к какой отрасли принадлежит заказчик. Согласитесь, уровни информатизации в ИТ-компании, у оператора связи, в банке и на промышленном предприятии отличаются. И уровень инвестиций в информационные технологии — тоже. А значит, будут разниться и уровни затрат на ИБ.

Третья составляющая — это личность руководителя информационной безопасности. Ограничится ли он в своей борьбе за бюджет только ИТ-подразделением или попробует прикоснуться к множеству различных источников: бюджету юристов, кадровиков, безопасников-экономистов, службы внутреннего контроля или иных бизнес-подразделений? От того, насколько успешно будет налажено взаимодействие с этими отделами, зависят и те деньги, которыми сможет оперировать служба ИБ.

Ещё один фактор, влияющий на размер инвестиций в ИБ, — масштаб компании. Очень часто крупные компании, имеющие разные филиалы и юрлица в разных странах мира или регионах России, предоставляют своим подразделениям свободу действий по части приобретения ИТ- и ИБ-решений. Это приводит к завышенным итоговым затратам, т.к. централизованное приобретение оборудования для всей компании позволяет рассчитывать на значительные скидки от производителя.

Наконец, нельзя сбрасывать со счетов такой фактор, как подверженность регулятивным рискам. Одни компании находятся в прицеле ФСТЭК, ФСБ, Роскомнадзора или Банка России, а других эта чаша миновала. Одни считают необходимым безоговорочно выполнять требования нормативных документов регуляторов, а другие смотрят в первую очередь на потребности бизнеса. Очевидно, что ориентация на регулятора повышает затраты на ИБ.

В целом же можно следующим образом систематизировать факторы, влияющие на размер бюджета на информационную безопасность (да и не только на неё):

- ***Корпоративные***:
  - географический охват;
  - размер компании;
  - траектория развития (спад, рост, постоянство);
  - тип бизнеса (схожие компании имеют схожий бюджет);
  - архитектура (структура);
  - внутренняя политика;
  - экспансия на международные рынки;
  - требования compliance.
- ***Айтишные***:
  - требования к готовности (5×8 или 7×24);
  - требования к поддержке;
  - требования к времени отклика;
  - требования к времени реагирования;
  - требования к доступу;
  - уровень квалификации пользователей;
  - архитектура ИТ;
  - уровень проникновения аутсорсинга и облаков;
  - наличие «багажа» (старые системы, «железо», проекты).

Иными словами, никто и никогда не скажет, какой процент ИТ-бюджета надо тратить на информационную безопасность, потому что эта функция зависит от множества изменчивых параметров.

7 плюс минус 2

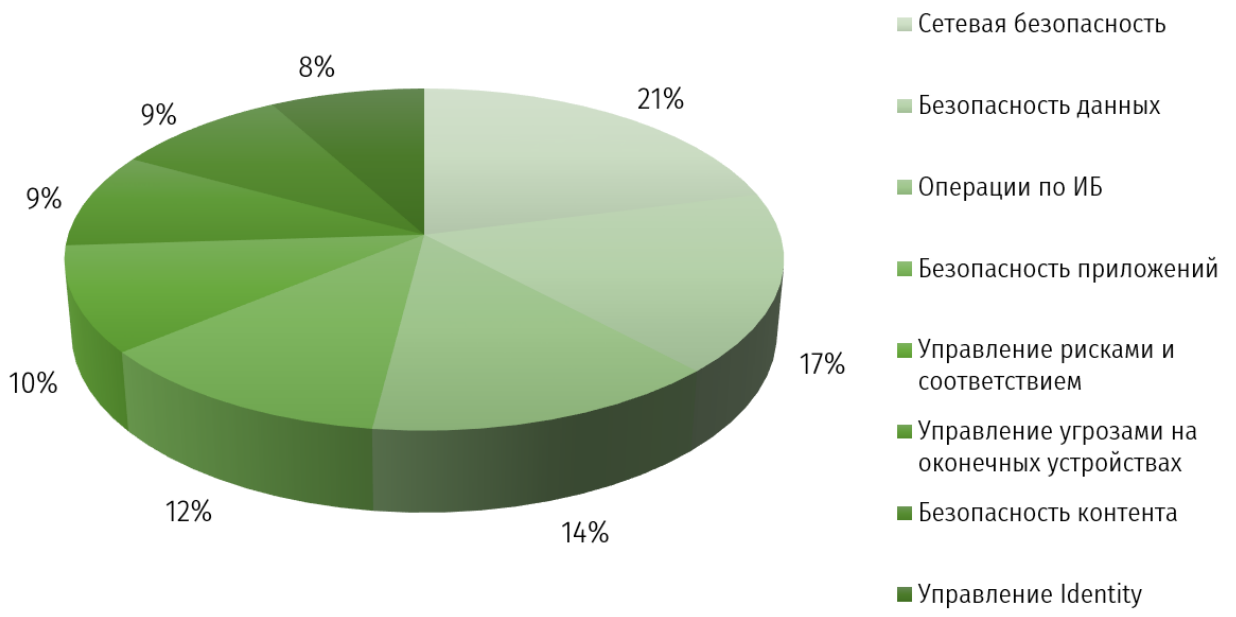
Но всё это отговорки, скажете вы. «Дайте нам конкретные цифры!» Видимо, желание узнать всеми правдами и неправдами эту магическую цифру настолько велико, что различные консалтинговые и аналитические компании регулярно публикуют некоторую «среднюю температуру по больнице».

В начале раздела были приведены цифры 2004-2005 годов. Разброс значительный: от 4,3 до 13%. Есть ли более свежие цифры? Да, есть! В 2011-м широко известный в узких кругах Ponemon Institute опубликовал исследование, согласно которому 39% организаций тратят от 6 до 10% на соблюдение правил безопасности; ещё 39% организаций тратят от 11 до 15%; 11% организаций тратят от 16 до 20% и 7% организаций тратят колоссальные от 21 до 25% своего ИТ-бюджета на соблюдение правил безопасности.

Согласно отчёту компании Forrester «2012 Budget and Planning Guide for CISOs», затраты на информационную безопасность составили 7,3% в 2010-м, 7,6% в 2011-м и 8,0% в 2012-м году. Ему вторит компания Wisegate, которая в 2013 году опубликовала ещё один отчёт — «2013 IT Security Benchmark Report». В нём приведены конкретные цифры распределения затрат на информационную безопасность. Согласно исследованию Wisegate:

- В среднем на ИБ тратится 7,5% от ИТ-бюджета.
- По отраслевому срезу больше всего на ИБ тратят финансовые организации и банки — 10,4%. Меньше всего расходуют государственные органы — 2,3%. Для промышленности эта цифра равна 8,9%, для страховщиков — 3,6%, для здравоохранения — 6,9%.
- Размер бюджета также зависит от размера компании. В том случае, если в компании

Рис. 3.4.1. *Распределение статей бюджета на ИБ.*



работало менее 1 тысячи сотрудников, то она тратила в 2,5 раза больше денег на ИБ, чем компании с 20 тысячами и более сотрудниками: 10% против 4%.

- Более зрелые компании тратят на ИБ больше своих менее продвинутых коллег: 9,0% против 5,6% от ИТ-бюджета.

Если окунуться ещё глубже и посмотреть, как тратится бюджет ИБ, то, согласно одному из последних отчётов Forrester, распределение статей бюджета выглядит следующим образом (Рис. 3.4.1).

От экспертной оценки – к теории игр

Понимая, что подход «Процент от ИТ-бюджета» неверен, специалисты стали искать другие методы оценки бюджетирования ИБ. Одной из первых работ по данной теме явилось исследование Лоуренса Гордона и Мартина Леба (The Economics of Information Security Investment, ACM Transactions on Information and System Security, Vol. 5, No. 4, стр. 438-457), которые в 2002 году опубликовали модель оценки оптимального уровня инвестиций в ИБ, исходя из стоимости защищаемой информации. По их мнению, этот уровень должен быть равен 36,8%. Правда, у данной модели есть одна сложность — мы должны оценить стоимость защищаемой информации, и тут ещё стоит подумать, что проще: оперировать процентом от бюджета или оценивать стоимость защищаемых активов (последняя задача для информации, то есть актива нематериального, имеет сразу несколько решений, что ещё больше осложняет доказательство для менеджмента).

Тремя годами позже Жан Виллемсон из Эстонии показал, что оптимальный уровень инвестиций может быть и выше, согласившись при этом с правильно выбранным Гордоном и Лебом подходом. В 2005-м Деррик Хуанг из Атлантического университета Флориды дополнил модель Гордона-Леба профилем риска человека, принимающего решение об уровне инвестиций в ИБ, и всё сразу встало на свои места. Можно ли утверждать, что уровень затрат в 36,8% действительно оптимальный? Чёткого ответа, особенно ввиду исследования Виллемсона, пока нет. Но модель Гордона-Леба дала начало активному применению экономики и смежных наук в области информационной безопасности. Мы сейчас только в начале пути...

Есть ли другие методы вычисления размера затрат на ИБ от ИТ-бюджета? Как оказалось, оба подхода используют 77% всех организаций. Ещё 22% применяют иные способы. Меньше одного процента «привязывают» свой бюджет на информационную безопасность к общим доходам предприятия.

Что у нас в сухом остатке? Чёткого и однозначного ответа на вопрос о том, сколько тратить на информационную безопасность от ИТ-бюджета, нет. Его не было 10 лет назад, его не появилось и до сих пор. И связано это с множеством факторов, влияющих на принятие решения об инвестировании. Наверное, это и хорошо. Самым правильным было бы формировать бюджет, исходя из потребностей организации и бизнеса, а не притянутых с потолка соотношений. Но мир не совершенен — всем хочется простого и быстрого ответа, и его дают нам последние проведённые исследования Wisegate и Forrester, согласно которым средний процент инвестиций в ИБ от ИТ составляет около 8%. Именно это значение можно использовать в качестве первого приближения к решению поставленной задачи.

Глава 3.5

Будущее ИБ на современном предприятии

Какие тенденции в области информационной безопасности будут определять ближайшее будущее ИТ-директора, отвечающего за вопросы ИБ? Это не банальные целенаправленные угрозы (APT), которые активно распространяются уже несколько лет и ничего нового в этом направлении не происходит. И это не уже набившие оскомину облака и мобильность. Про эти «тенденции» говорят уже много лет. Они действительно имеют важное значение в планировании деятельности службы ИБ на предприятии, но и нового в них ничего нет. Уже давно известно, как обеспечивать их безопасность. Аутсорсинг, видео-технологии, бизнес-аналитика, большие данные?.. Что в них нового?

Может быть, ничего действительно нового и вовсе нет, и специалистам по ИБ и готовиться больше не к чему? Может быть, пора прекратить гоняться за трендами и начать разгребать то, что есть? В условиях непростой экономической ситуации это неплохая стратегия — начать учиться более эффективно использовать то, что уже приобретено: сетевое оборудование, операционные системы, приложения, СУБД с точки зрения встроенного в них функционала по ИБ. Это всё так. Но... Всё-таки, грамотный специалист по безопасности отличается именно тем, что смотрит не только вперёд, не только вглубь, но и по сторонам. Что там можно увидеть? Есть ли какие-то скрытые тенденции, которые плавной поступью приходят в нашу жизнь и которые могут повлиять на информационную безопасность?

Ещё совсем недавно мы не думали о компании Apple, как об угрозе корпоративной безопасности. Но сегодня её устройства заполонили корпоративные сети, а подход Apple, Google, Samsung к упрощению, цифровизации и многократному росту удобства использования многих ранее «сложных» устройств привёл к «одомашниванию» сетей предприятия, в которых появляются устройства, ранее там «не прописанные» — кофеварки, игровые приставки, сантехника и т.п. А теневые облака? Они ведь тоже ещё совсем недавно не были проблемой для корпоративных заказчиков. А сегодня безопасники думают, как предотвратить использование «личных» облаков Dropbox, Google.Docs, Яндекс.Диск работниками, которые могут скачивать в «теневые» облака конфиденциальную информацию и хранить её там для более быстрого и удобного доступа из дома, из кафе и из других мест, где так удобно работать.

Поэтому нам хотелось бы обратиться к тому, что происходит на рынке и посмотреть, какие технологии могут стать головной болью специалистов по защите информации в ближайшее время. Мы не будем глубоко погружаться в каждую из них — скорее, наметим темы, о которых стоит задуматься.

Тёмный Интернет

Уходящий год запомнился многим активизацией усилий государства по контролю в Интернет. Антипиратское законодательство, закон о блогерах, выход в Интернет через Wi-Fi по паспорту, новая целевая аудитория для СОРМ, запрет на хранение персональных данных россиян за границей, блокировка Telegram... — вот лишь некоторые из нашумевших инициатив, которые превратились в обязательные для исполнения требования. Но при чём тут безопасность? На первый взгляд, действительно, ни при чём. Прямого отношения к информационной безопасности все эти нововведения не имеют. Но...

Мы понимаем, что число запретов только будет возрастать; особенно в условиях текущей геополитической, экономической и социальной ситуации. Чиновники уже не раз давали понять, что Россия может пойти по китайскому сценарию развития Рунета. И большинство россиян будет учиться обходить эти запреты. Это в природе человека! Мы уже видим серьёзный рост популяции пользователей Tor и торрентов. А ведь это только верхушка айсберга. Не случайно все чаще всплывает на поверхность термин «тёмный Интернет» (он же — тёмный Web, теневой Web или Dark Web). Несмотря на серьёзные усилия правоохранительных органов, в его «глубинах» можно найти информацию про оружие и наркотики, детскую порнографию, услуги по «заказу» людей и т.п. Он не индексируется обычными поисковыми сервисами, в нём почти невозможно (сейчас) найти пользователя.

А теперь представьте, что пользователи, научившись обходить государственные фильтры и пользоваться тёмным интернетом, захотят свои знания применить на работе с целью обхода корпоративных средств защиты периметра? Готовы ли мы к такому повороту событий? И тут не очень поможет опыт работы с теневыми облаками, ведь при использовании «теневого Web» используются специальные протоколы, позволяющие долго оставаться анонимными и скрывать свою активность от распространённых средств периметровой защиты. А если пользователи начнут делиться в «теневом Интернете» конфиденциальной информацией своего предприятия или обсуждать нелицеприятные для него вопросы? Уже сейчас в Dark Web есть свои блоги, социальные сети, форумы, платёжные системы, торговые площадки. Цифровой суверенитет и ограничение Рунета только усилят рост законопослушных пользователей, уходящих в теневую часть Интернета и создающих проблему для традиционных средств ИБ.

Анонимность

Кстати, продолжая тему анонимности, стоит заметить, что она набирает популярность. Вы, наверное, слышали о сервисе Secret, который просто взорвал Рунет? Его капитализация только за 6 месяцев взлетела с нуля до 100 миллионов долларов. Ещё бы — когда ещё можно было анонимно высказать о своём начальнике или работодателе или коллеге всё, что так хочется, не боясь быть раскрытым. Все устали от открытости привычных нам социальных сетей. Все хотят раскрывать душу, не будучи опознанными. Приватность

начинает править миром.

На этом фоне появляется большое количество сервисов, желающих поэксплуатировать эту потребность пользователей — Secret, Snapchat, WhatsApp, Viber, Telegram и т.п. Все они предлагают анонимность. Тот же Snapchat уже догнал по числу пересылаемых фотографий Facebook и отказался от предложенных за поглощение 3 млрд долларов. Аналогичный сервис для организации анонимных коммуникаций Whisper генерит около 1 миллиона сообщений в день.

А теперь представьте, что с помощью этих сервисов компанию «покидает» конфиденциальная информация? Мы готовы к обнаружению таких утечек и их блокированию? Ведь не секрет, что большинство DLP-решений (Data Leakage Prevention) рассчитаны на борьбу с простыми утечками по самым распространённым каналам — электронная почта, ICQ, Web-почта и т.п. Но мало кто из производителей способен сегодня контролировать Secret, Viber, WhatsApp, SnapChat, Telegram и т.п. А ведь ситуация будет только усугубляться.

Блокчейн / биткойн / распределённость

Давайте вернёмся к упомянутому ранее Tor. Чем характеризуется эта «теневая» система? Распределённостью! А распределённость сложна для контроля, что является основной задачей для тех, кто занимается безопасностью — информационной, физической, национальной...

Но Bitcoin — это всего лишь один пример распределённых технологий, которые сейчас начинают завоёвывать мир. Именно так в своё время создавался Интернет — распределённая сеть, не имеющая единого центра управления. Технология Blockchain представляет собой «Интернет» в мире финансовых транзакций — распределённая база данных и механизм денежных переводов. По этому принципу начинают строить сегодня и другие, нефинансовые приложения. Например, обмен данными или голосование. В частности, недавно появился стартап Gems, который является конкурентом WhatsApp, но при этом шифрует всю переписку между пользователями, и на серверах Gems она не хранится. Другой проект, использующий Blockchain, — Ethereum, который позволяет создать распределённый аналог любого Web-сервиса — от платёжной системы до файлообменника. Таким приложениям не нужны сервера, их сложнее контролировать и проводить расследование инцидентов. И это может создать препятствие для действий служб информационной безопасности (не говоря уже о правоохранительных и силовых структурах).

Интернет вещей

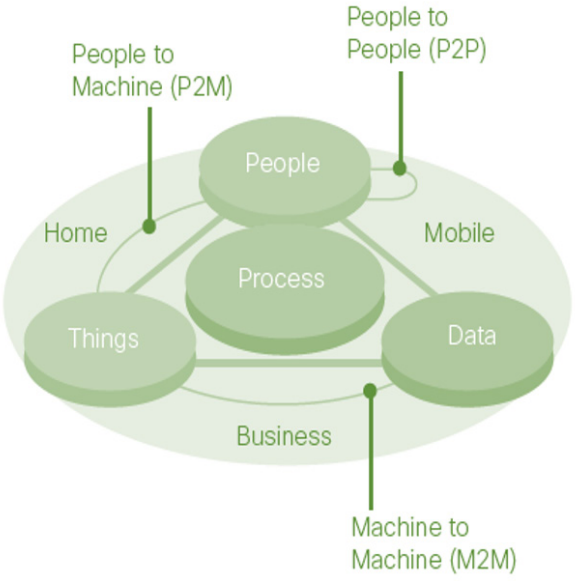
В последнее время аналитики обращают внимание на изменение картины взаимодействия в сети Интернет. От обмена данных между пользователями и вычислительными устройствами (классическая клиент-серверная модель) всё чаще и чаще начинается переход или внедрение взаимодействия «машина — машина», «человек — человек» и т.п. Например, люди, общающиеся в социальных сетях, являют собой замечательный пример взаимодействия «люди — люди». А автомобили, обменивающиеся информацией о

дорожной обстановке и о дистанции друг с другом, хорошо иллюстрируют модель «машина — машина» (M2M). И это не единственные примеры такого понятия, как «всепроникающий Интернет» (Internet of Everything), Рис. 3.5.1.

RFID-метки, размещаемые на мешках с деньгами в денежных хранилищах, сейсмические, климатические или экологические датчики, обменивающиеся информацией о состоянии контролируемой зоны, кардиостимуляторы, отправляющие информацию о сердечном ритме лечащему врачу, рояль, самостоятельно скачивающий из Интернет новые партитуры, телевизор, обновляющий свою прошивку без участия владельца — вот только несколько примеров проникновения Интернет во все сферы нашей жизни.

Да, пока они не столь активно применяются в повседневной жизни. Но ведь и мобильные телефоны ещё недавно были предметом роскоши, о которых многие могли только мечтать. А сегодня, по данным Cisco Annual Security Report 2013, 75% пользователей ежедневно использует от 2-х до 3-х устройств; ещё 8% — 4 и более. Технологии меняются так быстро, что мы не успеем оглянуться, как привыкнем к тому, что раньше считали фантастикой.

Рис. 3.5.1. *Всеобъемлющий Интернет.*



По данным Cisco, к 2020-му году в мире будет подключено к всеобщей сети около 50 млрд устройств (сейчас их около 20-ти). Вы представляете, какой это поток информации, и какие сложности встанут перед безопасниками, ориентированными на традиционные технологии? Позволю себе перечислить только некоторые из них:

- Рост объёмов трафика, что потребует более производительных решений по сетевой безопасности.
- Отсутствие человека, работающего за прибором в Интернете вещей, что потребует активного использования технологий аутентификации устройств.
- Миниатюризация устройств, требующая миниатюризации и защитных средств, и технологий (снижение объёма кода, повышенные требования к автономной работе и т.п.).
- Небольшие порции передаваемой информации, что потребует пересмотра криптографических технологий.
- Огромное число устройств, что потребует пересмотра вопросов распараллеливания обработки трафика и аутентификации такого количества устройств.
- Совершенно новые устройства (очки, часы, одежда, кардиостимуляторы, кофеварки, холодильники, сантехника и т.п.), что потребует пересмотра традиционного отношения к объекту защиты.

Готовы ли мы к этим инновациям с точки зрения информационной безопасности? Как

мы будем защищать взаимодействие между взаимодействующими через социальные сети людьми? Как мы защитим RFID-метку от направленного на неё негативного воздействия? Как мы отследим целостность информации, передаваемой по сети метеорологических сенсоров? Как, в конце концов, защищать индустриальные системы и системы управления технологическими процессами? Всё это требует не просто внимания, но и детальной проработки архитектуры, разработки совершенно новых подходов и средств защиты. Только представьте себе, что нам надо шифровать телеметрические данные, поступающие от системы мониторинга дорожной обстановки напрямую в автомобиль? Никакой ГОСТ 28147-89 по шифрованию встроить туда невозможно (если это не продукция отечественного автомобилестроения).

Но, может быть, можно хотя бы контролировать такой трафик? Традиционными централизованными механизмами — не всегда. Очень уж часто выходят они из строя и поэтому такое распространение получается технология mesh-сетей, т.к. полносвязных ячеистых сетей, в которых узлы сети связываются с другими узлами этой сети минуя некий центральный узел. Такая топология обладает не только высокой надёжностью, самоорганизацией и самовосстановлением, но и сложностью. Примером такой технологии являются беспроводные локальные или персональные сети, например, ZigBee.

«Теневые» ИТ

На различных западных конференциях и в специализированных СМИ стал активно использоваться термин «теневые» ИТ (shadow IT), который означает активное задействование сотрудниками компаний ИТ-сервисов, к которым работодатель не имеет никакого отношения. Самым банальным примером таких теневых ИТ является применение персональных облачных сервисов, таких как Dropbox, Google.Docs или Яндекс.Диск. Кто из нас не пользуется этими сервисами, чтобы «по-быстрому» обменяться файлами с коллегами по работе или с заказчиками/партнёрами? Кто из нас не «сливает» туда данные, чтобы с ними «поработать дома»? Мы даже не будем сейчас поднимать вопрос доступа к таким сервисам спецслужб (это проблема неуправляемая, и потому задумываться о ней смысла большого нет). Речь идёт об удобстве, которое приводит к все более массовому применения теневых ИТ-сервисов в деятельности многих компаний.

Проблема ли это? Для сотрудников — нет. Для ИТ? Скорее всего тоже нет, т.к. с ИТ-служб снимается часть проблем, которые сотрудники начинают решать самостоятельно. Да и затраты на использование таких сервисов сотрудники берут на себя. А что со службой информационной безопасности (ИБ)? Вот тут и начинаются все сложности. Мы ещё не успели привыкнуть к мысли переноса части своих приложений и данных в облака Amazon, Microsoft, Saleforce.com, Box.com, Webex и другие, как новая напасть. Согласно имеющейся статистике, компания знает только о 20% используемых сотрудниками облачных сервисов. О 20%! По оценкам Gartner, к 2016-му году до 50% крупных корпоративных заказчиков столкнутся с хранением данных своими пользователями в публичных ИТ-сервисах. На наш взгляд, это оценка слишком оптимистичная. А ведь среди этих данных могут быть (и скорее всего будут) сведения конфиденциального характера. К 2017-му году тот

же Gartner предрекает, что 90% (!) компаний столкнётся с невозможностью предотвращения использования своими сотрудниками теневых ИТ.

Что делать в такой ситуации? Вопрос непростой. Запрещать использование внешних ИТ-сервисов можно, но до определённого предела. Пользователи найдут способ обойти такие запреты. Закрыть глаза? Но это до первого серьёзного инцидента. С точки зрения ИТ гораздо эффективнее «возглавить» этот процесс и предложить пользователям контролируемый доступ к основным и, как следствие, наиболее популярным внешним сервисам. Для этого можно использовать решения из нарождающегося сейчас рынка облачных посредников (cloud access security broker), который предоставят возможность сочетать удобство, снижение затрат и безопасность при использование таких сервисов. Как промежуточный и более быстрый в реализации сценарий, больше ориентированный на традиционных безопасников, внедрить системы мониторинга доступа к облачным и иным внешним ИТ-сервисам. Это может быть функциональность имеющегося межсетевого экрана следующего поколения (NGFW), это может быть функция системы контроля доступа в Интернет (Web Security Gateway или Secure Internet Gateway), это может быть функция системы мониторинга сетевой активности (Network-based anomaly detection или Network Traffic Analysis). Главное — иметь возможность следить за использованием различных сервисов, и при превышении определённого заранее установленного лимита (по времени, по объемам данным, по количеству пользователей) начать решать этот вопрос более системно.

Изменение ландшафта угроз

Про «целевые», «целенаправленные», «таргетированные», «изощрённые» угрозы (они же APT) слышали многие. Но мало кто до конца понимает, что же это такое на самом деле, и как с этими угрозами надо бороться. На самом деле все просто. От обычной атаки целенаправленная отличается сфокусированностью на определённой жертве, а не массовостью, как это было раньше. Второе отличие — использование несколько векторов для атаки, проникновения, использования уязвимостей. Всё это делает борьбу с такими атаками задачей непростой, требующей немного иных подходов. Согласно недавно опубликованной версии отчёта Verizon, время на проникновение в корпоративные и ведомственные сети снижается, а вот время на обнаружение целенаправленных угроз оста-

Табл. 3.5.1. *Три набора решений для борьбы с изощрёнными атаками.*

Минимум	Неплохо бы	Идеально
• МСЭ и IPS. • Сегментация сети. • Системы контроля доступа в Интернет. • Защита ПК / ноутбуков.	• NAC. • Контроль приложений (чёрные / белые списки). • МСЭ / IPS следующего поколения. • SIEM. • Защита мобильных устройств.	• Анализ сетевого трафика. • Расследование инцидентов. • Анализ содержимого. • Адаптивный контроль доступа. • Система обнаружения брешей (BDS).

ётся практически неизменным, без тенденции к уменьшению.

Многовекторность целенаправленных атак означает, что сложно найти универсальное средство защиты, позволяющее бороться с APT. И, несмотря на появляющиеся на рынке продукты, безапелляционно заявляющие в своей рекламе об умении бороться с такими угрозами, сегодня, а видимо и завтра таких решений не будет. Эксперты выделяют три набора решений / технологий, которые позволят справляться с изощрёнными атаками (Табл. 3.5.1).

Разумеется, в основе должны находиться выстроенные процессы управления изменениями, управления уязвимостями, управления инцидентами и управления доступом.

Иными словами, для эффективного обнаружения современных угроз одного-двух широко распространённых средств защиты (МСЭ и антивирус) уже недостаточно — необходим целый комплекс, взаимоувязанных между собой технологий и решений, работающих как иммунная система, но не человека, а корпоративной / ведомственной сети.

Смена парадигмы информационной безопасности

Из чего исходила традиционная ИБ ещё совсем недавно? Ставилась задача обеспечения эшелонированной обороны, т.е. выстраивания защитной стены вокруг защищаемого объекта (системы или данных). Эту задачу неплохо решали такие технологии как межсетевое экранирование, идентификация/аутентификация, управление уязвимостями и патчами, управление приложениями. Иными словами, задача состояла в блокировании угроз на подступах.

Потом стали появляться DoS/DDoS-атаки, инкапсулированные атаки в разные протоколы и форматы файлов, что потребовало расши-

Рис. 3.5.2. *Привязка технологий ИБ к жизненному циклу атаки.*

рения защитной парадигмы за счёт обнаружения угроз в процессе их реализации. Эту задачу стали решать системы предотвращения вторжений (IPS), антивирусы, системы контентной фильтрации и т.п. И всё бы ничего, пока угрозы не стали настолько продвинутыми, что гарантировать их 100%-е обнаружение и блокирование стало невозможно. Более того, число успешных проникновений и утечек конфиденциальной информации стало расти, невзирая на колоссальные бюджеты, потраченные на безопасность.

И, как это не обидно признавать, но безопасность перестала справляться с задачей недопущения компрометации внутренних узлов организации. Кто-то закрывал на это глаза. Кто-то вообще не замечал успешных взломов, продолжая тратить средства не на то, что нужно. А кто-то пошёл дальше и, наступив на горло собственной гордости, признал, что существует вероятность проникновения злоумышленника или вредоносного кода внутрь предприятия. В таких условиях очень важно стало не просто бороться с атаками на подступах или в процессе их проникновения, а своевременно обнаруживать компрометацию и локализовывать её, не давая злоумышленникам расширять плацдарм и незаметно красть как можно больше и дольше критическую для бизнеса информацию.

Это означает, что организациям нужен набор решений/технологий, который позволит определить масштаб ущерба, ограничить негативные последствия от успешной атаки, восстановить скомпрометированные элементы сети и нормальное функционирование системы как можно скорее (Рис. 3.5.2). Это позволяют реализовать системы анализа журналов регистрации, SIEM-решения, системы расследования инцидентов, системы лечения/устранения вредоносного кода и т.п.

В современном мире эффективность системы защиты будет определяться не числом отражённых угроз, а способностью своевременно обнаруживать и локализовать проникновения злоумышленников внутрь организации. Примерно также защищённость любого ПО определяется не числом уязвимостей в нем, а оперативностью их устранения.

Возрастающая роль интеграции, автоматизации, оркестрации и ИБ-аналитики

Выше мы писали, что современная система защиты предприятия (не важно какого масштаба) должна работать как иммунная система человека — целостно и слажено. Именно поэтому возрастает роль интеграции и аналитики в контексте информационной безопасности. Ведь как было раньше? У нас были отдельные средства защиты, действующие независимо, с собственными системами управления и визуализации сигналов тревоги. Потом на рынке стали появляться первые SIEM-системы, которые выполняли только функцию сбора разрозненных событий безопасности без какой-либо обратной связи со средствами защиты. В любом случае, внедрение SIEM-решений представляло и представляет собой задачу нетривиальную и сопоставимую с внедрением какого-либо бизнес-приложения.

Далеко не все компании способны использовать SIEM-решения, но потребность в аналитике возрастает при этом всё больше и больше. Поэтому отдельные решения стали оснащаться возможностью работать с так называемыми признаками компрометации (indicators of compromise), идея кото-

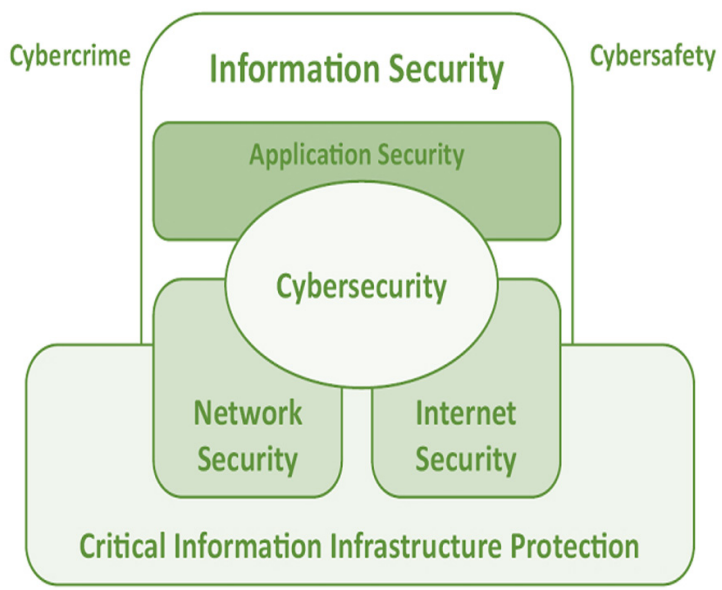
рых заключалась в анализе и корреляции большого количества разрозненных событий, объединённых в укрупнённые инциденты, сигнализирующие либо о свершившемся факте компрометации сети или отдельного её узла, либо о подготовке к данному неприятному факту. При этом, для работы с признаками компрометации можно было не использовать полноценную SIEM-систему, а ограничиться сбором различных событий от сенсоров, разбросанных по всей сети. Например, система защиты следующего поколения (next generation security) могла обнаруживать атаки по сигнатурам на сетевом уровне, анализировать сетевые аномалии, распознавать приложения и пользователей и всё это увязывать между собой. А интеграция средств сетевой безопасности со средствами защиты конечных устройств позволяла добиться ещё большего эффекта. И всё это без использования полновесного SIEM-решения.

Иными словами, сегодня уходит в прошлое ситуация, когда можно было напокупать различных продуктов безопасности, которые, может быть, и были лучшими в своём классе, но никак не интегрировались между собой и не умели обмениваться сигналами тревоги. Этакие независимые «островки» безопасности в корпоративной или ведомственной сети. Время точечных средств защиты проходит, и в современном мире успех будет сопутствовать тем, кто сможет увязать свои защитные решения и технологии в единый комплекс. Только так можно будет обнаруживать и отражать целенаправленные угрозы, упомянутые выше.

От информационной безопасности — к цифровой

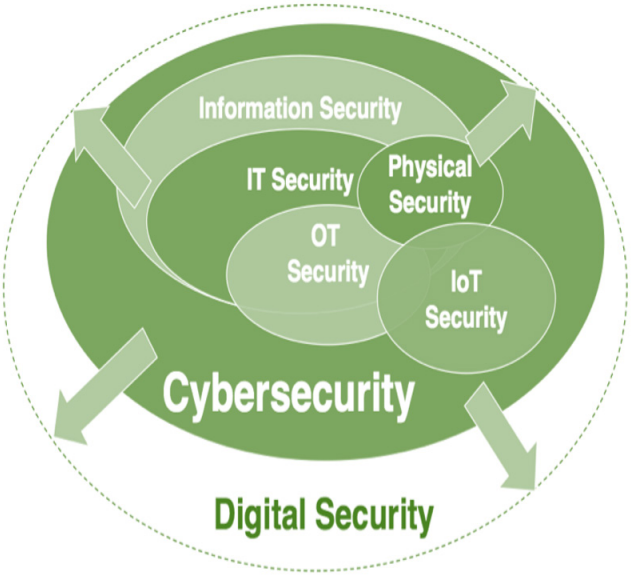
В июле 2012-го года был принят международный стандарт ISO/IEC 27032:2012 «Information technology -- Security techniques -- Guidelines for cybersecurity», определивший, что считать «кибербезопасностью». И хотя в России термин «кибербезопасность» на официальном уровне не употребляется, в жаргоне специалистов, журналистов и чиновников он проскакивает регулярно. Согласно мнению ISO, кибербезопасность у́же информационной безопасности (отечественные документы придерживаются схожей версии) и почти совсем не пересекается с безопасностью критической инфраструктуры. Но, в целом, картина, нарисованная ISO несколько лет назад, выглядит вполне разумно (Рис. 3.5.3).

Рис. 3.5.3. *Взаимосвязь терминов в области ИБ (версия ISO).*



И тут на сцену выходит Gartner, известная своими экспериментами с названиями и придумыванием новых терминов. Она не только вводит новый термин «цифровая безопасность» (Digital Security), но и меняет иерархию и связь элементов (Рис. 3.5.4).

Рис. 3.5.4. *Взаимосвязь терминов в области ИБ (версия Gartner).*



Известная по ISO «безопасность критических инфраструктур» у Gartner трансформируется в OT Security, т.е. безопасность операционных технологий. Появляется совершенно новое, но с маркетинговой точки зрения, активно продвигаемое направление безопасности «Интернета вещей» или «Всеобъемлющего Интернета». Физическая безопасность тоже целиком попадает в кибербезопасность, которая, в свою очередь, является подмножеством безопасности цифровой.

Всё бы ничего, если бы Gartner не имела такого веса на корпоративном рынке и не навязывала всем свою терминологию. Международная организация по стандартизации (ISO) тоже играет не последнюю роль в области информационной безопасности (чего только стоит серия стандартов ISO 270xx). Поэтому предвижу путаницу, которая обязательно возникнет из-за этой неразберихи.

Потребитель вторгается в корпорации

Эта тенденция хорошо заметна на примере многих компаний, внедряющих мобильные устройства в свои бизнес-процессы или просто разрешающие отдельным категориям сотрудникам подключать свои личные смартфоны или планшетники к корпоративной или ведомственной сети. Речь идёт о стирании границы между двумя ранее независимыми направлениями — рынка корпоративных и потребительских технологий. Вот несколько примеров:

- Пользователи не желают использовать выданную им на работе оргтехнику (лэптопы, смартфоны и т.п.) по 4-5 лет. Как раз наоборот, пользователи хотят жить как в обычной жизни: устарел компьютер или стал немодным — поменял его; понравилась новая модель смартфона — купил новую и т.д. И они это начинают диктовать своему предприятию. Само по себе на область информационной безопасности это влияет не сильно, но уменьшающийся жизненный цикл основных ИТ приводит к уменьшению жизненного цикла и средств защиты, что надо учитывать при бюджетировании и выработке стратегии тестирования и внедрения средств защиты. Нужно ускоряться — годовые или даже двухгодовые пилоты уже никого не устраивают.
- Концепция BYOD («Bring Your Own Device», «Принеси своё устройство»), которую многие начинают использовать. Одно дело — защищать корпоративные устройства, и другое дело — личные, на которых может находиться (и находится) личная

информация пользователя, его персональные данные, которые он не хотел бы делать достоянием, если не гласности, то уж ИТ/ИБ-службы точно. При этом всегда встаёт вопрос выбора средств защиты, которые поддерживают все многообразие мобильных платформ — от iOS до Android, от Windows Phone до Bada.

- За BYOD мягкой поступью идёт BYOT, т.е. «принеси свою технологию» («Bring your own technology»), когда пользователь начинает приносить свои приложения, делающие их работу удобней и эффективней. А это приводит к тому, что стандартизация ПО, о которой так ратуют многие апологеты ИТ, уже не является панацеей. Нет единого стандарта на используемое ПО — специалистам по ИБ приходится расширять свои знания в части изучения нового софта, новых уязвимостей, новых угроз, новых каналов утечки и т.д. Это требует ресурсов, о выделении которых надо думать заранее. При этом, попытка запретить использовать чуждые предприятию технологии — тоже не выход. Они действительно могут повышать продуктивность сотрудников, что благоприятно сказывается на бизнес-показателях.
- Размывание границы между личным и корпоративным не только в устройствах или технологиях, но и в действиях, которые пользователи осуществляют в рабочее время с личных устройств или с корпоративных устройств в нерабочее время. Не зря в развитых странах сейчас идёт борьба не ИТ и ИБ, а ИБ и т.н. Privacy (можно перевести как «частная жизнь»). Как совместить и то, и другое? Казалось бы, мы говорим о смежных темах (достаточно только вспомнить, что в Россию тему персональных данных активно продвигают именно службы ИБ). Но, оказывается, всё не так очевидно. Сторонники невмешательства в частную жизнь утверждают, что ИБ мешает им, стараясь как можно больше разнюхать, расследовать, сохранить в журналах регистрации. Как не нарушать конституционные права пользователя на частную жизнь и при этом обеспечивать эффективную работу сотрудника? Неоднократно поднимаемая тема контроля e-mail относится именно к этому направлению. Одно дело — запретить заниматься личными делами на работе (нарушает Трудовой Кодекс и тем более Конституцию, но многие работодатели так делают), и совсем другое дело, когда такого запрета нет. В этих условиях службам ИБ приходится отходить от концепции «замкнутой среды» и придумывать что-то более гибкое.
- Приход новых вендоров, не замеченных ранее на корпоративном рынке, а, следовательно, и не учитывающих потребности корпоративных пользователей или учитывающих не в полной мере. Речь идёт о Google, Apple, Dropbox и иже с ними. Загрузка корпоративных документов в iCloud, Google.Docs, Dropbox с их «мало-кем-читаемыми» политиками, с одной стороны, повышает надёжность хранения, гибкость доступа и удобство обмена с кол-

Рис. 3.5.5. *Кривая Роджерса.*

легами, а с другой ставит кучу непонятно как разрешаемых задач перед службами ИБ. Причём, именно перед безопасниками — «айтишникам» все эти сервисы никаких особых проблем не доставляют (если не вспоминать про синхронизацию данных).

