Информационная безопасность в условиях кризиса. Рекомендации Cisco

Многие компании стоят перед непростой задачей – сократить неприоритетные затраты с целью повышения своей устойчивости и обеспечить восстановление роста и развития бизнеса в случае улучшения экономической ситуации на рынке. Одним из направлений, часто подверженных сокращению затрат, является информационная безопасность (ИБ). Многие предприятия либо уже сократили бюджет на эту деятельность, либо находятся в ожидании соответствующих распоряжений со стороны топ-менеджмента. В ряде компаний пошли еще дальше и не только урезают бюджеты, но и сокращают персонал, которого и так не хватает.

Регулярно сталкиваясь в повседневной жизни с проявлениями кризиса, мы можем выделить из них наиболее распространенные и опасные:

- Заканчивается эпоха изобилия и финансовых ресурсов перестает хватать.
- Переход от эпохи изобилия к эпохе экономии сопровождается снижением операционных и капитальных затрат.
- Замораживание долгоиграющих проектов или отказ от проектов с неочевидной выгодой.
- Финансирование только проектов с быстрой отдачей.
- Сокращение «непрофильного» персонала или сотрудников, отдача от которых отсутствует или неочевидна.

Что делать в условиях нестабильной экономической ситуации службам информационной безопасности и их руководителям?

Сокращение затрат

Согласно результатам исследования компании Ernst & Young, проведенного в июле 2007 года, руководители большинства опрошенных компаний, несмотря на уверенность в том, что расходы надо оптимизировать, подтвердили, что принятые меры часто не приносят результатов. Вся причина в том, что якобы лежащие на поверхности решения о сокращении затрат были приняты слишком поспешно, направлялись на быстрый результат в ущерб достижению стратегических бизнес-целей.

Желание быстро сократить затраты и отчитаться перед руководством, как и практика равномерного снижения затрат по всем направлениям в компании, неэффективны и часто приводят к тому, что руководители служб ИБ закрывают важные долгосрочные проекты. Кажущиеся мало- или неэффективными проекты, которые могут принести существенную выгоду через год-другой, тоже лучше не сокращать. Это искушение надо побороть, т. к. вы можете оказаться в условиях, когда вернувшись в нормальное русло, вам придется начинать все с нуля, что потребует еще больших затрат, чем до кризиса.

Сокращение затрат — это важная задача, но не надо ставить ее во главу угла и делать «идеей фикс». Иногда дополнительные расходы могут сыграть положительную роль в бизнесе компании. Например, обучение сотрудников может ускорить те или иные процессы и процедуры, а использование технологий удаленного доступа позволит существенно как сэкономить на аренде площадей, так и высвободить дополнительное время, ранее растрачиваемое в пробках по дороге на работу.

Можно выделить 7 потенциальных областей сокращения расходов:

- Оптимизация ассортимента продукции
- Изменение стратегии продаж

- Сокращение затрат на персонал
- Повышение производительности
- Аутсорсинг
- Офшоринг
- Оптимизация использования и стоимости привлечения ресурсов.

Практически каждый из этих пунктов (кроме, может быть, оптимизации ассортимента) имеет прямое отношение к информационной безопасности.

Изменение стратегии продаж

К числу решений Cisco, предназначенных для защиты и предотвращения утечек различных видов тайн и конфиденциальной информации на вынесенных торговых площадках можно отнести:
- Cisco Security Agent
- Cisco ASA 5505
- И другие решения Cisco.

Информационная безопасность не часто рассматривается как инструмент, способствующий изменению стратегии продаж и увеличению выручки. Каким способом ее можно увеличить? Например, за счет роста числа клиентов, которого можно достичь осуществив экспансию и продажу продукции в ранее неохваченных местах. Именно так, в частности, действуют банки, выносящие точки продаж кредитных продуктов в торговые центры. Но можно ли в столь незащищенном месте массового скопления народа обойтись без защиты тех сведений, которые доверяют будущие заемщики? Особенно если точка продаж имеет удаленный доступ к центральной сети банка. С одной стороны такая точка приносит доход, а с другой — без системы информационной безопасности вы не способны обеспечить банковскую тайну и защиту персональных данных, требуемых по закону. Иными словами, безопасность способствует получению дохода и защищает от штрафов за несоблюдение законодательства.

