

Список потребностей СхО банка и как натянуть на них кибербезопасность

Алексей Лукацкий
Бизнес-консультант по безопасности
alukatsk@cisco.com

Обычно на банк мы смотрим не с той точки зрения



Как обычно продается безопасность?



«Простота» использования драйверов «продажи» ИБ

Compliance

- Самый простой способ «продажи» ИБ
- Можно вообще не знать особенностей и потребность заказчика и позицию руководства

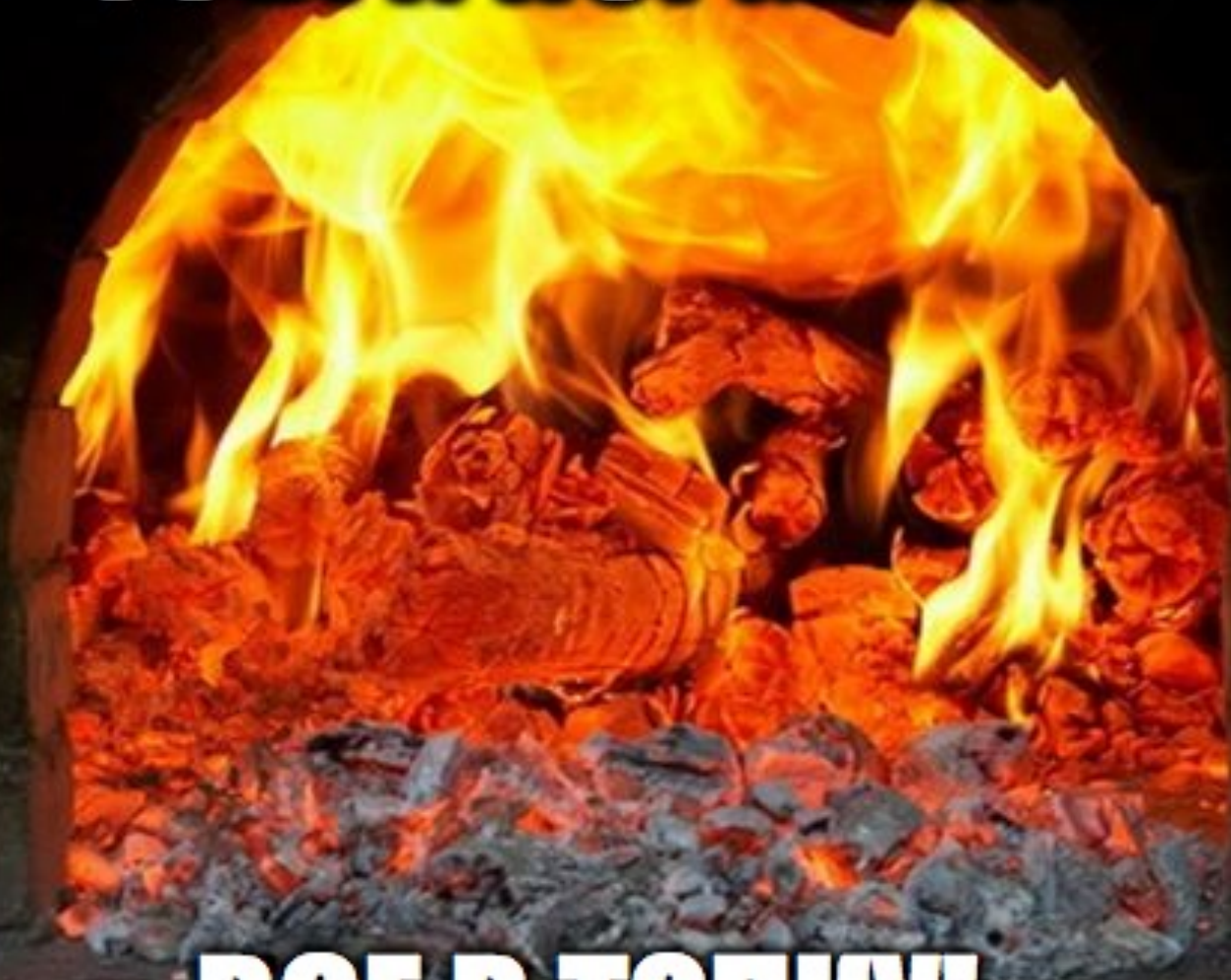
Страх

- Самый первый и самый привычный способ «продажи» ИБ
- Срабатывает, если угроза имела место в недавнем прошлом
- Требуется хорошего контакта с заказчиком/руководством

«Экономика»

- Новый и пока еще редкий способ «продажи» ИБ
- Требуется серьезного знания бизнеса заказчика
- Требуется выхода на уровень бизнеса
- Не реплицируется – каждое обоснование уникально
- Обоснование может показать, что ИБ невыгодна или не нужна заказчику!