- Использование социальных сетей для целей корпоративного маркетинга, привлечения новых клиентов, получения обратной связи от потребителя, формирования community и т.д. С другой стороны, социальные сети начинают использоваться для информационных войн (а кому с ними бороться как не представителям служб ИБ), слива (в т.ч. и случайного) конфиденциальной информации, нарушения этических норм и т.п. И обо всем этом тоже стоит задуматься до, а не после начала их активного использования. Пока же во многих компаниях нет даже политик работы с социальными сетями, не говоря уже о полноценных средствах их контроля и мониторинга.

Вышеуказанные шесть примеров — только верхушка айсберга, но даже они показывают, что слияние потребительских и корпоративных технологий ставит перед службами ИБ совершенно новые вопросы, ранее неизвестные. Прятать голову в песок можно, но недолго. Прогресс не остановить. Например, по данным ежегодного отчёта Cisco Annual Security Report 2013, в 2012-м году 20% всего времени в Интернет пользователи проводили именно в социальных сетях. Ещё 22% времени было потрачено на интерактивные видео-сервисы (Skype, Webex, Jabber и т.д.). Что делать с этими цифрами? Закрыть глаза или всё-таки задуматься, как их защищать?

Разумеется, можно попробовать запретить все эти «новомодные фишечки», которые только мешают размеренному темпу жизни сотрудников служб ИБ. Но есть законы, которые говорят, что запретить всё невозможно — пользователи начнут обходить все запреты. В маркетинге есть модель, называемая кривой Роджерса или кривой восприятия инноваций (Рис. 3.5.5). Суть её проста — любая инновация воспринимается не сразу, а постепенно. Сначала её начинают применять новаторы, потом ранние последователи, а уже за ними — раннее и позднее большинство.

Так уж складывается, что к новаторам и ранним последователям в описанных выше областях нередко относятся либо руководители высшего или среднего звена, либо ключевые сотрудники, приносящие компании немалую прибыль. А, следовательно, их мнение и поведение надо учитывать. Безопасники же почему-то всегда попадают в категорию «опоздавших». Пробовать им упирать на требования запретительных политик ИБ можно, но вот ответ на вопрос «кто проиграет в этой войне?», думаю, будет не за службой ИБ. И последние инциденты это демонстрируют с завидной регулярностью.

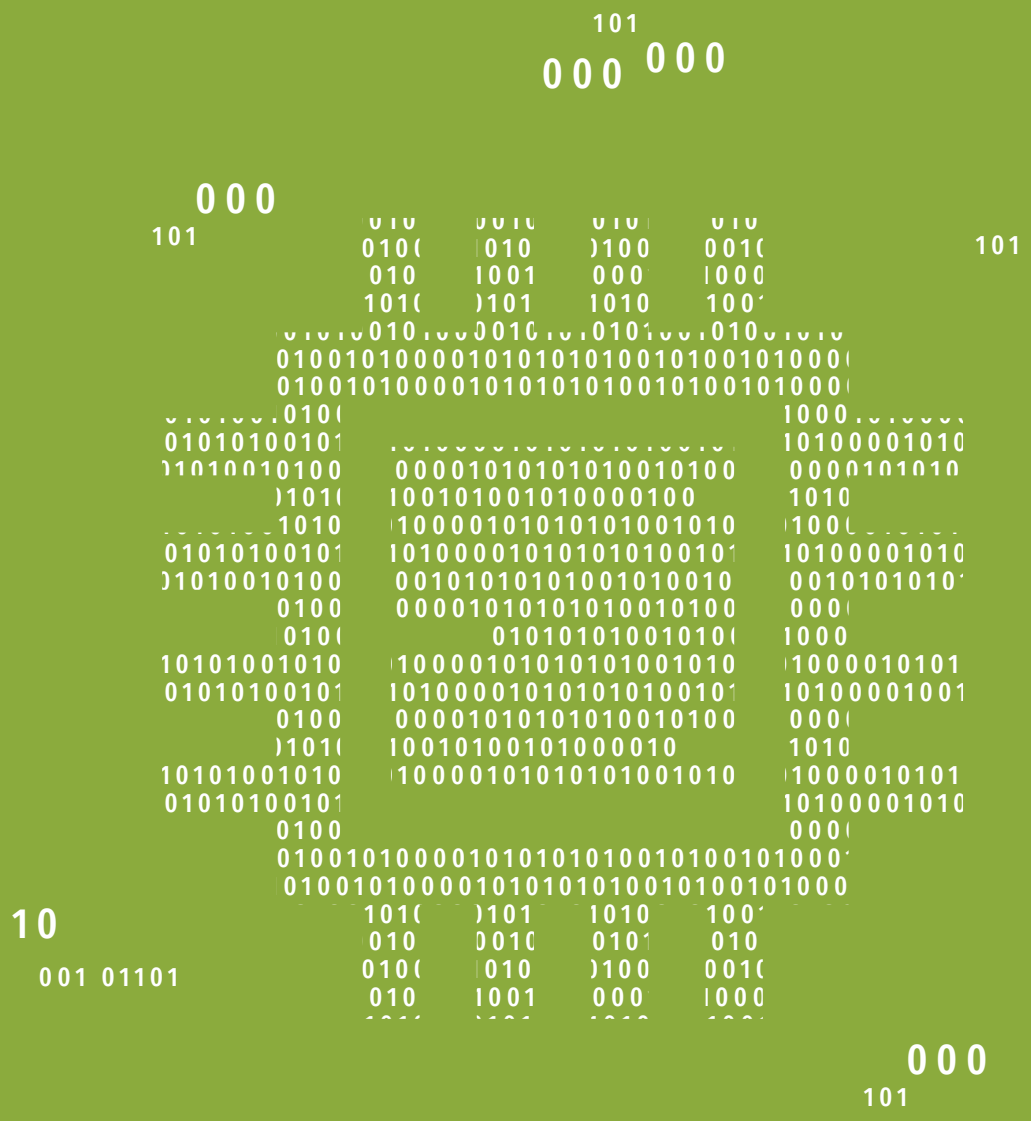
Заключение

Надо сразу признаться, что пока не для всех озвученных выше тенденций есть решения с точки зрения информационной безопасности. И специалисты по ИБ, работающие в компаниях, в которых эти тренды могут проявиться, пока предоставлены сами себе. Поэтому им надо, как минимум, задуматься о том, как нивелировать потенциальные проблемы с незащищенностью описанных технологий или, наоборот, их использовании корпоративными пользователями.

Агрессия потребительских технологий, всепроникающий Интернет — это не всё, с чем предстоит иметь дело специалистам служб ИБ в самое ближайшее время. Конвергенция и миниатюризация — вот ещё два ругательных слова для современных безопасников. Раньше всё было ясно и чётко — вот поток пользовательских данных, вот голосовой поток, вот видео, вот трафик сигнализации и управления. Сегодня в мире превалирует конвергенция — голос, видео и данные передаются по одной сети; сети систем физической безопасности интегрируются в обычную IP-сеть; на один порт коммутатора может одновременно подключаться IP-телефон, лэптоп, смартфон и планшетный компьютер... Как это всё разделить? Как контролировать и защищать?

Но конвергенция происходит не только на сетевом уровне. В магазинах сегодня нередко можно встретить ножи, спрятанные в кредитные карточки (их не определяет металлодетектор в аэропортах и на массовых мероприятиях). С точки зрения информационной безопасности, гораздо большую проблему представляют флешки, встроенные в кредитные карточки, просто лежащие в бумажнике. Или флешка, встроенная в авторучку или в обычные наручные часы. Даже физический досмотр или применение спецсредств не обнаруживает их, создавая проблему утечки конфиденциальных данных. А если вспомнить про недавно анонсированные очки Google, которые будут фиксировать, распознавать и передавать в сеть, всё, что видит их обладатель. Это ещё, конечно, не линзы с подключением к Интернет и тем более не встроенный в глазное яблоко микрочип с видеокамерой, но технологии продвинулись достаточно далеко. Как запретить использование Google-очков на предприятии, если они выполняют и свою основную функцию? Как пойти против Трудового Кодекса и Конституции? Вопросы, вопросы, вопросы... А ответ один.

Пора пересматривать традиционные подходы в области обеспечения ИБ и учитывать набирающее силу влияние новых технологий, поведения пользователей и новых методов работы на деятельность служб информационной безопасности. И делать это не только сотрудникам таких служб, но и регуляторам с их главенствующей методической ролью (как минимум в теории). Главное, чтобы не было поздно!



Часть 4

Современные концепции и технологии

Глава 4.1

DevOps: передовые практики организации ИТ-деятельности

Олег Скрынник

Введение

Методы управления ИТ-деятельностью не стоят на месте. Несколько десятков лет назад использовались одни подходы к разработке и эксплуатации информационных систем, сегодня — уже другие, а завтра придёт время следующих, переосмысленных способов и техник, опирающихся на новые знания, опыт и технологии. Бóльшую часть времени методы управления развиваются эволюционно, путём систематизации и оттачивания созданных ранее моделей, основанных на неких базовых принципах и постулатах. Однако, время от времени происходят скачкообразные изменения, позволяющие отдельным организациям-лидерам сделать существенный шаг вперёд в вопросах эффективности и рациональности применения информационных технологий.

На передовом крае ИТ-менеджмента находится движение ***DevOps*** (сокр. от англ. Development & Operations), названное так, в целом, довольно случайно. Новое имя собственное настолько же далеко от вкладываемого в него смысла, насколько аббревиатура ITIL далека от понятия «библиотека», а COBIT — от целей контроля (дополнительные сведения можно найти в предыдущей версии Учебника, в главе

> С публикацией COBIT 5 в 2012 году правообладатель подчеркнул, что, несмотря на то, что изначально аббревиатура COBIT являлась сокращением от «Control Objectives for Information and related Technology», теперь она является именем собственным.
>
> Компания AXELOS, управляющая ITIL с 2013 года, также не рекомендует использовать первоначальное наименование «IT Infrastructure Library», ограничиваясь именем собственным ITIL.
>
> Эксперты DevOps, стоявшие у истоков этого движения, признают ограниченность получившегося названия, призывая использовать более точные, на их взгляд, «BizDevOps», «DevSecOps» и подобные. Однако вероятность изменения названия в настоящее время является незначительной.

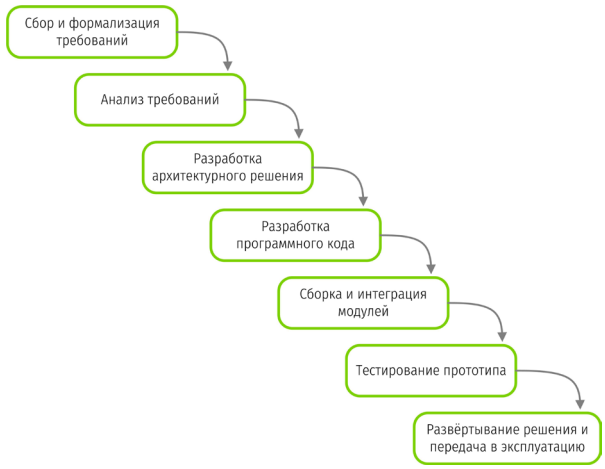
«Управление ИТ-процессами и услугами»).

Можно утверждать, что появлению DevOps в наибольшей степени способствовали два фактора: развитие гибких методов разработки программного обеспечения и управление ИТ-инфраструктурой, как программным кодом. Рассмотрим каждый из них.

Развитие гибких методов разработки программного обеспечения

В конце прошлого столетия доминирующей методологией разработки программного обеспечения была так называемая «водопадная модель» (или «каскадная модель»): последовательное выполнение заранее определённых этапов, каждый из которых занимает существенное время и завершается достижением заранее согласованных результатов, при этом переход на следующий этап во многих случаях происходит после полного и формального завершения предыдущего этапа (Рис. 4.1.1.). Дополнительным отличительным признаком такой модели является функциональная специализация исполнителей отдельных этапов: аналитиков, архитекторов, разработчиков, тестировщиков и т.д.

Рис. 4.1.1. *Пример водопадной модели разработки программного обеспечения.*



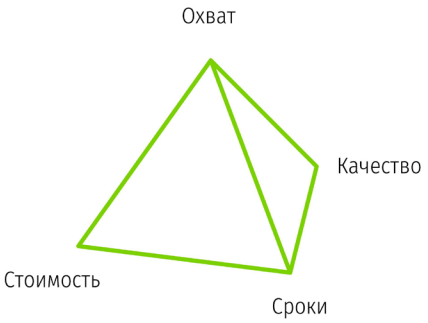
При разработке крупных информационных систем с конечной функциональностью, которую возможно определить и зафиксировать в самом начале работ, а также при отсутствии требования максимально быстрого завершения полного цикла разработки такая модель позволяет получать качественные выходные результаты при достаточно детальном контроле расходов.

Однако, в конце 90-х годов XX века, с бурным развитием Интернет-технологий и web-программирования, недостатки водопадной модели стали негативно влиять на взаимодействие и взаимопонимание заказчиков (бизнес-подразделений компании, либо внешних организаций) и исполнителей (программистов компании, либо внешних разработчиков программного обеспечения). Действительно, появляющиеся рыночные возможности для основного бизнеса требовали быстрого — за считанные месяцы — вывода на рынок новых продуктов. В то время как типичный цикл разработки от начала проекта до получения первого работающего результата занимал от 6 до 18 месяцев, а в крупных организациях — до 2-3 лет. Кроме того, в условиях появления ранее неизвестных, но потенциально перспективных рыночных возможностей требования заказчиков могли меняться по ходу проекта разработки, что было крайне сложно учесть при создании ИТ-системы без увеличения сроков, либо снижения качества выходных результатов (Рис. 4.1.2.).

Таким образом, накапливалось напряжение между заказчиками и исполнителями, между основным бизнесом и разработчиками ПО. Ответом на такой вызов стали инновационные подходы к программированию. К. Швабер выпустил несколько публикаций о Scrum (например, «Agile Software Development

with Scrum», K. Schwaber, 2001, ISBN: 978-0130676344). К. Бек опубликовал книгу об экстремальном программировании — XP («Extreme Programming Explained: Embrace Change», K. Beck, 1999, ASIN: B01FKT01PY). Однако, применение новых идей давало весьма скромные результаты, в основном потому, что такое применение фокусировалось лишь на одном из этапов цикла разработки ПО — на, собственно, программировании, при том, что задача ставилась намного более широкая. Требовалось что-то, что позволит упростить и ускорить весь жизненный цикл программного обеспечения.

Рис. 4.1.2. *Классическая пирамида взаимосвязанных ограничений проектного управления.*



В 2001 году К. Швабер, К. Бек, а также ещё пятнадцать экспертов встретились, чтобы обсудить имевшиеся проблемы и выработать решение. Итогом стал так называемый манифест Agile, призванный устранить разрыв понимания между бизнесом и разработчиками ПО (дополнительные сведения можно найти в главе «Управление разработкой ПО»).

Последовавшее развитие и принятие идей гибкой разработки сообществом программистов и менеджеров проектов сильно ускорили и перестроили разработку ПО.

Ключевыми элементами гибкой разработки являются более плотное взаимодействие между заказчиком и исполнителем, уменьшение размера задач, ритмичность выдачи результатов через короткие промежутки времени (циклы) и ограничение размера команд.

Группа разработки ПО, применяющая гибкие подходы, выдаёт готовый к эксплуатации новый код каждыедве-четыренедели. Конечные потребители плотнее вовлечены в создание продукта, а, значит, быстрая обратная связь значительно влияет на дальнейшее развитие продукта, что дополнительно добавляет вкуса к быстрым изменениям.

Однако, во многих компаниях отказ от водопадной модели в пользу гибкой разработки даёт куда меньший эффект, чем ожидается. Такие наблюдаемые в работе многих компаний результаты связаны не столько с какими-то преимуществами водопадной модели или недостатками Agile. Зачастую, полезный эффект нивелируется тем, что разработка кода — лишь одно из звеньев в цепочке создания ценности.

Действительно, до начала самой разработки имеется ещё значительный блок работ, направленный на выявление бизнес-потребностей, их проработку, анализ, приоритизацию и т.д.

Далее, по окончании разработки, готовый программный код необходимо быстро развернуть в среде эксплуатации, чтобы заказчики получили всю ту пользу, которую им обещали, а также могли предоставить обратную связь разработчикам относительно качества получившегося продукта. При этом, почти во всех организациях, возникших до 2010-х годов, ИТ-инфраструктура является жёсткой, основанной на дорогом аппаратном обеспечении, которое было приобретено достаточно давно, бюджеты на закупку

и настройку выделялись непросто, да и бюджетный процесс для новых закупок — долгий.

Более того, в подавляющем числе организаций ИТ-инфраструктура находится в довольно хрупком состоянии. Одним из факторов, усиливающих такую хрупкость, является комплексность, сложность применяемых ИТ-решений. Используется множество, десятки тысяч взаимосвязанных компонентов. Другим фактором служит слабое документирование, равно как и быстрое устаревание документации относительно применяемых ИТ-решений и ИТ-систем, в том числе устаревание знаний ИТ-персонала, а также потеря знаний вследствие текучки кадров.

Трогать ИТ-инфраструктуру во многих компаниях страшно. Изменение — самое большое зло для отдела эксплуатации ИТ-систем, а постоянный большой поток изменений может привести к катастрофическим последствиям.

Таким образом, передовые методы разработки ПО упираются в барьеры со стороны подразделений, ответственных за эксплуатацию информационных технологий, что нивелирует возможный положительный эффект применения гибких подходов.

Управление ИТ-инфраструктурой как программным кодом

Возникновению управления ИТ-инфраструктурой как программным кодом предшествовало появление и развитие двух технологий: виртуализации и облачных вычислений.

История виртуализации программных и аппаратных сред началась довольно давно — в 1964 году, с началом разработки операционной системы IBM CP-40. За годы последовательного развития этого направления был достигнут весьма значительный прогресс. Коммерчески доступные системы появились для мейнфреймов (70-80-е годы прошлого века) и для более распространённых в последующем машин на архитектуре Intel x86 (80-90-е годы).

Виртуализация позволила не только более эффективно использовать дорогое и мощное аппаратное обеспечение, но и ввести дополнительный уровень абстракции между исполняемым кодом, предоставляющим полезные результаты заказчику, и нижележащим системным программным обеспечением. Был сделан существенный шаг в сторону разделения компетенции и ответственности между, условно говоря, «прикладниками» и «системщиками», в широком смысле данных понятий.

Технология облачных вычислений развивалась ещё быстрее. До середины 90-х годов прошлого века телекоммуникационные компании предлагали своим клиентам организацию частных глобальных вычислительных сетей (WAN — Wide Area Network) путём прокладывания соответствующих соединительных кабелей для каждой точки, каждого заказчика, от пункта А до пункта Б. Но с появлением технологии частных виртуальных сетей (VPN — Virtual Private Network) возникла возможность по одним и тем же каналам передачи данных отправлять пакеты разных клиентов, обеспечивая должный уровень безопасности, приватности и качества сервиса. Именно тогда для наглядного отображения разграничения ответственности — где идёт «кабель от клиента», а где трафик попадает в общую разделяемую сеть, — провайдеры стали использовать символ облака.

Клиенты, получившие возможность передачи данных на большие расстояния, стали использовать данные технологии не только

для собственно обмена информацией между своими территориально удалёнными друг от друга системами, но и для распределения вычислительной нагрузки между разными узлами своих сетей. Напрашивалось появление технологии, упрощающей и удешевляющей такое взаимодействие. Небольшие провайдеры сделали первые шаги, а действительно масштабные изменения случились в 2006 году, когда компания Amazon представила своё решение ECC (Elastic Compute Cloud). Вскоре, в 2008 году, компания Microsoft запустила свой сервис Azure, а компания Google — сервис Google App Engine, впоследствии развившийся в Google Cloud Platform. Это, разумеется, не единственные, но самые крупные примеры предоставления вычислительных мощностей в аренду.

Виртуализация и облачные технологии сильно изменили вычислительный ландшафт. Предлагаемые коммерческими провайдерами ресурсы стали доступными по стоимости, надёжными и обеспечивающими необходимый уровень безопасности. Отношение клиентов к облакам и их использованию изменилось от «кто-то другой где-то управляет моим железом» на «у меня есть инфраструктура, которой я управляю на расстоянии» (дополнительные сведения можно найти в главе «Управление ИТ-инфраструктурой»).

Что же это означает — управлять инфраструктурой на расстоянии? Вспомним одну из ключевых парадигм Unix-систем: все необходимые действия с системой можно произвести из командной строки (а значит — и с помощью скрипта). Графические оболочки являются красивым, но опциональным инструментом.

Объединим теперь виртуальные облачные технологии и интерфейс командной строки для всех задач. В результате, ИТ-специалисты получили возможность с помощью текстовых команд создавать необходимые части ИТ-инфраструктуры, включая серверы, системы хранения данных, сетевые компоненты, все интерфейсы между ними, все настройки и конфигурации... Степень автоматизации существенно возросла, равно как и скорость выполнения необходимых изменений. Раньше для разворачивания ИТ-инфраструктуры, основанной на собственном аппаратном обеспечении, требовалось:

- обосновать и согласовать бюджет (недели и месяцы);
- дождаться очередного цикла закупки (месяцы);
- заказать оборудование у поставщика и оплатить его (дни);
- дождаться поставки (недели и месяцы);
- получить, установить, настроить, подготовить к использованию (дни и недели).

Теперь аналогичную по характеристикам ИТ-инфраструктуру можно создать так:

- запустить скрипт, дождаться окончания его выполнения (минуты, редко — часы);
- оплатить счёт облачного провайдера в конце месяца.

То есть, необходимая инфраструктура создаётся с помощью программного кода. И не только создаётся, но и может управляться как программный код — с хранением версий, отслеживанием изменений, отладкой, повторным использованием прошлых наработок и т.д.

В завершение отметим также вторую жизнь, которую получили давно придуманные технологии. К примеру, виртуализация на уровне операционной системы была доступна во многих UNIX-системах ещё в 80-е годы прошлого столетия. Однако, серьёзный коммерческий успех этой технологии, которую

чаще стали называть контейнеризацией, пришёл только во второй половине 2000-х, что совпадает по времени с событиями, описанными ранее. И если изначальный механизм chroot был довольно ограничен по функциональности и возможностям, то сейчас для контейнеров можно изолировать файловую систему, выделять дисковые квоты, ограничивать предоставляемые оперативную память, время процессора, ширину каналов ввода-вывода и т.д.

Неизбежность появления

Рассмотренные истоки возникновения DevOps позволяют сделать следующие выводы.

Во-первых, из-за появления новых способов взаимодействия с основным бизнесом, клиентами, и грамотного применения методов гибкой разработки назрела потребность строить работу и управление информационными технологиями иначе.

Во-вторых, с возникновением новых технологий управления инфраструктурой появилась возможность строить работу ИТ иначе.

Можно предполагать, что появление чего-то, аналогичного DevOps, было лишь вопросом времени.

Задачи, решаемые с помощью DevOps

Методология DevOps призвана решить три вполне конкретные задачи современной ИТ-организации.

Ускорение вывода на рынок

Компании, применяющие DevOps, наиболее часто сообщают о необходимости существенно сокращать время вывода на рынок (англ. Time to market). Под этим термином разные люди подразумевают разное. Часто встречающееся понимание — время от зарождения какой-либо бизнес-идеи до возможности клиенту приобрести новый продукт или получить новую услугу, являющуюся результатом воплощения бизнес-идеи в жизнь. Таким образом, в расчёт (а точнее — в оценку) времени вывода на рынок включается довольно большой промежуток, содержащий в случае необходимости привлечения ИТ-департамента следующие шаги:

- структурирование и первое формальное описание бизнес-идеи, а скорее — нескольких бизнес-идей, их обоснование;
- оценка и выбор бизнес-идеи для реализации;
- планирование необходимых действий для реализации, выделение финансирования;
- подготовка бизнес-процессов и персонала;
- одновременно с этим: формализация требований, разработка прототипа, первичное тестирование, разработка полнофункциональной ИТ-системы, её тщательное тестирование, передача в эксплуатацию, запуск, тиражирование;
- одновременно с этим: маркетинговые активности, подготовка рынка, подготовка механизма и каналов продаж;
- запуск нового продукта или новой услуги.

Описанному процессу присущи некоторые сложности.

Во-первых, его общая длительность может составлять годы, при том, что бизнесу хотелось бы сократить её до месяцев. Бизнес-обоснование здесь прозрачно: за время разработки нового продукта рынок может измениться настолько, что продукт будет уже неактуален, либо конкуренты выпустят аналогичный продукт раньше,

соберут сливки и закрепятся как лидеры. Ранний выход на рынок с привлекательным конкурентным предложением помогает занять доминирующее положение в новых нишах, которое, в свою очередь, даёт лидеру возможности в дальнейшем изменять рынок, подстраивая его под себя. Это существенное преимущество, которым обладают немногие, хотя стремятся к нему все. Кроме того, не следует забывать про всё возрастающую скорость изменений. Одна из наиболее наглядных иллюстраций данного тезиса — закон ускоряющихся возвратов (Law of Accelerating Returns), сформулированный в 1999 году Р. Курцвайлом. Согласно ему, скорость изменений в широком спектре эволюционирующих систем, включая новые технологии, но не ограничиваясь ими, стремится расти экспоненциально. На практике это означает, что прорывы в технологиях, в том числе информационных, случаются всё чаще. Компании, которые *увеличивают* темп изменений, становятся лидерами, а те, кто лишь *могут сохранять* свой быстрый темп, получают возможность не остаться на обочине. Что уж говорить про тех, кто не способен меняться быстро...

Вторая сложность описанного выше процесса заключается в необходимости чёткой координации и согласования взаимозависимых шагов, особенно выполняющихся параллельно. В этот момент многие компании попадают в классическую ловушку: пока нет готового продукта — нечего рекламировать и продавать, однако с появлением такового начало маркетинговых активностей приводит к продажам (а значит — и к финансовой отдаче) лишь с задержкой. Такая ловушка ещё больше увеличивает фактическое время вывода на рынок и требует ещё более аккуратной координации всех исполнителей.

Отметим, что роль традиционного ИТ-подразделения в увеличении срока вывода на рынок трудно переоценить. Действительно, в некоторых организациях из общего календарного времени в 1,5-2 года на ИТ-работы приходится более 50-70%.

Другое понимание термина «время вывода на рынок» менее глобально, но не менее значимо. Динамичные компании, создающие цифровые продукты, привыкли действовать быстро. Скрупулёзному и детальному планированию они предпочитают эксперименты, а слово «идея» заменяют на «гипотезу». В этом случае процесс выглядит примерно так:

- рождение гипотезы, разработка методов оценки её справедливости;
- реализация гипотезы на практике;
- измерение результата, A/B тестирование, сравнение с целевыми значениями;
- корректировка по итогам анализа, переход на первый или второй шаг.

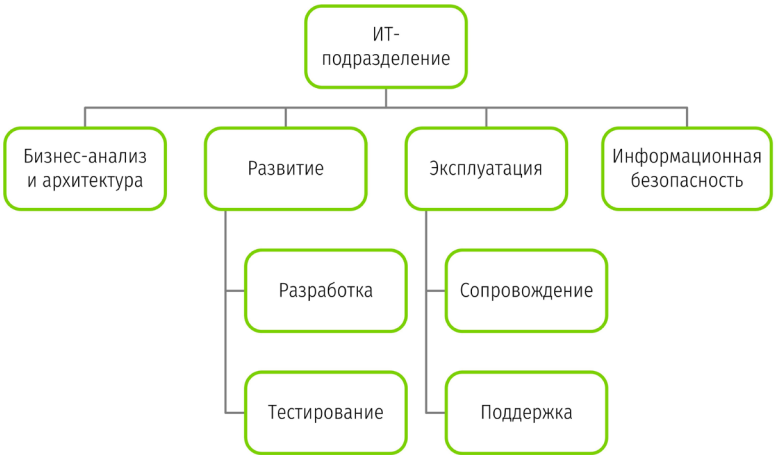
Несложно заметить возникновение цикла, ожидаемая скорость которого — недели. Такой быстрый темп необходим потому, что сама суть движения — в постоянном поиске. На старте, в самом начале, совершенно неизвестно конечное состояние, и, тем более, неизвестна дорога к нему. Долгосрочное планирование не имеет никакого смысла, компания видит лишь следующий, ближайший шаг — точнее, пытается его угадать. Проиллюстрировать данный тезис поможет широко известная метафора, сравнивающая выживание и развитие бизнеса с поиском реки с деньгами (Рис. 4.1.3). Один раз войдя в такую реку, нащупав новую нишу и новые возможности, компании будет необходимо всегда искать изменяющееся русло. При том, что традиционные процессы, регламенты, уже имеющиеся продукты будут с большой вероятностью увеличивать инерцию компании и, оставленные без внимания, приведут к выходу на берег.

Нетрудно догадаться, что вклад ИТ-департамента в замедление приведённого выше цикла высок. Действительно, в создании цифровых продуктов роль ИТ — ключевая, поэтому задержки на этапе реализации гипотезы в наибольшей степени происходят именно благодаря «медленному» ИТ-отделу, предлагающему вместо ожидаемых недель — месяцы.

Рис. 4.1.3. *Река с деньгами.*

Для уменьшения времени вывода на рынок DevOps предлагает множество техник, например: уменьшение размера задач, уменьшение количества передач работы, постоянные поиск и устранение потерь и др. Однако, важно сделать следующее замечание: наивно надеяться, что применение техник DevOps для ускорения работы ИТ-отдела одновременно приведёт к сокращению затрат на ИТ. Скорее, наоборот — расходы на информационные технологии вырастут, что обусловлено, в первую очередь, увеличением численности ИТ-персонала.

Рис. 4.1.4. *Функциональная структура традиционного ИТ-подразделения.*



Деиствительно, традиционная организация ИТ-отдела предполагает наличие отдельных функциональных подразделений, каждое из которых занимается всеми задачами в рамках своей предметной области (бизнес-анализ, разработка и тестирование, эксплуатация, поддержка, развитие и т.д.). При этом, внутри каждого такого функционального подразделения обеспечивается необходимая взаимозаменяемость специалистов, а среднее и большое число специалистов одинаковых квалификации и компетенций позволяют равномерно распределять между ними нагрузку (Рис. 4.1.4).

В отличие от такой схемы, в DevOps деление специалистов производится по командам, и каждая команда работает над своим продуктом. Будучи самодостаточной, команда включает в себя и владельца продукта, и архитекторов, и разработчиков, и тестировщиков, и ответственных за эксплуатацию, и за информационную безопасность (Рис. 4.1.5.). При большом количестве команд, каждая из которых сфокусирована исключительно на своём продукте, равномерность загрузки специалистов обеспечить сложнее, что может приводить к неполной утилизации персонала,

а значит — к повышению расходов на него.

Таким образом, можно утверждать, что традиционная организация ИТ-подразделения больше направлена на оптимизацию затрат (англ. Optimize for cost), в то время как организация по DevOps направлена на оптимизацию скорости (англ. Optimize for speed), и данные цели в общем случае являются разнонаправленными. Отметим также, что DevOps предлагает инструменты и способы ограничения роста затрат, такие как максимальная автоматизация всех рутинных операций, а также взаимозаменяемость в пределах одной команды. Кроме того, адепты DevOps справедливо указывают, что оптимизация скорости во многих случаях направлена на предоставление возможности бизнесу зарабатывать больше, что компенсирует возрастающие расходы на ИТ. В таком случае можно рассуждать об ИТ-отделе, как истинном бизнес-партнёре, а не центре затрат.

Рис. 4.1.5. *Пример состава DevOps-команды.*

Снижение технического долга

Понятие технического долга предложил У. Каннингем в 1992 году . Возникновение такого долга происходит, когда программист выбирает неоптимальный путь решения задачи для того, чтобы сократить сроки разработки. Уорд отмечал, что это естественный процесс, и, собственно, проблема заключается в том, что накапливающиеся неоптимальные решения приводят к постепенному ухудшению результатов разработки, и, как следствие, к деградации продукта. Со временем команда разработки будет вынуждена больше времени уделять исправлению последствий ранее принятых решений, то есть переделке кода, нежели разработке новых функциональных возможностей. Аналогия с финансовым долгом в этом случае является очень наглядной — для ускорения получения результата компания может «влезть в долги», однако, она не должна допускать ситуации, когда вся получаемая прибыль уходит на обслуживание долга.

Мартин Фаулер (Martin Fowler) в дальнейшем развил идею технического долга, предложив условную классификацию причин его возникновения (Табл. 4.1.1).

Его точка зрения в целом повторяет мысль У. Каннингема — в правильно организованной команде разработчиков увеличение технического долга может быть осознанным шагом для получения краткосрочных преимуществ; важно уделять внимание «выплате» этого долга.

В настоящее время понятие технического долга обычно употребляется намного более

Табл. 4.1.1. *Классификация технического долга по М. Фаулеру (источник https://martinfowler.com/bliki/TechnicalDebtQuadrant).*

	Беспечно	Рассудительно
Преднамеренно	*«У нас нет времени на разработку архитектуры»*	*«Мы должны выпустить продукт как можно скорее, осознавая последствия»*
Нечаянно	*«Что такое инкапсуляция?»*	*«Теперь мы знаем, как нам стоило это сделать»*

широко. При расширении его применения на вопросы эксплуатации поднимается целый пласт проблем традиционного ИТ-отдела: устранение сбоев с помощью перезагрузки устройств; установка программной заплатки, не протестированной должным образом; выполнение изменений ИТ-инфраструктуры без тщательного планирования; ручное исправление какого-либо скрипта или настройки сервера без документирования — это лишь отдельные примеры накопления технического долга, который в обычном ИТ-отделе никто никогда не будет «выплачивать». Некоторые ИТ-организации даже не планируют таких работ или проектов, другие тешат себя иллюзиями наведения порядка, как только для этого появится свободная минута — разумеется, свободной минуты в современном ИТ-подразделении не появляется.

Более того, можно утверждать, что некоторые общеизвестные практики, предлагаемые библиотекой ITIL, будучи применёнными неграмотно или изолированно, могут также приводить к увеличению технического долга. Например, процесс управления инцидентами, согласно ITIL, не имеет цели поиска и устранения причин возникновения сбоев. Его задача — скорейшее восстановление работы ИТ-системы (или ИТ-услуги, не принципиально), в т.ч. с помощью применения обходных, временных решений. Применение таких решений практически гарантирует повторение сбоев, а значит — новые затраты ИТ-организации на повторное их устранение. Авторы ITIL предполагали, что параллельно процессу управления инцидентами в организации будет работать процесс управления проблемами, чья задача — поиск и устранение корневых причин возникновения инцидентов: по сути, снижения технического долга в его широком понимании. Однако заметим, что в большинстве современных ИТ-отделов есть хоть как-то работающий процесс управления инцидентами, в то время как увидеть в дикой природе процесс управления проблемами наоборот, крайне сложно.

DevOps уделяет пристальное внимание вопросам снижения технического долга, а точнее — управлению им. Для примера можно привести две часто применяемые практики. Во-первых, постоянно выполняемый рефакторинг программного кода позволяет учитывать полученный при эксплуатации опыт, а работы по устранению ранее допущенных (осознанно или случайно) узких мест планируются наравне с созданием новой функциональности. Во-вторых, DevOps настоятельно рекомендует применять практику «проблемные шаги повторять как можно чаще», чтобы не допускать «застаивания» проблем, о которых все знают, но ни у кого не доходят руки их устранить.

Устранение хрупкости

Как уже упоминалось ранее, ИТ-инфраструктура большинства организаций находится в весьма шатком состоянии. Это обусловлено многими причинами, действующими в совокупности:

- технические решения создавались постепенно, годами, из разных составляющих;
- применяются большие системы сторонней разработки, сильно кастомизированные под задачи данной компании;
- применяются системы собственной разработки, при том, что и ключевые программисты, и команды целиком уже могут в компании не работать;
- настроено большое количество разнообразных интеграций систем между собой, а также с внешними источниками и потребителями данных;
- применяемые решения, не всегда опти-

мальны ввиду необходимости ускорения их реализации, а также ограничений бюджета;

- текущие работы по эксплуатации и поддержке добавляют временных, обходных решений, «костылей», только чтобы всё это продолжало работать дальше;
- документирование программного кода, архитектуры, инфраструктуры, технических решений и даже контрактных обязательств оставляет желать лучшего.

Дж. Ким, Дж. Хамбл, П. Дебуа и Дж. Виллис отмечают («The Devops Handbook: How To Create Worldclass Agility Reliabil-ity And Security In Technology Organizations», G. Kim, J. Humble, P. Debois, J. Willis, 2016, ISBN 978-1-942-78800-3, раздел «Downward Spiral In Three Acts»), что, по злой иронии, наиболее хрупкими являются именно те системы и приложения, от которых бизнес зависит в наибольшей степени, и которые приносят ему максимальную пользу. Уменьшать хрупкость таких систем крайне сложно ввиду больших рисков нарушения работы бизнеса, недопустимости простоя, а также постоянного потока новых изменений и доработок, связанных именно с этими системами.

Но и продолжать работать с такой неустойчивой инфраструктурой опасно для карьеры ИТ-руководителей и ИТ-менеджеров. Кроме того, помимо долгосрочных нависающих неприятностей, есть и оперативные сложности — внесение любых изменений является риском, а потому необходимы соответствующие инструменты его снижения: долгое и тщательное обоснование необходимости, планирование, согласование и утверждение, проработка, тестирование и, наконец, выполнение. Всё это существенно замедляет выполнение изменений, а также негативно отражается на способности ИТ-организации к инновациям.

DevOps предлагает бороться с хрупкостью ИТ-систем самым радикальным образом — путём её тотального устранения. В традиционной парадигме новый программный код находится в нерабочем состоянии до тех пор, пока тестирование не докажет его работоспособность. В DevOps, напротив, и код, и система в целом в любой момент времени полностью работоспособны, и, если очередное изменение нарушает такую работоспособность, оно немедленно откатывается назад — система же продолжает работать исправно.

В своей книге «Антихрупкость: как извлечь выгоду из хаоса» («Antifragile: Things That Gain from Disorder», N. Taleb, 2012, ISBN 978-1400067824) Н. Талеб рассуждает об особенностях сложных систем и вводит следующую классификацию: хрупкие системы, устойчивые системы и антихрупкие системы. Приведённое разделение помогает выбрать принципиальный подход к работе: хрупким системам в первую очередь нужна стабильность, их нужно как можно реже менять, а изменения тщательно проверять как до, так и после вмешательства. Устойчивые системы проектируются с учётом присущей им сложности и хрупкости, в них закладываются механизмы отказоустойчивости и выживания, позволяющие в процессе эксплуатации и при изменениях меньше беспокоиться о возможных негативных последствиях. Но наиболее совершенны так называемые антихрупкие системы, улучшающиеся при столкновении со сбоями и беспорядком (то есть — с реальностью корпоративных информационных технологий).