Другой способ увеличения выручки — увеличение числа сделок за тот же интервал времени. Иными словами мы должны ускорить процесс совершения сделок. Возьмем, к примеру, страхового агента, который приезжает к клиенту и заключает сделку прямо на месте, не возвращаясь в офис. Потом он едет к другому клиенту, затем к третьему. При этом информация обо всех сделках попадает в центральную базу данных, по которой страховой агент также проверяет клиента, его страховую историю и другие требуемые для заключения договора параметры. Как обеспечить связь агента с корпоративной сетью? С помощью смартфона, подключенного к Интернет. И вновь мы не можем обойтись без информационной безопасности в лице VPN-технологий, защищающих все передаваемые данные от перехвата и модификации.

Для защиты Интернет-площадки (банка или магазина) компания Cisco рекомендует различные программные и программно-аппаратные решения, в т. ч.:
- Cisco Web Application Firewall
- Cisco ASA 5500
- И другие.

Третий пример влияния ИБ на стратегию продаж — это появление новых, ранее недоступных каналов продаж, ярким примером которых является Интернет. Интернет-магазин, Интернет-банк, Интернет-трейдинг… Все это примеры, в которых защищенное подключение к Интернет позволяет одновременно решить сразу несколько бизнес-задач: увеличить выручку за счет роста числа новых клиентов, числа сделок с существующими клиентами и ускорения числа сделок, а также за счет снижения себестоимости таких сделок. Ведь работа через Интернет обходится значительно дешевле, чем содержание офисов, в которые клиенты вынуждены ходить лично.

Оптимизация использования ресурсов

Помимо уже перечисленных выше решений для защиты удаленного или мобильного рабочего места со стороны корпоративной сети компания Cisco рекомендует использовать следующие защитные решения:
- Cisco ASA 5500 для защищенного удаленного доступа большого количества пользователей
- Cisco ISR Security Bundles для защищенного удаленного доступа небольшого количества пользователей
- Cisco NAC Appliance для проверки соответствия подключающихся пользователей требованиям политики безопасности
- И другие.

Возьмем, к примеру, обычный восьмичасовой рабочий день рядового сотрудника отечественной компании. Его утро начинается со стояния в автомобильной пробке — на дорогу на работу он тратит не менее полутора часов в один конец. Приехав обозленным в офис, сотрудник проходит на свое рабочее место общей площадью не менее 6 квадратных метров. В обеденный перерыв он принимает пищу в корпоративной столовой. В течение дня сотрудник не раз пьет чай или кофе на офисной кухне, а вечером он едет домой. Получается, что ежедневно компания расходует свои деньги по следующим статьям бюджета:

- Аренда площадей
- Питание сотрудников
- Оплата канцтоваров
- Оплата проездных, бензина или автомобиля (в случае компенсации этих расходов компанией)

- Оплата электричества, отопления, водоснабжения и т.п.
- Оплата Интернет
- Прочие статьи.

Можно ли попытаться оптимизировать эти затраты? Разумеется. Достаточно перевести сотрудников на работу из дома, предоставив им подключение к корпоративной сети с помощью защищенного удаленного VPN-доступа и защитив их компьютеры от возможных атак из сети Интернет.

Для аутентификации, авторизации, разграничения и контроля доступа к различным ресурсам могут быть рекомендованы следующие решения:
- Cisco Secure Access Control Server
- Cisco Enterprise Policy Manager
- Cisco NAC Appliance
- И другие решения Cisco.

Другой пример влияния систем информационной безопасности и вообще информационных технологий на использование ресурсов заключается в решении задачи уменьшения складских запасов, но так, чтобы не увеличивать сроки поставки продукции потребителю. Сделать это можно следующим путем — предоставить удаленный доступ к информационной системе склада логистическим компаниям и поставщикам с тем, чтобы они самостоятельно отслеживали складские запасы и пополняли их в соответствии с установленными пороговыми значениями. В данном проекте на первое место выйдут технологии Identity & Entitlement Management (помимо уже упомянутых ранее технологий VPN, обеспечения доступности и защищенности Интранет-портала складской информационной системы и т. п.).

Cisco Capital предлагает простые и гибкие схемы финансирования, приобретения, аренды и лизинга, оплаты с отсрочкой устройств безопасности и сетевого оборудования Cisco для организаций любого размера и формы собственности. Благодаря этому предприятия могут реализовывать проекты, повышающие защищенность важнейших бизнес-приложений, даже в условиях нехватки финансовых ресурсов и нестабильной экономической ситуации.