УГРОЗЫ И НОРМАТИВКА



ВСЕ В ТОПКУ!

imgflip.com

Какова цель **любого** бизнеса?

- Предпринимательской является самостоятельная, осуществляемая на свой риск деятельность, направленная на систематическое получение **прибыли** от пользования имуществом, продажи товаров, выполнения работ или оказания услуг лицами, зарегистрированными в этом качестве в установленном законом порядке

Банк тоже хочет получать прибыль

Что такое прибыль?

Доходы - Расходы

Как руководство банка видит ИБ?

ПРИБЫЛИ (PROFIT)		&	(LOSS) УБЫТКИ	
Прошли проверку ЦБ	0 р.	X	XXX XXX р.	Фонд оплаты труда
Выполнили 382-П	0 р.		XXX XXX р.	Аренда помещений
Внедрили ГОСТ 57580.1	0 р.	X	XXX XXX р.	Оборудование
Снизили риски	0 р.	X	XXX XXX р.	Программное обеспечение
Сохранили банковскую тайну	0 р.			
Нашли 5 APT и 3-х инсайдеров	0 р.		XX XX р.	Бухгалтерское ведение
Отбили 2 DDoS-атаки	0 р.		XX XX р.	АХО
		X	XXX XXX р.	Консалтинг
			XXX XXX р.	Аутсорсинг

Дима, спасибо за идею картинки 😊

Расходы считать просто. Что с доходами / выгодами?

- Получение новых доходов
- Снижение/оптимизация расходов/потерь
- Снижение времени
- Снижение (высвобождение) числа людей
- Добавление новых качеств
- Не во всех компаниях это выгоды!

Поймите, что считается выгодой именно у вас



ИБ без привязки к бизнесу – это сферический конь в вакууме



Куда мы вкладываем деньги?

Продукт ИБ	Проект ИБ	Проект ИТ	Бизнес-проект
• Зачем нам конкретный продукт? • Какую задачу он решает?	• Зачем нам этот проект ИБ? • Какую задачу он решает?	• Зачем нам этот проект ИТ? • Какую задачу он решает?	• Зачем нам этот бизнес-проект? • Какую задачу он решает?

- Мы вообще понимаем, **для чего** нам ИБ?
- Варианты «так принято» и «чтобы было безопасно» не подходят!

Вариант «так требуют регуляторы» возможен ☺ но с оговорками

Какие расходы (потери) несет бизнес?

- Потери интеллектуальной собственности

Ноу-хау, патенты, списки клиентов, условия договоров

- Юридические потери

Штрафы и досудебные урегулирования

- Потери «собственности»

Курс акций, перехват управления АБС или процессинга, вывод из строя, информация, приводящая к задержкам в выпуске банковских продуктов или услуг, кража денег со счета

