Управление ИБ в условиях текущей неопределенности

Алексей Лукацкий
Бизнес-консультант по безопасности
27/10/15

3 сценария действий в кризис

- Занять выжидательную позицию в надежде, что
  - Курс стабилизируется
  - Девальвация повернет вспять
  - Ситуация нормализуется
- Срочно предпринимать «очевидные» действия
  - Сокращать расходы, в том числе ФОТ
  - Уменьшать штат сотрудников
  - Пересматривать обязательства и договоренности
- Провести тщательный анализ ситуации в своей отрасли, разработать и реализовать комплекс последовательных мер, направленных на поддержание конкурентоспособности компании/подразделения в новых условиях

Какие неопределенные моменты могут возникнуть?

1. Курс национальной валюты
2. Нестабильность собственного положения в компании
3. Взаимоотношения с поставщиками и контрагентами
4. Нестабильность положения подчиненных

1. Курс национальной валюты и девальвация

Активно использовать то, что есть

- Активно использовать то, что уже есть

  Пора начать пользоваться уже приобретенным на 90%, а не только покупать что-то новое

  Знаете ли вы, что в маршрутизаторах Cisco есть встроенный межсетевой экран, покрывающий до 80% функций, нужных для МСЭ?

  Знаете ли вы, что в ОС Windows (всех семейств) существуют встроенные возможности по разграничению доступа к файлам и приложениям? А про MS Security Essentials вы слышали?

- Повышение осведомленности персонала в области информационной безопасности

- Эффективное управление текущими решениями

  Управление событиями (SIEM), построение SOC

- Выстраивание процессов (incident/change/patch/vulberability/… management)

Разработка собственных решений?

- Разработка собственных решений по ИБ
  - Вы оценивали, что дешевле – делать свое или покупать чужое?
- Использование решений open source
  - Для внутренних задач
  - В качестве основы для своих продуктов для потребителя, например, IDS на базе Snort
- Считается, что open source – это тоже, что и коммерческое решение, только хуже поддержка и эргономика, а также отсутствуют гарантии
  - Готовы ли вы к таким рискам?

Чем (временно) заменить коммерческие решения?

Средство защиты	Аналог в open source
Антивирус	ClamAV, Immunet
Борьба с шпионским ПО	Nixory
Межсетевой экран / UTM	IOS Firewall, iptables, Endian, Untangle, ClearOS, NetCop, IPCop, Devil-Linux, Shorewall, Turtle Firewall, Vuurmuur
Прикладной межсетевой экран	AppArmor, ModSecurity
Антиспам	ASSP, SpamAssassin, SpamBayes, MailScanner
DLP	OpenDLP, MyDLP

Чем (временно) заменить коммерческие решения?

Средство защиты	Аналог в open source
Фильтрация Web	DansGuardian
Обнаружение вторжений на ПК	OSSEC
Обнаружение вторжений на уровне сети	Snort, Bro, Suricata
Управление паролями	PasswordMaker, KeePassX, KeePass Password Safe,
Шифрование на ПК	AxCrypt, TrueCrypt, Gnu Privacy Guard, NeoCrypt
Расследование инцидентов	ODESSA, The Sleuth Kit/Autopsy Browser, Cuckoo Sandbox, GRR, Maltego

Чем (временно) заменить коммерческие решения?

Средство защиты	**Аналог в open source**
Управление инцидентами	MozDef
Мониторинг сетевых аномалий	Wireshark, tcpdump, Security Onion, Network Miner
Многофакторная аутентификация	WiKID
Сканеры безопасности	OpenVAS, Nessus, Nmap, Metasploit, Nikto, Brakeman
SIEM	OSSIM, OpenSOC, ELSA
Анализ вредоносного кода	Volatility, Redline, FTK Imager, pdf-parser, pdfid

Курс валюты изменился. Что делать?

- Оптимизация затрат/инвестиций

  Взвешенное решение в отношении нужности и приоритезация планируемых инвестиций

- Использование различных финансовых схем

  Кредитование

  Лизинг

  Рассрочка и т.п.