Одна из замечательных практик DevOps, связанная с антихрупкостью — намеренное внесение хаоса и нестабильности в среду эксплуатации. Такая техника известна под разными названиями: игровой день (англ. Game Day), обезьяна хаоса (англ. Chaos Mon-

key), армия обезьян (англ. Simian Army), но суть сохраняется без изменений. Специально разработанные программные средства нарушают работу ИТ-систем, серверов, систем передачи и хранения данных и т.д. — случайным образом в неизвестные заранее моменты времени. Целевые ИТ-системы должны в ответ самостоятельно и максимально оперативно обнаруживать неисправность и восстанавливать свою работоспособность, в идеале таким образом, чтобы конечный пользователь ничего не заметил, а данные, разумеется, не были утеряны. Такую технику можно попробовать использовать и в традиционном ИТ-отделе, однако, во многих компаниях она может привести к полному блокированию работы бизнеса.

Итак, рассмотрены три основные задачи, которые ставятся перед DevOps: уменьшение времени вывода на рынок, снижение технического долга и устранение хрупкости. Решение каждой из них по отдельности способно дать существенные преимущества современному бизнесу, но три вместе представляют собой мощный драйвер изменений. Рассмотрение каждой из задач завершалось коротким упоминанием практик DevOps, помогающих в достижении соответствующих целей. Заметим теперь, что само по себе применение указанных практик не приведёт к решению обозначенных задач, этого недостаточно. Необходимо самым серьёзным образом менять *культуру работы* ИТ-организации, чтобы изменились не только применяемые инструменты, приёмы и техники, но и *отношение ИТ-персонала* к ключевым вопросам работы компании: роли заказчика, ценности информационных технологий, толерантности к известным недостаткам, необходимости постоянного совершенствования. Слепое применение идей DevOps — например, «*давайте построим конвейер, ведь без него DevOps не бывает*» — с большой вероятностью приведёт к явлению, известному как ***культ карго*** (англ. Cargo cult).

Некоторые частые заблуждения

Важно рассмотреть некоторые, наиболее часто встречающиеся, заблуждения относительно понятия DevOps. Это поможет яснее очертить границы явления и позволит перейти к рассмотрению следующих, более специфичных вопросов. Не имея задачи по наиболее полному охвату всех встречающихся недопониманий, для данного раздела были отобраны именно те из них, которые помогают понять, *что такое DevOps* с управленческой точки зрения, путём сравнения с тем, *чем DevOps не является*.

DevOps — это часть Agile

Любители современных подходов к разработке программного обеспечения иногда заявляют, что DevOps — не более, чем продолжение идей Agile. В основе такого ограниченной картины мира лежит тот факт, что гибкая разработка позволяет отлично выстроить отношения с бизнесом в части понимания его требований к программному продукту, а также достаточно быстро выдать такой программный продукт. Давняя проблема «*Что с готовым продуктом делать, чтобы он приносил пользу, и как его, собственно, эксплуатировать*» теперь имеет решение: у нас есть DevOps! Там и будут кем-то найдены ответы на эти неудобные вопросы.

Это, безусловно, очень ограниченный взгляд на DevOps, минимум по трём причинам. Во-первых, основываясь в существенной мере на Agile, DevOps, тем не менее, расширяет идеи гибкой разработки до гибкого ИТ-производства в целом — на всю организацию, на весь процесс, на всю цепочку создания ценности. Во-вторых, получение отдачи от DevOps требует более значительных культурных изменений в компании, чем это обычно происходит при применении Agile. В-третьих, задачи, которые ставятся перед DevOps, не ограничиваются лишь ускорением поставки — есть также необходимость снижения технического долга и устранения хрупкости.

DevOps — это автоматизация и инструменты

Другая точка зрения сводится к слову «автоматизация». Программных инструментов, помогающих работать современному ИТ-отделу, в последние годы развелось великое множество — они исчисляются сотнями. Многие вендоры будет уверять вас, что именно они и есть DevOps, либо что их инструменты тот самый DevOps обеспечат.

Маркетинговое давление вендоров очень велико. К ним уже присоединились большие компании, с большими целями по выручке и соизмеримыми бюджетами на рекламу. Многие могут заметить прямую аналогию с историей двадцатилетней давности с программным обеспечением по управлению ИТ-услугами — тогда производители ПО тоже вовсю заявляли, что ITSM — это программное обеспечение, надо только его инсталлировать, и процессы появятся сами собой. Лишь немногие видят и всерьёз обсуждают что-то за пределами ПО.

DevOps, действительно, зависит от наличия и работоспособности определённых инструментов автоматизации. Но, строго говоря, минимальный набор таких инструментов сводится к системе контроля версий для хранения всех исходных кодов и данных о конфигурации ИТ-инфраструктуры, плюс к системе автоматизации конвейера поставки ПО. Всё остальное, как принято говорить, можно добавить по вкусу. В то время как отдельные программные пакеты широко распространены, универсального списка программных инструментов DevOps, обязательных к применению, нет и быть не может.

DevOps — это новая профессия

Следующий вариант подсказывают нам кадровые агентства и сайты размещения объявлений о работе. DevOps — говорят они — это универсальный солдат, способный и код писать, и тесты создавать, и среды разворачивать, и с ИТ-инфраструктурой управляться. То есть, он может эффективно выполнять работу и программиста, и поддержки, получая при этом только одну зарплату.

Другой часто встречающийся случай — это подмена известной древней профессии «системный администратор» на более модную «DevOps-инженер». В таких вакансиях уже из описания становится понятно, что речь вовсе не о DevOps.

Третий случай — DevOps-гуру, который необходим для «внедрения» этого DevOps в конкретной компании. Примерно, как Agile-коуч или Scrum-мастер.

Всё это, разумеется, серьёзные заблуждения. DevOps — глубокое изменение основ работы ИТ-подразделения, которое невозможно выполнить, наняв некоторое количество DevOps-инженеров или пригласив DevOps-гуру. Умение построить технический конвейер поставки ПО не гарантирует успеха. Сэкономить финансовые ресурсы, применяя практики DevOps, скорее всего не получится, как было показано ранее.

Принципы DevOps

Словом «принципы» обозначим ключевые идеи, на которых базируется весь DevOps, без принятия и применения которых от DevOps остаётся совсем мало смысла.

Под «практиками» будем понимать действия, выполняемые в соответствии с принципами, направленные на получение полезного эффекта.

Принципы будут неизменны для любой организации, применяющей идеи DevOps, в то время как практики, скорее всего, будут выбраны и видоизменены в зависимости от конкретной ситуации, компании и решаемых задач.

Все основные принципы, описываемые международными экспертами DevOps, приведены далее.

Поток создания ценности

Одно из ключевых понятий DevOps, заимствованное из бережливого производства — поток создания ценности (англ. Value Stream). Это понятие используется довольно давно, однако, по мере расширения его применения к решению практических задач, появляются новые издания, достаточно полно рассматривающие поток с прикладной точки зрения.

Можно рекомендовать следующие издания для знакомства с Value Stream:

M. Rother, J. Shook, «Learning to See: Value-Stream Mapping to Create Value and Eliminate Muda», Lean Enterprise Institute, 2009, ISBN 978-0966784305

K. Martin, M. Osterling, «Value Stream Mapping: How to Visualize Work and Align Leadership for Organizational Transformation», McGraw-Hill, 2014, ISBN 978-0071828918

Считается полезным рассматривать работу организации с точки зрения создания ценности в ответ на запрос потребителя. Действия, выполняемые для реализации запроса, выстраиваются в последовательность, называемую потоком создания ценности. Обычно, в организации обрабатывается множество различных запросов. В то же время, традиционная организация работает над несколькими продуктами или услугами. Таким образом, и потоков создания ценности в компании много.

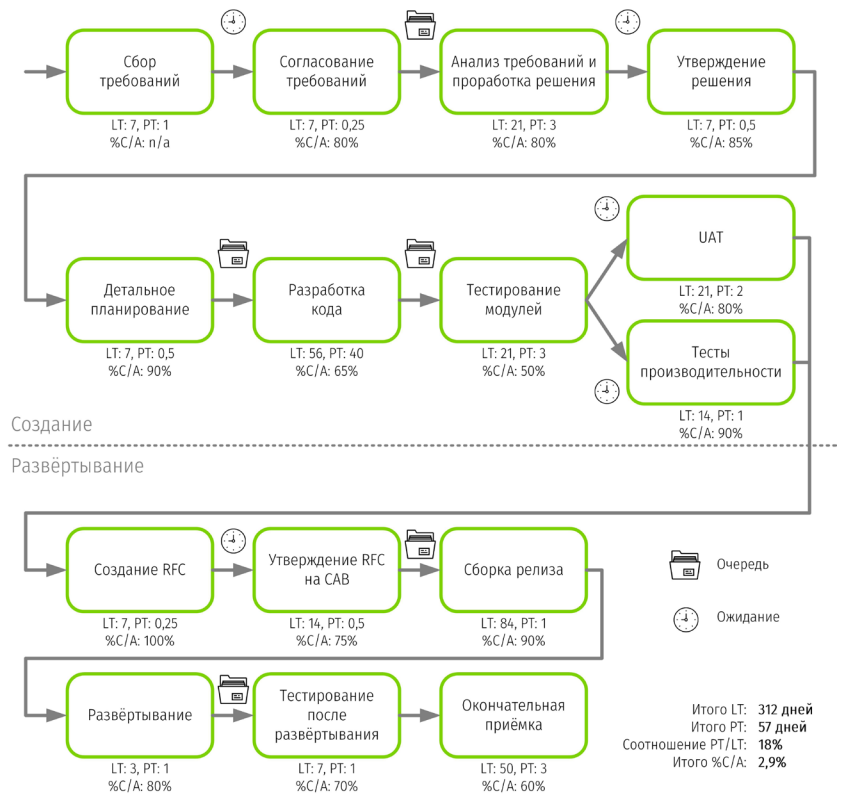
Работа по моделированию потока называется ***картированием*** (англ. Value Stream Mapping). Она начинается с выбора одного из продуктов: иногда с того, где руководству видятся наибольшие возможности по оптимизации, а иногда с того, где коллективу представляется возможным быстро добиться существенных улучшений, заодно изучив данную технику. Построение выполняется в два шага: сначала создаётся картина «как есть», затем — «как будет». Проработка будущего состояния важна по двум причинам. Во-первых, она помогает избежать локальной оптимизации, о которой будет сказано чуть позже. Во-вторых, понимание целевого состояния позволяет запустить механизм совершенствования, максимально приближенный к реальности, с чётким (насколько это возможно) направлением улучшений.

Собственно, упражнение по картированию потока выглядит несложным: необходимо определить ключевые шаги обработки запроса, для каждого указать суть выполняемой работы, выстроить данные шаги в последовательность получения полезного результата. Одна из возникающих трудностей — излишняя детализация блоков, когда общая схема не помещается на один лист. Авторы книг, упомянутых

выше, в качестве ориентира рекомендуют ограничиться пятнадцатью блоками, иначе дальнейшая работа с картой будет осложнена. Вторая трудность — договориться участникам упражнения о том, какие же именно шаги, как и кем выполняются. В некоторых организациях отсутствует общее понимание процесса, что приводит к многочасовым спорам.

Составив схему, можно приступить к наполнению её важными подробностями. Возможно, будет полезно добавить названия задействованных исполнителей. Не лишним также станет указание мест, где накапливаются очереди объектов, ожидающих обработки, а также места, где задержки возникают по причине ожидания какого-либо календарного события — например, ежемесячной встречи по рассмотрению запросов на изменения или ежеквартального рассмотрения скорректированного бюджета. Наконец, наиболее ценная информация — три метрики для каждого шага потока, а именно: ***время выпуска*** (англ. Lead Time, LT), ***время обработки*** (англ. Process Time, PT) и ***доля работ, выполненных без ошибок*** (англ. Percent Complete and Accurate, %C/A). Определение значений данных метрик на практике представляет собой большую сложность для организации, не имеющей инструментов и практики измерения подобных показателей. Группа сотрудников, выполняющая картирование, может занижать временные показатели, если обсуждаемые значения кажутся ей излишне высокими. Иногда, напротив, группа может вспоминать крайние случаи, когда отдельный запрос или запросы обрабатывались слишком долго, пытаясь таким образом завысить значение времени выпуска. Ещё хуже дело обстоит с показателем %C/A, так как его значение для каждого шага, как правило, не известно и может быть лишь оценено. Важно помнить, что для составления схемы «как есть» следует опираться именно на текущее состояние дел, а не описанное в каких-либо регламентах, существующее в фантазиях руководителей или применимое лишь для исключительных случаев. Абстрактный пример карты потока создания ценности приведён на Рис. 4.1.6.

Рис. 4.1.6. *Пример карты потока создания ценности.*



Зачем же нужно картирование потока и почему этот поток так важен для DevOps?

Во-первых, само упражнение по созданию карты и полученные значения ключевых метрик действуют на участников процесса очень отрезвляюще. Как правило, многие понимают, что при текущей организации деятельности есть точки неэффективности, однако, никто не догадывается о масштабах бедствия, тем более в цифрах. В приведённом выше примере соотношение продуктивного времени, потраченного на получение полезного результата (создание ценности), составляет лишь 18% от общего затраченного календарного времени. Данное значение приведено не в отрыве от реальности — в обычных ИТ-подразделениях получаются примерно такие числа. Ещё хуже дело обстоит с показателем %C/A, если в организации есть привычка отправлять обратно на предыдущие шаги задачу, которая была сделана не точно, не до конца или не в соответствии с заданием.

Во-вторых, наглядное представление деятельности позволяет концентрироваться на создаваемой ценности, а не на выполняемой работе. Сотрудникам и руководителям намного заметнее и понятнее ежедневные задачи, которые они решают (ответ на вопрос «что?»), в то время как получение полезного результата ускользает от внимания (ответ на вопрос «зачем?»).

В-третьих, карта потока создания ценности даёт возможность искать и устранять узкие места, избегая при этом ловушки локальной оптимизации — расходов времени и усилий по устранению затруднений, которые не дадут эффекта вовсе, либо полученный эффект будет незначительным. В соответствии с теорией ограничений, предложенной Илияху Голдратом (https://tocinstitute.org/theory-of-constraints.html), в любой системе в один момент времени есть одно и только одно действительно узкое место, замедляющее работу, и усилия, потраченные не на его устранение — потрачены впустую. Таким образом, с потоком можно работать как с единой системой. Очевидные вопросы после выполнения картирования, которые требуют осмысления, анализа и действий, следующие:

1. [%C/A] Почему на участках работы получены значения %C/A, отличные от 100%, и каким образом можно добиться полного отсутствия ошибок при передаче работы с одного участка на другой (и, таким образом, потерь времени и ресурсов на переделку работы)?

2. [LT] На что именно расходуется время выпуска, помимо создания полезного результата, и каким образом можно радикально уменьшить простои в очередях и ожидании?

3. [PT] Какие есть возможности изменения практик работы, позволяющие уменьшить время обработки на каждом из участков?

Следует отметить, что подобная работа по оптимизации не должна сводиться исключительно к анализу карты «как есть» и попыткам улучшения связанных с ней метрик. Напротив, необходима разработка карты «как будет», возможно, принципиально отличающейся от текущей схемы работы. Именно здесь появляются возможности применения инструментов и практик DevOps, изменяющих существующее положение вещей.

> Английские слова «***Stream***» и «***Flow***» зачастую переводятся на русский язык одинаково как «поток», в то время как существует, пусть сложно различимая, но всё же разница между этими понятиями. Для её подчёркивания в настоящем издании ***«Flow» переводится как «течение»***

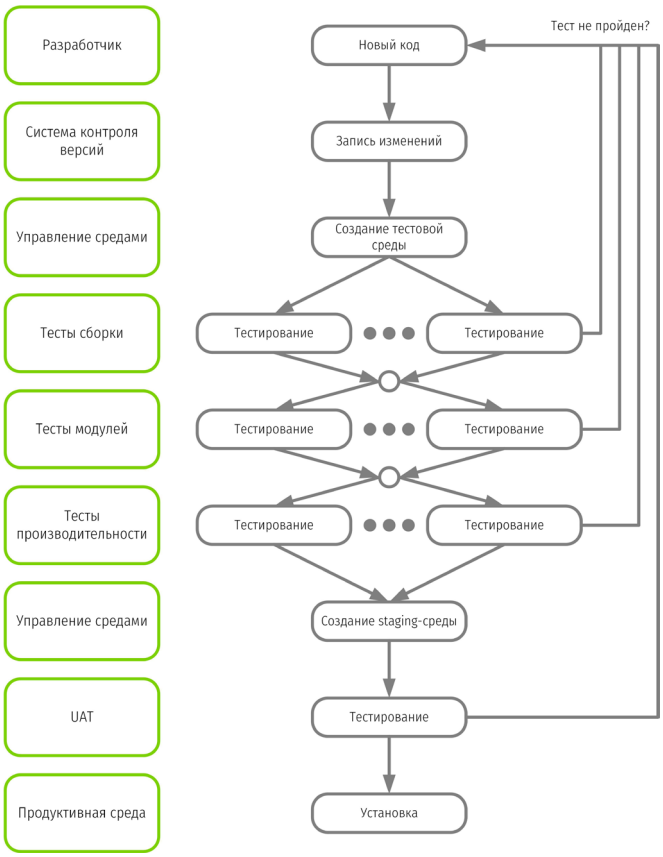
И, наконец, в-четвёртых, осознание потока создания ценности позволяет реализовать одну из основных идей DevOps — плавное и равномерное течение (англ. Flow) работы от участка к участку, позволяющее создавать результаты постоянно, ритмично, без лишних задержек и с оптимальной загрузкой ресурсов.

Конвейер развёртывания

Понимание потока создания ценности — необходимый и важный шаг на пути к DevOps. Однако, работа с потоком «на бумаге» не даёт столь значительных результатов, как ожидается. Необходимость построения чего-то, подобного конвейеру, наглядно иллюстрируется следующим примером: засеките время, которое необходимо для того, чтобы эффект от одной новой строчки программного кода в любом из ваших приложений появился в среде эксплуатации. Если измерения покажут результат в днях, неделях или месяцах — ваш поток создания ценности нуждается в серьёзном пересмотре. Помочь такому пересмотру призван конвейер развёртывания, под которым понимается максимально автоматизированное сопровождение изменения по всем шагам потока создания ценности, начиная с момента «Разработка завершена» вплоть до состояния «Развёрнуто в среде эксплуатации».

Работа конвейера может быть проиллюстрирована схемой (Рис. 4.1.7).

Рис. 4.1.7. *Работа конвейера развёртывания.*



Конвейер автоматически запускается после того, как разработчик разместит в системе контроля версий новую часть программного кода, при этом фиксируется: кто, когда и какое изменение внёс. По факту, новой записи автоматически создаётся необходимая временная тестовая среда, в которой последовательно запускаются заранее разработанные тесты. Логика размещение тестов проста: проверки, обеспечивающие выявление большинства потенциальных ошибок, располагаются максимально ближе к началу конвейера. Все тесты, требующие ручного труда (если таковые имеются), размещаются в конце конвейера. Невозможность прохождения какого-либо теста приводит к предоставлению разработчику обратной связи и остановке конвейера для данного изменения. Чтобы запустить конвейер вновь, разработчик должен исправить программный код. Помимо создания тестовой среды, возможно автоматическое создание других необходимых для конвейера сред. После использования ресурсы, занятые под эти среды, автоматически освобождаются. Разумеется, возможно

параллельное исполнение нескольких тестов, если это допускается логикой тестирования и исключает непродуктивную загрузку ресурсов на тестирование изменений, которые могли бы быть отброшены на предыдущих шагах конвейера.

Таким образом, конвейер позволяет решить четыре важные для DevOps задачи. Во-первых, конвейер экономит ресурсы, не задействуя следующие шаги при непрохождении предыдущих. Во-вторых, конвейер обеспечивает качество продукта — изменения, нарушающие функциональность, не доходят до установки в среду эксплуатации, и система всегда находится в рабочем состоянии (об этом будет дополнительно сказано позже). Под качеством в данном случае понимаются все вопросы, связанные с функциональностью, производительностью, доступностью, безопасностью и т.д. В-третьих, конвейер ускоряет доставку изменений до среды эксплуатации за счёт максимально возможной автоматизации каждого из шагов. Наконец, в-четвёртых, работа конвейера постоянно «оставляет следы» в журналах аудита, что позволяет обеспечить контроль всех проводимых изменений, а также снимать точные измерения на разных участках работы конвейера, предоставляя ценные данные для его оптимизации.

С построением эффективно работающего конвейера развёртывания на практике возникают следующие сложности:

1. Чрезмерное увлечение автоматизацией в ущерб идеологии (процессы, персонал, культура) приводит к созданию замечательно автоматизированных конвейеров, которыми никто не будет пользоваться. Решение очевидно: DevOps — это не только автоматизация, и это должен понимать каждый участник команды.

2. В исходном состоянии для устойчивой работы конвейера нет достаточного количества разработанных ранее тестов. В такой ситуации иного решения, как увеличивать покрытие кода тестами быть не может — накопленный технический долг придётся рано или поздно выплачивать.

3. В целевом состоянии тестов становится так много, что прохождение изменения по конвейеру занимает очень долгое время и требует очень больших вычислительных ресурсов, что особенно актуально при большом потоке небольших изменений. Компании, столкнувшиеся с данной проблемой, активно применяют ***анализ влияния тестирования*** (англ. Test Impact Analysis). За немного некорректным, но уже устоявшимся названием скрывается практика, при которой по особым меткам, а также с использованием средств искусственного интеллекта, система тестирования выбирает из всего многообразия тестов те, которые относятся к предлагаемому изменению, не выполняя оставшиеся тесты.

С построением конвейера развёртывания связаны ещё три важных для DevOps понятия: непрерывная интеграция, непрерывная поставка и непрерывное развёртывание (англ. Continuous Integration, Continuous Delivery и Continuous Deployment). Существуют их разные трактовки; следующее далее описание опирается на точку зрения экспертов, стоявших у истоков данных понятий.

Под ***непрерывной интеграцией*** принято понимать процесс постоянной сборки программного кода; «непрерывно» же означает, что сборка производится каждый раз, когда какой-либо разработчик размещает очередное изменение в системе контроля версий. Обычная практика разработки программного обеспечения подразумевает

множество отдельных веток программного кода, в которых различные программисты и команды довольно продолжительное время (дни, недели и месяцы) трудятся над созданием новой функциональности. По завершении своей части разработки, или, что ещё хуже, после ожидания, когда все команды, работающие над одним продуктом, завершат разработку, начинается болезненный процесс сборки всех наработок в единую базу программного кода. Так как программистов много, работают они в целом асинхронно, каждый над крупными изменениями, да ещё и долгое время, то процесс сборки сам по себе является трудоёмкой задачей, занимающей несколько недель. Действительно, необходимо учесть все изменения, сопоставить их друг с другом, обновить тесты с учётом изменений и сопоставления, переписать частично или полностью некоторую уже разработанную функциональность, и всё это повторять до тех пор, пока новый код не будет приведён в рабочее состояние. Сборка — важный этап разработки ПО, являющийся, по сути, первым тестом. От того, случилась сборка или нет, зависят дальнейшие работы.

Непрерывная интеграция, впервые описанная в книге К. Бека «Объясняем экстремальное программирование», заключается в упрощении сборки и превращении её в рутину. Ожидается, что программисты будут работать в минимальном числе веток, в идеале — в общей единой базе программного кода. Также подразумевается, что разработчики вносят минимальные изменения, порционно, каждое из которых несёт небольшой риск, но тут же запускает процесс сборки — таким образом, каждый программист размещает свои наработки в системе контроля версий минимум один раз в день. Первичное тестирование, выполняемое автоматически при каждой сборке, позволяет сразу же выявить ошибки и исправить их незамедлительно, что позволяет поддерживать систему всегда в рабочем состоянии.

Непрерывная поставка, подробно описанная Д. Хамблом в одноимённой книге, расширяет идею непрерывной интеграции: каждое сохранение изменений программного кода в системе контроля версий запускает не только процесс сборки, но весь конвейер развёртывания. Таким образом, все изменения, не прошедшие полное тестирование, не принимаются и требуют немедленного исправления. А все безошибочные изменения приводят систему к состоянию полной готовности развёртывания в среду эксплуатации.

Непрерывное развёртывание заключается в переходе от состояния «система всегда готова к развёртыванию с учётом всех выполненных изменений» к состоянию «любое изменение незамедлительно разворачивается в среде эксплуатации». Переход к непрерывному развёртыванию, в частности, требует переопределения понятия «релиз»: теперь не ИТ-, а бизнес-подразделение решает, когда будет доступна та или иная функциональность. Технически, функциональность уже присутствует в среде эксплуатации, сразу по факту завершения разработки и тестирования, но её активация может быть выполнена дополнительно через программные настройки, или флаги, тогда, когда это будет нужно, скажем, отделу маркетинга. Такая практика работы называется теневыми релизами (англ. Shadow Release) или тёмными запусками (англ. Dark Launches).

В любом случае, в основе данных практик — тот самый конвейер развёртывания, описанный выше.

Всё должно храниться в системе контроля версий

Современных разработчиков программного обеспечения не удивить системами контроля версий. Первые такие инструменты, называвшиеся системами хранения исходного кода, появились ещё в 1970-х годах. Сегодня сложно встретить программиста, не знакомого с Git, Subversion или Mercurial. Да что программисты — многие web-мастеры размещают в таких системах не только исходный код, но и копии среды эксплуатации, например, для интерпретируемых Интернет-систем или web-сайтов.

DevOps, как и во многих других областях, расширяет применение таких систем. Речь идёт о хранении не только исходного кода, но абсолютно всего, связанного с ИТ-системой: тестов, скриптов создания и модификации баз данных, скриптов сборки, скриптов создания сред (включая среду разработки), скриптов развёртывания, артефактов, используемых библиотек, создаваемой документации, конфигурационных файлов, даже средств разработки, компиляторов, IDE и прочих инструментов. Перед каждым элементом приведённого списка уместно поставить дополнение «всех»: всех тестов, всех скриптов и так далее. Исключение делается только для двоичного кода, являющегося результатом компиляции программы, по следующим соображениям: обычно код занимает значительное место (что существенно, если он пересоздаётся после каждого изменения) и может быть воссоздан при наличии в системе хранения версий всего остального.

Данный принцип позволяет иметь беспрецедентный уровень контроля за всеми составляющими частями работающей системы, недостижимый при использовании других инструментов. Разумеется, применение такого принципа требует изменения культуры работы с информацией и конфигурациями.

Одним из следствий его применения является возможность установить: что, когда и кем было изменено. Другая важная возможность — способность восстановить систему на любой момент времени в прошлом, в том числе вернуть «сломанную» систему в гарантировано рабочее состояние с минимальными трудозатратами.

Автоматизированное управление конфигурациями

Развивая далее принцип, описанный в предыдущем разделе, DevOps полностью перестраивает работу со средой эксплуатации (впрочем, равно как и с любыми другими средами). Традиционная практика многих компаний такова: новый сервер создаётся из заранее подготовленного образа, затем администратор вручную производит его настройку, устанавливая и конфигурируя дополнительные пакеты программного обеспечения, как системные, так и прикладные. В случае необходимости изменения состава пакетов или их конфигураций, администратор под своей учётной записью подключается к серверу и вручную производит необходимые настройки.

В мире DevOps такая практика работы полностью исключена: любые изменения любой среды могут выполняться только скриптами, располагающимися в системе контроля версий. Например, если с завтрашнего дня в тестовой среде необходимо иметь новую библиотеку, то администратор должен исправить скрипт создания тестовой среды, протестировать его работу и разместить его в системе контроля версий. Создание сред выполняется автоматически при работе конвейера развёртывания.

Многие описанные ранее отличия DevOps от обычной практики касались, в первую очередь, разработки и тестирования, и лишь

иногда затрагивали интересы эксплуатации. Этот же принцип требует полной перестройки практики работы отделов ИТ-поддержки и ИТ-сопровождения. Действительно, теперь администраторы не имеют права что-то менять в среде эксплуатации, за которую они отвечают, привычными им способами.

При использовании управления конфигурациями по DevOps получаются те же преимущества, что и от контроля версий, но в первую очередь — для ответственных за эксплуатацию. Теперь все изменения контролируются, систему можно быстро восстановить до рабочего состояния, знания с уходом ключевого персонала не будут утеряны, и так далее.

Некоторые апологеты DevOps настолько рьяно защищают такую практику работы, что предлагают устанавливать и тщательно настраивать системы тотального аудита ИТ-инфраструктуры для выявления несанкционированных изменений на любом участке с последующим немедленным увольнением персонала, позволившего себе вручную настроить какой-либо сервер или элемент сети. Для небольшого и среднего размера компаний, возможно, данная практика выглядит чрезмерной, однако, если у вас тысячи серверов и сотни инженеров, то другого пути обеспечения стабильности, качества и скорости может и не найтись.

Отдельные команды идут ещё дальше: автоматизированные системы регулярно изменяют административные пароли для доступа к разным средам, не сообщая новые пароли ИТ-сотрудникам. Таким образом обеспечивается отсутствие несанкционированных изменений в среде эксплуатации, хотя это правило действует для любых сред: разработки, тестирования, стабилизации и пр.

Определение завершения

Традиционное отношение любого обычного сотрудника к выполняемой работе можно условно обозначить фразой: «Я свою работу сделал, я молодец». Действительно, именно за выполнение своей трудовой функции сотрудник и получает заработную плату. Аналитик разработал функциональные требования — его работа завершена. Разработчик написал программный код — выполнил свою часть общего дела. Тестировщик протестировал — завершил свою часть, и так далее. Однако, в DevOps всё совсем не так.

Один из ключевых принципов: работа завершена не тогда, когда кто-то сделал свой объём, а когда заказчик получил или начал получать ту ценность, на которую рассчитывал. Это означает полное прохождение всего потока создания ценности вплоть до среды эксплуатации, только тогда работа будет считаться завершённой.

При достаточной очевидности данного принципа, следование ему не появляется само собой и требует управленческих усилий. Такие усилия в дальнейшем позволяют получить следующие преимущества:

1. Команда фокусируется не на выполнении работы (*что делаем*), а на результатах, ценности для клиента (*зачем делаем*).

2. Ограниченная ответственность за отдельные участки работы («*к пуговицам претензий нет?*») размывается, заменяясь коллективной ответственностью за общий результат команды («*костюм должен сидеть*»).

Радикально настроенные адепты DevOps настаивают на более жёстком определении завершения. Они предлагают использовать принцип, при котором создание новой функциональности завершено тогда, когда приложение работает в среде эксплуатации и все действия по сборке, тестированию и развёртыванию выполнены автоматически.

Обзор ключевых отличий DevOps-практик от традиционных

Сравнение DevOps-практик с условными «традиционными» практиками через подчёркивание отличий поможет уловить самое важное.

Релиз — это рутина

В обычной работе ИТ-отдела каждый релиз — это большая проблема. В релиз, как правило, включается множество изменений, связанных со множеством запросов заказчиков. Туда же добавляются изменения со стороны самого ИТ-отдела — то, что необходимо сделать, чтобы системы продолжали работать или работали ещё лучше (стабильнее, безопаснее, быстрее и так далее). Проверить такой большой релиз — отдельная задача, требующая внимательности, времени, привлечения множества специалистов. Все знают, что для любого релиза что-то обязательно пойдёт не так, поэтому ИТ-сотрудники:

- разрабатывают специальные документы, описывающие изменения (забывая при этом часть из них);
- готовят дополнительные резервные копии (для больших систем занимающие много места и долгое время, создавая дополнительную нагрузку на системы и сети, и всё равно кто-то забудет положить в них важные файлы);
- планируют специальные действия и разрабатывают пошаговые инструкции по возвращению системы, если это возможно, в исходное состояние, когда что-то пойдёт не так (особенно интересны случаи, когда релиз частично «установился», а частично — нет);
- ищут время в согласованном календаре изменений, позволяющем остановить работу системы — планово, если всё пройдёт хорошо, либо экстренно, если что-то пойдёт не так (такое время обычно находится в ночь с пятницы на понедельник);
- только после этого распространяют релиз, выполняя довольно большое число действий вручную (и не фиксируя промежуточные результаты).

В зависимости от тщательности проработки каждого из пунктов данного списка, длительность всего развёртывания может варьироваться от нескольких дней до нескольких недель. Количество бессонных ночей администраторов и разработчиков зависит от размера релиза, состояния ИТ-системы и усилий по подготовке и распространению релиза.

В DevOps релиз — это рутина. Релизы выполняются еженедельно, а то и ежедневно. Разумеется, для этого необходимо кардинально уменьшить размер вносимых изменений, но не только: также необходимо самым радикальным образом пересмотреть практику выполнения работ по подготовке и распространению релизов. Вспомним конвейер и практики непрерывной интеграции и непрерывной поставки — они позволяют документировать все изменения в системе контроля версий, большинство операций сделать с помощью автоматизированных средств, учесть в журналах все проведённые изменения, сразу же настроить мониторинг новых и изменённых компонентов. В случае каких-либо неполадок при развёртывании конвейер автоматически прекратит распространение, откатит назад уже внесённые изменения и оповестит команду для принятия мер.

Выпуск релиза — решение бизнеса

Строго говоря, в предыдущем разделе слово «релиз» используется не совсем корректно. Дело в том, что релиз в ITSM и релиз в DevOps — понятия различные. Для классического

ИТ-менеджмента релиз — совокупность нескольких изменений, распространяемых в среде эксплуатации совместно. В то время как в DevOps релиз — это включение новой функциональности, чтобы она полностью или частично стала доступна пользователям. Более правильно в предыдущем разделе вместо слова «релиз» применительно к DevOps использовать слово «поставка», однако, оно ещё не так хорошо вошло в русскую речь, потребуется ещё несколько лет, чтобы сделать его таким же привычным, как «релиз».

Итак, в обычной работе релиз — это решение ИТ-департамента. Есть некий календарь или политика релизов, определяющие возможные частоту и масштаб, и даже нумерацию версий. Бизнес-подразделение, которому необходимо получить новую функциональность для своих клиентов, встаёт в очередь и дожидается очередного релиза: в счастливом случае ближайшего, но зачастую — подальше, через один-два квартала.

При использовании непрерывного развёртывания в DevOps поставка новой функциональности в среду эксплуатации производится сразу же, как она разработана и протестирована. Пользователи её не замечают, так как она пока не активирована. Активация выполняется тогда, когда это необходимо бизнес-подразделению в соответствии с его маркетинговыми, рекламными или иными планами и соображениями. Такая практика не только позволяет передать управление релизами в руки заказчика, но и получить дополнительные преимущества.

Во-первых, радикально сокращается, вплоть до исчезновения, ***время простоя при распространении релизов*** (англ. Zero-Downtime Releases). Во-вторых, появляется возможность выполнять ***сине-зелёные развёртывания*** (англ. Blue-Green Deployments), для которых создаются две копии среды эксплуатации: «зелёная» и «синяя», соответственно. Переключение пользователей с одной среды, где они пока взаимодействуют с предыдущей версией приложения, на другую, где уже подготовлена новая версия, производится менее, чем за секунду. В-третьих, компании с большим числом пользователей могут использовать технику так называемых ***канареечных релизов*** (англ. Canary Releases), когда новая функциональность сначала становится доступной небольшому подмножеству пользователей. Убедившись, что всё в порядке с технической и с маркетинговой точек зрения, может быть принято решение о переключении всех остальных пользователей, при этом, первоначальная сегментация выполняется бизнес-подразделениями по той логике, которая им важна и близка: по территориальному признаку, тарифным планам клиентов, лояльности клиентов или иным. Наконец, в-четвёртых, многие компании начинают активно применять A/B-тестирование для проверки бизнес-гипотез, когда часть пользователей (контрольная группа) работает со старой версией системы, а другая часть (экспериментальная группа) использует уже новую версию. Измерение ключевых показателей и сравнение групп между собой позволяет бизнесу проверять свои идеи и корректировать дальнейшее развитие данной системы.

Всё перечисленное становится возможным только если изменяется сама суть релиза, и решение передаётся в руки бизнеса.

Автоматизируется всё, что только возможно

Известная пословица «*Лень — двигатель прогресса*» применительно к ИТ трансформируется в наблюдение «*Ленивый*

администратор в конце концов напишет скрипт, чтобы меньше работать». В традиционном ИТ-отделе ждать написания скриптов можно долго, единого хранилища нет, их работоспособность остаётся под вопросом, поэтому большинство операций, в том числе часто повторяемых, выполняется вручную. Среди них необходимо отдельно отметить:

- создание сред (тестирования, промежуточных и иных);
- конфигурирование элементов инфраструктуры;
- тестирование;
- развёртывание и тиражирование, включая настройку средств мониторинга.

Важное для DevOps повышение уровня контроля требует тотальной автоматизации всех ручных операций, в особенности — перечисленных выше. Необходимые для работы конвейера развёртывания среды создаются скриптами и автоматически под управлением системы управления конвейером. Также автоматически эти среды уничтожаются после использования, освобождая ресурсы. Быстрая работа конвейера требует максимальной автоматизации всего тестирования, насколько это возможно. Ручные тесты остаются на самый крайний случай, хотя новые достижения постоянно сдвигают границу такого случая: сегодня можно выполнять автоматическое тестирование не только модулей, интеграции, регресса, функциональности, производительности, но и пользовательского интерфейса, удобства использования, приёмочных испытаний. Развёртывание и тиражирование, как завершающие шаги конвейера, также выполняются автоматически, с необходимой подстройкой средств мониторинга систем и приложений. Данный шаг нельзя недооценивать — качественно настроенный мониторинг позволяет получать очень быструю обратную связь относительно новых релизов. Как бы сотрудники не старались приблизить конфигурацию тестовой среды к среде эксплуатации, разница может проявиться уже после развёртывания. В таком случае событие, зафиксированное системой мониторинга, может привести к автоматическому откату назад уже развёрнутого изменения для обеспечения стабильности среды и приложений.

Более того, при переходе от традиционных монолитных архитектур к микросервисным полный мониторинг компонентов становится насущной необходимостью, ведь это единственная возможность отследить не только работоспособность, но и фактическое использование данного сервиса или данной версии сервиса другими сервисами. Без такого контроля эволюционирующая архитектура не сможет развиваться, и в ней будут постоянно накапливаться уже умершие, но всё ещё не отключённые сервисы.

Устранение сбоев не подразумевает очереди

Типичный процесс управления сервисными инцидентами, когда о случившемся сбое сообщает пользователь, устроен так:

- пользователь обращается на первую линию поддержки через телефон, электронную почту, портал, онлайн-чат или мобильное приложение;
- первая линия поддержки (с помощью сотрудника, автоматизированной системы или средств искусственного интеллекта) регистрирует и классифицирует обращение, в том числе присваивая ему приоритет, влияющий на скорость дальнейшей обработки;
- обращение попадает в очередь, где ожидает своего часа (или дня).

Управление инфраструктурными инцидентами, когда информация о сбое поступает от ИТ-специалиста или системы мониторинга, устроено примерно так же, завершаясь очередью. Наличие очереди — механизм управления, связанный как с необходимостью упорядочивания работы, попыткой более равномерно загружать ресурсы, но ещё — с длительным временем решения инцидентов. Для каждого инцидента необходимо произвести расследование, выполнить диагностику, найти и применить обходное решение — всё это в подавляющем большинстве случаев выполняется вручную.