- Репутационные потери

Снижение лояльности → снижение ARPU, уход клиентов, негативные отзывы в прессе

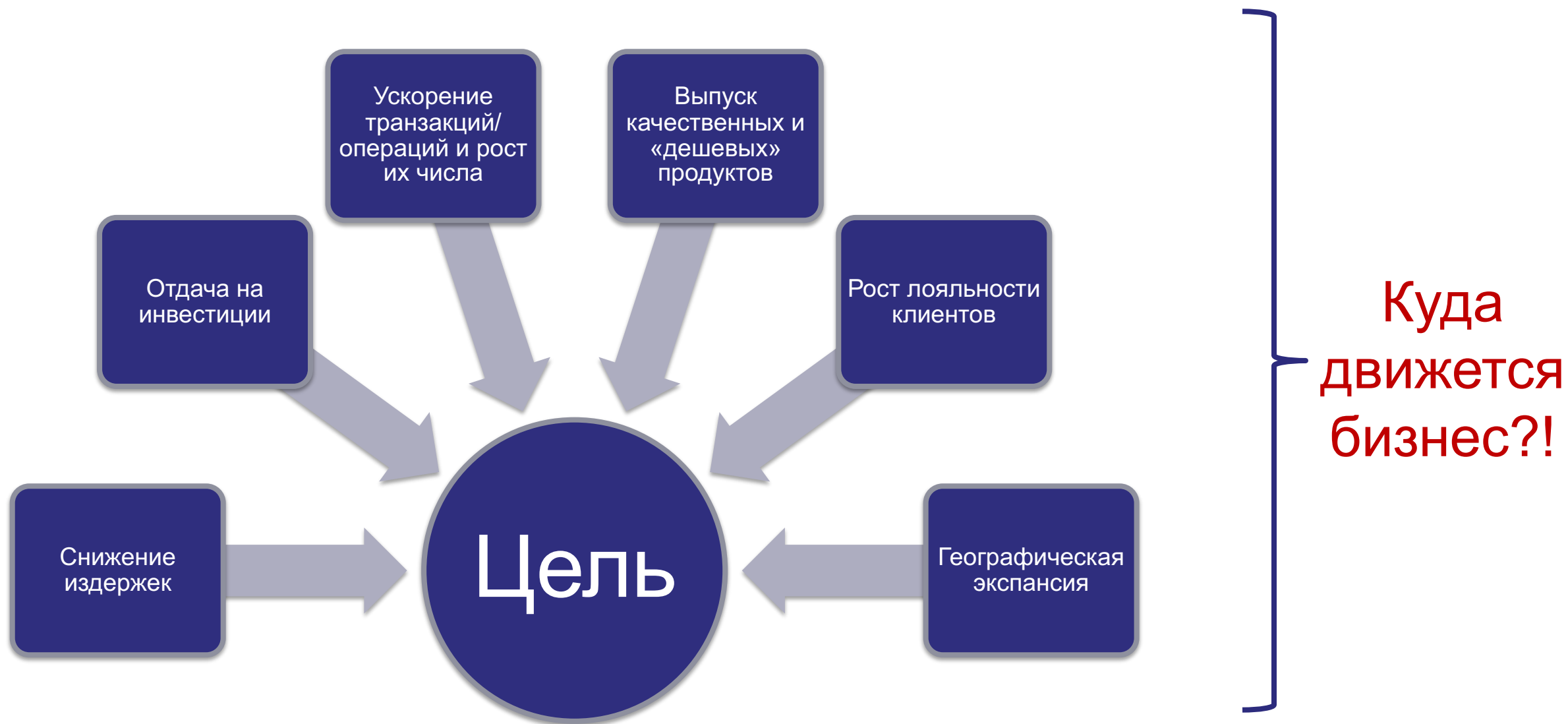
- Потери времени (простои) на восстановление и расследование

Какие расходы (потери) несет бизнес?

- Административные затраты на восстановление, взаимодействие с клиентами и регуляторами, возврат в предатакованное состояние
- Операционные
- Вред окружающей среде
- Ущерб жизни и здоровью
- Получение конкурентами преимуществ
- Подрыв доверия инвесторов и акционеров



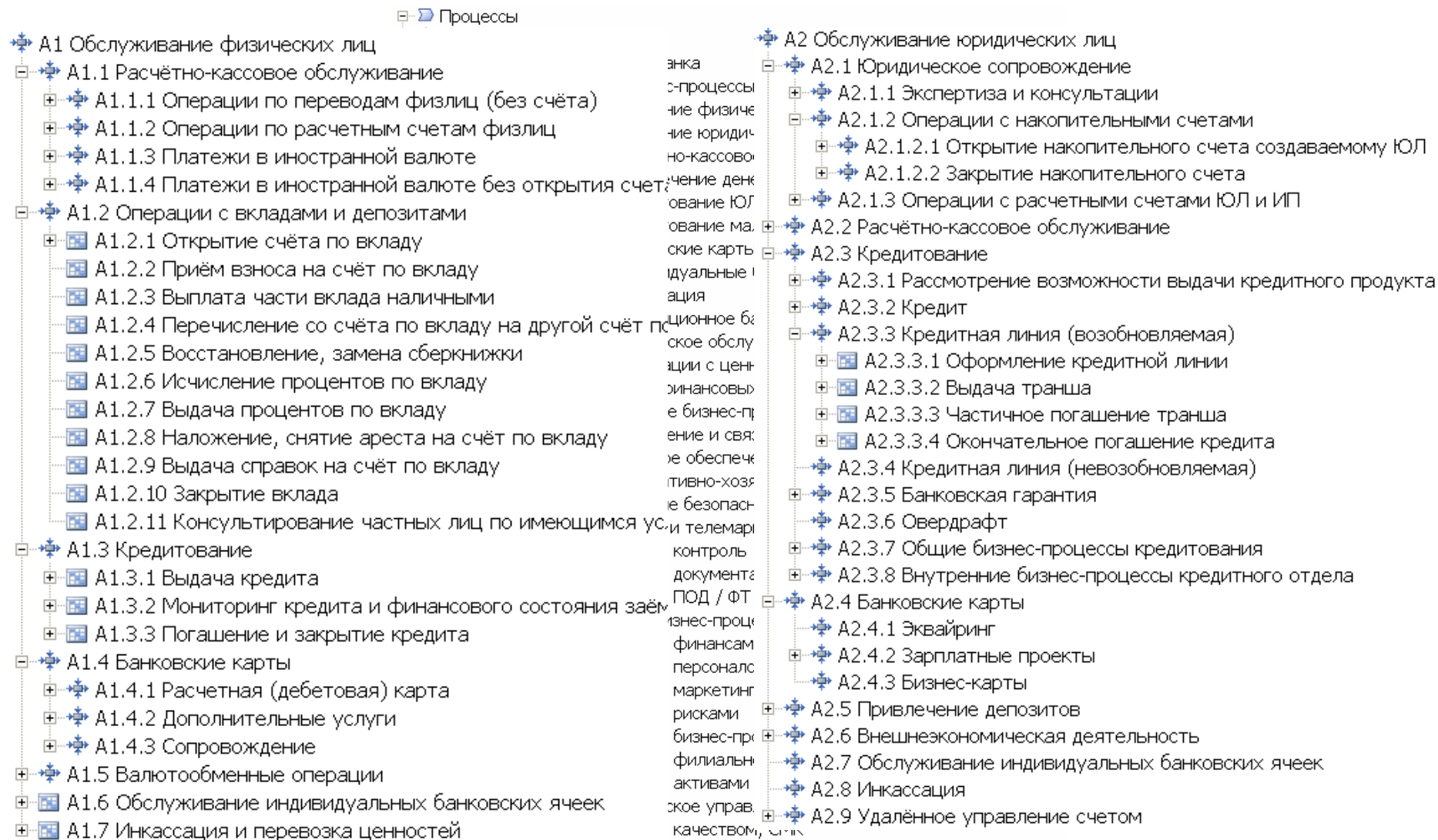
За счет чего растут доходы?