Оптимизация ресурсов и информационная безопасность стыкуются и еще в одном направлении — оплата средств защиты информации. Если раньше этот процесс не вызывал никаких проблем, то в условиях отсутствия свободных денег и отказа многих банков в выдаче кредитов по приемлемым ставкам, вопрос оптимизации финансовых затрат становится очень важным. Какие варианты существуют на сегодняшний день? В первую очередь финансовый или оперативный лизинг, который не только позволяет снизить финансовое бремя приобретения решений по информационной безопасности, но перевести их из разряда капитальных затрат в операционные и улучшить показатели EBITDA. Второй распространенный вариант покупки средств защиты — оплата в рассрочку, которая позволяет не только отложить первые выплаты, но и зафиксировать стоимость проекта в рублях на день заключения договора (что защищает от негативного изменения курса валют).

О повышении производительности

Может ли информационная безопасность способствовать повышению производительности? Причем как производительности сотрудников, так и оборудования. Безусловно. Начнем с того, что сотрудник, работающий из дома, не опаздывает на работу и не стремится уйти «пораньше». Во-вторых, помимо финансовой стороны вопроса, существует еще и психологические моменты. Учитывая темп жизни современного человека, он всегда стоит перед дилеммой — работа или семья? И он вынужден разрываться между домом и офисом. Такой стресс влияет на все стороны жизни человека, в т. ч. и на работу. Концепция виртуального офиса (NVO) является компромиссом, т.к. она дает возможность подключаться к корпоративной сети в любое удобное время и в любом удобном месте. Но мобильность несет с собой и угрозу, т.к. сотрудник уже не находится под защитой корпоративных систем защиты. В этом случае мы должны оснастить персональными средствами безопасности ноутбуки сотрудников, а также модернизировать периметр сети для поддержки концепции NVO.

Для защиты мобильного офиса компания Cisco предлагает ряд программных решений, которые не только реализуют защиту ноутбука или смартфона от различных атак, но и обеспечивают защищенное подключение к корпоративным информационным ресурсам по любым существующим каналам связи. К числу таких решений относятся:
- Cisco Security Agent
- Cisco Secure Desktop
- Cisco AnyConnect Client
- Cisco VPN Client
- И другие.

Удаленный доступ к корпоративным ресурсам может выполняться не только из дома, но и из любой точки пространства — из кафе, из офиса клиента, из аэропорта во время ожидания самолета. Эта задача может быть решена по разному; один из вариантов – внедрение концепции NVO, которая гласит, что «офис там, где сотрудник», а не «сотрудник там, где офис». Эта концепция подразумевает, что сотрудник находится все время «в поле», как можно ближе к своим проектам, клиентам, партнерам и т. п. Но для эффективной работы сотрудник не только должен быть все время на связи, но и иметь доступ к корпоративным информационным ресурсам. При такой постановке задаче каждый сотрудник оснащается ноутбуком или КПК с различными интерфейсами подключения к сети (CDMA, GPRS, UMTS, Wi-Fi и т.п.), встроенным клиентом IP-телефонии, почтовым клиентом и другими полезными приложениями. В итоге, сотрудник становится мобильным, но для всех он как будто по-прежнему находится на своем

рабочем месте. По разным оценкам рост продуктивности сотрудника при использовании этой концепции может составлять от 10 до 40 процентов.

Где еще найти резервы времени у сотрудников? Интернет и электронная почта. В первом случае контроль действий сотрудников в Интернет и блокирование доступа к непрофильным сайтам позволяет высвободить массу времени. Например, по статистике, сотрудники тратят в день не менее часа на общение в социальных сетях «одноклассники.ру», «вконтакте.ру», «мой круг» и т.п. С электронной почтой тоже все просто. Сотрудники, особенно в крупных компаниях, немало времени тратят на чистку своего почтового ящика от спама. Умножив это время на стоимость рабочего времени, мы получим не только существенный резерв времени, но и немалые потери, которая несет компания от спама. В качестве примера возьмем оценку эффективности антиспам-решения, внедренного в компании со следующими исходными данными:

Для защиты электронной почты от спама и в зависимости от масштаба предприятия компания Cisco рекомендует одно из следующих своих решений:

- IronPort E-mail Security Appliance
- Cisco Spam & Virus Blocker
- Cisco CSC-SSM для Cisco ASA 5500.