В идеальном DevOps всё не так. В случае, если инцидент связан с развёртыванием, которое недавно состоялось (то есть можно отследить причинно-следственную связь), система управления конвейером автоматически выполнит возврат к предыдущему известному рабочему состоянию. Вмешательство человека требуется для анализа проводимого изменения и его корректировки, что выполнить намного легче и быстрее, ведь данное изменение было совсем недавно, а не несколько месяцев или лет назад. Известны решаемая задача, заказчик, разработчик, тестировщик — все участники цепочки.

В том случае, если что-то «сломалось» в инфраструктуре, принимается решение без долгих разбирательств отключить сбойный элемент (например, сервер приложений) и создать этот участок инфраструктуры заново, пользуясь уже готовыми и отлаженными скриптами, с помощью которых элемент был создан ранее. Такая операция занимает намного меньше времени, чем при обычном процессе. Действительно, если под управлением ИТ-отдела находится, скажем, несколько десятков серверов, то можно каждый из них настраивать вручную, придумывать ему уникальное красивое имя, холить и лелеять. Но когда ИТ-подразделение управляет сотнями и тысячами серверов, такой способ вносит слишком большие ограничения и не является продуктивным. Альтернативный подход DevOps зачастую называется «***стадо, а не домашние любимцы***» (англ. Pets vs. Cattle). Напомним, что DevOps подразумевает максимальное абстрагирование от реального аппаратного обеспечения в пользу виртуализации, что было описано ранее.

Дефекты исправляются немедленно

В работе обычного ИТ-отдела выявленные при эксплуатации ошибки, которые каким-то образом прошли через тестирование, оцениваются, приоритизируются и встают в очередь. В самой описанной процедуре нет ничего негативного, кроме того факта, что многие из ошибок встают в очередь навечно, накапливая таким образом технический долг. Присвоив незначительный приоритет, команда откладывает устранение такой ошибки на длительный срок. К моменту, когда срок подходит, во-первых, все давно забыли, что за ошибка, почему происходит и как её устранить, а во-вторых, находится более важная и срочная работа. Первое требует восстановления контекста и дополнительных трудозатрат, второе делает невозможным устранение неприоритетных ошибок при наличии более приоритетной работы, которая, как правило, всегда есть.

Ещё одна сложность, наблюдаемая на практике, заключается в невозможности объективно оценить размер очереди ошибок, которая имеет тенденцию к разрастанию. Десять ошибок — это ещё допустимо? А пятьдесят? Пятьсот? Как сравнить ошибки разных приоритетов, значимости или ущерба? Может ли ошибка, находящаяся в очереди неделю, подождать ещё? А месяц? Год? Принимая во внимание, что очередь ошибок находится в недрах какой-либо

системы учёта, увидеть и осознать её — уже проблема. Особенно если к картине добавить аргументы вроде «*Эту ошибку устранять уже нет смысла, так как данный модуль через полгода планируем менять на другой*». Для реалистичности картины нужно обязательно указать, что ошибка находится в очереди уже не меньше года, а «планируем» вовсе не означает «заменим». И, как правило, не через полгода.

В DevOps исправление ошибок устроено иначе. В соответствии с принципом «система должна всегда находиться в рабочем состоянии», а также, в стремлении управлять техническим долгом, большинство выявленных ошибок получают приоритет, требующий немедленного устранения — например, в рамках того же или ближайшего спринта, если команда работает по Scrum. В случае выявленных минорных ошибок допускается выделение увеличенного срока на устранение, однако он должен быть не слишком большим и в любом случае должен быть соблюдён.

Как и многие другие практики, такой порядок означает большую перестройку в планировании, приоритизации и выполнении работ, а кроме того — серьёзные изменения в исходных принципах организации процессов. Многие руководители просто не согласятся с принципом «выявленные ошибки устраняем немедленно». Возможно, как ранее не соглашались с принципом из ITSM: «Все поступившие заявки должны быть зарегистрированы». В этом случае один из методов — работать с выявленными дефектами так же, как производится работа над новой функциональностью. Ошибки и пользовательские истории попадают в единую очередь и рассматриваются на равных. Действительно, выбор между реализацией той или иной возможности делается по тем же исходным основаниям, как и выбор — какую ошибку устранять. Равно как и предоставление предпочтения разработке новой функциональности в ущерб устранению дефектов — такое же управленческое решение, принимаемой для той же ИТ-системы, тех же ресурсов, тех же пользователей. В этом случае к управлению техническим долгом привлекаются заказчики, что сильно меняет как значимость такой работы, так и ответственность за её результаты.

Процесс улучшается постоянно

Ещё хуже в обычном ИТ-подразделении обстоит дело с изменением процесса работы. Консультанты, рабочая группа, состоящая из сотрудников компании, а то и специализированное подразделение разработали необходимые регламенты. Как правило, они описывают некую модель, в разной степени соответствующую желаемому порядку выполнения работ: как и любая модель, данные регламенты будут содержать разрыв между желаемой практикой и описанием. Например, сложно предусмотреть все возможные ситуации и отклонения, сложно описать мотивировочную часть — зачем и почему такая работа должна выполняться таким способом, сложно детализировать изложение до необходимого уровня, при этом никого не запутав и не превратив сотрудников в роботов. Следующий разрыв между реальностью и регламентов возникает, когда реальное выполнение работ становится не таким, как предполагалось. Где-то сотрудники будут срезать углы, где-то стараться работать лучше, чем диктуют инструкции. Третий разрыв связан с автоматизацией оперативных процессов, от которой эти процессы сильно зависят. Во многих случаях настройка инструмента автоматизации производится с большими задержками относительно выполнения процесса: работа уже выполняется иначе, но

система автоматизации пока не изменилась. Либо, что ещё хуже, работа выполняется не оптимальным образом потому, что нет возможности оперативного изменения системы автоматизации. В одной известной мне организации очередь на внесение изменений в ITSM-систему составляет два года, что сильно замедляет реализацию всех назревших корректировок процессов.

Такое большое количество разрывов крайне негативно влияет на практику выполнения работ. Поэтому в DevOps используется иное правило: любые выявленные недостатки процесса должны быть устранены немедленно. Например, если некорректно работает какой-либо скрипт, обеспечивающий работу конвейера развёртывания, его нужно незамедлительно исправить. Более того, в противовес традиционной практике, при которой проблемы можно отложить, в DevOps рекомендуется проблемные шаги повторять как можно чаще. Это позволит лучше понять, как именно их следует улучшить, исправить, и внести соответствующие корректировки в работу.

Стартап как ориентир

Некоторые DevOps-команды возникли в стартапах, с их необычной культурой, такой непривычной для корпоративных сотрудников. Компании, пытающиеся выстраивать DevOps у себя, стараются перенять этот дух предпринимательства и инноваций. Но что же это означает? В чём состоит разница, можно ли её сформулировать? Оказывается, можно — Табл. 4.1.2 перечисляет ключевые отличия.

Табл. 4.1.2. *Отличия в культуре обычных корпораций и стартапов.*

Характеристика	Культура обычных корпораций	Культура стартапов
Стиль управления	Командный, авторитарный	Автономный
Склонность к переменам	Консервативность	Эксперименты
Организационная структура	Функционально-иерархическая	Сетевая
Акцент результата	Проектно-ориентирован	Ориентирован на продукт
Модель	Водопадная	Гибкая, итеративная
Системная архитектура	Монолитная, тщательно спроектированная	Слабо связанная, микросервисная
Предпочтения в технологиях	Патентованные, проприетарные	Открытый исходный код

Похоже, по всем приведённым характеристикам DevOps-культура сильно отличается от привычной, что, конечно, препятствует прямому и быстрому изменению стиля работы в обычных корпорациях. Приведённая выше таблица хорошо суммирует основные различия, позволяя перейти к более детальному рассмотрению отдельных DevOps-практик. Напомним, что многие из них являются, условно говоря, заимствованиями из других известных областей, что не умаляет значимости как этих областей, так и DevOps.

Необычные команды

В таблице предыдущего раздела, в колонке «Культура стартапов» были приведены некоторые

отличия, делающими невозможным, либо крайне затруднённым использование традиционного функциональ-ного управления. В частности, автономный стиль, ориентация на продукт и сетевая организационная структура подталкивают к пересмотру способа группировки специалистов для достижения больших результатов. На первый план выходят команды, а не структурные подразделения.

DevOps-команда — удивительная боевая единица. Она отвечает за небольшой, но чётко обозначенный кусочек какой-либо ИТ-системы или ИТ-инфраструктуры. Обладая строгим фокусом, члены команды постепенно и неизбежно становятся экспертами в данной предметной области, сохраняя полную ответственность за неё.

Команда не является способом объединить сотрудников на время, например, на проект — напротив, команда создаётся на долгий срок. Более того, как правило срок жизни команды заранее не определяется и не фиксируется. Команда работает над своей областью ответственности до тех пор, пока область остаётся релевантной. В случае изменения траектории команда «поворачивает» вместе с областью ответственности; в случае отказа от данной области команда переключается на другую. Среди практиков нет устоявшегося мнения стоит ли время от времени разрушать команды. С одной стороны, распределение участников одной, хорошо поработавшей команды между другими позволяет ускорить обмен компетенциями и опытом. Однако многие эксперты возражают, что время и ресурсы, потраченные на создание эффективной сложившейся команды лучше реинвестировать в другие задачи, сохраняя миниколлектив, а обмен знаниями можно и нужно организовывать независимо от формирования команд, и другими способами. Участники команды работают в ней 100% своего рабочего времени: никакого больше разделения ресурсов, совмещения обязанностей там и тут, замены болеющего сотрудника в другом отделе и прочего. Полное погружение каждого участника упрощает координацию работ, убирает зависимости от внешних факторов и исключает возможность сослаться на другую загрузку. С другой стороны, такой подход увеличивает расходы на персонал.

DevOps-команда является кроссфункциональной — это означает, что она должна быть способна полностью выполнять всю работу в потоке создания ценности своей области ответственности. Только такой подход обеспечивает возможность единого и точного понимания определения завершения, только так можно доводить задачи до конца и полностью избавиться от незавершённой работы.

Размер команды имеет важное значение. С одной стороны, её не получится сделать слишком маленькой — небольшая команда не сможет стать кроссфункциональной, как описано выше. С другой, команды из двадцати и более человек сложны в координации и будут либо требовать создания уровней управления, либо будут склонны разваливаться на составные подкоманды. Кроме того, в больших командах возникают дополнительные расходы на коммуникации и неизбежная потеря информации между участниками. Всё это негативно сказывается на скорости работы.

Небольшой размер и необходимость кроссфункциональности выдвигают дополнительное требование к DevOps-командам: сотрудники должны быть максимально универсальными. Чёткая специализация привычна: вот это — программист, а это — тестировщик, а вот это — специалист по

информационной безопасности. Но DevOps-команда требует стирания границ: в идеале каждый должен быть способен выполнять работу каждого. Такая особенность не означает, что все станут одинаково плохими, к примеру, разработчиками или администраторами баз данных. Понятно, что экспертиза сотрудников в отдельных областях может и должна быть глубокой. Однако универсальность позволяет членам команды помогать друг другу, обмениваться компетенциями, на экспертном уровне понимать, как всё устроено. Всё это выравнивает загрузку и создаёт единую ответственность команды как боевой единицы, а не отдельных гуру.

Среди небольшого числа участников DevOps-команды нет формального руководителя, нет координатора или супервайзора. Команда должна быть способна самостоятельно решать все возникающие управленческие вопросы, а в сложных случаях — обращаться за поддержкой к экспертам или наставникам. Проводя аналогию со Scrum, владелец продукта не обладает голосом бóльшим, чем любой другой член команды, а Scrum-мастер не является специально выделенным человеком — это всего лишь роль, время от времени передаваемая от одного участника другому. Иначе говоря, команда должна быть самоорганизующейся, что вполне достижимо для команд небольшого размера.

Важно, чтобы все члены команды физически располагались рядом, в одном помещении. Необходим постоянный личный контакт, не на расстоянии и не только через электронные средства коммуникации. Такое строгое требование имеет серьёзные основания: во-первых, коммуникации формата «напиши — прочитай» скрывают эмоциональную составляющую, независимо от способа передачи информации (электронное сообщение, мгновенное сообщение, формальный документ), точности формулировок и наличия смайликов. В совершенно очевидных случаях получателю понятно — похвалили его или предъявили претензию, но во всех остальных ситуациях основной эмоциональный посыл отправителя остаётся за кадром. Известны случаи, когда безобидные с точки зрения написанного текста комментарии вызывали бурю негодования, а сравнение с определёнными известными персонажами воспринималось как публичное оскорбление. Хорошо, если такая реакция станет заметной сразу же! Однако стоит помнить, что многие из работающих в ИТ-отрасли специалистов являются интровертами, имеющими склонность накапливать обиды. Стоит добавить к придуманным негативным эмоциям практически безграничные технические возможности, доступ к исходному коду и в среду эксплуатации — получится взрывоопасная смесь.

Во-вторых, расположение всей команды в одном помещении делает неизбежным ежедневный контакт каждого с каждым при отсутствии физических барьеров. Сообщение электронной почты, находящееся в папке «Входящие», можно игнорировать неделями. Телефонные звонки можно просто не принимать, ссылаясь на загрузку, совещания, встречи и т.д. А на неудобные вопросы стоящего рядом коллеги отвечать придётся сразу же: условно говоря, программисту теперь не скрыться от тестировщика, а тестировщику — от специалиста по эксплуатации. Некачественная работа, дефекты, инциденты будут не только заметны и зарегистрированы в какой-либо информационной системе, они будут также максимально оперативно устранены и исправлены, при том совместными усилиями разных членов единой команды. Характерно, что такой стиль работы группы не требует

наличия руководителя, координатора или иного «разводящего».

DevOps-команда сама отвечает за используемые ею инструменты. Как и из чего строить конвейер, какие применять технологии, какие версии библиотек использовать — все подобные вопросы передаются в зону ответственности команды. Она должна быть способна оценить последствия любых проводимых изменений. Данные утверждения не исключают необходимости следования корпоративным стандартам, в том числе в области архитектуры, информационной безопасности и аудита.

Область применения и ограничения DevOps

DevOps — это один из инструментов, пусть и новых, в руках современного ИТ-менеджера. Как и прочие управленческие инструменты, он не является лекарством от всех болезней, а лучше всего подходит для решения определённых задач. Более того, как и другим подходам, ему присущи некоторые ограничения.

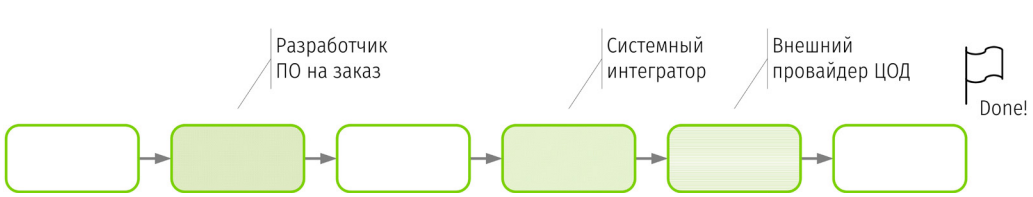
Начнём с того, что далеко не каждой организации в принципе следует задумываться про DevOps. Для начала, отсечём особые случаи — компании, разрабатывающие программное обеспечение (в том числе на заказ), системные интеграторы, подрядчики на разных участках ИТ-работ и чисто проектные организации. Общее для перечисленных случаев — участие лишь на ограниченном участке потока создания ценности (Рис. 4.1.8).

Изучение применимости DevOps для таких ситуаций является задачей, достойной отдельной публикации. Сфокусируемся на более традиционной компоновке: бизнес, имеющий внутреннее или внешнее ИТ-подразделение, полностью отвечающее за все вопросы применения информационных технологий. Собственно, область деятельности и форма собственности такого бизнеса не так важны — это может быть финансовое учреждение, страховая компания, торговая организация, некоммерческое партнёрство, производство товаров или предприятие сферы услуг. Главное, что в этом бизнесе используются информационные технологии, а где они — там и задачи по получению максимальной отдачи от ИТ.

Интерес к DevOps для такого рода компаний возникает при выполнении следующих условий:

- основной бизнес компании сильно зависит от информационных технологий (зависимость несложно оценить по косвенным критериям, например, по доле затрат на ИТ в общем бюджете организации и месту высшего руководителя по ИТ в иерархии управления компании);
- темп изменений, происходящих в используемых данной организацией информационных технологиях, высок;
- основной бизнес требует быстрых изменений, вызванных необходимостью проверки новых идей или гипотез;

Рис. 4.1.8. *Особые случаи, не рассматриваемые далее.*



- существуют связанные с информационными технологиями угрозы для основного бизнеса, оцениваемые владельцами или высшим менеджментом, как неприемлемые;
- все остальные испробованные способы повышения эффективности больше не дают ощутимых результатов.

Если для данной организации пункты приведённого выше списка являются релевантными, применение DevOps в том или ином виде имеет потенциальную ценность.

Отдельно следует упомянуть случаи, когда компании рассматривают применение DevOps для резкого снижения накопленного технологического долга, либо устранения хрупкости ИТ-инфраструктуры. Нужно помнить, что для сложных ситуаций увлечение DevOps, скорее всего, не принесёт большой пользы и совершенно определённо не даст быстрых побед — напротив, организационные и технологические перемены могут привести к хаосу и потере остатков управляемости. Исправлять запущенные проблемы следует аккуратно, вдумчиво и рассудительно, не надеясь на DevOps как на лекарство от хронических заболеваний.

Перейдём к рассмотрению второго аспекта — реализуемости. Во всех ли компаниях можно «построить» DevOps? Мнение большого числа зарубежных экспертов сводится к положительному ответу, однако, трезвый взгляд на реальность показывает иное.

DevOps не очень подходит тем, у кого нет собственной разработки программного обеспечения — например, если всё основное применяемое ПО является уже готовым, «коробочным», и настраивается через интерфейсы взаимодействия с пользователем или администратором. Раз в компании нет собственной разработки — нет и начала потока создания ценности, нет возможности контроля версий исходного кода (так как нет доступа к исходному коду и нет необходимых компетенций с этим кодом разбираться). Зато есть существенная зависимость от компании-разработчика и от компании-поставщика применяемого программного обеспечения. Негативные следствия такой зависимости хорошо известны: какой бы крупной и известной ни была ваша организация, вы, как правило, будете лишь одним из множества заказчиков, и, несмотря на все заверения менеджеров по работе с клиентами, будете находиться в той же очереди ожидающих внимания разработчика, что и все остальные. При этом существенным является не место в очереди, а сам факт её наличия. Другое негативное следствие зависимости от внешнего разработчика «коробочного» ПО — крайняя медлительность многих компаний, производящих программное обеспечение ввиду применения ими тех самых водопадных моделей и долгих релизных циклов. Известны случаи, когда критичные дефекты в новой версии ПО остаются без исправлений более девяти месяцев, отдельные сбои «не получается» диагностировать более полугода, а клиенту предлагается безрадостный выбор: либо оставаться на устаревшей на 2-3 года версии ПО с длительной поддержкой (англ. LTS, Long Term Support), в которой вроде бы дефектов меньше, либо постоянно переходить на каждую новую версию, исправляющую предыдущие ошибки и вносящую новые.

Сложности применения DevOps возникнут и в организациях, где разработка программного обеспечения есть, но программисты выведены из штата: разработка выполняется другими компаниями на заказ, либо программисты не являются сотрудниками данной компании, а работают по договору подряда, фриланса, аутстаффинга или подобного. В таком случае полноценно включить их в поток создания ценности может

быть затруднительно из-за совершенно различной мотивации участников. Сотрудники компании, находящиеся в штате, как правило более заинтересованы в удовлетворении потребностей основного бизнеса, в процветании компании, в собственном карьерном росте, а значит — в быстро полученном и качественном конечном результате работы всех участников команды. В то время как внешние разработчики могут стремиться максимально ограничить свою ответственность рамками договора и стараться выдавать результаты в строгом соответствии с полученным техническим заданием, зачастую завышая трудозатраты и перезакладываясь по срокам. К рассмотрению следует добавить возможную частую смену исполнителей, их неполное выделение в данную команду, а также типичную ситуацию, когда об объёме и условиях привлечения договариваются одни (скажем, руководитель отдела развития со стороны потребителя с менеджером по работе с клиентами со стороны подрядчика), а реально ежедневно взаимодействуют другие (собственно внешние разработчики с остальными членами команды). В описанном случае искажаются или становятся невозможными многие принципы, изложенные в разделе о командах.

Следующее ограничение применения DevOps — устоявшиеся, сложившиеся процессы, подкреплённые иерархией принятия решений, организационной структурой, внутренней нормативной документацией, бюрократией и корпоративной культурой. Некоторые крупные организации трезво оценивают свои способности меняться как ограниченные, в то время как переход к DevOps требует большой перестройки не только ИТ-отдела, но и принципов работы бизнес-подразделений. Достаточно вспомнить отличия культуры традиционных больших корпораций от культуры стартапов, приведённые ранее, чтобы оценить масштаб необходимых преобразований. Важно отметить, что для многих организаций полное изменение имеющейся практики работы является принципиально невозможным, несмотря на демонстрируемые краткосрочные успехи в отдельных частях компании.

Наконец, последним значимым препятствием является монолитная, жёстко связанная ИТ-архитектура. Организация небольших команд требует возможности закрепить за каждой из них отдельную область ответственности. В ситуации, когда рассматриваемая ИТ-система до сих пор разрабатывалась и поддерживалась десятками и сотнями сотрудников как единое целое, выделить из неё части для отдельных самостоятельных команд, работающих асинхронно, будет достаточно сложно.

К перечисленным сложностям следует добавить ещё несколько факторов, ограничивающих, по мнению многих, применение DevOps. Однако, прежде необходимо заметить, что эти факторы некорректно рассматривать как проблемы, ставящие крест на DevOps-инициативах. Правильнее относиться к ним как к ограничениям, которые можно устранить, то есть как к задачам, имеющим решения. Вот эти дополнительные ограничения:

- Неготовность к созданию DevOps-команд. В некоторых организациях, к примеру, поощряется удалённая работа без необходимости присутствия в офисе в определённые часы. Встречаются территориально распределённые компании, где, в т.ч. и сотрудники ИТ-подразделения не находятся все в одном месте. Наконец, во многих компаниях организационная структура настолько жёсткая, что не подразумевает создания кроссфункциональных команд. Все эти примеры иллюстрируют приведённый выше тезис — они не являют-

ся стоп-фактором на пути к DevOps, они лишь требуют соответствующих изменений, корректировок, пусть непростых, но, тем не менее, возможных.

- «Особые» требования к информационной безопасности или соответствию внешним критериям. Слово «особые» намеренно взято в кавычки — более внимательное рассмотрение вопроса в конкретной компании может показать, что в действительности данная организация ничем принципиально не отличается от аналогичной, работающей в той же отрасли. Да, требования соответствия или требования к информационной безопасности следует учитывать, однако, это больше вопрос подхода и технологии, а не необходимости работать исключительно общепринятым способом.
- Минимальное применение виртуализации и облачных вычислений, либо отказ от этих технологий вовсе, равно как использование сильно устаревших языков программирования. Аргументы, приведённые в первой части книги (в частности, инфраструктура как программный код, автоматизированное управление конфигурациями) показывают необходимость использования облачных вычислений. Компании, ограниченно использующие виртуализацию, будут иметь известные затруднения в организации DevOps. Однако, выбор тех или иных технологий — решение конкретной компании, и если новые управленческие инструменты требуют применения новых информационных технологий, то соответствующие изменения могут быть запланированы и воплощены в жизнь.

Очевидно, что наличие одного из ограничивающих факторов не делает DevOps невозможным в данной компании. Некоторую пользу можно получить и в сложных условиях, а многие ограничения можно обойти тем или иным способом. Также очевидно, что совокупность ограничивающих факторов усложняет применение DevOps всё больше и больше. Когда наступает (и наступает ли) тот предел, при котором ограничения складываются в непреодолимый барьер — неизвестно.

Опасность культа карго

Огромное количество команд, стремящихся освоить новые управленческие инструменты, не придают должного внимания слову «управленческие», фокусируясь на практиках. Сейчас модно строить разработку итеративно? Хорошо, мы организуем у себя двухнедельные спринты. Все вокруг устраивают ежедневные Scrum-встречи? Отлично, у нас такие теперь есть. Говорят, визуализация в виде канбан-досок имеет смысл? Прекрасно, мы заведём у себя канбан. Конвейер DevOps без автоматизации не бывает? Что ж, поручим ребятам выбрать и настроить несколько систем. И так далее.

Данное поведение, при котором вместо целей, сути и принципов акцент смещается в сторону ритуалов, имеет название ***культа карго*** (англ. Cargo — товар). Понятие было впервые применено в 1945 году в области, не имеющей никакого отношения к информационным технологиям — антропологии. Учёные, изучавшие обычаи и особенности Папуа-Новой Гвинеи, выявили и обобщили явление, при котором, по мнению аборигенов, наличие материальных и духовных благ зависит в большей степени от воли духов и богов. Для получения таких благ необходимо совершать определённые действия и обряды, как правило — под руководством шамана или старейшины. Примеры и подтверждения культа карго были обнаружены и в более ранние времена — самым давним документированным примером является культ на островах Фиджи в 1885 году. Говорят, некоторые проявления такого культа сохранились в отдельных

частях Океании до наших времён.

Бездумное воспроизведение ритуалов гибкой разработки программного обеспечения, бережливых практик или DevOps-затей в надежде ускорить вывод продуктов на рынок встречается в практике различных компаний чаще, чем следует.

Заключение

DevOps имеет свои истоки, предпосылки появления. Для возникновения DevOps-движения к 2010-м годам сложились определённые условия, сформировавшие как потребность, так и возможность строить разработку и эксплуатацию информационных технологий иначе.

DevOps — не лекарство от всех болезней, как его зачастую преподносят различные «евангелисты». С его помощью можно решать три актуальные и непростые задачи: уменьшать время вывода на рынок, снижать технический долг и устранять хрупкость информационных систем.

DevOps опирается на мощный фундамент, основанный на бережливом производстве и гибкой разработке программного обеспечения. Некорректно утверждать, что DevOps — лишь использование уже известных идей; напротив, DevOps не только расширяет упомянутый фундамент, но и привносит несколько важных новых принципов.

Основываясь на этих принципах, можно искать, придумывать и применять практики. Многие из них будут непривычны для ИТ-отделов, работающих традиционным образом, однако за каждой из практик стоит достаточное основание, а зачастую холодный, в чём-то циничный расчёт.

Ещё один-два года назад можно было бы спорить о том, что такое DevOps, что входит в это понятие, что находится за границей, зачем всё это нужно и из чего состоит. Однако, к 2018 году в этих вопросах картина стала предельно ясной. Новые технологичные компании, созданные в последние пять лет, уже не представляют себе работу иной, для них DevOps — естественная часть корпоративной культуры, даже если само слово не произносится ежеминутно и не размещено на флаге. Традиционные компании с унаследованными ИТ-инфраструктурой, ИТ-решениями, процессами и персоналом ограничены в гибкости, однако активно присматриваются к новой модной теме, делают первые шаги, экспериментируют, ошибаются, учатся. Некоторые из них демонстрируют ошеломительные достижения, другие строят планы и питают надежды. Наибольшее число открытых вопросов, требующих поиска ответов, связано именно с корпоративными информационными технологиями. Если с техническими вопросами (например, как организовать конвейер развёртывания) всё более-менее понятно, то самый интересный вопрос— как получить управленческую пользу от DevOps в традиционных компаниях.

Глава 4.2

Облачные вычисления

Марина Аншина

Принципы и определения

К облачным вычислениям (или «облакам») существует два принципиально разных подхода: технический и управленческий.

Технический подход фокусируется на технических вопросах. Например: как разработать ПО, которое приспособлено для работы в облачной модели SaaS, как организовать биллинг публичного облака, как сформировать аутентификационные и авторизационные модели и т.д.

Управленческий подход занимается вопросами функциональной модели облачных сервисов, в частности: формированием правильных договоров, контролем облачных провайдеров, коммерческой и ролевой моделями облачных вычислений, стандартизацией и методологией.

Понятно, что эти подходы — две стороны одной медали, одно без другого существовать не может и не должно.

С точки зрения технической, облака логично выросли из виртуализации, т.е. «*предоставления набора вычислительных ресурсов или их логического объединения, абстрагированного от аппаратной реализации, и обеспечивающего при этом логическую изоляцию друг от друга вычислительных процессов, выполняемых на одном физическом ресурсе*». Конечно, в этом определении ничего не говорится о разделении сервисов, но никто не запрещает размещать на одной аппаратной реализации вычислительные ресурсы, относящиеся к различным сервисам. Виртуализировать можно различные ресурсы, такие как: сети, операционные системы, память, процессорные мощности. Наиболее популярный тип виртуализации — виртуализация операционных систем, которая даёт возможность разместить на одном физическом сервере несколько логических серверов, что позволяет эффективно использовать оборудование и централизовать его обслуживание.

Однако, популярность облачных сервисов связана, скорее, со вторым подходом. Именно его определяет в качестве одного из важнейших современных трендов Gartner. Имен-

но он лежит, в частности, в основе цифровой трансформации. Такой подход зафиксирован в определении:

> ***Облачные вычисления*** *— «метод управления ИТ, когда используемые активы не принадлежат компании-потребителю, и ИТ-сервисы пользователям или ресурсы, их обеспечивающие, предоставляются через Интернет»* ***(Gartner)***.

Вот и ещё ряд определений облаков.

> ***Облачные вычисления*** *— это технология распределённой обработки данных, в которой компьютерные ресурсы и мощности предоставляются пользователю как Интернет-сервис* ***(Википедия)***.

> ***Облачные вычисления*** *представляют собой модель для обеспечения удобного сетевого доступа к общему пулу настраиваемых вычислительных ресурсов (например, сетей, серверов, систем хранения данных, приложений и услуг) по требованию, которые можно быстро выделить и предоставить с минимальными управленческими усилиями или минимальным вмешательством со стороны поставщика услуг* ***(NIST)***.

> ***Облачные вычисления*** *— это парадигма обеспечения сетевого доступа к масштабируемому и гибкому пулу распределяемых физических или виртуальных ресурсов, предоставляемых в режиме самообслуживания и администрируемых по требованию* ***(ISO/IEC 17788:2014. Information technology — Cloud computing — Overview and vocabulary)***.

> ***Облако*** *— это стиль, в котором масштабируемые и эластичные ИТ предоставляются как сервисы пользователям через Интернет.*

Облачные вычисления включают в себя (по Gartner):

- «всё как сервис»,
- «инфраструктура как сервис»,
- «платформа как сервис»,
- «программное обеспечение как сервис»,
- «рабочее место как сервис»,
- «данные как сервис»,
- другие технологические тенденции, общим в которых является уверенность, что сеть Интернет в состоянии удовлетворить потребности пользователей в обработке данных».

В последнем определении Gartner выделяются различные типы облаков, среди которых наиболее известны:

- ***IaaS*** — Infrastructure as a Service — «инфраструктура как сервис»,
- ***PaaS*** — Platform as a Service — «платформа как сервис»,
- ***SaaS*** — Software as a Service — «программное обеспечение как сервис».

Список можно расширить. Например, становятся все более популярны «бизнес-процессы как сервис», «безопасность как сервис», «вычисления как сервис», «данные как сервис».

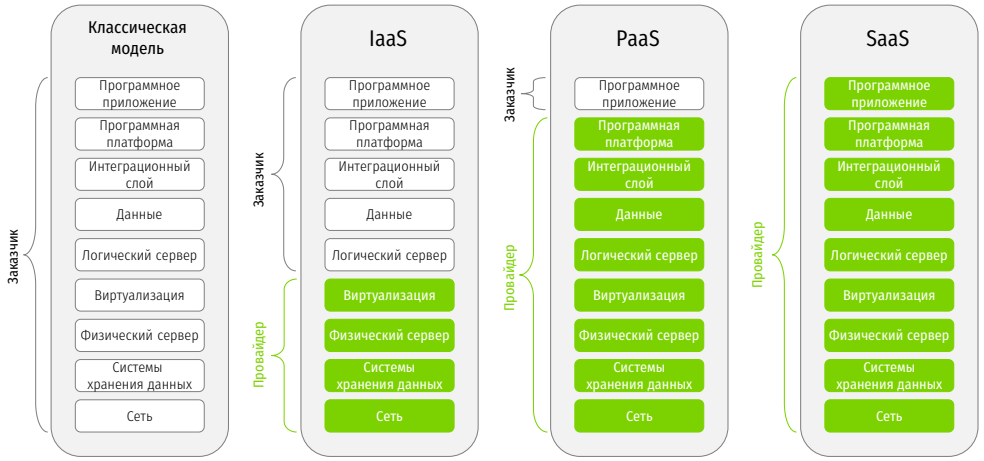
Типы облаков

С точки зрения финансов, облака позволяют перевести капитальные платежи в операционные, так как заказчик освобождён от необходимости приобретать оборудование, программные платформы или программное обеспечение, выполнять дорогостоящие проекты. Инвестиционные затраты в эти активы несёт провайдер облачных сервисов, он же обычно осуществляет их эксплуатацию и обслуживание. В данном аспекте достаточно подробно принцип разнесения затрат и подходы к нему расписаны в предыдущей версии Учебника – в главах «Управление финансами» и «ИТ-аутсорсинг». В этой же главе мы рассмотрим именно «облачную» составляющую

ИТ-процессов.

Рис. 4.2.1 на схеме архитектуры поясняет владение активами в классической дооблачной модели и в наиболее популярных типах облачных моделей.

Рис. 4.2.1. *Владение активами различных архитектурных уровней в моделях облачных вычислений.*



Следует отметить ключевые характеристики облачных сервисов, которые, несомненно, способствуют их быстрому распространению.

- Широкие возможности сетевого доступа — при наличии сети к сервисам могут получить доступ различные пользователи, вне зависимости от их физического расположения по отношению к ресурсам.
- Измеримость сервиса — облачная модель подразумевает измеримость сервиса, которая является основой финансовой модели.
- Мультиарендность — доступ к сервису в случае публичного облака получают различные компании-заказчики, которые могут арендовать его на гибких условиях.
- Самостоятельное конфигурирование сервисов по требованию — в общем случае грамотный облачный провайдер предоставляет заказчику возможность разумного конфигурирования сервиса, не оказывающего влияния на сервисы других заказчиков.
- Высокие эластичность и масштабируемость — грамотный облачный провайдер предоставляет огромные возможности по гибкости и масштабируемости, что не под силу организовать в классической модели.
- Объединение ресурсов в пул позволяет повысить эффективность их использования.

Кроме классификации по типу владения активами различных архитектурных уровней, облака делят по типу развёртывания и потребления. Структура такой классификации приведена в Табл. 4.2.1.

Модель NIST, приведённая на Рис. 4.2.2, объединяет вышеприведённые классификации и основные характеристики облаков.

Табл. 4.2.1 (начало). *Типы облаков.*

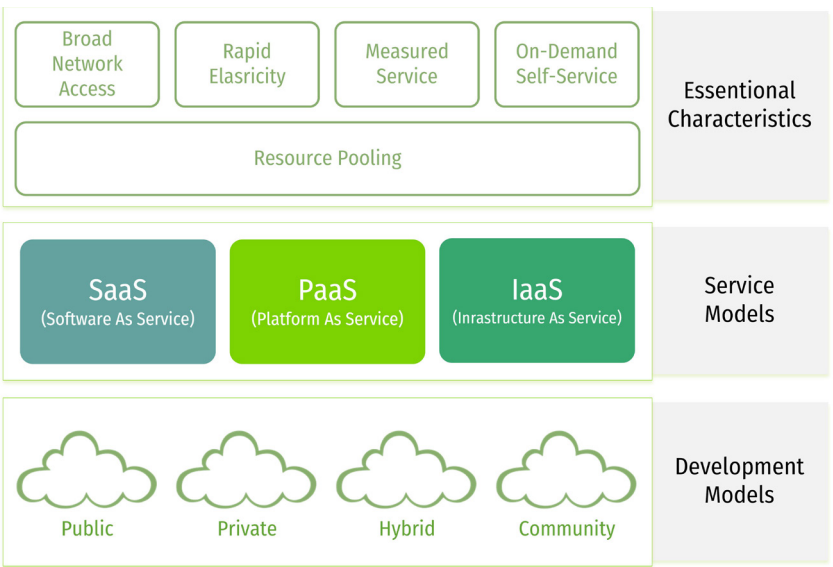
English / Перевод	Описание	Определения
Private / Частное	Предназначено для одной организации	Реализация модели облачных вычислений на ресурсах, имеющихся в распоряжении у компании-заказчика для обслуживания внутренних потребителей Облачная инфраструктура функционирует целиком в целях обслуживания одной организации. Инфраструктура может управляться самой организацией или третьей стороной и может существовать как на стороне потребителя, так и у внешнего провайдера.

Табл. 4.2.1 (продолжение). *Типы облаков.*

English / Перевод	Описание	Определения
Community / Коммунальное	Предназначено для ограниченного числа организаций, объединённых логически или юридически	Облачная инфраструктура используется совместно несколькими организациями и поддерживает ограниченное сообщество, разделяющими общие принципы (миссию, требования к безопасности, политики, требования к соответствию регламентам и руководящим документам и пр.), например, холдинг. Такая облачная инфраструктура может управляться самими организациями или третьей стороной и может существовать как на стороне потребителя, так и у внешнего провайдера.
Hybrid / Гибридное	Интеграция двух или более интероперабельных облаков для доступа к данным и портируемым приложениям	Облачная инфраструктура является композицией (сочетанием) двух и более облаков (частных, общих или публичных), остающихся уникальными сущностями, но объединённых вместе стандартизированными или частными (проприетарными) технологиями, обеспечивающими портируемость данных и приложений между такими облаками (например, такими технологиями, как пакетная передача данных для баланса загрузки между облаками).
Public / Публичное	Предназначено для нескольких организаций	Облачная инфраструктура создана в качестве общедоступной или доступной для большой группы потребителей, не связанных общими интересами, но, например, принадлежащими к одной области деятельности (принадлежность к одной области деятельности / индустрии может предполагать специфичные для этой индустрии приложения, потребность в которых испытывают организации, ведущие аналогичную деятельность или работающие на одном рынке.). Такая инфраструктура находится во владении организации, продающей соответствующие облачные услуги / предоставляющей облачные сервисы.

Публичные и гибридные облака позволяют получить компаниям среднего и малого бизнеса (СМБ) доступ к современным технологиям, которые в классической модели из-за высокого уровня начальных инвестиций им были недоступны.

Рис. 4.2.2. *Модель NIST облачных вычислений.*



Грамотно сформированная облачным провайдером арендная плата, когда заказчик платит только за объём потребляемых сервисов, даёт возможность увеличить выгоды, получаемые от использования ИТ-сервисов. Это, в свою очередь, стимулирует развитие облаков, рост конкуренции между облачными провайдерами и смену моделей предоставления ИТ на облачную.

Все мировые эксперты показывают и прогнозируют

существенный рост рынка облаков, в последнее время всё больше внимания уделяя гибридным облакам, как наиболее гибкому типу.

Гибридные облака — самый сложный тип облаков для интеграции сервисов. Возможно, именно поэтому при несомненной выгоде гибридных облаков, они очень медленно приобретают популярность. С точки зрения архитектурных уровней, до настоящего времени наиболее популярными являются сегменты IaaS и SaaS.

Безопасность при использовании облачных решений

Первое время распространению облаков препятствовали опасения по поводу информационной безопасности, ответственность за которую, по крайней мере частично, ложится на плечи облачного провайдера. Однако, для большинства компаний среднего и малого бизнеса уровень информационной безопасности, предлагаемый грамотными провайдерами, существенно превосходит тот, который они в силах организовать сами.