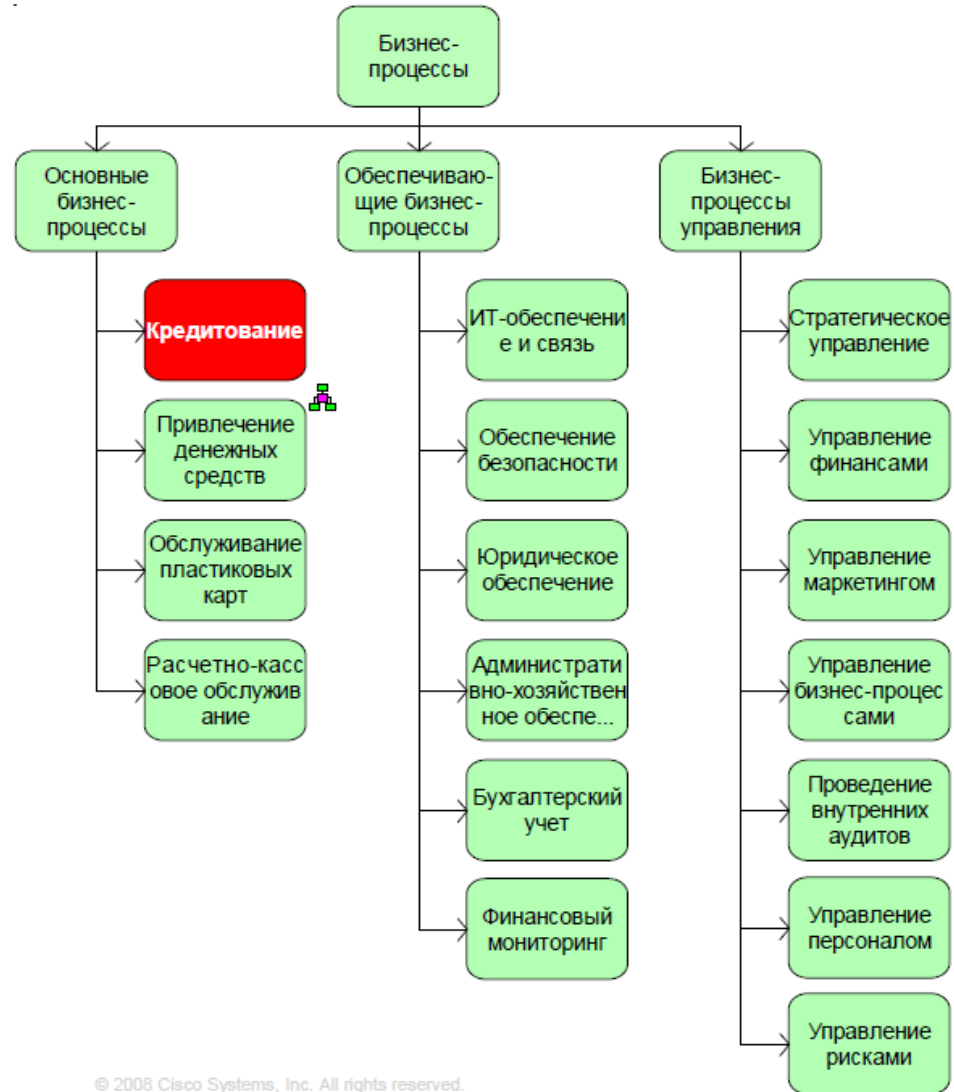
Пример: как ИБ влияет на доходы банка?