- Перевод CapEx в OpEx

  Вы общались со своим финансовым директором? Что ему важно в текущее время?

- Выстраивание долгосрочных отношений с партнерами

  Фиксация курса при условии долгосрочных партнерских отношений и «размывании» разницы по нескольким проектам

Как оптимизировать затраты с помощью матрицы Эйзенхауэра

- «Самые срочные решения редко бывают самыми важными»

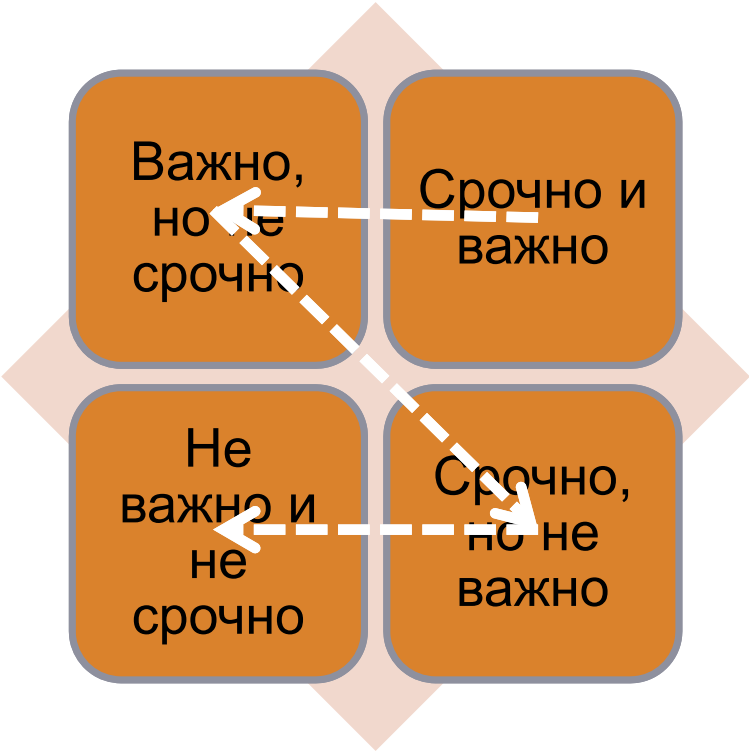
  Дуайт Эйзенхауэр

- Матрица Эйзенхауэра позволяет отделить важное от срочного

- Сфера применения