- число почтовых ящиков — свыше 7000;
- объем корреспонденции — 70 тысяч сообщений в сутки;
- объем спама — 60% или 42 тысячи сообщений в сутки;
- время обработки одного спам-сообщения — 10 секунд;
- суммарные дневные затраты на спам — 14,583 человеко-дня;
- усредненная стоимость сотрудника для компании в месяц — 1500 долларов США.

Реальная экономия от внедрения антиспама составила:

- в день — 994,29 доллара США.
- в месяц — 21784,5 доллара США.
- в год — 248573,86 доллара США.

Защита унифицированных коммуникаций обеспечивается функциями, встроенными в:

- Cisco ASA 5500
- Cisco ISR
- Cisco Security Agent
- И другие.

В любой компании есть определенная группа сотрудников, которые регулярно ездят и летают в командировки, проводя в них по несколько дней. Это приводит к существенным затратам — на авиа- или железнодорожные билеты, гостиницы, питание, командировочные расходы, страховку (для заграничных командировок) и т.п. Как оптимизировать ресурсы и, сократив затраты на поездки, обеспечить тот же уровень взаимодействия с удаленными клиентами, партнерами и иными контрагентами? Один из вариантов — использовать концепцию NVO, позволяющую работать даже в аэропорту, на вокзале, в месте командировки и т.п. Второй вариант — внедрить систему унифицированных коммуникаций в виде средств видеоконференцсвязи или системы Telepresence, которые заменяют личное общение виртуальным. И нам опять не обойтись без защитных систем, предотвращающих несанкционированный доступ к переговорам.

Об аутсорсинге

В условиях нестабильной экономической ситуации многие предприятия начинают задумываться не только о сокращении персонала, но и о передаче части функций аутсорсинговым компаниям. Это логично, и информационная безопасность не является исключением из правила. Почему-то считается, что защиту информации нельзя отдавать на откуп внешним подрядчикам. Но это только на первый взгляд. Ведь доверяете вы свои секреты консультантам аудиторских, юридических, финансовых компаний? Доверяете вы перевозку своих денег внешним инкассаторам? Доверяете вы охрану своих физических активов и топ-менеджмента нанятому ЧОПу? Почему ИБ должна быть исключением?

Что дает аутсорсинг информационной безопасности? Ключевых преимуществ пять:

1. Круглосуточная защита ваших ресурсов.
2. Решение задачи нехватки специалистов ИБ (особенно в условиях сокращения персонала).
3. Разгрузка существующего персонала по ИБ или его переориентация на более важные задачи.
4. Получение «в штат» высококлассных специалистов.
5. Экономия за счет отказа от приобретения непрофильного оборудования.

Разумеется, при аутсорсинге есть свои тонкости, своя область применения, свои достоинства и недостатки. Но если компания приняла решение о переходе на аутсорсинг информационной безопасности, необходимо четко понять, что любое взаимодействие требует тщательной проработки контракта, а в условиях кризиса это правило становится важным как никогда. Необходимо не только защитить себя от возможных конфликтных ситуаций, но и получить максимальную выгоду от такого сотрудничества.

Компания Cisco предлагает аутсорсинг безопасности по трем направлениям:

- Реагирование на инциденты
- Удаленный мониторинг средств защиты
- Удаленное управление средствами защиты
- Управление средствами защиты электронной почты
- Услуга защищенной электронной почты
- Уведомление об уязвимостях в практически любом ПО, установленном у заказчика.

Для начала необходимо оценить, что и в каком объеме вы готовы отдать на аутсорсинг. От ответа на эти вопросы зависит, к какой компании обратиться. Одно дело передать внешней компании несложные задачи, например, поддержку антивируса. В этом случае вы можете без серьезного ущерба для себя поменять одного провайдера услуг на другого. Гораздо серьезнее выглядит задача управления инцидентами. Аутсорсинговую компанию в данном сценарии приглашают не столько ради экономии, сколько из-за наличия компетенции или повышения уровня удовлетворенности внутренних заказчиков. Тут потребуется более серьезная интеграция вашего бизнеса и аутсорсинговой компании и ее замена выглядит уже не такой простой (хотя и возможной). И уже совсем другое дело — внедрение системы сбалансированных показателей и KPI по информационной безопасности или полная поддержка всей инфраструктуры ИБ. Поменять такого аутсорсера дело практически безнадежное, т.к. он настолько тесно интегрирован с вами и погружен в ваш бизнес, что найти ему замену становится невозможным.