Вы знаете, чем занимается банк?

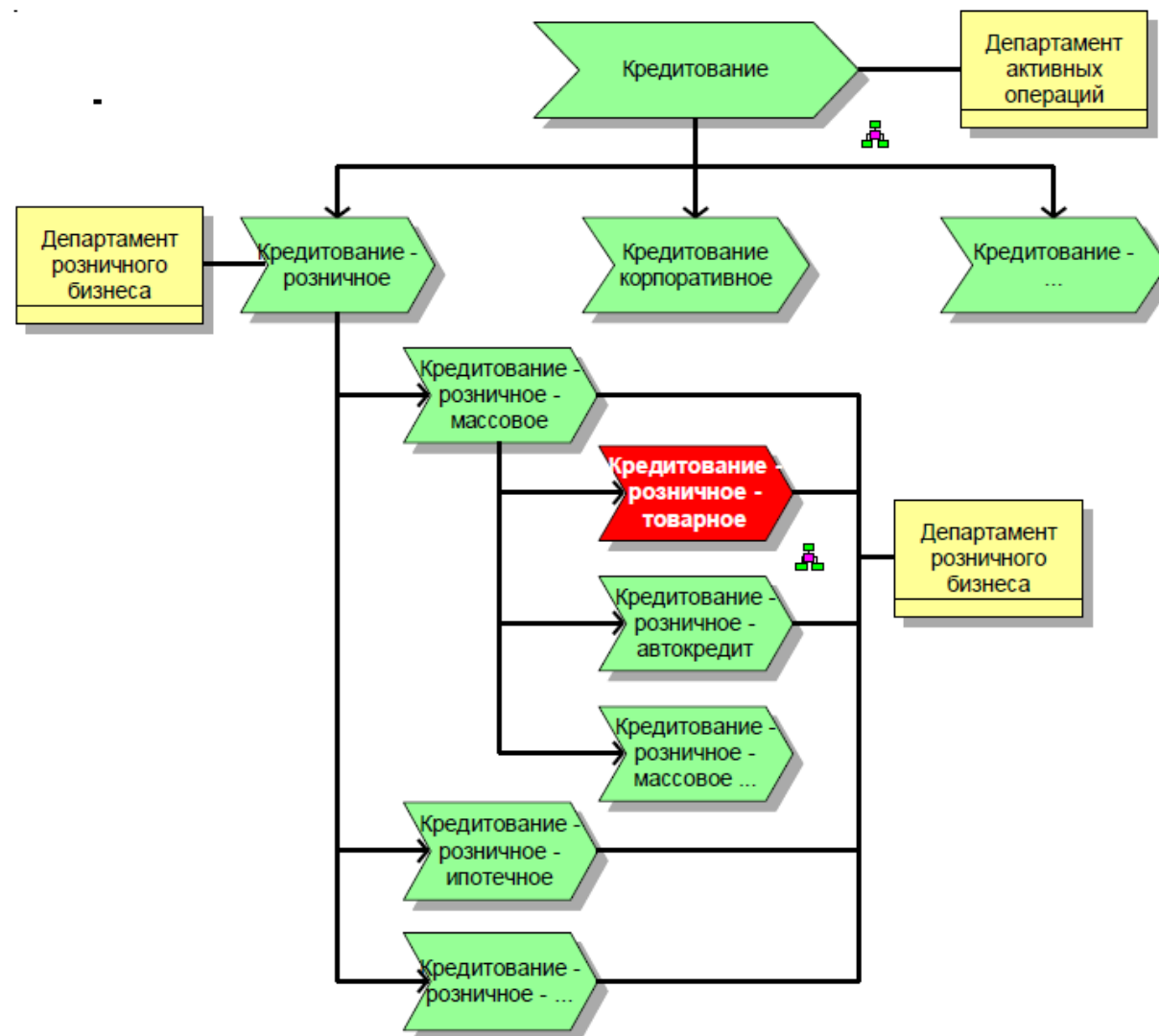


Возьмем для примера процесс кредитования

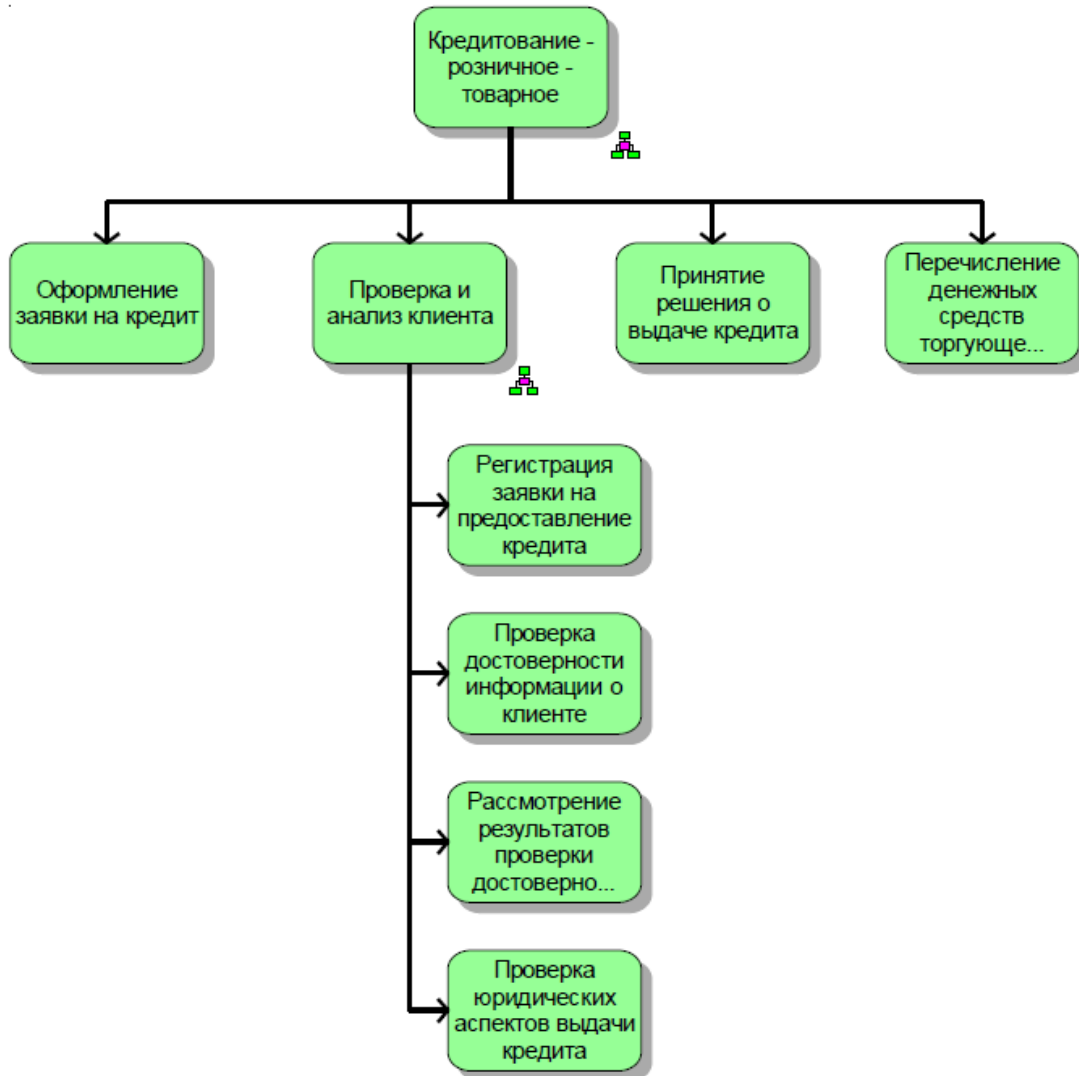


© 2008 Cisco Systems, Inc. All rights reserved.

Детализация процесса кредитования



Элементы процесса кредитования



- Типичный подход безопасника
Защитить персональные данные заемщика
Проверить на вирусы анкеты заемщика, получаемые по e-mail
- Все это бизнесу неинтересно ☹
- Бизнес интересуется выгоды и убытки
- Мы должны понимать бизнес-процесс, его составные части и статьи доходов/расходов

Регистрация заявки заемщика

- Какой ключевой показатель процесса?

- Ключевой показатель процесса
Время регистрации заявки заемщика

- Что может помешать процессу?
Недоступность сайта банка

- К чему это приведет?
К потере клиента, то есть к потере денег

- Знаем ли мы, сколько нам денег приносит средний клиент?
Да!