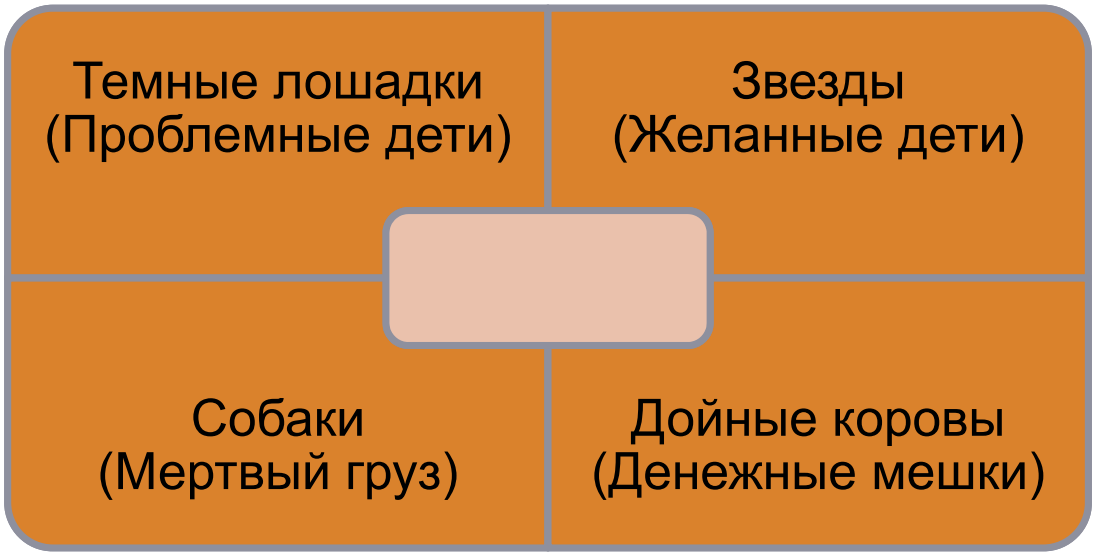
  Приоритезация проектов

  Подписание документов



Оптимизация затрат с помощью Бостонской матрицы

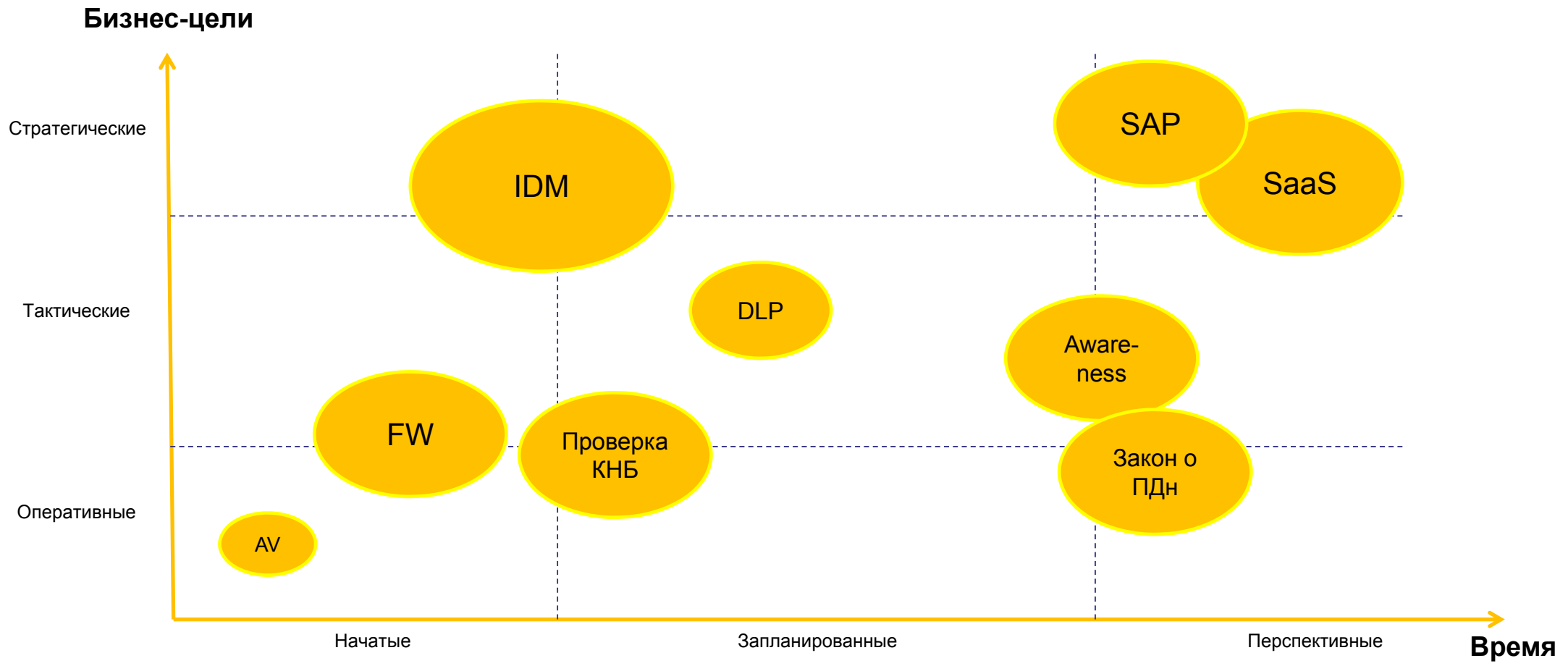
- Бостонская консалтинговая группа в 70-х годах разработала метод, позволяющий оценить ценность портфельных инвестиций в то или иное предприятие
- Сфера применения
  - Как выбрать наиболее выгодные проекты?
  - Как выбрать центры силы в компании, которые могут сказать «да» проекту по ИБ?
  - Как ранжировать угрозы по их ущербу?