Международная организация The Cloud Security Alliance с 2009 года занимается вопросами безопасности облачных вычислений. В настоящее время она опубликовала уже 4-ую версию Руководства по безопасности для облачных вычислений, основанную на модели NIST, приведённую на Рис. 4.2.2, «Security guidance. For Critical Areas of Focus In Cloud Computing 4.0». В этом документе описываются различные аспекты информационной безопасности облачных сервисов, а также основы ***SecaaS*** — Security as a Service («безопасность как сервис»).

The Cloud Security Alliance описывает два практических метода оценки уровня информационной безопасности, предлагаемого провайдерам облачного сервиса:

- Шаблон для анкеты оценки соответствия безопасности и уровня контроля провайдера (The Consensus Assessments Initiative Questionnaire — CAIQ).
- Матрица контроля безопасности (The Cloud Controls Matrix — CCM), которая отображает соответствие безопасности соответствующим стандартам и может использоваться также для документирования ответственности провайдера.

Оценка облачного провайдера проводится различными способами:

- самоаудит облачного провайдера;
- оценка заказчиком;
- аудит третьей стороной;
- или любой комбинацией указанных выше способов.

Оценка заказчиком по рекомендации The Cloud Security Alliance включает в себя следующие вопросы:

- Надёжен ли сервис и прост ли в использовании?
- Как будут использоваться сервера для обработки данных?
- Как будет эксплуатироваться и обеспечиваться сервис?
- Как будут располагаться данные по отношению к данным других заказчиков?
- Как будут защищаться данные от вторжения и разрушения?
- Как будет изменяться цена во времени?
- Будет ли облачный провайдер учитывать потребности в доступе и вычислениях заказчика?
- Планирует ли облачный провайдер оставаться в бизнесе в течение нескольких следующих лет?
- Каково финансовое положение провайдера?
- Какие показатели информационной безо-

пасности измеряются?

- Что происходит в случае нарушения безопасности?
- Каков будет уровень предоставляемого сервиса?

Российское подразделение The Cloud Security Alliance представлено Ассоциацией профессионалов в области информационной безопасности RISSPA (Russian Information Systems Security Professional Association), созданной в июне 2006 года, которая, в частности, перевела опросник по информационной безопасности для облачных провайдеров на русский язык.

На основании модели NIST, о которой упоминалось выше, в ИСО/МЭК в 2014 году подготовлено два стандарта: ISO/IEC 17788:2014 «Information technology -- Cloud computing -- Overview and vocabulary» (принят в 2016 году как ГОСТ ИСО/МЭК 17788-2016 «Информационные технологии. Облачные вычисления. Общие положения и терминология») и ISO/IEC 17789:2014 «Information technology -- Cloud computing -- Reference architecture» (ГОСТ Р ИСО/МЭК 17789 «Информационные технологии. Облачные вычисления. Эталонная архитектура» — в стадии обсуждения).

Кроме того, серьёзней угрозой для модели облачных вычислений являются не только прямые вопросы безопасности, но и так называемые теневые облака, когда функциональные подразделения, независимо друг от друга и без согласования с архитекторами и ИТ-специалистами, а также с руководством компании, приобретают облачные сервисы. Данные, приводимые экспертами удручают. Так, согласно исследованию Cisco, для хранения критичных данных в компаниях используется в 15 раз больше облачных сервисов, чем утверждено руководством. Очевидно, что теневые облака представляют собой обратную сторону доступности. Но, при этом, они разрушают архитектуру предприятия, ведут к кардинальному ухудшению качества корпоративной информации, делают невозможной интеграцию сервисов, приводят в потере управления ИТ. ИТ-директор должен в полной мере осознать опасность теневых облаков и довести это до сведения сотрудников организации.

Ролевая модель в облачных решениях

Рис. 4.2.3. *Роли и подроли эталонной архитектурной модели облачных вычислений.*

В этих стандартах определяются три стороны облачных вычислений:

1. Сторона, использующая облачные сервисы.

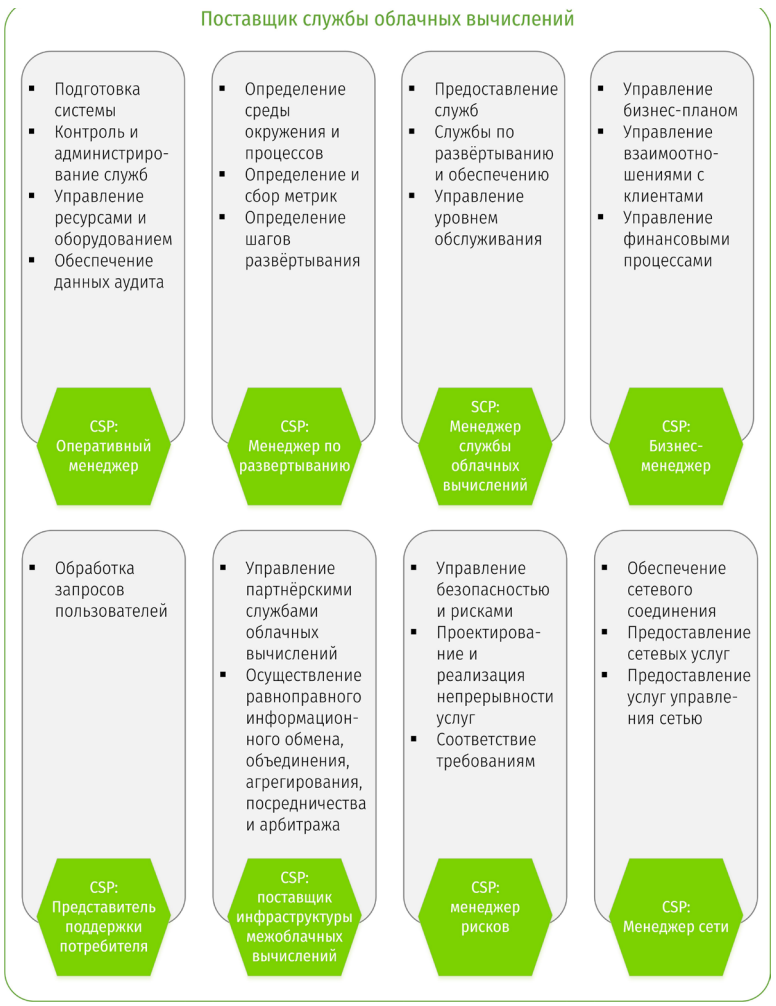
2. Сторона, предоставляющая облачные сервисы.

3. Сторона, поддерживающая облачные сервисы.

В стандартах определяются роли и подроли облачных вычислений, а также подробно описываются функциональные компоненты, представляющие собой строительные блоки, формирующие их деятель-

Рис. 4.2.4. *Деятельность потребителя облачных вычислений.*

Рис. 4.2.5. *Деятельность поставщика облачных вычислений.*



ность. На Рис. 4.2.3 приведены роли и подроли облачных вычислений стандарта 17789. На Рис. 4.2.4, Рис. 4.2.5 и Рис. 4.2.6 приведены деятельности ролей эталонной архитектуры облачных вычислений.

Кроме того, в стандарте 17789 описаны сквозные аспекты, которые должны обеспечивать все участники ролевой модели облачных вычислений в своей деятельности:

- проверяемость, возможность аудита;
- доступность;
- управление;
- интероперабельность;
- сопровождение и управление версиями;
- производительность;
- портируемость;
- защита персональных данных;
- нормативное регулирование;
- устойчивость, способность к восстановлению;
- реверсивность;
- безопасность;
- уровень сервиса и договор об уровне сервиса.

В настоящее время в ИСО/МЭК идёт работа над стандартами, описывающими фреймвок управления договорами об уровне сервиса для модели облачных вычислений серии 19086 «Information technology — Cloud computing — Service level agreement (SLA) framework».

Такая сложная ролевая модель обусловлена, в частности, серьёзной проблемой, связанной с техническими и организационными вопросами интеграции облачных сервисов, которые в общем слу-

Рис. 4.2.6. *Деятельность партнёра облачных вычислений.*

чае могут предоставляться разными провайдерами.

Другие важнейшие вопросы связаны с юридическими аспектами этой модели, в частности с вопросами:

- юридической защиты сторон — ролей облачных вычислений и разделения между ними ответственности;
- правовой поддержки профессионалов-специалистов;
- вопросов экспертизы и её юридической обоснованности;
- грамотных договоров, которые в развитых странах мира занимают сотни страниц;
- страхования.

Финансовые аспекты облачных технологий

Модель облачных сервисов активно развивается, в частности, потому, что является весьма привлекательной в финансовом плане.

В Табл. 4.2.2 и Табл. 4.2.3, по материалам Gartner, приведена информация о вариантах оценки финансовой выгоды облачной модели для разных типов облаков. В Табл. 4.2.4 приведены выгоды от облачной модели, которые реально посчитать. А в Табл. 4.2.5 приведены сводные данные по затратам на облака.

Табл. 4.2.2. *Материальные финансовые выгоды от облачных сервисов.*

№ п/п	Материальные финансовые выгоды			Тип облака		
	Выгода	Детализация	Тип	IaaS	PaaS	SaaS
1	Сокращение затрат	Затраты на системных администраторов и руководство ими	Прямые, вычисляемые, регулярные	Стоимость обеспечения сервера X кол-во серверов, передаваемых провайдеру + Σ часть времени рук-ва (пропорционально кол-ву серверов)	Стоимость обслуживания сервера приложений X кол-во серверов, передаваемых провайдеру + Σ часть времени рук-ва (пропорционально кол-ву серверов приложений)	Стоимость администрирования передаваемых систем + стоимость администрирования баз данных + Σ часть времени руководства
2		Расходы на разработку ПО	Прямые, вычисляемые, периодические			Затраты на разработку ПО по передаваемому ПО – прогноз
3		Лицензии на ПО (модель SaaS) и затраты на поддержку	Прямые, вычисляемые, регулярные			Стоимость лицензий на ПО и на поддержку (25-30% от стоимости лицензий)
4		Поддержка пользователей и оборудования	Прямые, вычисляемые, регулярные	См. п.1	См. п.1	Стоимость лицензий на ПО и на поддержку (25-30% от стоимости лицензий)

Табл. 4.2.2 (продолжение). *Финансовые выгоды от облачных сервисов.*

№ п/п	Материальные финансовые выгоды			Тип облака		
	Выгода	Детализация	Тип	IaaS	PaaS	SaaS
5	Сокращение затрат	Сопровождение — апгрейды, апдейты, патчи	Прямые, вычисляемые, периодические	См. п.1	См. п.1	См. п.1
6		Хостинг	Прямые, вычисляемые, регулярные	Затраты на хранение серверов и оборудования	Затраты на хранение серверов и оборудования	Затраты на хранение серверов и оборудования
7	Рост продуктивности	Мобильность пользователей и доступность	Прямые, вычисляемые, периодические	Сокращение периода неработоспособности оборудования X стоимость простоя оборудования	Сокращение периода неработоспособности платформы X стоимость простоя платформы	Сокращение периода неработоспособности АС X стоимость простоя АС
8	Оптимальное использование ресурсов	Компания использует ресурсы в том объёме, который ей необходим. Сокращение затрат неиспользуемого рабочего времени	Прямые, вычисляемые, периодические	Затраты на подключение сервера	Затраты на подключение платформы	Затраты на подключение АС
9	Улучшение безопасности / согласованность	Провайдер может предоставить высокий уровень защиты данных	Прямые, вычисляемые, регулярные	Затраты на обеспечение безопасности собственных серверов	Затраты на обеспечение безопасности собственной платформы	Затраты на обеспечение безопасности собственной АС
10	Доступ к компетенциям и возможностям	Использование высококвалифицированного персонала без роста затрат (найм, зарплата, обучение)	Непрямые, сложно вычисляемые, периодические			
11	Масштабирование	Выделение ресурсов по требованию, сокращение затрат на планирование мощностей	Прямые, сложно вычисляемые, периодические	Затраты на планирование мощностей	Затраты на предоставление доступа пользователю	Затраты на предоставление доступа пользователю
12	Скорость	Сокращение сроков внедрения, сокращение сроков разработки / тестирования	Прямые, сложно вычисляемые, периодические	Затраты на выделение сред разработки и тестирования	Затраты на выделение сред разработки и тестирования	Затраты на выделение сред разработки и тестирования
13	Удовлетворённость заказчика	Сокращение времени отклика на запросы заказчиков	Прямые, сложно вычисляемые, регулярные	Сокращение времени обработки инцидентов и изменений	Сокращение времени обработки инцидентов и изменений	Сокращение времени обработки инцидентов и изменений
14	Надёжность	Провайдер может предоставить высокую надёжность серверов и средства восстановления после сбоя.	Прямые, сложно вычисляемые, периодические	См. 13	См. 13	См. 13
15	Производительность	За счёт мониторинга со стороны провайдера	Прямые, сложно вычисляемые, периодические	См. 13	См. 13	См. 13

Табл. 4.2.3. *Нематериальные финансовые выгоды от облачных сервисов.*

№ п/п	Нематериальные финансовые выгоды			Тип облака		
	Выгода	Детализация	Тип	IaaS	PaaS	SaaS
1	Широкое использование современных технологий для бизнеса	Эффективное использование современных технологий	Непрямые, сложно вычисляемые, периодические	Σ прибыль от инновации	Σ прибыль от инновации	Σ прибыль от инновации
2	Фокус на ключевые потребности бизнеса	Использование ИТ-ресурсов по запросу	Непрямые, сложно вычисляемые, периодические	Сокращение времени обработки инцидентов и изменений	Сокращение времени обработки инцидентов и изменений	Сокращение времени обработки инцидентов и изменений
3	Удовлетворённость сотрудников / инновации	Мобильность и хорошая производительность	Непрямые, сложно вычисляемые, периодические	Σ уволившийся сотрудник X затраты на увольнение	Σ уволившийся сотрудник X затраты на увольнение	Σ уволившийся сотрудник X затраты на увольнение
4	Взаимодействие	Взаимодействие может улучшить качество и использование инноваций	Непрямые, сложно вычисляемые, периодические	Затраты на взаимодействие по обслуживанию	Затраты на взаимодействие по обслуживанию	Затраты на взаимодействие по обслуживанию
5	Передача риска	Передача отдельных рисков провайдеру (безопасность, потеря данных, восстановление после сбоя)	Непрямые, сложно вычисляемые, периодические	Затраты на управление переданными рисками	Затраты на управление переданными рисками	Затраты на управление переданными рисками

Табл. 4.2.4. *Выгоды от облачной модели, которые реально посчитать.*

Выгоды	IaaS	PaaS	SaaS
Уменьшение затрат на обслуживание	Затраты на обслуживание серверов и оборудования: оплата сотрудников (зарплата. мотивация, обучение, административные расходы) + затраты на содержание + затраты на обновление	Затраты на обслуживание программных платформ: оплата сотрудников (зарплата. мотивация, обучение, административные расходы) + затраты на содержание + затраты на лицензии + затраты на поддержку	Затраты на обслуживание АС: оплата сотрудников (зарплата. мотивация, обучение, административные расходы) + затраты на содержание + затраты на поддержку
Рост гибкости, сокращение затрат на подключение новых пользователей (масштабирование) и нового функционала	Затраты на расширение и смену серверов и оборудования	Затраты на подключение нового ПО и пользователей	Затраты на расширение функционала и подключение новых пользователей
Сокращение затрат на обработку инцидентов и изменений	Затраты на расширение и смену серверов и оборудования Затраты на обработку инцидентов и изменений	Затраты на обработку инцидентов и изменений	Затраты на обработку инцидентов и изменений

Табл. 4.2.4 (продолжение). *Выгоды от облачной модели, которые реально посчитать.*

Выгоды	IaaS	PaaS	SaaS
Сокращение простоев пользователей	Сокращение простоев серверов и оборудования X стоимость простоя	Сокращение простоев платформы X стоимость простоя	Сокращение простоев АС X стоимость простоя
Сокращение затрат на обеспечение безопасности и организации восстановления после сбоев	Затраты на обеспечение безопасности и организации восстановления после сбоев серверов и оборудования	Затраты на обеспечение безопасности и организации восстановления после сбоев программной платформы	Затраты на обеспечение безопасности и организации восстановления после сбоев АС

Табл. 4.2.5. *Затраты на облака.*

Постоянные затраты	
Техническая готовность	Расширение полосы пропускания
Внедрение Cloud	Профессиональный сервис для внедрения, внешние консультанты
Интеграция	Профессиональный сервис для интеграции cloud с внутренними системами
Конфигурация / кастомизация	SaaS
Обучение	ИТ-специалистов и пользователей
Организационные изменения	Реинжиниринг (управление изменениями, мониторинг использования ресурсов, прогноз доступа пользователей, внутренний аудит)

Периодические затраты	
OPEX вместо CAPEX	Расширение полосы пропускания
Управление изменениями	
Управление вендорами	
Координация облаков	Если несколько провайдеров
Смягчение рисков	

Разовые затраты	
Возврат или смена провайдера	

Вывод

В настоящее время эксперты все чаще говорят, что после периода Cloud 1.0, когда в основном решались вопросы, как сэкономить время, используя облака для выполнения приложений и хранения данных, а основными параметрами качества были безопасность и надёжность, наступает период Cloud 2.0, когда встают вопросы, как вести бизнес и действовать в изменяющихся условиях, какое значение имеет полученная информации и как её можно использовать.

Глава 4.3

Интернет вещей

Вадим Подольный

Что такое Интернет вещей (IoT)?

Самое простое определение может звучать так:

> ***Интернет-вещей (IoT)*** *— совокупность устройств, обладающих интерфейсами сопряжения с сетью, и сама эта сеть.*

Важно отметить, что устройство может подсоединятся к данной сети через промежуточное сопряжение или даже цепочку сопряжений. Простейший пример: сопряжение фитнес-трекера с сетью через мобильный телефон. Приведём ещё пару распространённых определений.

> ***IoT*** *— это сеть физических объектов, которые имеют встроенные технологии, позволяющие осуществлять взаимодействие с внешней средой, передавать сведения о своём состоянии и принимать данные извне.* ***(Gartner)***

> ***IoT*** *— концепция вычислительной сети физических предметов («вещей»), оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой, рассматривающая организацию таких сетей как явление, способное перестроить экономические и общественные процессы, исключающее из части действий и операций необходимость участия человека.* ***(Википедия)***

Наряду с термином IoT, часто также используется и другой термин, который появился существенно раньше – ***M2M (Межмашинное взаимодействие, Machine-to-Machine)*** *— общее название технологий, которые позволяют приборам обмениваться информацией друг с другом.* Это проводные и беспроводные системы датчиков, которые передают информацию от одного устройства другому. Стек технологий M2M можно определить как подмножество IoT.

Одной из первых разработок в области мобильного межмашинного взаимодействия является OmniTRACS — решение Qualcomm, разработанное в 1989 году для отслеживания коммерческого транспорта.

Фактически, M2M позволил технологиям АСУ ТП в режиме онлайн получать доступ к объектам, ранее не доступным в связи с отсутствием

возможности постоянного прямого кабельного соединения с ними. Такие объекты можно разделить на два класса: удалённые объекты от кабельных сетей и подвижные объекты. Драйвером роста технологий M2M стало существенное развитие систем глобального позиционирования GPS/ГЛОНАСС и др.

Концепция IoT появилась в 1999 году, когда появилась технология радиочастотной идентификации физических предметов (RFID). Активная реализация, развитие технологических платформ на основе концепции началась с 2010 года. Драйверами развития IoT стали технологии межмашинного взаимодействия (M2M), развитие технологий связи 4G, развитие протокола IPv6, облачных технологий (SaaS, PaaS, IaaS и др.) программно-определяемых сетей (SDN) и программно-определяемых дата-центров (SDDC).

Таким образом, термины M2M и IoT в настоящее время являются равноправными.

В первом десятилетии XXI века стала активно развиваться доступная беспроводная связь, и она стала драйвером для развития технологий межмашинного взаимодействия.

Основными отраслями применения IoT стали:

1. Системы мониторинга и управления:

- транспортом;
- ЖКХ;
- медицинскими устройствами.

2. Системы мониторинга и управления безопасностью:

- автомобилей, судов (противоугонные системы);
- домов, квартир и офисов;
- людей и животных.

3. Системы мониторинга промышленного оборудования.

Промышленный интернет вещей (IIoT)

Отдельного рассмотрения заслуживает вопрос применения IoT в промышленности, где данное направление образует отдельный, целостный широкий кластер технологий, который называется индустриальный (промышленный) интернет вещей (Industrial IoT, IIoT). Промышленный интернет вещей — это совокупность устройств (датчиков, контроллеров, установленных на узлах и агрегатах промышленного объекта), средств передачи, сбора, обработки, визуализации и интерпретации информации, сопряжённых в единую сеть.

Фактически, такое определение можно дать и автоматизированной системе управления технологическими (производственными) процессами (АСУ ТП, АСУ ПП).

АСУ ТП и IIoT

Корни концепции АСУ ТП уходят к середине XX века и начинаются с таких технологий, как тепловая автоматика, релейная защита и автоматика (РЗА), на которых строятся схемы управления промышленным оборудованием в концепции жёсткой (не программируемой) логики, зарождается первое поколение АСУ ТП. Человек, обслуживающий такие системы, называется главным механиком, главным технологом; его роль заключается в том, чтобы обойти все устройства, проконтролировать их корректную работу, снять показания, занести в таблицу.

При развитии технологий микроэлектроники появляются программно-логические контроллеры (ПЛК, Programmable Logic Controller, PLC), позволяющие задавать алгоритмы управления в виде программ, что, в свою очередь, обеспечивает высокую гибкость, стандартизацию и формирование отрасли, появляется АСУ ТП второго поколение. Развитие сетевых комму-

никационных технологий и объединение ПЛК в сети образуют АСУ ТП поколения 2+.

Третье поколение АСУ ТП связанно с появлением мощных микропроцессорных систем, серверов на базе них, рабочих станций, коммутаторов и маршрутизаторов. Существенно разгружается логика ПЛК, часть функций низовой автоматики забирают на себя системы верхнего уровня (СВУ). Появляются сложные промышленные сети, большое разнообразие контроллеров и программного обеспечения. Выделяются направления:

- средства (сквозного) проектирования АСУ ТП в целом;
- средства программирования ПЛК;
- SCADA/HMI.

В начале XXI века компьютерные технологии развиваются, процессоры усложняются, их мощность растёт, и одновременно существенно падают на них цены. Расширяется спектр решаемых задач на микропроцессорной технике, появляются методы обеспечения надёжности (резервирования, диагностики, безопасности) такой техники. Появляются алгоритмы функционально-группового управления (ФГУ) совокупностью исполнительных механизмов и производством в целом, построенных по принципу обратной связи. Такие АСУ ТП принято называть поколением 3+.

Важно отметить, что в АСУ ТП поколения 2, 2+, 3, 3+ присутствует роль человека — оператора АУС ТП, получающего информацию и осуществляющего оперативное управление через СВУ.

Во втором десятилетии XXI века появляются «интеллектуальные» технологии и методы, которые принято называть технологиями «искусственного интеллекта» (ИИ), под которыми понимается совокупность следующих методов и технологий:

- нейронные сети (neural networks);
- нечёткая логика (fuzzy logic);
- генетические алгоритмы (genetic algorithm);
- машинное обучение.

Суть всех перечисленных методов в том, что они являются оптимизирующими (аппроксимирующими, уточняющими) методами решения математических (алгоритмических) задач.

Появляется ряд технологий, которые сильно меняют подход к построению АСУ ТП:

1. Контроллеры с нейропроцессорами, обеспечивающие мгновенную идентификацию состояния узла или подсистемы.

2. Контроллеры с нечёткой логикой (нечёткие контроллеры), обеспечивающие автономное принятие решения.

3. На мощных серверах локальных ЦОД, появляются технологии построения аналитических систем для идентификации и прогнозирования состояния систем, управляемых АСУ ТП, которые, в свою очередь, используют технологии машинного обучения на структурированных и не структурированных данных (big data).

4. Появляются математические сопроцессоры, ускоряющие решения базовых уравнений, описывающих наиболее распространённые технологические процессы:

- волновое уравнение (радиоэлектронная аппаратура, связь, РЭБ);
- уравнение непрерывности, Эйлера, Навье-Стокса, диффузии и др. (гидродинамика, движение жидкости, газа, аэродинамика, двухфазные потоки);
- вероятностных уравнений (метод Монте Карло, перенос частиц, нейтронно-кинетические расчёты);
- уравнения химии и радиохимии (расчёт химических процессов, в т.ч. испытывающих радиоактивный распад);
- уравнения физики прочности (расчёт сопротивления, прочности и надёжности материалов), и др.

Моделирование технологических процессов в режиме реального времени становится реальностью, нейросетевые апроксиматоры позволяют в режиме увеличенного пространственно-временного шага решать сложнейшие системы дифференциальных уравнений, описывающих технологические процессы с достаточно высокой точностью рамках задачи прогнозирования управления на 30-60 секунд вперёд, что раньше занимало достаточно длительное время счёта и требовало серьёзных вычислительных ресурсов.

Таким образом, оператор получает мощнейшие инструменты, помогающие идентифицировать (оценить) ситуацию и предлагающие (в режиме советника) пространство вариантов для действий. Класс таких решений называется ***системами поддержки приятия решения (СППР)***.

Совершенно не исключено, что повторяемые действия оператора по совету СППР можно, в свою очередь, автоматизировать — таким образом оператор становится супервайзером (наблюдателем). Часть функций управления отдаётся машине. Как минимум, за более крупный объект автоматизации могут отвечать меньшее число операторов. Например, АСУ ТП современной АЭС, которая обрабатывает и управляет десятками тысяч датчиков и исполнительных механизмов, сотнями тысяч рассчитываемых в режиме онлайн переменных, управляется всего двумя операторами и одним начальником смены.

Многие современные устройства низовой автоматики (датчики, контроллеры) стали интеллектуальными, они самостоятельно идентифицируют шум и отделяют его от реального изменения параметров, тем самым снижая общий поток данных в СВУ; они стали обладать коммуникационными интересами, которыми сопрягаются с системой в целом, а не сухими контактами, как в предыдущих поколениях. Много конечного оборудования — турбины, насосы, задвижки — сразу оснащены контроллерами диагностики и управления, поэтому эти устройства следует отнести к IIoT.

Такие решения классифицируются как АСУ ТП четвёртого поколения и напрямую лежат в пространстве концепции «Индустрия 4.0».

В целом концепция «Индустрия 4.0» обеспечивает возможность построения бережливого производства; в рамках неё ставится задача оптимизации управления технологическими процессами для снижения аварийности и продления ресурса эксплуатируемого оборудования, что иногда формулируется как переход от планово-предупредительного ремонта — к ремонту по состоянию. Таким образом, к задачам управления АСУ ТП четвёртого поколения добавляется задача оптимизирующего (усовершенствованного) управления. Такие АСУ ТП называются ***системами усовершенствованного управления технологическими процессами (СУУ ТП, Advanced process Control, APC)***. В состав СУУ ТП должны входить достаточно мощные средства долгосрочной предикативной аналитики. На промышленных производствах анализируется такие параметры, как появление дефектов, охрупчивание, изменение химического состава стали элементов конструкций (что может привести к их разрушению), осаждение, стенозис частиц, уменьшение толщины из-за образивной полировки трубопроводов (что может привести к разрыву), оценивают вибрацию и её влияние на свойства конструкций, их соединений и многое другое. Если производство целиком управляется СУУ ТП, то такое решение называется АСУ ТП поколения 4+.

Табл. 4.3.1. *Этапы совершенствования АСУ ТП.*

Промышленность			Автоматизация	+
Индустрия 1.0	Сила воды и пара	Поколение 1	Тепловая автоматика	РЗА
Индустрия 2.0	Сила электричества	Поколение 2	ПЛК	Сети
Индустрия 3.0	Сила ЭВМ	Поколение 3	ЭВМ	ФГУ
Индустрия 4.0	Сила IoT	Поколение 4	IIoT	СУУ ТП

Технологический прогресс не стоит на месте и, так или иначе, «машина» забирает на себя всё больше функций управления промышленным предприятием. С одной стороны, это хорошо — снижается «человеческий фактор», с другой стороны, одна ошибка в алгоритме ФГУ и проблемы могут быть существенными.

Надёжность и безопасность IIoT зависит от многих факторов, которые могут найти своё отражение на каждом из этапов жизненного цикла любого из компонентов системы в целом. Построение надёжной и безопасной системы зависит от проработанности технологий проектирования и эксплуатации как отдельных компонентов, так и системы в целом, что определяется технологической платформой, в которой система разрабатывается и эксплуатируется.

Связь в IoT

Особая роль в реализации концепции IoT уделяется вопросам связи. Это обусловлено тем, что развитие технологий IoT требует высокого технологического разнообразие средств и каналов связи, обеспечения их стандартов, надёжности и безопасности связи в целом.

Проводная связь

Исторически сложилось, что самый надёжный и простой способ передачи данных между устройствами — это физическое их соединение кабельным каналом связи.

Конечные простейшие датчики традиционно присоединяются «сухими контактами» к контроллеру (АЦП, ЦАП).

С развитием технологий автоматизации и существенным удешевлением микроэлектроники датчики становятся «умными», «интеллектуальными» либо шлюзуются через умный контроллер в сеть и часто имеют «на борту» разъёмы для соединения с Ethernet, в т.ч. и по оптическому каналу.

Современные проводные сети используют, как правило, витую пару и порты стандарта RJ-45. Работа проводных сетей описываются стандартами IEEE 802.3. На сегодняшний день используется следующие стандарты:

- IEEE 802.3u с максимальной пропускной способностью 0,1 Гбит/сек.
- IEEE 802.3ab с максимальной пропускной способностью 1.0 Гбит/сек. и др.

Существует также стандарт IEEE 802.3an с максимальной пропускной способностью 10 Гбит/с, разъем SFP+.

Однозначным плюсом применения проводных сетей является их надёжность и безопасность. Для осуществления вмешательства нарушите-

лю необходим физический доступ к кабелю. Указанные выше стандарты сохраняют свои характеристики при длине кабеля до 100 м.

Power Line Communication (PLC)

Важнейшей современной технологией проводной связи для IoT является связь через линии электропередачи (ЛЭП, Power Line Communication, PLC). Такая сеть может передавать данные, накладывая аналоговый сигнал поверх стандартного переменного тока частотой 50 Гц или 60 Гц. PLC включает BPL (англ. Broadband over Power Lines — широкополосная передача через линии электропередачи), обеспечивающий передачу данных со скоростью до 1 Гбит/с, и NPL (англ. Narrowband over Power Lines — узкополосная передача через линии электропередачи) со значительно меньшими скоростями передачи данных до 1 Мбит/сек.

PLC технология удобна для подключения узлов к сети Интернет, сопряжения в сеть бытовых устройств в квартире и офисе, а также в ЖКХ и в системах безопасности.

Рис. 4.3.1. *Бытовой Power Line контроллер TP-Link.*

Радиосвязь

И всё же, основным драйвером развития технологий IoT является беспроводная радиосвязь. В большинстве случаев устройства IoT являются зависимыми от автономного питания, и встаёт вопрос об энергии, затрачиваемой на коммуникации, а чем меньше будет потреблять модуль передачи данных (радио модуль), тем лучше.

Таким образом, можно классифицировать применяемые модули по радиусу действия:

- малый — NFC, Bluetooth, нательная компьютерная сеть;
- средний — WiFi, ZigBee, мобильная связь, LTE, 5G;
- дальний — спутниковая связь, LPWAN, LoRa.

Устройства, обеспечивающие передачу данных, при их приближении наименее всех расходуют энергию, однако обладают низким радиусом действия и малой скоростью передачи данных.

NFC (ISO 14443)

Ближняя бесконтактная связь (Near Field Communications, NFC) — технология беспроводной передачи данных малого радиуса действия, которая даёт возможность обмена данными между устройствами, находящимися на расстоянии около 10 см, анонсирована в 2004 году. Особенность данной технологии — отсутствие постоянного соединения.

Применяется для считывания данных со смарт-карт, смартфонов, смартчасов и прочих носимых с собой устройств для осуществления бесконтактных платежей и идентификации.

Считыватель NFC может работать только с одним источником данных на расстоянии не более 0,2 м. Скорость установки соединения — менее 0,1 сек. NFC полностью совместим с RFID.

Bluetooth (IEEE 802.15.1)

Протокол относится к беспроводным персональным сетям (Wireless Personal Area Network, WPAN).

Bluetooth — достаточно устоявшийся стандарт и обеспечивает обмен информацией между большой разновидностью устройств, как компьютерной периферии (мышки, клавиатуры, джойстики, принтеры), так и мобильных, но-

симых устройств (мобильные телефоны, смарт часы, трекеры, гарнитуры).

Bluetooth позволяет этим устройствам сопрягаться, когда они находятся в радиусе до 10 м друг от друга (дальность сильно зависит от преград и помех), даже в разных помещениях. Скорость установки соединения — от 5 сек.

Наиболее распространён стандарт Bluetooth 4.X, скорость передачи информации в котором может достигать до 3,125 МБ/сек и поддерживать его на расстоянии до 50 м (без препятствий). В стандарте Bluetooth 5.0 скорость удваивается до 6,25 МБ/сек, а расстояние — до 200 м (без препятствий), и, что важно, при меньшем потреблении электроэнергии. Стандарт Bluetooth 5.0 разработан для IoT устройств в 2016 году.

ZigBee (IEEE 802.15.4)

ZigBee относиться к семейству протоколов WPAN. Данный протокол можно отнести к переходному между низким и средним радиусом действия. Расстояние работы адаптеров не более 75м (до 1,5 км с усилителем ZeegBee Pro). Скорость передачи данных очень низкая — до 250 КБ/сек.

Основная особенность технологии ZigBee заключается в том, что она при малом энергопотреблении поддерживает не только простые топологии сети («точка-точка», «дерево» и «звезда»), но и самоорганизующуюся и самовосстанавливающуюся ячеистую (Mesh) топологию с ретрансляцией и маршрутизацией данных, и содержит возможность выбора алгоритма маршрутизации в зависимости от требований приложения и состояния сети, механизм стандартизации приложений — профили приложений, библиотека стандартных кластеров, конечные точки привязки, гибкий механизм безопасности, а также обеспечивает простоту развёртывания, обслуживания и модернизации.

ZigBee, в основном, применяется в промышленной автоматизации в устройствах IIoT.

Мобильная связь (LTE, 5G)

Мобильная связь стала основным драйвером роста рынка IoT устройств. При повсеместном вводе в эксплуатацию сетей 5G, рост рынка IoT будет лавинообразным. Базовые станции 5G смогут обслуживать одновременно миллионы устройств, обеспечивая надёжные соединения с ними на скоростях до нескольких ГБ/сек при меньшем расходе энергии батарей, чем в сетях 4G. Конечно же, сначала 5G будет доступен только в крупных городах, а расстояние до базовых станций составит сотни метров. Возможно, 5G вытеснит WiFi, в силу большого расхода энергии батарей WiFi адаптерами.

Особенность 5G сетей заключается в том, что в рамках физической 5G сети можно создавать программно-определяемые сети (SDN) и создавать Mesh сети с задаваемыми параметрами маршрутизации и ретрансляции данных.

Важным драйвером роста IoT в сетях 5G будет отказ от физической SIM карты и переход к виртуальной SIM карте, что одновременно и уменьшит, и удешевит конечные потребительские устройства.

Энергоэффективная сеть дальнего радиуса действия (Low-power Wide-area Network, LPWAN)

LPWAN беспроводная технология передачи небольших по объёму данных на дальние расстояния, разработанная для распределённых сетей телеметрии, M2M и IoT. Технологии LPWAN позволяют передавать данные на расстояния до 15 км при достаточно низком энергопотреблении. Особенность LPWAN заключается в высокой проникающей способности радиосигнала в городской застройке при частотах меньше.

В LPWAN выделяют технологии NB-IoT и LoRa.

NB-IoT разработана на базе существующих стандартов мобильной связи. Сети NB-IoT работают в лицензируемом спектре частот. Стандартизация технологии завершилась в июне

2016 года. Курирует разработку этой сети 3GPP. В NB-IoT обеспечивается поддержка более 100 тысяч соединений на соту; аккумулятор устройства, подключенного к NB-IoT, может работать до 10 лет без подзарядки. Технология проприетарная и требует лицензирования.

Технологию LoRa продвигает LoRa Alliance, в который входят IBM, CISCO и ещё более 500 компаний. Наиболее известный протокол LoRa – LoRaWAN – это аппаратный протокол управления связью между LPWAN шлюзами и конечными узлами устройств. Сеть LoRaWAN (Long Range Wide-Area Networks – глобальная сеть большого радиуса действия) развёртывается в частотном спектре, не требующем лицензирования. Устройства в сети LoRaWAN асинхронно передают данные для отправки на шлюз. Затем несколько шлюзов, получившие эту информацию, отправляют пакеты данных на централизованный сервер сети, а от него – на серверы приложений.

Услуги связи LoRaWAN оказывают мобильные операторы связи более чем в 250 городах мира. Такую популярность этого стандарта специалисты объясняют низким уровнем энергопотребления (устройства могут работать до 10 лет без подзарядки), большой территорией покрытия и невысокой стоимостью адаптеров.

Нательная компьютерная сеть (Body Area Network, BAN, IEEE 801.15.6)

Тело человека проводит радиоволны и электричество, что позволяет создавать нательную сеть. BAN устройства могут быть имплантированы в тело, прикреплены к поверхности тела в фиксированном положении или совмещены с мобильными переносными устройствами.

Устройства, сопрягаемые BAN, прежде всего, выполняют функцию в области медицины. Такие (IoT) устройства собирают информацию о состоянии здоровья человека и с помощью мобильных устройств передают её потребителю данной информации.

Особенности маршрутизации в сетях IoT

Важным вопросом является маршрутизация в IoT сетях. Как уже было сказано выше, многие IoT устройства оснащены лишь коммуникационными модулями ближней связи и требуют ретрансляционное устройство для передачи данных по назначению.

По различным оценкам аналитиков к 2020 году количество IoT устройств составит до 50 млрд единиц, а, как известно, пространство IPv4 адресов заканчивается. На помощь приходит IPv6 адресное пространство.

Однозначно, именно IoT становится драйвером перехода со старого доброго IPv4 к пространству IPv6.

IPv6 обеспечивает сквозную связь, с более распределённым механизмом маршрутизации. IPv6 поддерживается обширным сообществом разработчиков и исследователей, которые непрерывно совершенствуют функций безопасности, включая IPSec.

Существует разработка усечённого протокола IPv6 для сокращения размера IP адреса в малых сетях IoT 6LoWPAN, при этом пограничные маршрутизаторы могут преобразовывать эти сжатые адреса в обычные IPv6.

Благодаря большому адресному пространству, IPv6 позволяет поднимать (Web) сервисы на любом устройстве IoT. Для этого создан протокол Constrained Application Protocol (CoAP, RFC 7252), который предназначен для использования в устройствах с сильно ограниченными ресурсами, он обеспечивает возможность передачи данных через Интернет (Web Transfer Protocol) с полной поддержкой архитектуры REST.

IPv6 предоставляет мощные функции не только для поддержки мобильности конечных узлов, но и обеспечивает мобильность узлов маршрутизации сети, что, в свою очередь, позволяет создавать не только классические сети, но и такие как сети ячеистой топологии (mesh) или гибридные (Рис. 4.3.2).