- Что надо сделать?
Обеспечить доступность сайта и проверку корректности заполнения полей Web-анкеты

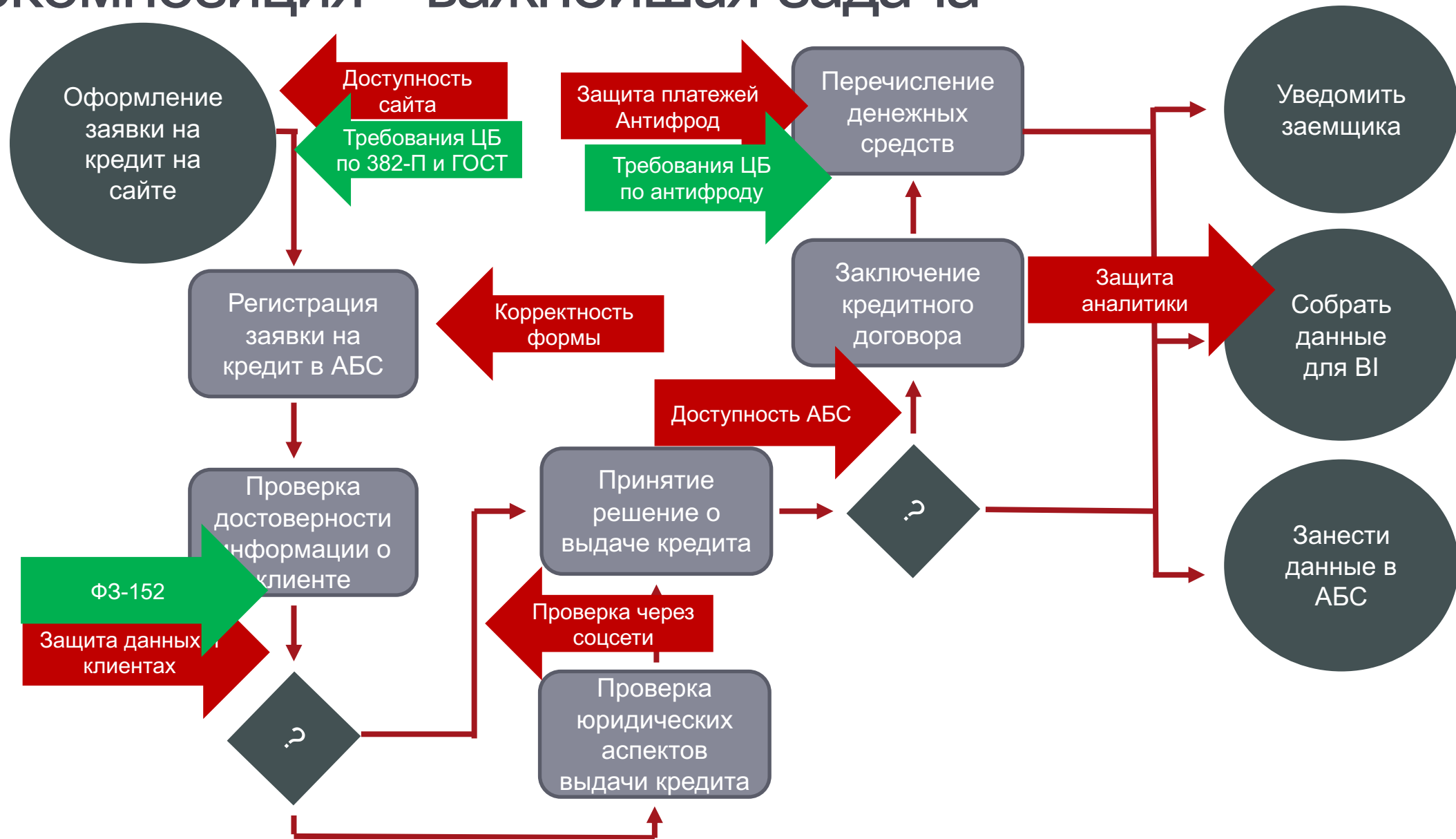
Вы отражаете не
DDoS-атаки, вы
защищаете свои
деньги!

Проверка достоверности информации о заемщике

- Какой ключевой показатель процесса?
- Ключевой показатель процесса
Время проверки информации
- Как можно ускорить процесс проверки?
Применить средства анализа социальных сетей
- К чему это приведет?
К снижению времени на проверку заемщика, росту его лояльности и увеличению числа проверяемых заемщиков, что **может** привести к росту числа клиентов и денег от них
- Что надо делать?
Внедрить средство автоматизации анализа соцсетей

Вы вообще не защищаете информацию в данном кейсе, вы защищаете свои деньги!

Декомпозиция – важнейшая задача



Private Banking

- Какой ключевая особенность процесса?