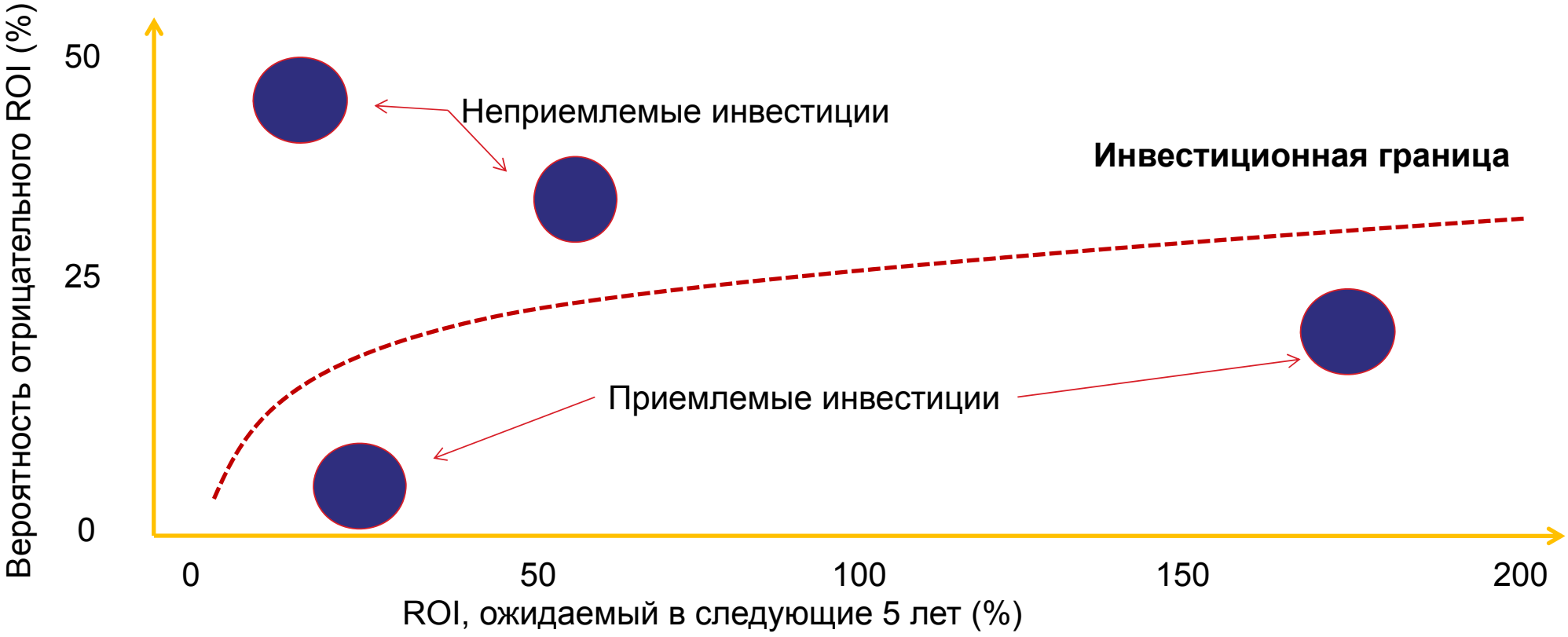
Третий подход к оптимизации затрат

- Служба ИБ обычно запускает или участвует в множестве проектов
  - Как научиться держать все в поле зрения?
- Матрица управления портфелем проектов позволяет окинуть взглядом все проекты по ИБ, в контексте разных пар факторов
  - Затраты и время
  - Достижение бизнес-цели и затраты
  - Любые другие комбинации
- Затраты – это не только деньги, но и люди и время

Пример: распределение проектов по ИБ



Пример: оценка риск-аппетита для проектов ИБ



2. Нестабильность собственного положения

Важность ИБ внутри компании во время кризиса

- В условиях кризиса возрастает число внутренних нарушений

  Утечки, снижение дисциплины, шантаж, блокировка учетных записей, уничтожение активов, компромат, «письма счастья» и т.п.