Сети ячеистой топологии (Mesh):

Ячеистая топология —топология сети, построенная по принцу ячеек, в которой узлы сети соединяются друг с другом и способны выполнять роль маршрутизатора для остальных подключенных узлов. Такая топология сети является достаточно сложной в настройке, однако, при такой топологии реализуется высокая отказоустойчивость. Как правило, узлы соединяются по принципу «каждый — с каждым (доступным)». Таким образом, большое количество связей обеспечивает широкий выбор маршрута трафика внутри сети — следовательно, обрыв одного соединения не нарушит функционирования сети в целом. Mesh сети обеспечивают возможность ретрансляцию трафика от источника постоянного соединения с глобальной сетью к отдалённым, мобильным устройствам (IoT).

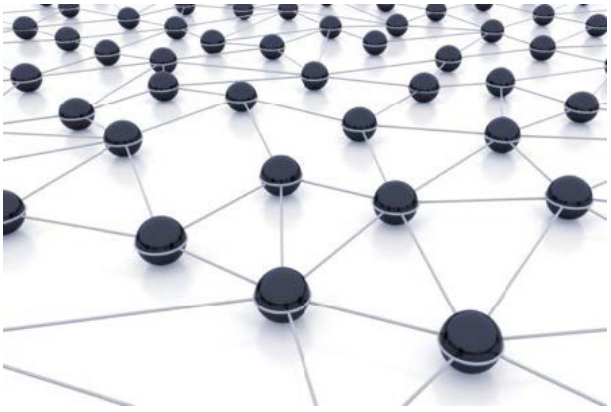
Mesh сети бывают проводными, однако наибольшее распространение получили их беспроводные реализации, которые называются беспроводными ячейковыми сетями. Выделяют следующие особенности таких сетей:

- ***Самоорганизация сети.*** Является ключевой особенностей беспроводной Mesh сети. Это означает, что при подключении каждый узел автоматически получает информацию обо всех других узлах и определяет свою роль.
- ***Самовосстановление сети.*** При выходе из строя одного из узлов сеть способна перенаправить данные, т.е. переопределить маршруты автоматически.
- ***Быстрое и недорогое развёртывание.*** Развёртывание ячеистой сети не требует дорогостоящей инфраструктуры. В силу способностей к самоорганизации и самовосстановлению, такая сеть является экономной в эксплуатации.

Многие протоколы по умолчанию поддерживают ячеистую организации сети. Например, Bluetooth поддерживает протокол Bluetooth Mesh, протокол ZigBee поддерживает ячеистую структуру. Из WiFi маршрутизаторов достаточно просто собрать Mesh сеть. Принцип работы сетей 5G включает возможность организации режима Mesh сети.

Наибольшее распространение mesh сети нашли в современной армии и военной технике, но будущее, конечно, у этой технологии за устройствами IoT.

Рис. 4.3.2. *Топология Mesh сети.*



Энергоэффективность сетей

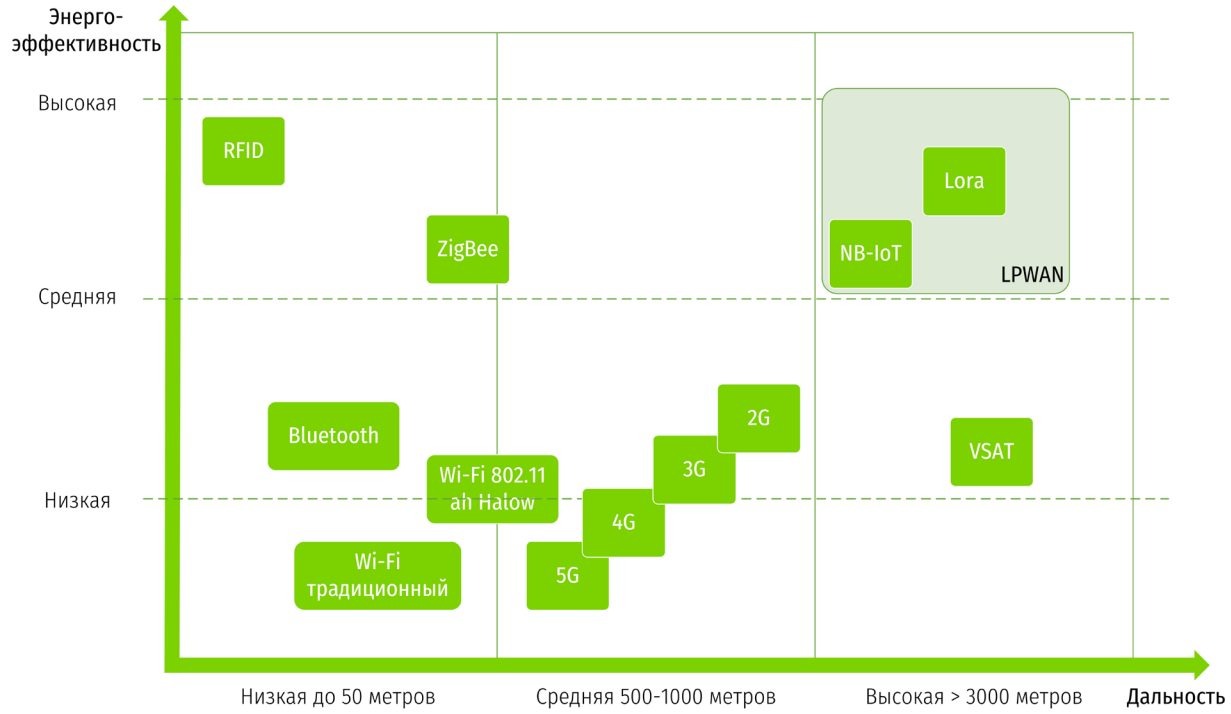
Мы уже затрагивали вопрос энергоэффективности в IoT. Остановимся на нём чуть подробнее.

Дело в том, что в массе своей IoT-устройства пытаются максимально минимизировать по размеру, и, естественно, очень остро встаёт вопрос обеспечения автономности данного устройства. Идеально, когда устройство может быть пассивным (не требовать дополнительного питания для своего функционирования) или оно встраивается в инфраструктуру другого объекта, которое и обеспечивает IoT блок необходимым питанием (например, IoT-кофеварка, где датчик запуска кофеварки легко может питать от сети питания самой кофеварки). Но всё чаще возникает задача и автономного питания для IoT-устройства. И в этот момент одним из приоритетных вопросов становится вопрос обеспечения связи на продолжительном (желательно бесконечном) горизонте времени.

И вопрос энергоэффективности сетевых ком-

муникаций выходит на первый план. На Рис. 4.3.3 схематично представлена зависимость между расстоянием и энергоэффективностью для рассмотренных выше сетевых технологий.

Рис. 4.3.3. *Схема энергоэффективности для различных сетевых технологий.*



Области применения IoT

Умный дом

Домашняя автоматизация (home automation), или умный дом (smart home) — это система домашних устройств, сопряжённых в сеть по различным каналам связи, способных выполнять действия и решать повседневные задачи без участия человека.

Задачи, решаемые контроллерами автоматизации умного дома, разделяются, как и в обычной промышленной автоматизации, на контроль (мониторинг) и управление.

Система умного дома включает три типа устройств:

- шлюзовые контроллеры (хабы) — управляющие устройства, соединяющие все элементы системы друг с другом и обеспечивающие централизованный доступ к системе (по единому протоколу, API, приложению и др.);
- датчики (сенсоры) — устройства, получающие информацию о внешних условиях;
- актуаторы — исполнительные устройства, непосредственно исполняющие команды.

Датчики и актуаторы – IoT устройства, в составе которых есть модуль сопряжения через сеть с сетью умного дома с хабом.

Разделяются:

- контроллеры управления водоснабжения, газоснабжения, электроснабжения, Smart Grid и др.;
- контроллеры домашнего климатического оборудования (кондиционеры, увлажни-

тели, отопительная техника др.);
- контроллеры управления освещённостью;
- контроллеры управления бытовыми устройствами (чайник, духовка и др.);
- контроллеры управления медиа устройствами (аудио, видео, связь);
- контроллеры клинингового оборудования (робот пылесос, робот мойщик окон);
- контроллеры голосового управления;
- контроллеры управления жестами;
- контроллеры систем безопасности (системы контроля и управления доступом — СКУД, мониторинг движения, голоса, пирометрии и т.д.).

Существует три механизма управления умным домом:
- автономное управление;
- управление пользователем;
- управление внешним оператором.

Умный дом с автономным управлением выполняет базовые простейшие сценарии управления:
- зашёл в комнату — включился свет;
- все покинули дом — все системы перевелись в энергосберегающий режим.

Пользовательское управление заключается в прямых осознанных действиях пользователя:
- хлопнул в ладоши два раза — выключился свет
- сказал «чайник кипяти», или нажал кнопку в мобильном приложении — включился чайник, если есть вода;
- перевёл дом в режим сна — все системы перевелись в энергосберегающий режим.

Управление умным домом внешним оператором — это отдельный бизнес будущего, элементы которого можно наблюдать уже сегодня, например, мониторинг безопасности домов и квартир. Внешнее оперативное управления можно разделить на два типа: автоматизированное и ручное. Потребителю будут доступны пакеты услуг (пакеты сценариев) управления его умным домом. С каждым новым устройством сложность управления умным домом будет расти, и на помощь придут соответствующие приложения, которые будут загружаться в умный дом (контроллеры, хабы, серверы управления) или будут доступны в режиме SaaS (Software as a Service). Возможно, что в умном доме будущего не будет даже сервера и хаба, все контроллеры будут управляться в режиме IaaS (Infrastructure as a Service; SHaaS — Smart Home as a Service). Такие сервисы будут обеспечивать выполнение сложных задач, таких как:
- анализ содержимого холодильника и заказ продуктов — сервис будет анализировать запах и внешний вид в холодильнике, принимать решение? какой продукт испортился, информировать об этом пользователя и предлагать перечень продуктов к закупке, возможно, и без информирования пользователя; служба доставки привезёт новые продукты, положит их в холодильник и утилизирует испорченные или просроченные;
- анализ чистоты помещений — управление клининговой техникой, возможно, доставляемой при необходимости по подписке, вызов клининговой службы и контроль её работы;
- управление медиаконтентом в умном доме и др. активности.

Очевидно, что для управления IoT умного дома потребуется платформа, сопрягаемая с огромным количеством сервисов, обеспечивающая функционально-групповое управления (ФГУ) устройствами, как в автономном интеллектуальном режиме, так и в режиме оперативного управления.

Smart Grid

Современный умный дом — это не только потребление электроэнергии из сети, но и её ге-

нерация. В умном доме могут быть установлены солнечные батареи, реже — частные ветрогенераторы, ещё реже — генераторы, работающие на биогазе или истопники геотермальной энергии.

Такие умные дома непременно подключены к умной сети распределения электричества (Smart Grid), и они могут не только обеспечить собственные нужны умного домохозяйства, но и отдавать часть сгенерированной электроэнергии в сеть. Концепция Smart Grid предусматривает компенсацию за принятое в сеть электричество домохозяйству согласно тарифам.

Также концепция Smart Grid включает механизмы автономного накопления электроэнергии и её использования в случае нехватки мощности автономных источников домохозяйства. Также в случае блэкаута (аварии в энергосистеме), Smart Grid может перераспределить электроэнергию автономных домохозяйств на важнейшие источники потребления в округе, например, в больницу.

Естественно, что узлы Smart Grid являются узлами IIoT и могут централизованно управляться местным оператором.

Умное здание

Умное здание отличается от умного дома тем, что в здании могут не только жить, но и работать. Управление умным зданием требует большей ответственности, следовательно, многие системы должны быть резервированы, в т.ч. и IoT устройства, управляющие умным зданием. Управление умным зданием может быть сопряжено с планируемыми бизнес-показателями, бизнес-единицами, его занимающими. Умное здание может содействовать в выполнении поставленных бизнес-показателей, корректируя поведение каждого отдельного постоянного и временного пользователя умного здания:

- СКУД умного здания может ограничивать нахождение пользователя на рабочем месте, напоминать о необходимости размяться, пообедать, закончить курить, покинуть рабочее место;
- видеонаблюдение СКУД может контролировать не только перемещение сотрудника, но и его эмоциональное состояние;
- климатические контроллеры умного здания могут создавать требуемые климатические условия для повышения эффективности труда;
- умное здание может быть сопряжено с личными IoT устройствами пользователей и контролировать их медицинские показатели и др.

Сценарии управления умным зданием станут высокодоходным бизнесом крупных корпораций, которые, в свою очередь, получат контроль и влияние над потребителями подобных услуг.

Умный город

Умный город — это концепция сопряжения различных автоматизированных систем управления объектами городской инфраструктуры в единую управляемую глобальную систему управления городом. Большая роль в концепции отведена IoT устройствам. По оценкам ООН, к 2050 году две трети населения Земли будут проживать в городах.

Цель создания умного города заключается в:

- повышении эффективности управления города в целом;
- повышении эффективности использования бюджетных средств города;
- управление ресурсом инфраструктуры города;
- повышении интегральной безопасности города;
- планировании управления городом в целом.

Концепция умного города подразумевает «переиспользование» как инфраструктуры, так и данных.

В современном городе масса различных объ-

ектов инфраструктуры:

- гражданские строения и здания (жилые и офисные, гостиницы, торговые центры, школы, больницы, поликлиники);
- промышленные инфраструктурные объекты:
  - генерация, транспорт и распределение электричества;
  - водоочистка, распределение, водоотведение;
  - теплоснабжение;
  - газоснабжение;
  - ЦОД (информационное снабжение), большие данные;
- транспортная инфраструктура:
  - метро, инфраструктура трамвайного и троллейбусного движения, дороги, мосты, эстакады, тоннели, светофоры, речные шлюзы, порты, аэропорты;
  - геоинформационные системы;
  - общественный и частный транспорт;
  - обслуживающий и ремонтный транспорт;
- службы реагирования (МЧС, скорая помощь, пожарная охрана и др.):
  - ситуационные центры;
  - системы поддержки принятия решений;
  - система 112;
- инфраструктура безопасности — видеонаблюдение, видеоаналитика, фотофиксация;
- человек:
  - биометрия;
  - дополненная и виртуальная реальность.

Каждый объект инфраструктуры города (подсистема) уже так или иначе автоматизирован, и встаёт несколько важных вопросов:

- пригодность существующих подсистем к сопряжению и их модернизация;
- оснащение автоматизацией неавтоматизированных систем;
- с чем сопрягать все подсистемы;
- куда складывать собираемые данные;
- как и где обрабатывать собираемые данные;
- что «вытаскивать» из обрабатываемых данных;
- каким образом результат обработки использовать в сопрягаемых системах и обеспечивать обратную связь;
- как обеспечить информационную безопасность сопрягаемых систем и сопряжения в целом;
- как обеспечить прозрачность и управляемость системы в целом.

Умный транспорт

В умных городах общественный транспорт будет (а в некоторых уже) оснащён контроллерами IoT. Кроме мониторинга позиционирования, такие контроллеры выполняют много различных функций.

В коллективном общественном транспорте:

- приём платежей и контроль проезда;
- контроль безопасности пассажиров и водителя;
- контроль расхода топлива;
- управление интервалами движения.

В личном и персональном общественном транспорте (например, в каршеринге):

- разблокировка и активация двигателя с помощью личных IoT устройств;
- контроль и получение информации о состоянии транспортного средства;
- управление маршрутами и пробками;
- контроль и экстренное реагирование при авариях (например, ЭРА ГЛОНАСС);
- прослушивание салона и анализ речи в целях рекламных и обеспечения безопасности.

Умный транспорт, оснащённый IoT, позволит и позволяет оптимизировать маршруты, управлять загруженностью дорог. Умный транспорт

сам становится IoT устройством и позволяет контролировать своё состояние, вовремя предупреждает о необходимости технического обслуживания. Умный транспорт сопрягается с сервисами оператора технического центра, дорожными службами, службами экстренного реагирования через специальные платформы сопряжения.

Интеллектуальная транспортная инфраструктура

В состав умного города входит интеллектуальная транспортная инфраструктура, которая, в свою очередь, сопрягается с подсистемами умного транспорта (ИТС). Частью ИТС являются умные дороги, в состав которых включены решения для сбора и обработки данных о транспортных средствах и дорожной инфраструктуре с целью принятия решений, включая:

- детекторы транспортного потока;
- адаптивные (умные) светофоры;
- системы автоматизированного управления освещением;
- средства автоматической фиксации нарушений правил дорожного движения;
- электронные средства безостановочной оплаты проезда;
- паркоматы;
- подключенные информационные табло.

В приоритетную национальную программу «Цифровая экономика» включены направления цифрового транспорта, в котором ставятся задачи цифровизации самих подвижных объектов и транспортной инфраструктуры в целом.

Медицина

Перспективное направление развитие технологий IoT — применение IoT в медицине. Здесь необходимо различать два класса устройств:

1. Бытовые устройства, в основном обеспечивают диагностику и мониторинг.

2. Профессиональное медицинское оборудование, которое, в свою очередь, можно разделить на два подкласса:

- пассивное — для диагностики и мониторинга;
- активное, которое с помощью исполнительных механизмов производит манипуляции с телом человека (важно отметить: в акцептном и безакцептном порядке).

В качестве бытовых медицинских IoT можно привести пример носимых трекеров, в состав которых могут входить различные датчики физической активности, термометры, пульсометры, тонометры, глюкометры и др., например: мотоциклетный шлем, измеряющий активность головного мозга и качество реакции, устройство слежения за зрачками водителя и оценки его реакции при вождении. Бытовые медицинские IoT устройства чаще всего вмонтированы в носимые трекеры, используют смартфоны для ретрансляции информации в соответствующие сервисы или ограничиваются её передачей на смартфон.

Профессиональное медицинское IoT оборудование для диагностики и мониторинга принципиально мало чем отличается от носимых

Рис. 4.3.4. *Часы-тонометр Omron Zero 2.0.*

Рис. 4.3.5. *Glucowear — неинвазивный глюкометр.*

бытовых устройств, но оно однозначно отличается качеством сенсоров и стоимостью приборов. К такому классу оборудования можно отнести, например, IoT холтеры — приборы, непрерывно снимающие ЭКГ, давление и другие параметры, капсулы для гастроскопии. Такие IoT устройства имеют свой канал связи с целевой IoT платформой сбора и обработки информации.

Профессиональное медицинское IoT оборудование может применяться и для манипуляций с телом человека. Например, носимые IoT устройства могут по расписанию или по состоянию вводить лекарства в организм, например, инсулин диабетикам или адреналин военным при получении ранения. Такие IoT устройства могут быть встроены, скажем, в униформу военного, пожарного, в бронежилет полицейского.

Не только мобильные медицинские устройства можно отнести к классу IoT. Существует масса примеров стационарного оборудования, которое можно отнести к данной категории. Профессиональное медицинское оборудование, применяемое для диагностики и манипуляций, в XXI веке сопряжено с сетью и позволяет решать массу полезных задач:

- возможность мониторинга состояния пациента из любой точки мира профильным специалистом;
- возможность проведения манипуляций в удалённом режиме профильным специалистом — одним или несколькими;
- мониторинг и диагностики самого оборудования для своевременного технического обслуживания и ремонта (если оборудование сломается при проведении манипуляции вряд ли кто-нибудь будет доволен, кроме, возможно, злоумышленников).

Самым современным медицинским устройством на сегодняшний день является медицинский робот-хирург Da Vinci, который позволяет профильному хирургу проводить операции пациенту, находящемуся на другом конце света, а в будущем, вероятно, — и на космической станции.

Ближайшее будущее медицинских IoT заключается в роботизации клиник, повышении автономности пациентов, которым необходим мониторинг и своевременные манипуляции. Позже появятся наноботы, и их группы для манипуляций с организмом человека, которые будут подчинены роевому принципу управле-

Рис. 4.3.6. *Робот-хирург Da Vinci.*

ния.

Важнейший драйвер роста IoT устройств в медицине — это совершенствование методов диагностики, выявление заболеваний на ранней стадии и общее повышения знаний о теле человека. Этому будут способствовать методы сбора, обработки больших данных, машинное обучение и искусственный интеллект.

Следует отметить, что тема кибербезопасности медицинских IoT устройств и платформ является важнейшим вопросом и камнем преткновения.

По прогнозам исследователей (компания Allied Market Research), рынок медицинских IoT-гаджетов и IoT-приложений до 2021 года вырастет до $140 млрд.

Военное применение

Применение IoT в армии исторически является классической задачей Автоматизированных Систем Управления Войсками (АСУВ), таких как, например, Единая Система Управления Тактическим Звеном (ЕСУ ТЗ).

Задача ЕСУ ТЗ определяется классически: необходимо связать воедино большой набор децентрализованных автономных систем, обеспечить слаженность работы системы в целом, её безопасность и целостность, увязать воедино всех разработчиков различного вида оборудования и контроллеров, определить протоколы связи и обеспечить их сопряжение с единой децентрализованной системой, обеспечить прозрачный контроль выполнения команд и задач в рамках функционирования системы в боевом режиме. Современные АСУВ типа «Акация» и «Заря 22» («Заря 21») — чем не IoT? Удивительно, но до сих пор не определён термин Military IoT (MIoT), давайте его, наконец, определим.

В целом, все АСУВ движутся в сторону повышения автономности РСУ (DCS), повсеместно внедряются технологии автономных интеллектуальных исполнительных устройств и

Рис. 4.3.7. *Российская АСУВ.*

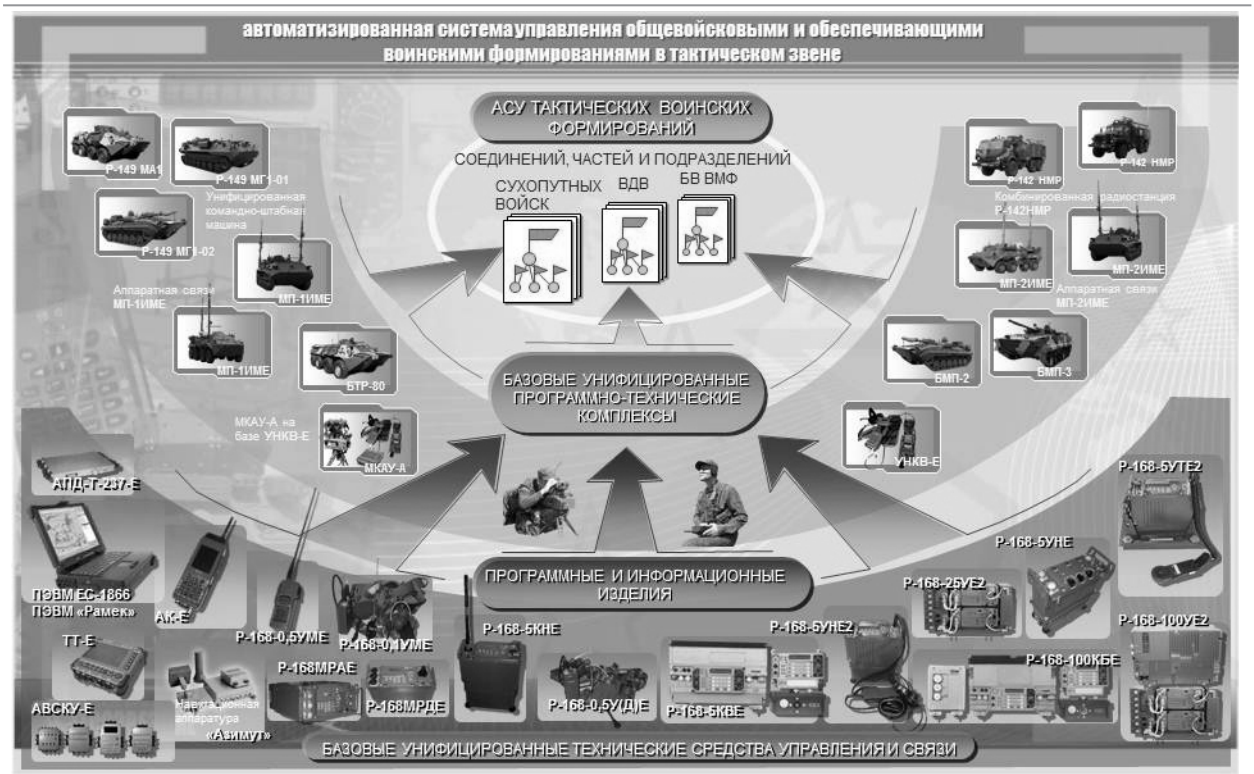


Рис. 4.3.8. *Десантируемый облачный ЦОД Nutanix.*

датчиков (IoT, IIoT), искусственного интеллекта и машинного обучения, технологии дополненной и виртуальной реальности (AR, VR), технологии анализа неструктурированных данных (Big Data), технологии надёжных распределённых архивов (Block Chain). Некоторые функции АСУВ выносятся в облачные сервисы, в т.ч. локальные частные облака, распределённые мобильные ЦОД, в которых они размещаются.

Современный российский комплект снаряжения «Ратник 3.0» представляет собой целую сеть MIoT устройств: контроллер экзоскилета, шлем дополненной реальности, средства связи с высокой криптостойкостью, средства позиционирования, набор медицинских IoT для контроля состояния военнослужащего — это, не считая интеллектуального оружия.

Концепция армии США Future Combat Systems (FCS) также полностью включает весь приведённый стек технологий. Американская компания Nutanix, создающая технологии гражданской виртуализации для ЦОД, создала для военных сил США мобильный ЦОД для построения локальных частных облаков прямо на поле боя, тактический дата центр, фактически десантируемый мобильный облачный ЦОД в рамках проекта Deployable Joint Command and Control System.

В военной технике отрабатываются передовые средства связи, как, например, уже сейчас проектируются и испытываются средства беспроводной связи 6-го поколения. Именно военные технологии определяют будущее гражданских технологий, ведь в основном, лишь на военные бюджеты можно отработать и отладить технологии до их коммерческого применения.

В армии давно уже эксплуатируются сложнейшие MIoT, не только с удалённым управлением средствами разминирования, наземным транспортом доставки боеприпасов, различными роботизированными комплексами, но и полностью автономные летающие дроны со сверх- и гиперзвуковыми скоростями, с офф-флайн средствами идентификации и распознавания цели, и алгоритмами ИИ принятия решения о её поражении.

Именно в армии впервые появились полноценные работающие Mesh сети, позволяющие строить системы управления роем (вооружения), именно эти технологии в дальнейшем определят стандарты управления роем автомобилей и других подвижных устройств на дорогах общего пользования, а также иных автономных роботизированных комплексов в любой среде эксплуатации.

Армия является сильнейшим драйвером развития технологий IoT. И не забывайте, многие IoT могут по запросу мгновенно превратится в MIoT.

Телеком

Операторы связи становятся операторами трафика с IoT устройств. Как отмечалось выше, существуют операторы, у которых объём бизнеса обслуживания трафика с подключенных устройств IoT (раньше некоторые операторы указывали M2M), составляет порядка половины. В недалёком будущем объем трафика с IoT устройств увеличиться и в какой-то момент достигнет половины от трафика, генерируемого людьми (ориентировано 2025 год) — это станет переломным момент для телеком операторов в связи с изменением структуры оплаты за трафик. Можно привести простой пример: в какой-то момент все мы начнём оплачивать установку и оплату трафика с умных счётчиков (тоже IoT устройства) горячей воды, электричества, газа и даже чистого воздуха в квартирах.

Появится масса отраслевых виртуальных операторов (Mobile Virtual Network Operator, MVNO), которые будут решать каждый свой перечень задач.

Многие телеком операторы обладают серьёзными мощными ЦОД, в рамках которых развёртываются отраслевые сервисные платформы (в т.ч. IoT платформы) для предоставления сервисного обслуживания потребителям соответствующих услуг. Также телеком операторы выстраивают бизнес на основе агрегации сервисных услуг платформ, предоставляемых внешними ЦОД и провайдерами услуг.

Телеком услуги разделяются на два типа: передача данных по каналам связи и предоставление по этим каналам связи доступа к сервисным услугам. В последнее время операторы начинают предоставлять пакетные услуги (для конечных потребителей, бизнеса, государственных учреждений), в состав которых входят необходимые сервисы и службы, включая модели обслуживания IoT устройств.

В России лидером данного направлении является компания «Ростелеком» в связке с «большой тройкой» операторов мобильной связи (МТС, Мегафон, Билайн). В США, Европе таким лидером скорее является Amazon в связке с локальными операторами мобильной связи.

Платформы IoT

Платформа — это набор технологий, которые определяют реализацию задач части или всего жизненного цикла изделия (продукции, решения). Платформа может решать задачи, как проектирования (разработки, design time), так и выполнения (эксплуатации, run time).

Чем сложнее система (больше число узлов, компонентов, соединений и их разнообразия), тем тяжелее проектировать и эксплуатировать такую систему; необходимо следить за актуальной версией прошивки (ОС, ПО) на каждом конечном устройстве системы в целом. Современные технологии позволяют эффективно решать данные вопросы.

Значимые платформы IoT

Прежде всего, IoT платформы создают операторы связи, предоставляя коммуникационные механизмы, например, LTE, NB-IoT (в будущем 5G).

Крупные интернет гиганты создают программные технологические IoT платформы, среди которых нужно отметить следующие:

- AWS IoT;
- Microsoft Azure IoT;
- Google Cloud Platform;
- SAP Leonardo IoT Platform;
- Oracle Integrated Cloud;
- IBM Watson IoT Platform.

Производители железа не отстают и создают свои IoT платформы, например, интересно выделить следующие: Cisco IoT Cloud Connect,

HPE Universal of Things (IoT) Platform, Siemens Mindsphere, Bosch IoT Suite, General Electric's Predix.

Следует отметить также следующие OpenSource разработки: Kaa IoT platform, IoTivity, ThingsBoard IoT Platform.

Кибербезопасность IoT

Важнейшей задачей в IoT является обеспечение информационной, компьютерной и в целом кибербезопасности. Появляются абсолютно новые модели угроз, нарушителей защиты. Обеспечивать кибербезопасность необходимо на каждом из этапов жизненного цикла не только вещей, но и человека.

В современном мире, где уже появилось множество IoT, требуется обеспечивать защиту:

- сетей связи;
- конечных устройств (стационарных и мобильных);
- узлов сопряжения, граничных и периферийных узлов;
- серверных узлов.

С точки зрения ПО, необходимо обеспечивать защиту широкого класса его разновидностей:

- ОС и прошивок IoT, конечных устройств, серверов и др.;
- платформ виртуализации и облачных платформ;
- виртуальных сетей, виртуальных ЦОД и платформ их организации;
- платформ хранения данных;
- платформ сопряжения, обработки и предоставления интерфейсов доступа к данным.

Подробнее о способах и инструментах обеспечения информационной безопасности смотрите в разделе Учебника «Информационная безопасность».

Интернет всего (IoE)

Цифровизация (или диджитализация — как не назови) шагает по планете и охватывает всё новые и новые отрасли и сферы. Устройства наравне с людьми становятся потребителями связи, данных, вычислительных ресурсов. Обычный Интернет людей сопрягается с Интернетом вещей и становится единой сетью сопряжения, которую принято называть Интернетом всего (Internet of Everything, IoE).

В какой-то момент времени, а возможно, где-то уже и сейчас, платформы и сервисы перестанут различать потребителей-людей от машин. Глобальный океан данных позволит воспользоваться любому его участнику глобальной сети теми или иными данными для решения поставленных задач. Такая доступность данных и вычислительных ресурсов приведёт к существенному ускорению глобализации.

Тотальная автоматизация, доступность вещей в сети является существенным драйвером к глобализации человечества. Тотально контролируемые вещи, казалось бы, должны сообщать и о неисправностях в самих вещах, и о «неисправностях» в теле человека, его действиях, обеспечивать повышение эффективности их применения и бережливого отношения к ним. Но общество потребления устроено так, что и человек, и вещи должны ломаться, поэтому лучше, если это будет прогнозируемо, причём своевременно.

Важно отметить, что основным драйвером роста IoT является общество потребления. В мире однозначно появятся глобальные и локальные регуляторы IoE, которые будут определять нормы допустимости применения технологий.

Глава 4.4

Философия искусственного интеллекта

Алексей Максимов

Константин Максимов

Искусственный интеллект – что это такое?

Одно то, что Википедия даёт несколько определений понятия «искусственный интеллект» (ИИ), говорит о том, что однозначного понимания, что же это такое, ещё не выработано.

Итак, под ИИ понимается:

1. Наука и технология создания интеллектуальных машин, особенно интеллектуальных компьютерных программ.

2. Свойство интеллектуальных систем выполнять творческие функции, которые традиционно считаются прерогативой человека (источник: Аверкин А.Н., Гаазе-Рапопорт М.Г., Поспелов Д.А. Толковый словарь по искусственному интеллекту. — М.:Радио и связь, 1992).

При этом, первое определение впервые прозвучало в 1956 году в Дортмунде в докладе Маккарти, который, в отличие от многих своих современников, не стал привязывать процедуру машинного мышления напрямую к человеческому интеллекту. Системы с искусственным интеллектом, в понимании Маккарти, могут сами выбирать алгоритм, необходимый для решения поставленной задачи, даже если представленный способ будет принципиально отличаться от логики человеческого мышления.

История создания искусственного интеллекта

История искусственного интеллекта начинается с момента создания первых ЭВМ в 40-х годах XX века.

С появлением электронных вычислительных машин, обладающих высокой (по меркам того времени) производительностью, стали возникать первые вопросы в области искусственного интеллекта: возможно ли создать машину, интеллектуальные возможности которой были бы тождественны интеллектуальным возможностям человека (или даже превосходили возможности человека)?

Основным направлением «движения мысли» исследователей ИИ того времени было воссоздание мыслительных процессов человека и реализации сходного механизма интеллекта в вычислительных машинах.

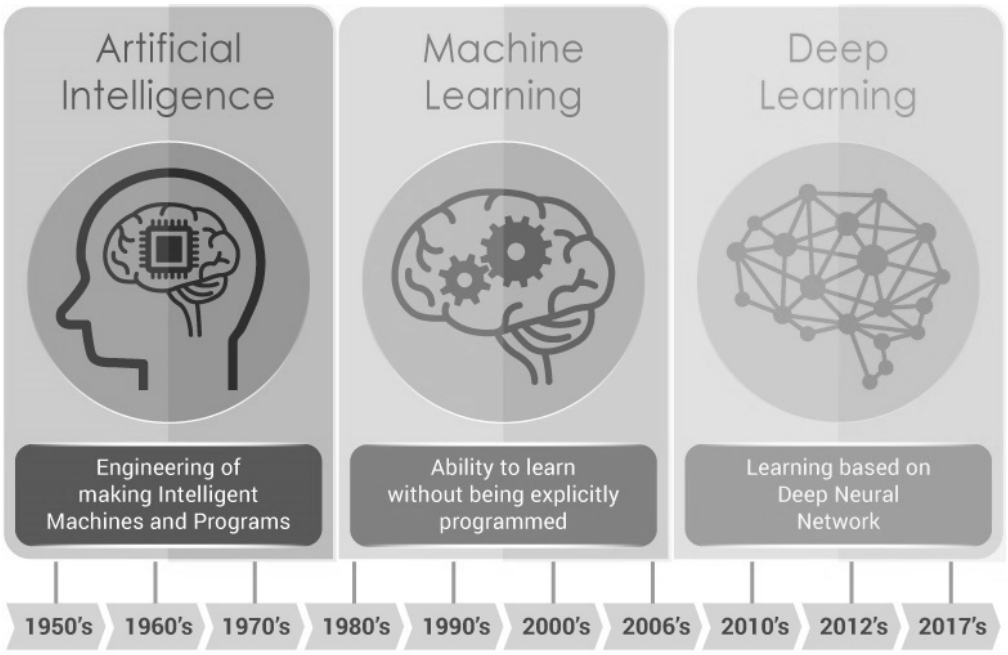
В 1950-м году в журнале «Mind» была опубликована статья Тьюринга «Computing Machinery and Intelligence» (в переводе Даниловой «Может ли машина мыслить?»), в которой рассматривается возможность создания машины, способной мыслить, как человек. Суть теста заключается в том, что участники не видят друг друга при общении, и задача человека – распознать что он общается с компьютером, а задача компьютера состоит в том, чтобы ввести в заблуждение человека, что он общается с компьютером, отвечая на заданные вопросы. Описанная в этой статье система (тест Тьюринга) широко используется до сих пор. Согласно тезисам Тьюринга, мыслящей машиной может считаться только система, способная давать логичные ответы на вопросы так, чтобы сторонний наблюдатель не смог отличить данные ей ответы от ответов живого человека. Тьюринг хотел найти сходство в математической модели функционирования нервной системы и цифровых вычислительных машин. Но ни Тьюрингу, ни его коллегам в полной мере достигнуть в тот период описанной цели не удалось.

Примерно тогда же появляется концепция Baby Machine, подразумевающая пошаговое обучение искусственного интеллекта вычислительной машины.

Однако, технические возможности вычислительной техники того времени существенно ограничивали возможности исследований.

Дальнейшими вехами на пути развития ИИ были работы Маккарти (разработка языка программирования Lisp для работы с системами с искусственным интеллектом), Боброва (понимание семантики естественного языка системами с искусственным интеллектом), Маслова (автоматический поиск решения теорем), Турчина (создание языка рекурсивных функций), Вайценбаума (создание первого интерактивного собеседника – Элизы), Фейгенбаума (создание первой экспертной системы).

Рис. 4.4.1. *История создания искусственного интеллекта.*



Существенный прорыв в практических приложениях искусственного интеллекта произошёл в 70-х годах, когда на смену поискам универсального алгоритма мышления пришла идея моделировать конкретные знания специ-

алистов-экспертов. В США появились первые коммерческие системы, основанные на знаниях и способные частично заменить специалиста-эксперта в разрешении проблемной ситуации (Википедия) – ***экспертные системы***. Пришёл новый подход к решению задач искусственного интеллекта – представление знаний. Созданы «MYCIN» и «DENDRAL» – ставшие уже классическими экспертные системы для медицины и химии. Обе эти системы в определённом смысле можно назвать диагностическими, поскольку в первом случае («MYCIN») по ряду симптомов (признаков патологии организма) определяется болезнь (ставится диагноз), во втором – по ряду свойств определяется химическое соединение. В принципе, этот этап в истории искусственного интеллекта можно назвать рождением экспертных систем.

Следующий значимый период в истории искусственного интеллекта – это 80-е годы, связанные с прорывами в построении ***искусственной нейронной сети (ИНС)***.

ИНС – математическая модель, а также её программное или аппаратное воплощение, построенная по принципу организации и функционирования биологических нейронных сетей – сетей нервных клеток живого организма. Это понятие возникло при изучении процессов, протекающих в мозге, и при попытке смоделировать эти процессы ещё в 1943 году.

Однако, именно в 80-ых годах XX столетия появились алгоритмы, позволяющие обучать Искусственные нейросети.

В этот период появляется направление ***машинного обучения (Machine Learning)*** – класс методов искусственного интеллекта, характерной чертой которых является не прямое решение задачи, а обучение в процессе применения решений множества сходных задач. Для построения таких методов используются средства математической статистики, численных методов, методов оптимизации, теории вероятностей, теории графов, различные техники работы с данными в цифровой форме .

До этих пор перенесение знаний специалиста-эксперта в машинную программу было утомительной и долгой процедурой. Создание систем, автоматически улучшающих и расширяющих свой запас эвристических (не формальных, основанных на интуитивных соображениях) правил – важнейший этап в последние годы.

В 2000-ых годах получил развитие раздела машинного обучения под названием ***глубокое обучение (Deep Learning)*** – совокупность методов машинного обучения (с учителем, с частичным привлечением учителя, без учителя, с подкреплением), основанных на обучении представлениям, а не специализированным алгоритмам под конкретные задачи .

Системы машинного обучения начали преуспевать в таких задачах, как распознавание лиц, распознавание речи, распознавание объектов, перевод, и многих других. В отличие от программ с закодированными вручную инструкциями для выполнения конкретных задач, глубокой машинное обучение позволяет системе научиться самостоятельно распознавать шаблоны и делать прогнозы.