Не раз уже упоминая про переход к пониманию бизнеса, мы должны договориться с аутсорсинговой компанией не только об измеримом уровне качества предоставляемых услуг, но и о метриках, показывающих влияние переданных в чужие руки процессов, на ключевые бизнес-показатели.

Заключаемый контракт должен предусматривать возможный его пересмотр или даже прекращение в случае серьезных финансовых проблем у аутсорсинговой компании. В этом же разделе необходимо предусмотреть возможность перехода контроля информационной безопасности к другой компании (желательно без существенных дополнительных затрат).

О сокращении персонала

Не секрет, что многие предприятия начинают бороться с кризисом, с сокращения персонала и не в последнюю очередь за счет ИТ/ИБ-персонала. И хотя это самое последнее, о чем стоит думать при сокращении затрат, такая практика существует. Она порочна по двум основным причинам:

- Как правило, никто не знает, кого уволят следующим. Следовательно, люди больше начинают думать не о том, как улучшить свою работу, а о том, как не попасть под сокращение, где найти «запасной аэродром», кто виноват... Начинается недобросовестная конкуренция между сотрудниками, препятствующая достижению поставленных перед подразделением целей.
- Сотрудники начинают думать: «Если меня рано или поздно уволят, то зачем я буду напрягаться?» Продуктивность сотрудников падает, и желание работать на благо компании пропадает.

Почему в первую очередь сокращают подразделения ИТ и маркетинга? Потому что руководство не видит их вклад в цепочку создания ценности для организации и ее бизнеса. Продемонстрируйте отдачу от своей работы, и сокращение минует вас или затронет не так сильно. Все, что нужно сделать, — это повернуться к бизнесу лицом и связать свои проекты с его целями, продемонстрировать свое влияние на бизнес-показатели и всеми силами идти в русле бизнес-стратегии, а не рядом с ней и, конечно, не против нее.

Надо понимать, что сокращение — это последняя мера, которую нужно предпринимать. Если уж компания приняла решение экономить за счет персонала, то сокращению персонала есть ряд альтернатив, с внедрения которых и лучше начать:

- Неоплачиваемый отпуск.

- Сокращение рабочей недели.
- Уменьшение соцпакета.
- Снижение переменной части зарплаты или бонусов.
- Снижение фиксированной части зарплаты.

Все эти шаги неприятны, но они позволяют оставить за собой рабочее место, что, в условиях нестабильной ситуации и избытка свободных специалистов на рынке труда, уже немало. Если же все варианты исчерпаны и руководитель службы ИБ встает перед непростой задачей увольнения своих подчиненных, то можно воспользоваться следующими простыми рекомендациями.

Не секрет, что во многих компаниях существуют люди, которые пришли пересидеть сложные времена, которых взяли по знакомству, но загрузить нечем, которые выполняют никому ненужную работу. Такие люди всем известны, но во времена процветания они никому не мешают. Сейчас надо отдавать себе отчет в том, что именно они являются первыми кандидатами на сокращение. Да, их жалко! Но гораздо больнее увольнять ценных для компании сотрудников, которые обязательно понадобятся после стабилизации экономики и возврата бизнеса в нормальное русло.

В крупных компаниях службы информационной безопасности достаточно велики и включают несколько уровней иерархии — департамент, управление, служба, отдел, группа и т.д. В эпоху изобилия среднее управленческое звено росло как на дрожжах; в условиях сокращения им необходимо пожертвовать с целью удаления звеньев, удлиняющих цепочку создания стоимости. В конце концов, многие такие псевдоруководители занимаются только тем, что защищают большого начальника от подчиненных, а подчиненным передают указания Большого Босса, снабдив их еще и своими комментариями, зачастую полностью меняющими смысл первоначального распоряжения.

Самое главное — не увольняйте специалистов только потому, что вы закрыли проекты, в которых они участвовали; потом может быть очень трудно найти им замену. Лучше дать им другой фронт работ, временно перевести на другие позиции или даже в другие, смежные подразделения.