- Также будет расти число увольнений
- ИБ может помочь бороться с такими явлениями

  Если сможет обосновать свою роль в улучшении ситуации

- Активизация взаимоотношение с экономической безопасностью

При этом нестабильность своего положения

- Демонстрация своей нужности

  Кризис приводит к урезанию доходов и снижению затрат на «непонятные» направления, неприносящие прибыли в краткосрочной перспективе. ИБ - одно из таких направлений ☹

- Налаживать контакты с бизнес-подразделениями и показывать свою нужность для бизнеса, а не для кого-то еще

  Показывать свою эффективность; и не только труда

  Начать разбираться в финансах

- Что вы можете дать бизнесу?

Подготовка запасного аэродрома

- Умерьте аппетиты
- Обновите резюме
- Подготовьте план отступления и контрнаступления
- Следите за сайтами поиска работы или тематическими группами
- Займитесь собой

Займитесь собой

- Рост интереса к самообразованию и обычному образованию
  - Онлайн-курсы и краткосрочные курсы повышения квалификации
  - Необязательно курсы по ИБ – финансы, управление людьми, психология, английский или китайский…
- ИБ-сообщества
  - BISA, RISSPA, RISC, LinkedIn (Information Security Community KZ)…
  - Онлайн-семинары
  - Очные мероприятия
  - Группы в социальных сетях
  - Формирование социальных сетей знакомств
- Главное – не опускать руки!!!

SWOT-анализ

- Разрыв между планами и их реализацией обычно связан не с низкой компетенцией сотрудников, а с нечетко поставленными задачами
- Исследования Стэнфордского университета в США в 60-х годах
- SWOT
  - Strengths
  - Weaknesses
  - Opportunities
  - Threats

SWOT-анализ для самооценки

- Решаемые вопросы
  - Как максимально использовать сильные стороны и компенсировать слабые?
  - Как максимально использовать возможности?
  - Как защититься от рисков?
- Сфера применения
  - Оценка проектов по ИБ
  - Оценка собственных возможностей в целях карьерного роста или сохранения работы
  - Оценка продуктов по защите информации

3. Взаимоотношения с поставщиками

Взаимоотношение с поставщиками

- Непростая экономическая ситуация обострит конкуренцию на
  - Рынке интеграции
  - Рынке труда
  - Рынке производителей
- Нестабильное положение поставщиков продуктов и услуг
  - Потенциальный рост цен
- Проверяйте контрагентов
  - Вендоры в текущих условиях готовы на разные варианты сотрудничества – рассрочка, скидки, бандлы и т.п.
  - Не все игроки переживут 2015/16-й год
  - А те, что переживут начинают повышать цены на свою продукции/услуги

Рынок меняется

- Снижение капитальных затрат и переход на операционные затраты может привести к росту интереса к сервисной модели ИБ
  - Cloud Security
  - Security as a Service
  - Security on demand
- Вы рассматривали операторов связи в контексте нового бизнес-партнера по информационной безопасности?
- Рост интереса к эффективному управлению лицензиями на ИБ-продукты
  - Не годовые, а по мере использования (по времени, по ресурсам)

4. Нестабильность положения подчиненных

Нестабильность положения подчиненных

- Кем (чем) заменить сокращаемых сотрудников?
- Снижение капитальных затрат и переход на операционные затраты может привести к росту интереса к сервисной модели ИБ
  - Cloud Security
  - Security as a Service
  - Security on demand
- Проработка вопроса перехода к аутсорсингу
  - При соответствующем обосновании

“Любой кризис – это новые возможности”

Уинстон Черчилль

Благодарю за внимание