Ещё одним важным этапом в развитии искусственного интеллекта стало использование в системах ИИ генетических алгоритмов. ***Генетический алгоритм*** — эвристический алгоритм поиска, используемый для решения задач оптимизации и моделирования путём случайного подбора, комбинирования и вариации искомых параметров с использованием механизмов, аналогичных естественному отбору в природе . Сами по себе генетические алгоритмы использовались при решении задач ещё с 60-ых годов XX века, но именно совмещение систем машинного обучения с генетическими алгоритмами позволило существенно продвинуться в создании систем ИИ.

Среди ключевых новостей и успехов искусственного интеллекта и машинного обучения

в частности, можно отметить:

- ***1997 год.*** Суперкомпьютер Deep Blue компании IBM обыграл чемпиона мира по шахматам.
- ***2005 год.*** Состоялось соревнование DARPA Grand Challenge между беспилотными автомобилями, где ИИ успешно преодолел трассу.
- ***2006 год.*** Команда Google Translate запустила статистический машинный перевод.
- ***2011 год.*** 40 лет DARPA CALO привели к созданию облачного персонального помощника Apple Siri.
- ***2011 год.*** IBM Watson победил в телевизионной игре Jeopardy!
- ***2011-2015 годы.*** На соревновании ImageNet по классификации миллиона изображений доля неверно классифицированных изображений упала с 25% до 3,5%. При этом доля ошибок у людей составляет 5%.
- ***2012 год.*** Компания Google X Lab: распознавание видеокадров с котами.
- ***2014 год.*** Система DeepFace компании Facebook распознает лица с точностью 97%.
- ***2015 год.*** Илон Маск и Сэм Альтман инвестируют 1 млрд. долларов в фонд исследовательской компании OpenAI, занимающейся ИИ.
- ***2016 год.*** Команда Google Translate запустила нейронный машинный перевод.
- ***2016 год.*** Программа AlphaGo компании Google DeepMind обыграла чемпиона мира по игре Го.

Победа алгоритма машинного обучения в игру Го является на сегодня одним из самых примечательных прорывов в развитии систем искусственного интеллекта

Основные компоненты искусственного интеллекта

Для решения любых задач системам с искусственным интеллектом требуются исходные данные. Именно поэтому, понятие искусственного интеллекта традиционно связывают с наукой о данных (Data Science). Наука о данных изучает данные, их изменения и алгоритмы их анализа.

Хотя сам термин «data science» впервые был использован П. Науром ещё в 1974 году, но широкое распространение он получил только в начале 2000-х, благодаря статье Кливленда, в которой автор описал перспективы развития технических аспектов статистических исследований и отметил науку о данных, как отдельную академическую дисциплину, в которой описаны все эти аспекты.

Именно специалисты по Data Science занимаются анализом данных и поиском оптимальных решений на их основе, используя для этого методы математической статистики, оптимизации, обучаемые искусственные нейронные сети, алгоритмы машинного обучения (machine learning) и глубокого обучения (deep learning), которые как раз и лежат в основе современных систем искусственного интеллекта.

Искусственная нейронная сеть

Именно искусственные нейронные сети лежат сейчас в основе систем ИИ.

Как мы уже говорили, Искусственная нейронная сеть – математическая модель или программа, имитирующая сеть нервных клеток человека. По сути, это сеть соединённых и передающих друг другу определённые данные искусственных нейронов.

Нейронная сеть – это последовательность нейронов, которые соединены между собой синапсами. Данная структура пришла в технический мир из биологии, имитируя мозг человека, в котором миллионы нейронов передают информацию в виде электрических импульсов.

Благодаря такой структуре, компьютеры могут анализировать и запоминать информацию.

Нейрон – это вычислительная единица, которая получает и производит вычисления над информацией и передаёт её далее. Существует три основных типа нейронов: входной нейрон, скрытый нейрон и выходной нейрон.

Синапс – это связь между нейронами, имеющая параметр «вес», благодаря которому информация изменяется, переходя от нейрона к нейрону.

Возьмём три входных нейрона, которые передают информацию следующему. Связь между каждым из трёх входных нейронов и одним выходным, имеет разный параметр «вес». Таким образом у выходного нейрона, информация будет состоять из совокупности трёх нейронов, с преобладанием того нейрона, у которого параметр «вес» больше.

Совокупность нейросети или ***матрица весов*** – это, можно сказать, своеобразный мозг системы, и благодаря этим весам, входная информация обрабатывается и получается результат.

Чтобы обрабатывать и получать результат, необходимо активировать, или обучить, нейронную сеть. Перед тем как начать процесс обучения нейронной сети, необходимо ввести ряд терминов.

Функция активации – это способ обработки или нормализации входных данных, т.е. на входе будет большое число, после применения функции, входные данные будут в необходимом для нас диапазоне.

Существуют три основные функции активации:

- ***Линейная функция –*** это функция в основном для тестирования или передачи данных без преобразований.
- ***Сигмоид*** или ***логистическая функция*** – основная функция, большинство примеров показано на её использовании, диапазон её значений – [0,1].
- ***Гиперболический тангенс*** – данная функция имеет диапазон [-1,1], т.е. может иметь как отрицательные данные, так и положительные значения (например, курс доллара может идти и вверх, и вниз).

Тренировочный сет – последовательность данных, поступающих в нейронную сеть.

Итерация – счётчик, который каждый раз увеличивается при прохождении тренировочного сета.

Эпоха – при активации нейронной сети, данный параметр выставляется в 0 и устанавливается вручную потолок для количества итерации. Важно не путать итерацию и эпоху – в эпохе может быть от одной до N количества итераций. Также важно избегать ошибок.

Ошибка – процентная величина, которая формируется каждую эпоху и должна стремиться к нулю.

Machine Learning

Однако, любую искусственную нейронную сеть необходимо обучить.

Нейросеть учится не так, как человеческий мозг. К примеру, мы хотим научить компьютер распознавать объекты на изображениях. Как будет выглядеть этот процесс? Мы берём нейронную сеть, которая представляет собой последовательность математических матриц и операций между ними. Затем показываем картинку и спрашиваем, что на ней, раз за разом отбраковывая неправильные ответы.

Здесь нам на помощь и приходит машинное обучение. Машинное обучение по сути – это создание, анализ и применение алгоритмов обучения нейросетей, способных совершенствоваться, благодаря получению дополнительной информации.

Традиционно выделяют два основных типа машинного обучения:

- ***Индуктивное обучение*** (именно его обычно и называют машинным обучением), основано на обучении системы, в ходе исследования определённых прецедентов. Входные и выходные данные для ряда прецедентов известны заранее. Алгоритм проводит их анализ, создаёт математическую модель и делает прогнозы для последующих прецедентов.
- ***Дедуктивное обучение*** предполагает использование для обучения структурированной базы данных (его обычно относят к области экспертных систем).

Алгоритм обучения должен получить ряд прецедентов и на их основе сформировать определённую математическую модель. Полученная модель исследуется, и на её основе делаются прогнозы для будущих прецедентов. При наличии достаточного объёма данных, прогнозы для новых прецедентов, созданные на основе построенной модели, должны с высокой вероятностью соответствовать действительности.

Рассматривая тот или иной алгоритм и ряд прецедентов, служащий исходными данными, помимо прочего, оценивается время его обучения. Для каждого случая используется своё предельное значение времени обучения.

Результаты математических моделей, рассматриваемых в теории вычислительного обучения, далеко не всегда подходят для практического применения.

Многие предположения, сделанные при составлении теоретической модели, не соответствуют реальным условиям. Практическая работоспособность того или иного метода в машинном обучении обычно доказывается результатами экспериментов, проводимых на реальных данных.

Как же все-таки сделать так, чтобы нейронная сеть давала правильные ответы?

Для решения данной задачи, используют различные методы обучения.

Метод обратного распространения

Основным и широко применяемым методом обучения нейронных сетей является Метод обратного распространения, и данный метод использует градиентный спуск.

Градиент – это вектор, который определяет крутизну склона и указывает его направление относительно какой-либо из точек на поверхности или графике.

Градиентный спуск – это способ нахождения локального минимума или максимума функции с помощью движения вдоль градиента.

Таким образом, метод обратного распространения можно определить, как последовательную передачу информации от входных нейронов к выходным. После чего мы вычисляем ошибку и, основываясь на ней, делаем обратную передачу, которая заключается в том, чтобы последовательно менять веса нейронной сети, начиная с весов выходного нейрона. Значение весов будут меняться в ту сторону, которая даст нам наилучший результат.

Обучение с учителем

Данный процесс или метод, основан на том, что в роли учителя выступает человек, а в роли обучаемого – нейронная сеть.

Учитель подаёт входные данные и ожидаемый результат, ученик, смотря на входные данные, стремиться получить ожидаемый результат.

Обучение без учителя

Данный метод, используется для группировки данных по определённым категориям. Например, на вход подали 100 тысяч различных статей, нейронная сеть должна разложить статьи по тематикам (программирование, история и т.д.).

Переобучение

Как и следует из названия, для случаев перенасыщения нейронной сети, эта проблема возникает при постоянном обучении на одних и

тех же данных. Таким образом, нейронная сеть не обучается, а запоминает («зубрит») данные. Мы будем постоянно, раз за разом показывать чёрные машины, и при показе белой машины она не сможет определить, что это машина, так как она запомнила, что машина – это всегда чёрная машина.

Deep learning

Глубокое обучение (Deep Learning) – это процесс обучения, с использованием искусственных нейронных сетей, построенный на принципе многослойности.

В процессе обучения на нескольких уровнях представления система формирует слои, соответствующие уровням понятий. В системе существует строгая иерархия, где признаки данных высокого уровня являются производными от признаков данных более низкого уровня. Состав слоёв для каждого случая (определённого типа решаемой задачи) будет своим.

Сложные задачи, предполагающие использование нескольких разных алгоритмов, обозначены были довольно давно. Это распознавание человеческой речи, художественный машинный перевод и ряд других неординарных задач. Однако, недостаточная теоретическая база и слабые технические возможности вычислительной техники не позволяли в полной мере реализовать их до середины 2000-х.

Существенный сдвиг в обучении нейронных сетей произошёл после разработки глубокой сети доверия (вид стохастической рекуррентной нейронной сети), которая объединила в себе несколько слоёв ***ограниченных машин Больмана***, что позволило такой сети обучаться без учителя, используя алгоритм обратного распространения ошибки, что, в свою очередь, позволило эффективно решать задачи высокого уровня сложности.

Сигнал, передающийся от входного слоя к точке выхода, в алгоритмах глубокого обучения подвергается большому количеству параметризированных преобразований, то есть сигнал от точки входа до точки выхода проходит через несколько блоков обработки данных с обучаемыми параметрами.

Чёткого определения количества преобразований для глубокого обучения нет, но принято считать, что при глубоком обучении в системе есть несколько нелинейных слоёв. То есть нить преобразований сигнала (credit assignment path, CAP) состоит минимум из трёх преобразований.

Архитектуры, применяемые при глубоком обучении, содержат многочисленные нелинейные преобразования. Существуют системы, в которых нить преобразований сигнала может насчитывать более 10 преобразований.

Роль технического оборудования

Развитие ИИ в последние годы связано с развитием алгоритмов, вычислительных мощностей, а также больших объёмов данных, обучение на которых и привело к выдающимся результатам.

Из этого следует, что одной задач по развитию ИИ, является разработка современных инженерных технологий, позволяющих обрабатывать огромные массивы данных для принятия решения машиной или думать как человек.

Но чтобы «думать» как человек, искусственный интеллект должен работать подобно человеческому мозгу. А наш мозг одновременно обрабатывает информацию из разных источников и не перегружается от этого, для него это – привычная ежедневная работа.

Т.е., для того, чтобы думать, необходимо обработать огромное количество информации.

Основные задачи по обработке данных возлагаются на CPU или GPU.

Как CPU (англ. – central processing unit), так и GPU (англ. – graphics processing unit) являются процессорами, и между ними есть много общего, однако сконструированы они были для выполнения различных задач.

Есть множество различий и в поддержке мно-

гопоточности: CPU исполняет 1–2 потока вычислений на одно процессорное ядро, а GPU может поддерживать несколько тысяч потоков на каждый мультипроцессор, которых в чипе несколько штук! И если переключение с одного потока на другой для CPU «стоит» сотни тактов, то GPU переключает несколько потоков за один такт.

Если CPU - это своего рода «начальник», принимающий решения в соответствии с указаниями программы, то GPU – это «рабочий», который производит огромное количество однотипных вычислений. Выходит, что если подавать на GPU независимые простейшие математические задачи, то он справится значительно быстрее, чем центральный процессор.

Именно поэтому для решения задач по обучению ИИ, часто пользуют именно GPU при разработке алгоритмов на базе нейросетей.

Люди

И, конечно, для реализации проектов в области ИИ не обойтись без высококвалифицированных специалистов по анализу данных (data scientist).

В основном, под data scientist понимают совокупность дисциплин: программирование, статистика, математика, а также знание предметной области. Сочетать в одном специалисте все дисциплины достаточно сложно, в связи с чем необходимо распределить задачи на несколько ролей.

1. Бизнес-аналитик

- предметная область;
- постановка задачи;
- разработка метрик.

2. Data engineer

- организация процесса сбора, очистки и предобработки данных.

3. Data Scientist

- анализ данных;
- извлечение информации/закономерностей;
- построение моделей.

Подводные камни ИИ-проектов

Можно выделить следующие проблемы, которые могут возникнуть при работе с проектами, связанными с машинным обучением:

- проблемы в данных,
- проблемы с постановкой задачи,
- проблемы с метрикой.

Проблемы в данных

Наиболее важным в машинном обучении и анализе данных являются сами данные. Необходимо понимать, каким образом эти данные были получены и собраны. От качества сбора данных зависит качество сделанных выводов и моделей.

Рассмотрим несколько примеров.

Пример 1. В 1948 году в Штатах проводились выборы. Было два основных кандидата: Дьюи – от республиканцев и Труман – от демократов. В день выборов проводился телефонный социологический опрос с целью выявления кандидата-победителя. Компания, проводившая опрос, пришла к выводу, что победит Дьюи. Как известно, в тех выборах победил Труман.

Такая ситуация произошла по следующим причинам:

- у бедных в 1948 году телефонов было значительно меньше, чем у богатых;
- бедные голосовали за Трумана. В итоге собранные данные состояли в основном из богатых людей и, соответственно, отражали мнение богатых людей, а не всего общества.

Пример 2. В Бостоне проводилось исследование, в каком районе города находится больше ям. Для этого разработали мобильное приложение, отслеживающее перепады высот, и на основе этого детектировались ямы на дороге. Больше ям по их исследованию получилось в богатых районах, хотя по факту ям больше в бедных районах. Причины для такого результата их эксперимента следующие:

- у жителей бедных районов меньше современных телефонов;
- у жителей бедных районов меньше машин.

Получается, что собранные данные, как и в примере выше, были нерепрезентативны.

Постановка задачи

При построении моделей машинного обучения очень важно понимать, какой вклад в бизнес она принесёт, и для чего решать данную задачу.

Рассмотрим пример с плохой постановкой задачи.

Некоторая компания коммуницирует со своими клиентами с помощью e-mail рассылки: раз в месяц она отправляет всем своим клиентам сообщение с интересными предложениями. Менеджеры данной компании решили, что нет смысла коммуницировать со всеми клиентами, надо отправлять только тем, кто откликается на предложение.

Частое заблуждение заключается в том, что надо строить модель, предсказывающую вероятность отклика клиентом на предложения в данный момент времени и рассылать только тем клиентам, у которых данная вероятность была бы наибольшей, но никакого хорошего результата для бизнеса данная задача в такой постановке не принесёт, даже, более того, прибыль компании от такого решения просядет. Произойдёт это по следующей причине: мало заинтересованные клиенты все равно откликаются, но делают это намного реже, чем заинтересованные, а значит, все равно приносят прибыль, а стоимость коммуникации по каналу e-mail равна нулю, следовательно, не отправляя им предложения, провоцируем уменьшение общей прибыли.

С другой стороны, данная задача имеет смысл в следующих ситуациях.

В случае наличия коммуникационной политики, которая запрещает постоянно «спамить» всех клиентов, нужно правильно выбирать момент времени, в который следует коммуницировать с клиентом.

Если канал коммуникации имеет ограниченную пропускную способность или большую стоимость таких коммуникаций (к примеру, коммуникации с клиентов проходят посредством звонков), в таком случае модель должна учитывать и стоимость коммуникации, и потенциальную пользу.

Если имеется большой перечень предложений, и в коммуникации необходимо выбрать одно или несколько самых важных предложений для данного клиента в данный момент времени, то в таком случае строится модель отклика на конкретное предложение.

Перед внедрением машинного обучения или любой другой системы необходимо понимать ожидаемый результат и проводить эксперименты с целью подтверждения и корректировки ожиданий, чтобы минимизировать риски и потери.

Проблема с метрикой

Основополагающей в постановке задачи является метрика, поэтому правильно уже до построения модели выбрать, каким именно образом будет измеряться качество, более того, надо правильно учесть особенности задачи в этой метрике.

Представьте, что вы владелец небольшого магазина и вы регулярно закупаете товар, который попадает на полки. Вы знаете, что у вас есть товар скоропортящийся и не скоропортя-

щийся, часто покупаемый и редко покупаемый. Вы хотите выбрать, когда и сколько какого товара вам надо закупать и завозить.

Если вы закупите очень много товара, есть риск, что он испортится или будет занимать слишком много места, и не хватит места для другого товара, или вы потратите много кредитных денег на закупку этого товара. С другой стороны, если вы закупите очень мало товара, вы рискуете потерять прибыль и лояльность клиентов, которые не смогли удовлетворить свою потребность в вашем магазине.

Из постановки задачи может показаться, что надо использовать стандартные метрики для задачи регрессии, но стандартные метрики не учитывают особенности бизнес-процесса.

Приведём примеры: штраф за ошибку в предсказании зависит от категории товара; необходимо учитывать стоимость закупки и доставки товара; необходимо учитывать потери, связанные со сроком годности товара.

Все эти нюансы должны быть явно отражены в метрике. Метрику формирует data scientist, но без знаний особенностей бизнес-процесса он не сможет это сделать правильно.

Практическое применение

Рассмотрим некоторые варианты применения искусственного интеллекта.

Главный плюс применения ИИ во многих ситуациях – это возможность оперативной обработки огромных массивов разнообразных, часто не связанных между собой напрямую данных и получение аналитических выводов.

Подобный инструмент может пригодиться во многих областях жизни.

Кейсы в разрезе технической реализации

Прогнозирование временных рядов

Временные ряды – это последовательность значений признака, измеряемого через постоянные временные интервалы.

Задача прогнозирования временных рядов – спрогнозировать значение признака в будущем, зная значение признака в прошлом.

Примеры задачи прогнозирования временных рядов:

- прогнозирование финансовых показателей;
- прогнозирование состояний технических устройств;
- прогнозирование пользовательской активности.

Анализ поведения пользователей

Задача анализа поведения пользователей отвечает на вопрос: как пользователь работает с сервисом (как он его изучает, как он решает или не решает с его помощью свои задачи).

Примеры задач:

- Описание целевой аудитории;
- Сегментация клиентов;
- Привлечение пользователей;
- Влияние на ключевые показатели;
- Прогнозирование оттока.

Анализ текстов

Направление в искусственном интеллекте анализа коллекций текстовых документов естественного языка

Примеры задач анализа текстов:

- Примеры задач анализа текстов;
- Предсказать рейтинг статьи;
- Определить эмоциональный окрас комментария;
- Определить тематику статьи;

- Сгруппировать новости по сюжетам;
- Найти слова, похожие по смыслу на данное;
- Выделить все упоминания имён в тексте;
- Построить краткую аннотацию текста;
- Построить модель, отвечающую на вопросы;
- Сгенерировать новый текст, похожий на заданный набор текстов.

Популярные системы, построенные на методах анализа текстов:

- Диалоговые системы;
- Чат боты.

Примеры диалоговых систем и чат ботов:

- Dialogflow – ранее назывался проект OpenAI, после покупки его компанией Gooogle, проект стал называться Dialogflow, и обеспечивает создание от простых FAQ до сложных сценарных проектов, на основе ML, NLP.
- Чат боты – Алиса от компании Яндекс, SIRI от компании Apple, OK Google от одноименной компании, а также Cortana от Microsof и Alexa от компании Amazon.

Компьютерное зрение

Создание систем, которые получают информацию из изображений и могут производить обнаружение, отслеживание и классификацию объектов.

Опишем наиболее часто выделяемые задачи компьютерного зрения.

Поиск по изображению

Сейчас существует несколько сервисов, которые позволяют искать картинки. Изначально для поиска использовались текстовые запросы. Некоторое время назад в части из таких сервисов появилась возможность поиска по загруженному изображению. От пользователя требуется загрузить картинку, а сервис будет искать похожие на неё изображения в интернете.

Это работает следующим образом. Сначала индексируются изображения из интернета. Для них строятся некоторые цифровые представления, из которых формируется структура данных, по которой можно быстро производить поиск. Для пользовательской картинки также используется цифровое представление, по которому в сформированной структуре данных ищутся дубликаты или похожие картинки.

Данная задача является сложной в структурном смысле. В интернет загружены миллиарды изображений, и использование сложных методов сравнения невозможно, потому что необходимо достигать высокой производительности.

Распознавание текста

Ключевая задача – найти изображение текста на картинке и представить его в виде текстовых данных, с которыми можно будет работать, например, в редакторе. Эта технология используется в разнообразных приложениях. В частности, это удобный способ вводить текст в онлайн-переводчик. Достаточно сфотографировать этикетку, текст на ней будет распознан, и переводчик выполнит перевод

Биометрия

Ещё одна задача, решаемая в рамках науки о компьютерном зрении – это биометрия, распознавание людей. Для этого может использоваться изображение лица, радужная оболочка глаза, отпечатки пальцев. Однако, в основном компьютерное зрение занимается распознаванием лиц. С каждым годом эта технология работает всё лучше и лучше, и находит широкое применение.

Видеоаналитика

В мире устанавливается всё больше камер:

на дорогах для регистрации движения автомобилей или в общественных местах, для отслеживания потоков людей и детектирования аномалий (например, оставленные вещи, нелегальные действия). Как следствие, возникает задача анализа огромного потока появившейся информации. Компьютерное зрение помогает в решении этой задачи. Оно позволяет детектировать номер автомобиля, его марку, нарушает ли он правила дорожного движения.

Анализ спутниковых снимков

В данный момент накоплен огромный массив спутниковых снимков. Используя эти данные, можно решать разнообразные задачи: улучшать карты, детектировать лесные пожары и другие проблемы, которые видны со спутника. Технологии компьютерного зрения шагнули в последнее время далеко вперёд, и с их использованием автоматизируется всё больше ручной работы в этой области.

Компьютерное зрение и авто

Современные автомобили оснащены огромным количеством датчиков: несколько видеокамер, радары, стереокамера. Методы компьютерного зрения помогают анализировать информацию, получаемую с этих датчиков. С использованием этих методов созданы системы предотвращения ДТП, столкновения с пешеходами и предупреждения водителя о разнообразных препятствиях.

Кроме того, сейчас активно развивается область автопилотируемых автомобилей. В них технологии компьютерного зрения используются для ориентирования в пространстве.

Кейсы в разрезе сферы деятельности

Искусственный интеллект в большом городе

Попробуем оценить возможность использования искусственного интеллекта в работе диспетчерских служб такси в мегаполисе.

Работа такой службы состоит в том, чтобы направлять машины такси к ожидающим их клиентам. Но сколько нужно машин? В какой части города стоит сосредоточить основную часть водителей, чтобы добиться оптимального времени обслуживания клиентов? Использование искусственного интеллекта в службе такси, за счёт обработки всего доступного массива данных, может существенно снизить количество простоев и увеличить экономическую эффективность парка.

Служба такси – показательный, но довольно узкий пример.

В большом городе искусственный интеллект мог бы эффективно решать десятки технических и административных вопросов от оценки времени разрушения дорожного покрытия (с учётом всех особенностей грунта, климата и т.п.) при использовании разных методов ведения дорожных работ до оценки эффективности тех или иных решений, принятых городской администрацией.

Ещё одним примером использования искусственного интеллекта в городе, это в США научили ИИ распознавать необходимость проведения дорожных работ.

В различных странах выявление локаций, где требуется ремонт дорог и мостов, выполняется двумя способами. Первый – это обычные поездки рабочих ремонтных бригад по окрестностям с целью обнаружения проблемных мест. Второй способ – приблизительно то же самое, только с использованием высокотехнологичных камер, которые быстрее, чем человек, выхватывают участки, которые не соответствуют стандартам.

Искусственный интеллект на службе у военных

Одним из перспективных направлений использования искусственного интеллекта можно назвать модернизацию военной техники. В современной войне уже довольно давно кро-

ме героизма и мужества большую роль играет техническое оснащение. Воздушные беспилотные летательные аппараты уже не только ведут разведку местности, но и активно вступают в боевое взаимодействие. Наземные беспилотные самоходные аппараты отлично себя проявили в борьбе с террористами.

Военная техника нашего времени ещё не оснащена искусственным интеллектом. Многие образцы военной техники могут работать в автономном режиме. Прописанные разработчиками алгоритмы позволяют торпедам находить путь между скал и рифов, «умным» ракетам выбирать подходящую цель, но полноценного искусственного интеллекта (системы, способной не только принимать решения, но и самообучаться в ходе получения новой информации) на вооружении ещё нет.

Однако, во многих странах мира (в их числе Россия и США) заявлено о ведущихся разработках оружия с искусственным интеллектом.

Параллельно ведётся разработка системы поддержки принятия решений должностных лиц. Предполагается, что система с искусственным интеллектом будет оценивать вероятные последствия принятых решений с учётом всех имеющихся данных.

Помимо этого, в вооружённых силах создаются и эксплуатируются экспертные системы. Они постепенно накапливают знания в определённой области, анализируют их, а результаты анализа используют для решения практических задач. Использование искусственного интеллекта переводит военное дело на новый качественный уровень, предполагающий, кроме прочего, большие возможности для сохранения жизни и солдат, и мирного населения.

Искусственный интеллект в медицине

Во всех развитых странах мира ведётся активная разработка систем медицинского прогнозирования. Такая система на основе личной медицинской карты пациента, результатов его обследования (результаты анализов, суточное изменение температуры и артериального давления и т.п.) способна составить прогноз возможных заболеваний для этого человека.

Своевременная диагностика заболевания в разы повышает вероятность благоприятного исхода лечения.

Другим направлением применения искусственного интеллекта в медицине являются диагностические системы.

Известная система IBM Watson занимается диагностированием сложных или редких случаев заболеваний, ищет симптомы заболеваний на ранних стадиях (когда они ещё не доступны врачебной диагностике врачей-людей).

Помимо прочего, анализируя миллионы карт, IBM Watson выводит ранее не известные медицинские закономерности.

IBM Watson – не единственная известная система с искусственным интеллектом. В разных странах есть целый ряд систем с искусственным интеллектом, специализирующихся на диагностике инсультов (путём сравнения снимков томограмм головного мозга), инфарктов (путём анализа кардиограммы), прогнозировании изменения в состоянии пациентов.

Отдельного внимания заслуживают поддерживающие медицинские системы с искусственным интеллектом. Например, система для больных с расстройствами памяти запоминает их нормальный суточный ритм, и если больной отклоняется от нормального вектора движения, такая система посылает сигналы и помогает вернуться домой или самостоятельно вызывает медицинскую помощь.

Эти системы способны помогать справляться со всеми бытовыми нуждами, включая приготовление пищи, уборку и т.д.

Разработка медицинских систем с искусственным интеллектом является приоритетным направлением использования ИИ. Создание, совершенствование и внедрение медицинских систем активно поддерживается рядом государств и крупных коммерческих компаний.

Искусственный интеллект в автомобилях

Новые технологии не только меняют машины, пересаживая пользователей с бензиновых «повозок» на электромобили. Они меняют сам авторынок, позволяя экономить производителям и создавая для них новые угрозы.

Разработки решений автопрома на базе алгоритмов машинного обучения и искусственного интеллекта сегодня сфокусированы в основном в области будущего беспилотников. Однако практическое применение и экономическую эффективность этого можно увидеть уже сегодня.

Дорожная ситуация – это десятки разрозненных факторов, каждый из которых обязательно необходимо учесть при движении автомобиля. Миллионы пикселей в секунду, которые необходимо принять, собрать в единую картину, проанализировать, и принять единственное правильное решение в текущей ситуации. Компьютерам прошлого десятилетия справиться с таким объёмом информации было не под силу. Внедрение систем с искусственным интеллектом позволило десяткам стран мира создать свои модели беспилотных автомобилей.

Созданный человеком искусственный интеллект помещён в автомобиль. Он ориентируется на местности, соблюдает ПДД, но готов ли человек полностью доверить свою жизнь машине? Эта психологическая проблема находится под большим вопросом.

Искусственный интеллект и коммунальные службы

Во многих городах вместо устаревших электросчётчиков сейчас ставят счётчики с прямой передачей информации на обслуживающую станцию. Это помогает оператору видеть текущие графики потребления и реагировать в случае аварийных отключений. Но кроме этого, подобный подход позволяет перевести систему электроснабжения под программное управление искусственного интеллекта. За счёт гигантского массива получаемой информации и статистических данных система может прогнозировать прыжки и падения энергопотребления в сети и эффективно их компенсировать, тем самым позволяя экономить энергоресурсы и беречь ресурс технических систем станции.

В скором будущем вся информация, поступающая от городских систем, будет обрабатываться с использованием искусственного интеллекта: от оптимизации времени работы врачей в больнице – до оперативного изменения графика движения в больших городах. Эффективность такого подхода столь очевидна уже сейчас.

Искусственный интеллект и интернет вещи

Поисковые системы и контекстная реклама, прогнозирование конверсии, просмотров, продаж, внимательный собеседник, личный помощник и заботливая няня, рассказывающая сказку перед сном – все эти функции выполняют системы с искусственным интеллектом.

Взаимодействие между искусственным интеллектом и интернетом вещей похоже на отношение между человеческим телом и головным мозгом. Тело собирает информацию через зрение, слух, осязание. Мозг её обрабатывает и придаёт смысл - превращает свет в узнаваемые объекты, а звуки в понятную речь. Затем мозг принимает решения и подаёт телу сигнал, например, взять что-то или начать говорить.

Все подключенные датчики интернета вещей

работают как наше тело – собирают исходные данные о том, что происходит в мире вокруг. Искусственный интеллект, как и мозг, интерпретирует эту информацию и решает, какие действия предпринять. Затем устройства, подключенные к интернету вещей, выполняют команду или взаимодействуют между собой.

Искусственный интеллект и интернет вещей стали важными и перспективными технологиями благодаря друг другу.

За последние годы машинное и глубокое обучение привели к прорыву в области искусственного интеллекта. При машинном и глубоком обучении компьютер обрабатывает большое количество данных, которые собирают миллиарды датчиков, составляющих интернет вещей.

Развитие ИИ также будет способствовать внедрению интернета вещей и приведёт к стремительному росту обеих областей.

Искусственный интеллект и искусство

В прошлом году вышли и мгновенно стали популярными приложения, использующие нейросети для обработки фото и видео: MSQRD от белорусских разработчиков (в дальнейшем сервис выкупила Facebook), и российские Prisma и Mlvch.

Другой сервис, Algorithmia, раскрашивает чёрно-белые фотографии в цветные с помощью искусственного интеллекта.

Яндекс успешно экспериментирует с музыкой: нейронные сети компании уже записали два альбома: в стиле Nirvana и «Гражданской обороны».

Японский алгоритм написал книгу «День, когда Компьютер написал роман». Несмотря на то что с характерами героев и сюжетными линиями неопытному писателю помогали люди, компьютер проделал огромную работу – в итоге одна из его работ прошла отборочный этап престижной литературной премии.

Нейросети также написали продолжения к Гарри Поттеру и Игре Престолов.

В 2015 году нейросеть AlphaGo, разработанная командой Google DeepMind, стала первой программой, победившей профессионального игрока в Го.

Заключение

Сейчас, в двадцать первом веке, очевиден ответ на вопрос Тьюринга, приводившийся в начале главы. «Может ли машина мыслить?» – «Бесспорно».

Своими трудами учёные, инженеры, исследователи, десятилетиями совершенствовавшие сложные машины, показали нам дорогу в будущее – то самое, с беспилотными автомобилями и машинами, рассказывающими детям сказки.

Также стоит отметить открытость среди исследователей и специалистов по ИИ, машинному обучению и анализу данных.

Большинство успехов в применении ИИ и машинного обучения достигнуты благодаря открытости взаимодействия сообщества, практически все системы следуют концепции открытого исходного кода (open source). Это приводит к тому, что скорость развития новых методов, ранее исчисляемая годами и даже десятилетиями, сегодня составляет месяцы, а статьи успевают устаревать за полгода.

Часть 4. Современные концепции и технологии

Глава 4.5

Гиперконвергентные инфраструктуры

Максим Шапошников

при поддержке Nutanix

Что такое гиперконвергентные инфраструктуры?

В начале 2010-х годов стало понятно, что концепция построения инфраструктуры, придуманная в начале 90-х – технологическая архитектура IT-систем, состоящая из отдельно серверов, отдельно систем хранения данных (СХД) и сети передачи данных между ними (SAN, Storage Area Network) – постепенно перестаёт удовлетворять требованиям современных задач из-за высокой стоимости владения при необходимости масштабирования, а также из-за недостаточности производительности при использовании современных устройств хранения, таких как SSD, NVMe и подобных им. Всё чаще компании начали сталкиваться с проблемами, решение которых привычными традиционными методами построения IT-инфраструктуры приводило к её неоправданному удорожанию, усложнению, увеличению сложности управления и к росту затрат на обслуживание.

Уже в начале 2010-х HCI существовала как идея и развивалась как внутренние проекты многих крупных интернет компаний, таких как Google, Facebook, Amazon. Именно они, во-первых, сделали ставку на широкое использование ***commodity***, то есть типовых универсальных x86-серверов стандартной архитектуры вместо специализированных, уникальных (и дорогостоящих) решений; во-вторых, построили IT-решение как «software-defined» – «программно-определяемое», реализуемое полностью на основе ПО; и, в-третьих, поставили во главу угла способности к широкому масштабированию решения, абсолютно необходимые для компаний такого размера и темпов роста.

Идея, что будущее не только IT-компаний, но и любых enterprise-решений лежит не в специализированных «аппаратных» продуктах, а в универсальных commodity платформах, «поверх» которых реализованы software-defined системы – легко масштабируемые, модернизируемые, часто с открытым исходным кодом – постепенно начала завоёвывать признание, и появилось понятие ***«гиперконвергентная инфраструктура» (HCI, Hyper-Converged Infrastructure)***.

Гиперконвергентными называют инфраструктуры, в которых объединение серверов, SAN и СХД сделано непосредственно на внутриархитектурном уровне. При этом, они объединяются

в неразрывное целое, в единую сущность хранения и обработки информации – «кирпичик» LEGO современного датацентра, модуль обработки и хранения информации, из которых, добавляя и соединяя их между собой, можно создавать инфраструктуру обработки и хранения любого масштаба. Одной из ключевых характеристик, позволяющих говорить об именно «гиперконвергенции» являются:

1. Полная интеграция функциональности хранения и обработки данных на одних и тех же узлах.

2. Использование полностью software-defined подхода, «поверх» вычислительной платформы общего применения (серверы x86).

3. Однородность создаваемой структуры и ее управления, позволяющей масштабировать решение как по объёмам хранения, так и по вычислительной мощности.

> ***Гиперконвергентность*** *– платформа, которая интегрирует хранение данных и вычислительные ресурсы, базируясь на программно-определяемых СХД и вычислительных мощностях, общедоступном аппаратным обеспечении, с унифицированным интерфейсом управления.Основная ценность гиперконвергентных систем заключается в ПО, кардинально упрощающим работу с аппаратным обеспечением.* ***Gartner*** *https://www.gartner.com/newsroom/id/3308017.*

Собственно, само слово «гипер» потребовалось в определении, чтобы отличаться от появившихся на несколько лет ранее так называемых ***конвергентных*** систем (пример: VCE vBlock, Cisco-NetApp FlexPod), которые, строго говоря, вообще никакой архитектурной «конвергенции», т.е. совмещения функций, в себе не имели, а были просто способом удобно продать прединсталлированную инфраструктуру из серверов, SAN и СХД в одном шкафу, ничего не меняя в архитектуре системы по сути. Это были по-прежнему классические СХД и классические же серверы. «Гипер» (а, по сути, и просто «конвергентность», как диктует сам термин) – это именно совмещение функций и образование в процессе единой сущности, чем и являются современные HCI.

Основные преимущества HCI – это гибкость масштабирования («купи, сколько нужно и добавь, когда потребуется»), возможность строить интегрированную инфраструктуру под разные задачи, объединяя их в рамках единого «квазиоблачного» инфраструктурного решения, без необходимости выделять «ресурсные острова» и дробить единое решение, и при этом обеспечивая крайне высокую его производительность. Идея гиперконвергенции и её практическая реализация в онлайн-бизнесах (Facebook, Google и др.) показывает возможность масштабирования систем почти неограниченно, однако, на практике у абсолютного большинства поставщиков гиперконвергентных решений есть жёсткие лимиты. Иногда эти лимиты оказываются неожиданно низкими, как, например, всего 8 или 12 серверов в единой системе.

Наконец, быстрота развертывания (и масштабирования в дальнейшем) решения, сокращающая Time-to-Market – время выхода продукта компании на рынок. Тот самый ***«business agility »*** – способность бизнеса быстро и адекватно реагировать на возникающие новые задачи и вызовы, о котором в России широко заговорили примерно два года назад.

> **Business agility** – концепция развития, свойствами которой называют адаптацию к изменяющимся обстоятельствам, тесное, ежедневное общение клиента с бизнесом на протяжении всего проекта, готовность меняться и менять долгосрочные планы ради следования рынку.

Как устроен типичный HCI?

Несмотря на то, что сегодня на рынке присутствуют десятки гиперконвергентных систем, в реализации их архитектур есть много общего.

Прежде всего, на что обратит внимание привыкший к построению «классических» инфраструктур специалист, – это полный отказ

от привычного SAN. Вместо этого диски, хранящие данные, подключены непосредственно к серверам, где эти данные обрабатываются. За счёт этого обеспечивается возможность реализации предельно короткого пути от исполняемого кода программы к её данным, что критически важно для современных Flash, NVMe и подобных хранилищ. В них вынос SSD во внешние для сервера SAN СХД по блочным протоколам, например, FCP, приводит зачастую к падению их потенциальных возможностей по производительности ввода-вывода в десятки раз просто за счёт многочисленных задержек буферизации и коммутации на пути данных. Как результат, растёт latency – задержки времени выполнения операций, критически важного параметра для высокопроизводительных систем.

Однако, использованию DAS (англ. Direct-attached storage – система хранения данных с прямым подключением – запоминающее устройство, подключённое к серверу или рабочей станции без помощи сети хранения данных), подключаемых непосредственно к серверу хранилищ, при всех плюсах с точки зрения производительности, мешает проблема обеспечения отказоустойчивости и необходимость организовать совместный доступ к хранимым данным с разных серверов.