Что же делать, если сокращение затронуло службу ИБ вашей компании (особенно часто это возникает в региональных представительствах и филиалах)? Необходимо рассмотреть следующие возможности:

- Передача части функций ИБ внешним подрядчикам (аутсорсинг).
- Автоматизация задач, выполнявшихся ранее вручную. К их числу могут быть отнесены анализ защищенности, установка патчей, управление инцидентами, управление политиками безопасности для средств защиты, их обновление, управление конфигурацией, опечатывание USB-портов компьютеров и т.п. Для каждого из этих классов задач на рынке существуют средства защиты, которые в среднесрочной перспективы могут обойтись дешевле стоимости одного сотрудника для компании.
- Распределение человеческих ресурсов.
- Повышение производительности оставшихся сотрудников за счет высвобождения времени (при переходе на модель NVO) или автоматизации рутинных задач.
- Также надо понимать, что сегодня, когда рынок труда переполнен высококвалифицированными кадрами, существует отличная возможность подыскать себе классных специалистов с редкими талантами. Если топ-менеджмент сегодня не готов перераспределить сокращаемые штатные единицы и принять на работу ценные кадры в условиях кризиса, то вы можете оставить эти резюме «до лучших времен» и вам не придется после кризиса заново осуществлять поиск специалистов, тратя на это месяцы своей работы.

Если все-таки, несмотря на все вышеперечисленные рекомендации, дошло до сокращения, то неправильно было оставлять все «как было раньше». Необходимо пересмотреть свою работу с оставшимися людьми. Нельзя работать по-старому, как в

Компания Cisco предлагает целый спектр средств управления информационной безопасностью, среди которых:

- Cisco Security Manager, который автоматизирует процесс управления политиками ИБ на средствах защиты Cisco.
- Cisco Security MARS, который автоматизирует процесс мониторинга средств защиты различных производителей и реагирование на инциденты безопасности.
- Cisco Network Compliance Manager, который автоматизирует процесс аудита средств защиты и сетевого оборудования различных производителей.
- Cisco NAC Appliance, который автоматизирует процесс проверки и приведения в соответствие требованиям политик безопасности ПК, лэптопов, серверов и КПК.

докризисные времена. Нужны новые организационная структура, инструкции, процессы, технологии, средства автоматизации. Более того, почему бы не подумать об увеличении сотрудникам зарплаты? Вы сократили персонал, у вас высвободился фонд оплаты труда. Разделите его часть между оставшимися кадрами, и вы получите сплоченную и лояльную команду, которой будет не страшен любой кризис.

О защите бизнеса

Компания Cisco предлагает решение Cisco DLP Solution, которое включает в себя разнообразные средства и рекомендации по борьбе с утечками информации:

- Cisco IronPort E-mail Security Appliance
- Cisco Web Security Appliance
- Cisco Security Agent
- Cisco NAC Appliance
- И другие.

Еще одно направление, в котором информационная безопасность может помочь в условиях кризиса, — это защита активов компании. Не секрет, что при увольнении некоторые сотрудники могут попытаться нанести ущерб своему работодателю, попытавшись вывести из строя какие-либо элементы инфраструктуры, внеся вредоносные закладки в программное обеспечение или совершив хищение важной и конфиденциальной информации. Все эти действия наносят серьезный ущерб бизнесу компании, который выливается в следующие факторы:

- затраты на восстановление выведенного из строя оборудования,
- затраты на восстановление удаленной информации,
- затраты на оплату претензий со стороны клиентов, пострадавших от утечек информации,
- затраты на оплату исков со стороны регулирующих органов,
- удар по репутации предприятия,
- снижение стоимости акций на фондовой бирже (в ряде случаев),
- затраты на устранение иных последствий негативных факторов.

Подразделение информационной безопасности совместно с юридической службой и отделом кадров — это те силы, которые способны реально бороться с такими злонамеренными действиями сотрудников.

О лидерстве

В условиях нестабильности приобретают особое значение лидерские качества у руководителя службы информационной безопасности. Из всех существующих рекомендаций можно выделить 3 ключевых:

1. Начальник здесь Я! Не существует самой лучшей схемы управления государством. Все схемы имеют свои достоинства и недостатки. Тоталитаризм хорош тем, что решение принимает один человек и никто ему не мешает. Но минус тоталитарного государства в том, что и в обсуждении решения принимает участие только один человек, а значит он может упустить из ввиду множество мелочей и альтернативных действий. В демократическом обществе ситуация обратная — обсуждение того или иного решения открыто для всех, что позволяет найти большое количество различных выходов из проблемы. Но вот принятие решения в условиях демократии обречено на провал — очень трудно найти консенсус при большом числе участников. В условиях кризиса, когда надо быстро принимать трудные решения, руководитель подразделения ИБ должен прислушиваться к мнению подчиненных, но право принятия окончательного решения должно принадлежать только одному человеку.
2. Я отвечаю за результат! Руководитель службы информационной безопасности должен быть не только примером для сотрудников, но и персонально отвечать за принимаемые решения и за результат всех преобразований.
3. Я не боюсь открыто говорить о проблемах! В условиях кризиса многие российские компании предпочитают стратегию улитки, которая предполагает сокрытие от сотрудников всех новостей. Любое закрытое собрание руководства всегда вызывает тревогу и вопросы: «Зачем они собрались?», «Нас уволят?», «Нам порежут зарплату?» и т.п. Сокрытие ответов на эти вопросы приводит к росту недовольства,

ухудшению психологического климата, снижению продуктивности и т. д. Основная причина кризиса — недоверие. Необходимо прямо и открыто говорить с подчиненными обо всех непростых задачах, вставших перед подразделением информационной безопасности. Отсутствие коммуникаций повышает недоверие и порождает фантазии; открытые коммуникации управляемы.

О реальных и мнимых бизнес-преимуществах

Надо понимать, что при оценке эффективности очень часто смешиваются два понятия: непосредственные, прямые результаты от внедрения мер информационной безопасности и преимущества с точки зрения бизнеса. Первые достигаются сразу после внедрения того или иного решения или процесса. Вторые требуют участия бизнеса. Допустим, внедрение системы удаленного доступа позволит нам перевести часть сотрудников компании на дистанционную работу из дома, тем самым сократив арендуемые площади и сэкономив на этой, достаточно весомой в бюджете любой компании статье расходов. Выгода для бизнеса на лицо, но… Преимущества, которые организация получает от такого снижения арендной платы, зависит от менеджеров, которые, собственно, и решают, воспользоваться ли такой возможностью или нет. Может сложиться такая ситуация, что деньги на систему удаленного доступа потрачены, а работники на дом не переведены, арендуемые площади не сокращены и компания по-прежнему тратит столько же, сколько и раньше. Так стоила ли овчинка выделки? В данной ситуации проект удаленного доступа не только не принес никаких выгод (ведь ими не воспользовались), но и даже увеличил расходы компании.

Возьмем другой пример — внедрение системы контроля доступа к сети Network Admission Control (NAC), которая позволяет автоматизировать процесс проверки и приведения узла в соответствие с требованиями ИТ-политики и политики информационной безопасности. По оценкам компании Cisco такое решение позволяет сэкономить время и усилия следующим образом — идентифицировать несоответствующие устройства, определять их местоположение и приводить в соответствие. Итого мы сэкономили 4 человеко-часа на одно рабочее место. Но как мы воспользовались этой экономией? И воспользовались ли вообще? В данном примере экономия времени — это как раз непосредственные результаты от внедрения системы защиты. А вот бизнес-преимущества зависят от руководства, которое может воспользоваться дарованным резервом времени, а может и не воспользоваться.

Таблица 1. Экономия от внедрения решения NAC

Статья экономии	Оценка (человеко-часов)	Цена* (долл. США)
Идентификация несоответствующих компьютеров	1,0	12,00
Определение местоположения несоответствующих компьютеров	1,0	12,00
Приведение в соответствие	2,0	24,00
Потенциальна экономия на 1 компьютер		**48,00**

* Стоимость часа указана, исходя из среднемесячной зарплаты ИТ-специалиста в 2 тысячи долларов США.

Иными словами в условиях кризиса нужно не только демонстрировать, что служба ИБ может эффективно работать в контексте существующей бизнес-стратегии, предлагая те или иные бизнес-решения, но и добиваться внедрения этих решений в жизнь.

Заключение или резюме для стратегии выживания службы ИБ в условиях кризиса

Вкратце рассмотрев возможные сценарии и действия службы информационной безопасности предприятия в условиях непростой экономической ситуации, можно резюмировать все вышесказанное в следующих пунктах:

- *Выработка стратегии подразделения ИБ в условиях кризиса.* Логично предположить, что раз поменялась окружающая среда, то необходимо менять и правила работы и действия подразделения ИБ внутри компании. Причем желательно учесть как оптимистические сценарии развития событий, так и пессимистические.
- *Бизнес-ориентация.* При запуске проектов больший акцент необходимо делать на его бизнес-составляющей. Что даст бизнесу запуск проекта? И что компания потеряет при его остановке? Как он повлияет на основные бизнес-показатели — доходы, прибыль,

себестоимость, расходы и т.д.? Не случайно на Западе все чаще звучит термин «бизнес-технологии» (BT) вместо «информационные технологии» (IT). Без понимания этой связи ИБ обречена на неудачу. Сейчас настал именно тот момент, когда службы ИБ должны все больше усилий тратить на связь с бизнесом.