Эта проблема в HCI сегодня решается путём организации поверх DAS-хранилища распределённой избыточной кластерной файловой системы. Блок данных или же объект, располагающийся на локальных дисках, одновременно присутствует в инфраструктуре на дисках другого сервера как его избыточная копия. Иногда это реализуется в форме Network RAID (HPE SimpliVity, VMware VSAN), иногда в виде распределённого блочного хранилища (Nutanix). В любом случае, данные VM (от Virtual Machine – виртуальная машина) надёжно защищены от сбоев и доступны всем подключенным к системе серверам, что принципиально отличает подобную схему от обычного Direct-attached Storage, и позволяет масштабировать решение до любых желаемых размеров как по числу серверов, так и по объёмам хранения.

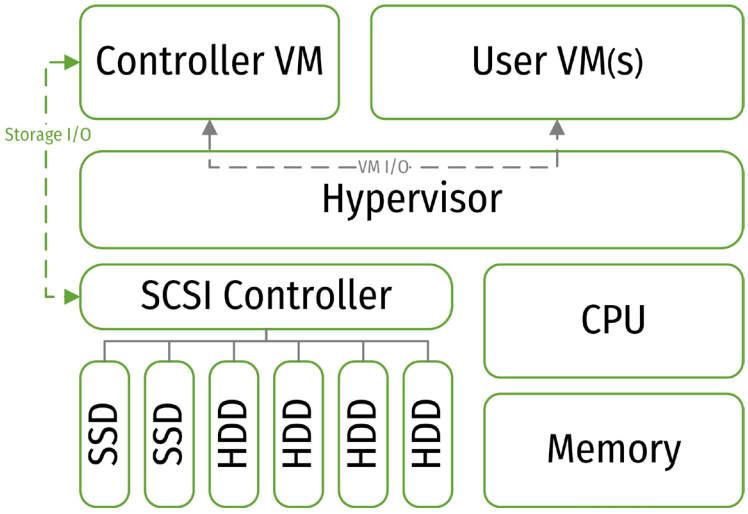
Несмотря на то, что большинство HCI-решений имеют практически идентичные аппаратные платформы, они могут работать совсем по-разному. Как было выше упомянуто, использование локальных дисков позволяет сократить путь от точки исполнения данных (процессор) до точки хранения (диск), но в силу различных архитектурных особенностей и вариантов реализации отказоустойчивости не все HCI-системы пользуются этим оптимальным способом.

Поскольку для работы HCI требуется исполнять на локальном сервере определённые параллельно различные функции, которые обслуживают инфраструктуру, абсолютно все реализации HCI используют нижележащий гипервизор – программу или аппаратную схему, обеспечивающую или позволяющую одновременное, параллельное выполнение нескольких операционных систем на одном и том же хост-компьютере .. В зависимости от выбранной архитектуры, код HCI либо исполняется в ядре самого гипервизора (VMware VSAN) и при этом оказывается жёстко связанным с кодом и особенностями его работы, либо работает как отдельная виртуальная машина (Nutanix, HPE SimpliVity, Cisco HyperFlex и большинство других) вместе с VM пользователя и позволяет, по крайней мере потенциально, обеспечить переносимость и использование разных гипервизоров по выбору пользователя.

Внутри служебной виртуальной машины HCI (она может называться Nutanix CVM, Controller VM, или, например, SimpliVity OVC, OmniStack Virtual Controller) работает код, обеспечивающий функциональность HCI, например, защиту данных, распределённое хранение на подключенных в неё дисках, оптимизацию и повышение эффективности хранения – функции компрессии, дедупликации, и т.д.

Все служебные виртуальные машины HCI соединены между собой. Как правило, для этого используется обычная IP-сеть на наиболее недорогом и распространённом 10G Ethernet, а в последние годы – также на 25G и 40G для наиболее требовательных и производительных систем. В отдельных случаях используется даже Infiniband, что, однако, ломает идею стандарти-

Рис. 4.5.1. *Принципиальная схема служебной виртуальной машины HCI.*



зации и совмещения функций. В этом случае Fiber Channel заменяется на Infiniband, но выделенная сеть хранения данных остаётся.

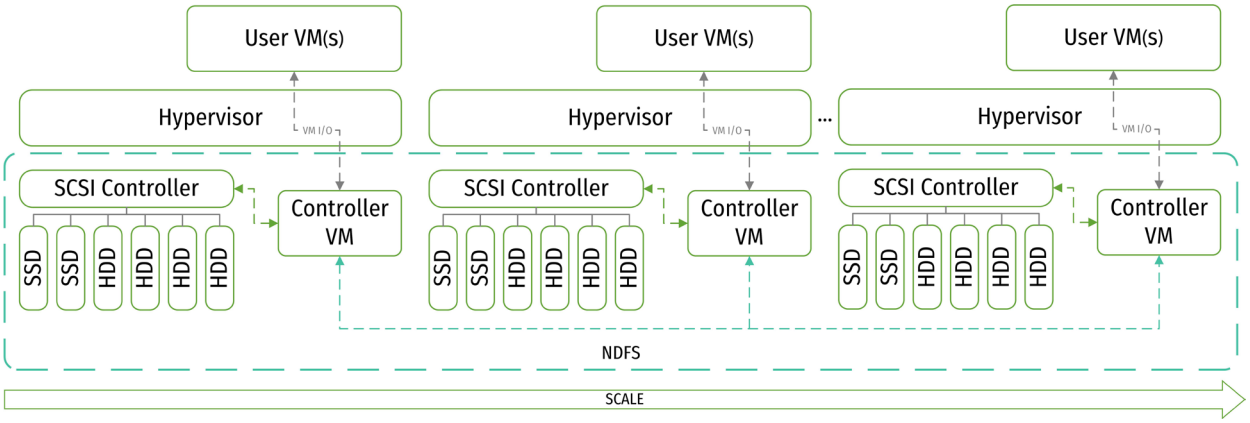
Внутренние механизмы кластера работают в соединённых между собой по сети CVM (Controller VM) и обеспечивают передачу по ней избыточных блоков, синхронизацию метаданных кластерной файловой системы. В некоторых случаях управляющие кластером сервисы работают распределённо в каждом из контроллеров, но в большинстве случаев для этого требуется выделенный сервер (виртуальная машина).

Если необходимо увеличить число узлов в кластере, в него просто добавляется нужное количество новых узлов-серверов. Происходит автоматическое / полуавтоматическое обнаружение новых узлов и расширение кластера, а пользователю становятся доступны новые хосты виртуализации для развёртывания его VM, после чего увеличивается общее доступное место хранения, видимое всей инфраструктуре. Несмотря на то, что каждый хост-сервер обслуживает свою часть дисков, включенных в него локально, кластер HCI, как платформа в целом, используя кластерную файловую систему, видит общее пространство, состоящее из суммы всех имеющихся в кластере и включенных в локальные серверы дисков.

Так как структура хранения не использует единый RAID-массив, расширение ёмкости не требует перестроения массива хранения и может быть выполнено очень быстро, обеспечивая линейное масштабирование без узких мест, характерных для масштабирования «классических» инфраструктур.

Немаловажным компонентом также является общий инструментарий управления инфраструктурой. Обычно такие средства реализуют-

Рис. 4.5.2. *Принципиальная схема кластера HCI.*



ся производителем HCI либо как надстройка к инструментарию гипервизора, например, как плагин для VMware vCenter (HPE SimpliVity, Cisco HyperFlex), либо создаётся самостоятельный продукт, взаимодействующий с инструментарием гипервизора, как, например, Nutanix Prism. Архитектурная распределённость и масштабируемость решения HCI предъявляет особые требования к такому инструментарию управления.

«Классическая» и/или гиперконвергентная инфраструктура?

Ответ на это вопрос очевиден: безусловно, сегодня следует рассматривать возможность сосуществования HCI совместно с «классической» инфраструктурой.

Любые производители HCI трезво понимают, что, каким бы ни было потенциальное превосходство HCI над «классикой» в будущем, впереди у всех нас многие годы сосуществования различных архитектур в датацентрах enterprise-компаний. Одномоментно «выбросить» большие инвестиции в SAN, в СХД, сделанные за многие годы развития, для большинства компаний– расточительно, да и просто невозможно. Разумеется, остаются ниши, в которых «классическая» инфраструктура хорошо себя чувствует и будет чувствовать многие годы. Как телевизор не убил книги, так и, допустим, жёсткие диски не уничтожили магнитные ленты, но вытеснили их в ниши, где они существуют и будут существовать очень долго. Но сейчас всё большему числу IT-специалистов видно, что мы стоим на пороге назревших больших перемен в инфраструктуре. И как когда-то жёсткие диски вытеснили магнитные ленты во времена мэйнфреймов, как в 90-е годы дисковые массивы SAN постепенно заполнили датацентры, вытеснив DAS, как в 2000-е появившаяся серверная виртуализация пробила себе путь в подавляющее число корпоративных датацентров, так и HCI сегодня потенциально является следующим важным эволюционным шагом для инфраструктуры датацентров.

Как хороший пример, можно привести вариант использования HCI с системой SAP HANA. В настоящий момент сервер HANA поддерживается SAP в production, как правило, только на физическом «железе» без виртуализации (либо с большими ограничениями на используемый гипервизор). Однако, кроме сервера самой HANA, значительную часть решения обычно составляют многочисленные серверы приложений, использующих в своей работе отдельную внешнюю in-memory HANA DB, а также среда разработки, QA-подразделение и так далее. Компании часто устанавливают под сервер HANA DB физический сервер без виртуализации, что полностью поддерживается SAP, а затем развёртывают множество клиентов, серверов приложений на HCI-узлах в гиперконвергентной среде – и это тоже поддерживаемый вариант.

Обзор гиперконвергентных решений

В настоящий момент на рынке присутствует несколько практических реализаций концепции «гиперконвергентности», сделанных разными компаниями и отличающихся в деталях, но достаточно сходных в принципиальных моментах, чтобы всех их называть HCI.

Nutanix, как одна из компаний-пионеров решения, разработала Nutanix Enterprise Cloud – кроссгипервизорное решение, поддерживающее любой тип используемого пользователем гипервизора. Компания также развивает собственный гипервизор Acropolis Hypervisor (AHV), который использует открытый под лицензией GNU исходный код Linux KVM. Nutanix имеет наиболее широкую сеть OEM-партнёров (в т.ч. DellEMC, Lenovo, IBM и Fujitsu), поставляющих его решение со своим платформами.

VMware, как разработчик популярнейшего

промышленного класса гипервизора и системы виртуализации на его основе – ESXi/vSphere – добавила в него модуль программной СХД VSAN и таким образом получила ПО для гиперконвергентных решений. Можно собрать на основе vSphere/VSAN гиперконвергентную платформу самостоятельно, взяв серверы у поставщика по собственному выбору, или купить готовый программно-аппаратный комплекс DellEMC VxRail.

VMware и DellEMC, наряду с Nutanix, названы аналитической компанией IDC в середине 2018 года «имеющими наибольшую рыночную долю из всех HCI-вендоров».

HPE продолжает разработку приобретенного продукта SimpliVity, наиболее важной функциональной особенностью которого является сквозная и эффективно реализованная дедупликация хранимых данных.

Продукт ***NetApp*** SolidFire завоевывает рынок качественно реализованным механизмом QoS и предсказуемой производительностью, хотя и не полностью следует «гиперконвергентной концепции», разделяя узлы compute и storage функций.

В 2016 году аналитическая компания ***Gartner*** назвала HCI: ***«Мэйнстримом в индустрии в течение следующих пяти лет», с общим ростом в 79%***, и достигшей ещё в 2016 году объёма в 2 миллиарда долларов США (источник: https://www.gartner.com/newsroom/id/3308017).

Сегодня, глядя из 2018 года, мы видим, что прогнозы развития и темпов роста технологии HCI не только оправдались, но и превзойдены.

Cisco HyperFlex демонстрирует наиболее полную и глубокую интеграцию в Cisco UCS (Unified Computing System) – разработки самой Cisco популярную серверную инфраструктуру, включающую в себя серверы blade- и rack-формата, а также сетевую и SAN-фабрику, инструментарий управления.

Huawei FusionCube также предлагает поддержку различных типов гипервизоров (VMware vSphere и Hyper-V), наряду со своей реализацией гипервизора на базе кода Xen и KVM. И, хотя компанию преследуют различные проблемы на рынке США, она активно развивается на рынках многих других стран, включая Россию и страны Азии.

Заключение

Основными преимуществами при переходе к HCI в инфраструктуре современного корпоративного датацентра являются большая гибкость, упрощение администрирования (как следствие – снижение стоимости и числа ошибок), повышение надёжности, увеличение производительности, экономия на эксплуатационных расходах, большая динамичность IT, позволяющая быстрее откликаться на требования бизнеса, повышая его конкурентоспособность.

Непрерывное развитие IT за последние несколько десятилетий обнажило факт того, что инфраструктура хранения и обработки данных, в своих базовых идеях оформившаяся ещё 30 лет назад (в начале 90-х), неизбежно встретится с требованием перемен и развития. Новые прорывные технологии, как всегда «стоящие на плечах гигантов», заставляют нас вспомнить слова Чарльза Дарвина: *«В эволюционной борьбе побеждает не самый сильный или самый проворный, а тот, кто сможет лучше всего приспособиться к изменениям»*. Крупные изменения, назревшие в последнее десятилетие в IT-отрасли, и продиктованные новыми задачами, заставляют меняться и такие традиционные области, как архитектуры датацентров. Архитектура, где со времени ухода мэйнфреймов и прихода на их места тогда «лучше приспособившихся к меняющимся условиям» серверов стандартной архитектуры и СХД, использующих открытые протоколы, появление HCI, возможно, является крупнейшей инновацией нынешнего десятилетия.

Участие в ИТ-сообществе

Участие в ИТ-сообществе

Алексей Кравченко

Директор управляющего офиса
Клуба ИТ-директоров 4CIO

В мире множество ассоциаций профессионалов в области ИТ. Одна из старейших — американская ассоциация AITP (Association of Information Technology Professional), основанная ещё в 1951 году. Именно в это время начался бурный прогресс компьютерной техники, зарождалось программирование и сама профессия «айтишник». Появление персональных компьютеров, доступных каждому, и зачатков Интернета в 80х привело к взрывному росту использования ИТ в бизнесе. Росло и количество объединений профессионалов в области ИТ.

Эпоха 90-х с её стремительным ростом технологий, особенно в области коммуникаций, принесла в мир новый подход к общению людей невербальный. ИТ-профессионалы находились на передовой развития технологий общения, и поэтому именно они стали первыми использовать такие средства в своих ассоциациях и клубах.

В конце 90-х годов возникло и российское движение CIO. Сегодня в России насчитывается уже более 20 клубов CIO. Старейшие из них клуб топ-менеджеров 4CIO, Клуб ИТ директоров Санкт-Петербурга и клуб профессионалов АСУ Урала. Кроме того, в 2007 году клубное движение CIO объединилось в Союз Директоров ИТ России (СОДИТ).

Что даёт участие в профессиональном сообществе?

Первое и самое важное – общение. Зачастую CIO вынужден решать задачи в одиночку. Однако это требует времени, да и риск возникновения «подводных камней» очень велик. Проще обратиться к тем, кто уже прошёл этот путь и знает, как решать данный вопрос, то есть близким по профессии и духу людям. Конечно, есть люди, утверждающие, что профессиональное общение им не нужно, что они достаточно образованы и имеют достаточно богатый опыт, чтобы самостоятельно решить ту или иную проблему. Но трудно представить, что эти люди смогут постоянно двигать компанию вперёд, ведь они зажаты в рамках своего образовательного уровня и далеко не всеобъемлющего по рыночным меркам опыта. Никакие образовательные курсы не дадут столько информации, сколько можно получить от своих коллег по «цеху».

Второе и не менее важное – поддержание компетенции. Только всесторонне образованный руководитель, постоянно находящийся в поиске новых решений, анализирующий опыт коллег и изучающий предложения рынка, может добиться успеха. Тот, кто всегда поддерживает свою компетенцию в актуальном состоянии. Конечно, в выступлениях поставщиков можно видеть лишь рекламу и очередную попытку «что-то продать». Но ведь на ту же самую информацию можно посмотреть и под другим углом — как на источник новых знаний о продуктах, которые мы используем в повседневной жизни. Есть много примеров, когда одно выступление партнёра клуба решало проблемы, над которыми многие CIO бились в течение нескольких месяцев!

И третье, но не последнее — поддержка и помощь. Для многих клуб — это болельщики для футбольной команды, про которых говорят, что это двенадцатый игрок, помогающий побеждать. Например, один CIO поделился с членами клуба 4CIO проблемой, связанной с производительностью одной очень известной системы. Оказалось, что большинство членов клуба тоже с ней сталкивались. Решений данной проблемы оказалось несколько, каждое из них приводило к небольшим улучшениям системы, но в целом картина оставалась такой же. В итоге, применив комплексный подход к решению проблемы, основанный на нескольких высказанных рекомендациях, CIO удалось добиться качественно нового результата. Более того, на очередном заседании клуба он выступил с рассказом об этом решении и достигнутых результатах.

Каждый из членов профессионального ИТ-клуба уже чего-то добился, и клуб помогает обмениваться этим багажом — знаниями, идеями, опытом. И судя по тому, что в России клубное движение CIO набирает обороты — это верный курс.

Почему сказанное выше относится не только к CIO?

Почему важно участие в сообществе поставщиков услуг или товаров? В рыночных отношениях есть несколько участников, и роли у них разные. Во всём мире давно признано, что бизнес строится, прежде всего, на личных отношениях. То есть интересны не только, и может быть, не столько, доклады поставщиков, сколько те люди, которые их представляют. Если вам нужно обсудить использование того или иного решения в своей компании, к кому Вы в первую очередь обратитесь? Конечно же, к тому, кого знаете, хотя бы по выступлениям и общению в клубе.

Есть и другая сторона медали именно в профессиональном сообществе, в конструктивном диалоге, поставщик может получить информацию, необходимую для формирования корректного предложения. А значит, растёт вероятность того, что российские CIO получат именно то, в чём нуждаются.

В последнее время руководители нашей страны часто упоминают о «глобальной связи между участниками рынка». И это касается не только мировой экономики, но и нашей повседневной деятельности. Объединив наши усилия, поддерживая друг друга, мы сможем добиться гораздо более весомых и ярких результатов, нежели поодиночке.

Наши авторы

Пестряков Павел

Создатель Клуба 4CIO

2014–н.в.: Член СД CDC (Центр Корпоративных Разработок).
2010–н.в.: Accenture RUS Advisory, Board member.
2012–н.в.: Группа Nexia Pacioli, Советник ГД.
2013–2014: Заместитель ГД Пермэнергосбыт.
2011–2012: Группа Черкизово CIO, член Правления.
2008–2011: Консорциум Альфа Групп. CIO.
2006–2008: Четвертая Оптовая Генерирующая Компания, Заместитель генерального директора, член Правления Компании.
2004–2006: Корпорация ИНКОМ-недвижимость, Технический директор.
2001–2004: Управляющая компания группы РУСАГРО, Директор Департамента информационных технологий – и.о. Директора по развитию.
1999–2001: Управляющая компания группы East line, Заместитель начальника управления Технологического Развития.
1992–1999: Московский Индустриальный Банк, Заместитель начальника управления информационных технологий.
1988–1992: Госкомитет СССР по вычислительной технике и информатике «Московский Экспериментальный ВЦ», Объединение «ЭЛЕКС» Начальник отдела тех.обеспечения.

Образование: ИБДА АНХ, Executive MBA, Стратегическое управление.
Финансовая Академия, экономист по банковскому делу, диплом с отличием.
Московский Авиационный Институт, Радиотехника.

Реализованные проекты: Сын; Клуб 4CIO; Автоматизированная банковская система Московского Индустриального Банка – в 1998 году один из первых проектов реформирования банка, реализованных на деньги всемирного банка; ГК РУСАГРО – первый проект корпоративного внедрения 1С – стал основой стандарта корпоративного внедрения от компании 1С; Корпорация ИНКОМ – благодаря созданию уникальных систем, компания стала № 1 на риэлтерском рынке и ведущей инвестиционной компанией на рынке загородного строительства; Все компании-работодатели – лидеры рынка, с моей помощью успешно решали задачи с использованием современных информационных технологий; После себя оставляю успешно работающие системы, мотивированные коллективы и подготовленных руководителей ИТ, способных развивать компанию с помощью ИТ.

Кирюшин Сергей

Член Совета Клуба 4CIO

с 2018: Советник генерального директора АО «ВЭБ-Лизинг».
05.2014-06.2018: Советник руководителя Федерального агентства по туризму РФ.
05.2013-04.2014: Советник Председателя Правления Пенсионного Фонда России.
05.2011-04.2013: Заместитель генерального директора ФГУП «Почта России».
03.2010-08.2010: Начальник департамента информатизации и бизнес-технологий ОАО «Холдинг МРСК».
07.2003-09.2009: Заместитель генерального директора - директор департамента ИТ ОАО «Аэрофлот - российские авиалинии».
10.2001-07.2003: Генеральный директор ЗАО «Технический центр РТС».
01.2001-10.2001: Старший вице-президент, 1-й зам.CIO ОАО «Альфа-Банк».
01.1999-01.2001: Председатель правления НКО «Расчетная палата РТС».
02.1998-01.2001: Вице-президент НП «Фондовая биржа РТС».
07.1993-10.1997: Директор Главного клирингового (впоследствии - Расчетного, Информационно-расчетного) центра Сбербанка России.

Образование: Академия Народного Хозяйства им. Г.В. Плеханова.

Реализованные проекты: Создание расчетно-клиринговой системы Сбербанка России, построение Процессингового центра Сбербанка России, создание НКО «Расчетная палата РТС» и системы биржевой торговли в РТС, миграция Аэрофлота на систему бронирования и продажи билетов Sabre, внедрение электронных билетов в РФ, запуск интернет-продаж билетов Аэрофлота, написание в партнерстве с коллегами Учебника 4CIO, разработка ИТ-стратегии для ряда компаний, запуск Национального туристического портала Russia. Travel и пр.

Кравченко Алексей

Директор управляющего офиса Клуба 4CIO

Трудовая деятельность началась в 1983 г. и продолжает преследовать меня по сей день. И все время в ИТ. С самого начала деятельности.

Образование: 1990: Московский энергетический, АВТФ.

Реализованные проекты: Администрирование клуба 4СИО считаю главным достижением трудовой биографии. Работа моя гармонично сочетает в труд и интересную жизнь. Общаясь со многими людьми, я получаю огромное удовольствие. Думаю, что за время моего руководства клубом с 2006, мы вместе с вами достигли очень высоких показателей, прежде всего, сделали сообщество интересным для участников и полезным для внешнего представления. Очень надеюсь, что хватит сил и энергии поддерживать и развивать ИТ сообщество и в дальнейшем.

Алфёров Павел

2016–2017: Член Правления АО «РВК», Первый заместитель директора Проектного офиса Национальной технологической инициативы.
2014–2016: Руководитель Центра методологии, экспертизы и контроля проектной деятельности ПАО «Интер РАО».
2013–2014: Заместитель генерального директора по управлению проектами и информационным сервисам НИПК «Электрон».
2008–2013: АНО «Оргкомитет «Сочи 2014». Директор Департамента знаний, информации и методологии.
2007–2008: ТНК-ВР. Директор ИТ проектов Блока переработки и торговли.
2006–2007: Консорциум Альфа Групп, X5 Retail group. Заместитель директора по ИТ.
2004–2005: ТНК-ВР. Руководитель Центра экспертизы и контроля ИТ-проектов.

Образование: 1998: Московский энергетический институт. Инженер-физик. 2003: Академия народного хозяйства при Президенте РФ. Школа IT-менеджмента. ИТ-менеджер. 2016: Экономический факультет МГУ совместно с Национальной ассоциацией корпоративных директоров. Корпоративный директор.

Реализованные проекты: Управление проектами/программами/портфелями проектов - более 20 лет опыта. Практическая реализация проектов и программ высокой сложности. Управление информацией и знаниями - 7 лет опыта. Построение комплексной системы управления знаниями Оргкомитета Сочи 2014. Цифровая трансформация бизнеса - более 25 лет опыта внедрения ИТ-систем.

Аншина Марина

Президент фонда «ФОСТАС».
Председатель Комитета по стандартам Российского Союза ИТ-директоров.
Член Совета по профессиональным квалификациям в области ИТ.
В течение 20 лет – руководящие позиции в области ИТ в российских и зарубежных компаниях, в системных интеграторах.

Образование: 2004: Стажировка по теме «Стандарты в области ИТ» по программе SABIT Министерства Торговли США. 2008: Диплом с отличием российско-бельгийской программы EMBA. Международный сертификат по управлению проектами GAPPS (2008), сертификаты MCSE и MCDBA.

Реализованные проекты: Автор книг и статей по тематикам стратегии ИТ и архитектуры предприятия, оценки эффективности ИТ и управления проектами ИТ, технологии CORBA и пр. Руководитель рабочих групп по разработке профессиональных стандартов РФ. Руководитель магистерских и преподаватель курсов Высшей школы бизнеса МГУ, Финансового университета (MBA для CIO в Школе ИТ-менеджмента), АНХ при Правительстве РФ (MBA). Разработка стратегии ИТ (ТМКонсалт) и др.

Борисов Евгений

Начал свою карьеру в 1996 году в компании Newbridge Systems Integration. Позднее переведён на позицию менеджера по продажам в канадской компании Newbridge Networks. После приобретения компании Alcatel-Lucent перешёл на работу в компанию Datatel, где являлся директором по продажам и одновременно совладельцем компании. Позднее возглавил компанию InStroyTek, а также руководил развитием бизнеса в компании Naumen.
Образование: Академия Народного Хозяйства при Правительстве Российской Федерации по специальности финансовый менеджмент.
Реализованные проекты: Реализованы проекты различного масштаба для таких организаций как Аэрофлот, Alcatel, Астелит, AT&T, British Telecom, Вымпелком, C&W, Coca Cola, Комкор, Eastline, Equant, Евраз-холдинг, Федеральной миграционной службы, Федеральной службы охраны, Ростелеком, Газком, Госкорпорации по организации воздушного движения, ГПКС, МЧС, Мегафон, МГТС, МВД, МТС и др.

Валиев Рустем

2003-2005: ОАО Альфа Банк. Ведущий инженер ДИТ.
2005-2009: АО Хьюлетт-Паккард. Менеджер по решениям в области ИТ.
2009-н.в.: Генеральный директор ООО «ССК Консалтинг».
2016-н.в...: Преподаватель Всероссийской академии внешней торговли при Министерстве экономического развития Российской Федерации.
Образование: 1999: Высшее. Магнитогорский государственный технический университет им. Г.И. Носова. 2005: Дополнительное высшее. Экономист международного бизнеса. 2009: Дополнительное высшее (MBA) Московский институт международного бизнеса. 2015: Кандидат экономических наук.
Реализованные проекты: Разработка и внедрение решений по клиентскому сервису, решений Интернет-банка, телефонного банка и мобильного банка. Проектное управление по внедрению технологий RFID для производственных предприятий. Преподавание дисциплин: бизнес-планирование, информационные технологии в международной логистике, экспертные технологии, инструменты бизнес-аналитики (data mining).

Зимин Константин

Главный редактор журнала Information Management. В течение 15 лет был главным редактором ряда ведущих российских ИТ-изданий. Соавтор книги «Эффективность инвестиций в ИТ. Альманах лучших работ». Автор серии исследований «Практика использования ИТ в российских компаниях» в 2006-2012 годах. Независимый эксперт в области управления знаниями и анализа управленческих ситуаций. Член правления Союза Директоров по ИТ России. Один из инициаторов создания портала GlobalCIO и экспертной сети Expinet.
Образование: Московский физико-технический институт. Высшие курсы ИТ-директоров Союза директоров ИТ России (СОДИТ) и Высшей школы экономики.

Иншаков Дмитрий

Профессионально работает в сфере ИТ с 1993 года. С 2001 года – в крупнейших международных компаниях (Unilever, WPP, PwC), в основном на позициях уровня CIO. Более 8 лет (2007-2015 гг.) был ИТ директором PwC в России, из них 6 лет также являлся заместителем CIO по региону Центральная и Восточная Европа. Управлял ИТ в компаниях различных секторов: аудит и консалтинг, производство (FMCG), реклама и СМИ. Отвечал за разработку и выполнение ИТ-стратегии; внедрение и интеграцию ERP, CRM и других бизнес-систем; реструктуризацию ИТ департамента в масштабе нескольких стран; построение ИТ-инфраструктуры и ИТ-департамента «с нуля» и т.д.

Образование: 1996: СПбГЭТУ (ЛЭТИ), диплом с отличием. 2000: Кандидатская диссертация на тему «Моделирование адаптивных систем управления на параллельных вычислительных структурах». 2002 и далее: более 15 бизнес-тренингов. 2007-2008: сертификаты по ITIL. 2008-2009: участвовал в международной учебной программе “Аполло” для ключевых директоров PricewaterhouseCoopers.

Реализованные проекты: На 90-х на радиостанции Балтика одним из первых в России настроил автоматическое составление ежедневных музыкальных программ (плей-листов). В 2006 году «с нуля» построил ИТ департамент компании GroupM. В PwC Russia собрал «dream team» ИТ-руководителей, вместе с которой реализовал много ИТ/бизнес проектов. В течение 6+ лет являлся заместителем CIO по региону Central & Eastern Europe (29 стран).

Киракосян Роберт

2001–2008: Группа ГАЗ, начальник управления информационных технологий. Отвечал за всю инфраструктуру холдинга, построение единого информационного пространства, выбор и внедрение систем CAD/CAM/CAE PLM, внедрил систему SAP BW, осуществил два проекта по переезду компании, всех дочерних управляющих компаний в единый офис, а также переезд компании в Нижний Новгород, 600 рабочих мест. Создал Совет по информационным технологиям холдинга.

2008–2010: Группа Компаний En+ заместитель Генерального директора. Осуществил проекты переезда компании, внедрение системы управления персоналом.

2010–2016: Заместитель Генерального Директора ОАО «ЛИНТЕХ СЕРВИС». Осуществил проекты по техническому переоснащению и построению серверных помещений для НПО «МОТОР» г. Уфа, это опытное производство и КБ компании «Уфимские моторы» и ПАО «Сокол» Нижний Новгород».

2016–н.в.: Генеральный Директор компании К2-ТЕХНО - системный интегратор, поставка всего спектра компьютерного и серверного оборудования, поставка и внедрение ПО, включая 1С, DLP системы, разработка мобильных приложений.

Образование: 1997-1983: Московский Институт Электронной Техники. Факультет микроприборов и технической кибернетики, специальность инженер электронной техники по разработке электронных устройств

Лукацкий Алексей

В области информационной безопасности работает с 1992 года. Работал специалистом по защите информации в различных государственных и коммерческих организациях. Прошёл путь, начиная от программиста средств шифрования и ИТ/ИБ-администратора, заканчивая аналитиком и менеджером по развитию бизнеса в области информационной безопасности. В настоящий момент отдаёт всего себя компании Cisco, выполняя сразу несколько ролей – внешних и внутренних.

Образование: Основное – МИРЭА (Российский технологический университет), «Прикладная математика» (специализация «Защита информации»).

Реализованные проекты: Опубликовал несколько сотен статей и 4 книги по информационной безопасности. Разработал несколько авторских курсов по кибербезопасности, которые читает в различных учебных заведениях и организациях, в том числе в ВШБ МГУ. Участие в экспертизе и разработке нормативно-правовых актов в области информационной безопасности и персональных данных. Публичных государственных и ведомственных наград не имеет, в отличие от отраслевых дипломов и почётных грамот от Банка России, Совета Безопасности, МВД России и др. Cisco Security Ninja Blue Belt. Первый Cisco Security Champion в компании (внутренняя ИБ).

Максимов Алексей

2017–н.в.: Директор R&D Безопасные коммуникации.
2012–2017: Директор ИТ в РТКомм.РУ.
2010–2012: Генеральный директор Телефоникум.
2006–2010: Технический директор Комтехтрэйд.

Образование: .1998: Высшее. Череповецкое высшее военное инженерное училище радиоэлектроники. 2009: Высшее. МИСИС. Прикладная информатика.

Реализованные проекты: Участие в разработке и запуске продукта по управлению мобильными устройствами под брендом «яРядом», Строительство ЦОД для предоставления SAAS, IAAS, PAAS услуг клиентам, Создание облачной АТС операторского класса, Создание Автоматизированной системы расчётов.

Реализовано более 10 AI проектов в Retail и Транспортной сферах, в том числе: разработка систем прогнозирования заказов; разработка платформы построения AI-ботов с применением алгоритмов NLP, ML; разработка автоматизированной систем принятий решений, по заказам и предзаказам транспорта, с применением алгоритмов ML; разработка сервиса по анализу звуковых записей и автоматизация работ с жалобами.

Максимов Константин

2016–н.в.: Руководитель направления развития ИТ, DS в ПАО Сбербанк.
2011–2016: Руководитель развития аналитических решений в Ай-теко.
Образование: 2011: Высшее. Высшая школа экономики. Институт электроники и математики. САПР. 2015: Высшее. Финансовый университет при Правительстве РФ. Экономика.
Реализованные проекты: Разработка автоматизированных банковских систем принятий решений с применением алгоритмов ML.

Подольный Вадим

Начал карьеру в 2001г. в Центре информационной безопасности МИФИ.
С 2004 до 2008 г. работал во ГК Росатом, ОАО «ВНИИАЭС», руководил разработкой Российской программной платформы Системы Верхнего Уровня АСУ ТП для новых АЭС ГК Росатом (Программное Обеспечение Распределенных Технологий Автоматизации Лицензированное, ПОРТАЛ), эксплуатируется по настоящее время на 13 Российских и зарубежных энергоблоках с реактором ВВЭР 1000, ВВЭР 1200, БН 800.
2009 ИТ-директор оператора Единая Национальная Диспетчерская Система - «ЕНДС «Глонасс-Навигатор».
2011-2014 ГК Ростех, АО «ЦНИИ-ЭИСУ», руководитель разработки ОС «Заря» (ИТБВ.00158-10).
2016 ГК Росатом, АО «РАСУ» Заместитель Технического директора — директор департамента разработки ПО и Кибербезопасности;
С 2015-2017 занимал позиции советника в ГК Ростех (АО Концерн «Созвездие»), ОАО РЖД (АО «НИИАС»), ОРКК (ОАО «НИИКП»).
С 2018 Заместитель Генерального директора по Системной интеграции и Кибербезопасности в «Московский завод «Физприбор». Занимается разработкой новых платформ АСУ ТП / IIoT для Критических Информационных Инфраструктур (АЭС и др.).
Образование: МИФИ, Факультет технической физики.

Потоцкий Михаил

Основатель и руководитель компании IT Expert, один из признанных авторитетов в области становления и развития управления ИТ в России. 10-летний опыт реализации подходов

ITIL во многих российских компаниях различных отраслей. Свою профессиональную карьеру в этой сфере начал в компании Hewlett-Packard Россия, где HP участвовал во внедрении ИС в Центральном Банке РФ, региональных Главных Управлениях ЦБ РФ, Мост-банке, Внешторгбанке, Внешэкономбанке, Альфабанке, Лукойле и др. Руководил отделом ПО Московского представительства HP, специализируясь на развитии рынка корпоративных программных решений HP (программные платформы HP Open View и др.), теории и практике современной организации работ в отделах ИТ.

Образование: .1984—1990: Московский Авиационный Институт, диплом с отличием. Сертификация: Practitioner's Certificate in IT Service Management / Release and Control (EXIN); Manager's Certificate in IT Service Management (PinkRoccade/EXIN); российские и международные сертификаты по ИТ сервис менеджменту и корпоративному управлению, в т.ч. по развитию корпоративной стратегии и реорганизации бизнеса (MIT Sloan Executive Education), финансам и другим областям профессионального менеджмента.

Реализованные проекты: С момента создания IT Expert в 2002 году наряду с организацией и управлением бизнесом активно участвовал в текущих ITSM-проектах компании, развивал маркетинговые стратегии и новые направления деятельности, проводил тренинги по ITIL/ITSM. Автор многочисленных статей и публикаций по управлению ИТ, регулярный докладчик на крупных тематических конференциях.

Селютин Александр

2010–2015: Комитет информатизации и связи Республики Коми. Руководитель.
2010–2012: Администрация Главы Республики Коми и Правительства Республики Коми. Референт Главы Республики Коми.
2009–2010: Компания S&T. Директор российского представительства.
2003–2008: ОАО «РАО ЕЭС России». Заместитель начальника департамента ИТ.

Образование: 1998: Высшее. Московский государственный университет экономики, статистики и информатики. Информационные системы в экономике. 2008: Дополнительное высшее (MBA). Академия народного хозяйства при Правительстве РФ. CIO.

Реализованные проекты: Создание органа исполнительной власти региона «с нуля». Участие в создании / создание ИТ-подразделения крупного холдинга. Создание территориально-распределённой сервисной ИТ-организации. Внедрение ITIL и PMBOK в практику. Формирование ИТ-кластера в регионе. Запуск региональной Федерации компьютерного спорта. Внедрение системы прогнозирования крупного предприятия – построение прогнозной финансово-экономической отчётности с горизонтом более года. Внедрение централизованных региональных отраслевых и межотраслевых информационных систем. Внедрение систем управления на предприятиях различной специфики (экономика, производство, логистика).

Скрынник Олег

2009–2017: Управляющий партнёр, Cleverics.
2004–2009: Начальник отдела ИТ-консалтинга, IT Expert.
2004–2004: Начальник технологического отдела, Инком-Недвижимость.
2001–2004: Начальник отдела ИТ-поддержки, Инком-Недвижимость.
Образование: 2016: DevOps Master. 2007: ITIL Expert. 2004: IT Service Manager. 1999: Microsoft Certified Systems Engineer.
1998: Московский государственный технический университет им. Н.Э. Баумана, факультет информатики и систем управления.
Реализованные проекты: Организационное планирование коммерческой службы по ИТ-услугам. Анализ операционных рисков, связанных с применением ИТ, проведение Business Impact Analysis. Разработка концепции автоматизации системы управления ИТ-деятельностью. Управление финансами ИТ. Внедрение процесса управления уровнем сервиса. Выбор ПО автоматизации ITSM. Обследование управления ИТ. Разработка методики расчёта стоимости ИТ-услуг. Построение службы поддержки пользователей. Подготовка ИТ-ресурсов к аутсорсингу. Внедрение управления доступностью. Внедрение системы автоматизации работ ИТ. Реорганизация департамента ИТ.

Шапошников Максим

Родился и вырос в городе Норильск (крайний север). Со школы увлекался разработкой ПО, UNIX системами, телекоммуникациями, проблематикой хранения и обработки больших объемов данных. После окончания ВУЗа подключился к команде специалистов, в последствии создавшей многие ключевые интернет проекты как в Российской Федерации, так и за рубежом — Spylog, Begun, Mamba, Badoo, в масштабах на сотни миллионов пользователей. Всегда выступал в команде как одих из ключевых IT специалистов, занимаясь дизайном архитектуры и дальнейшей эксплуатацией сверхкрупных проектов с нуля. С 2012 года подключился к команде Nutanix сначала в роли технического директора по региону (РФ / СНГ / Восточная Европа / Турция / Израиль), затем как Директор по Передовым Технологиям на глобальном уровне.
Образование: Физико-Математический Колледж с углубенным изучением IT технологий. Высшее образование — Обнинский Институт Атомной Энергетики, где организовал одну из первых крупных кампус сетей с сотнями подключенных пользователей и выходом в интернет.

Над учебником работали

Сергей Кирюшин
Главный редактор

Александр Селютин
Выпускающий редактор

Алексей Кравченко
Организационное обеспечение

Феликс Карасев
Организационное обеспечение

Ольга Селютина
Редактура, вёрстка

Ильсур Аптуков
Дизайн

Антон Прасолов
Корректура

Специальная сокращённая версия
Выпуск к XII Конгрессу «Подмосковные вечера»

2018