- *Сохранение команды.* В сложных экономических условиях необходимо не только сохранить команду высококвалифицированных сотрудников, но и повысить эффективность их работы, настраивая на результат. Не забывайте сообщать своим подчиненным последние новости на предприятии, разъясняя их смысл и последствия для бизнеса и сотрудников. Они не должны чувствовать себя брошенными на произвол судьбы, как это часто бывает.
- *Сокращение нецелевых затрат.* Необходимо сократить нецелевые траты и прекратить финансирование убыточных проектов. Оставшийся портфель проектов необходимо пересмотреть с целью учета принятых на предприятии антикризисных мер. Приоритет должен быть отдан тем проектам, которые позволяют достичь прямых, а не косвенных преимуществ, и при этом реализуются в течение одного года.
- *Будьте проводником изменений.* Не забывайте, что одно дело предоставить возможность для бизнеса и другое — воспользоваться ею на практике. Будьте проводником предлагаемых вами изменений.
- *Взаимодействие.* Как никогда важно привлекать все заинтересованные в безопасности службы и подразделения — юридическую, ИТ, HR и т.п.
- *Оценка эффективности.* В процессе запуска и после него большое внимание надо уделить оценке эффективности проекта, позволяющей своевременно определить, насколько он отклонился от заданных показателей эффективности, можно ли достичь поставленных целей в поставленные сроки и уложиться в заложенный бюджет и т.д. Эффективность системы ИБ, результат работы персонала подразделения, отдача от проекта по ИБ… все это показатели, которые должны и могут измеряться. Настало время задуматься о том, как это сделать.
- *Стандартизация.* Стандартизация систем ИБ и постановка процессов, не позволяют отклоняться от намеченного курса и обеспечивают оптимизацию ресурсов.
- *Совершенствование системы управления.* Внедрение системы эффективного управления инфраструктурой и приложениями информационной безопасности позволяет не делать скоропалительных решений, увязывать все действия и решения в единый комплекс и оптимально использовать выделенные ресурсы.
- *Общение с поставщиками.* Рассмотрите новые варианты взаимодействия с поставщиками. Скорее всего, вы уже не можете платить так, как раньше. А они как никогда нуждаются в вас и в более крепком и прогнозируемом взаимодействии с вами. Договоритесь о новых способах оплаты приобретаемых продуктов и услуг, которые позволят снизить финансовое бремя вашего предприятия. Таким примером можно назвать лизинг или оплату в рассрочку, которые позволяют распределить финансовые выплаты во времени, сняв с себя часть налоговых выплат и улучшив другие финансовые показатели (в частности, EBITDA).
- *Будьте готовы к неожиданностям.* Ситуация на рынке меняется очень быстро. Вчера вы думали о том, как сохранить за собой рабочее место, а уже сегодня у вас появилась возможность нанять новый персонал и запустить ряд отложенных проектов по ИБ. Готовьтесь к неожиданностям заранее – это позволит не упустить возможности, которые вам дает рынок и компания.
- Перестаньте бояться будущего!

Cisco
Россия, 115054, Москва,
бизнес-центр «Риверсайд Тауерс»,
Космодамианская наб., 52, стр. 1, 4-й этаж.
Телефон: +7 (495) 961 1410
Факс: +7 (495) 961 1469
www.cisco.ru
www.cisco.com

Cisco
Россия, 191186, Санкт-Петербург,
бизнес-центр «Регус»,
Невский пр-т, 25, 2-й этаж, офисы 9, 30.
Телефон: +7 (812) 336 6531
Факс: +7 (812) 346 7800
www.cisco.ru
www.cisco.com

Cisco
Россия, 630099, Новосибирск,
бизнес-центр «Росевроплаза»,
Димитрова пр-т, 2, 5-й этаж.
Телефон: +7 (383) 230 2670
Факс: +7 (383) 230 1795
www.cisco.ru
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**