- Особенности процесса

Процентные ставки и условия обслуживания определяются банками индивидуально для каждого клиента

- Что может помешать процессу?

Раскрытие информации широкому кругу лиц

- К чему это приведет?

К потере клиента, то есть к потере денег

- Что надо сделать?

Защитить информацию о VIP-клиентах

**Вы защищаете не
персональные данные,
вы защищаете свои
деньги!**

Управление финансами

- Что надо финансовому директору?

- Финансовый директор имеет потребность в оптимизации финансовых затрат

Предсказуемость финансовых потоков, кредит/рассрочка, снижение налогов на прибыль и имущество, ускоренная амортизация и т.п.

- Что надо сделать?

Предложить финансовые услуги (кредит, лизинг, рассрочка) или новые виды сервисов ИБ (аутсорсинг, ИБ из облака и т.п.)

**Вы вообще не
защищаете
информацию в данном
кейсе, вы экономите
деньги!**

Удержание персонала

- Какой ключевая особенность процесса?

- При удержании персонала важно своевременно узнать о желании сотрудника уйти

- К чему это приведет?

К простою вакансии и недополученной прибыли (поиск и удержание персонала – 4:1)

- Что надо сделать?

Мониторить e-mail в части рассылки резюме и получения job offer, а также мониторить доступ к сайтам для поиска работы

**Вы вообще не
защищаете информацию
в данном кейсе, вы
экономите деньги!**

Рост продуктивности сотрудников

- **Зачем надо думать о продуктивности работников?**
 - Что снижает продуктивность работников?
Спам и бессмысленный Интернет-серфинг
 - К чему это приводит?
К временным затратам на чтение спама и посещение ненужных для работы сайтов, что в свою очередь выливается в недополученную прибыль
 - Что надо делать?
Внедрять средство защиты от спама и контроля доступа в Интернет
- Вы вообще не защищаете информацию в данном кейсе, вы повышаете продуктивность работников!**

Снижение затрат на командировки

- При чем тут командировки и ИБ, если речь не про удаленный доступ?
- Необходимо обеспечить снижение затрат на командировки высококвалифицированных экспертов на удаленные площадки
- К чему это приводит?

К росту затрат на командировки и увеличению времени на запуск того или иного процесса/продукта на удаленной площадке

- Что надо делать?

Внедрять средства унифицированных коммуникаций с защитой передаваемой информации

Вы вообще не защищаете информацию в данном кейсе, вы снижаете издержки!

Дистанционное банковское обслуживание

- К чему могут привести проблемы с ДБО?

- Некорректная реализация сервиса ДБО может привести к хищениям средств со счетов клиентов

- К чему это может привести?

Не только к необходимости возмещения средств клиентам (не всегда и необязательно), сколько к снижению лояльности клиентов и их оттоку

- Мы знаем число ушедших клиентов и причины их ухода, а также «стоимость» одного клиента?

Да!

- Что надо делать?

Внедрять систему защиты ДБО

**Вы защищаете не ДБО,
вы сохраняете клиентов
и их деньги!**

Гостевой Wi-Fi-доступ

- **Причем тут вообще гостевой Wi-Fi-доступ?**
- Необходимо предоставить гостевой Wi-Fi доступ для клиентов (в т.ч. и VIP) банка на время нахождения в очереди или при ожидании оформления договора
- К чему это приводит?
 - К росту лояльности клиентов, отслеживанию их поведения и предложения персонализированных услуг
- Что требуется для предоставления гостевого доступа?
 - Отвлечение сотрудников ИТ на создание, ведение и удаление временной учетной записи
- Что надо делать?
 - Внедрять средство обеспечения гостевого доступа

**Вы вообще не защищаете
информацию в данном кейсе,
вы зарабатываете деньги!**

Стандартизация ИТ-платформы

- **Зачем нужна стандартизация ИТ-платформы?**
- Необходимо защититься от установки неразрешенного ПО и подключения к банковской сети неразрешенных устройств
- К чему это приводит?

К поиску несоответствующих ИТ-политикам устройств, заражению банковской сети с несоответствующих политике устройств и т.п.

- Что надо делать?

Внедрять средство контроля сетевого доступа и анализа/профилирования сетевого трафика (NGFW/AVC)

**Вы вообще не защищаете
информацию в данном кейсе, вы
повышаете доступность и
управляемость инфраструктуры!**

Борьба с криптолокерами

- Что такое криптолокер не с точки зрения ИБ?

- Чем характеризуется криптолокер?

Шифрованием диска и вымогательством денег

- К чему приводит шифрование диска?

К потере доступа к файлам и простою (компьютера, сотрудника, процесса), что приводит к потере денег

- Что надо делать?

Внедрять средство защиты от вредоносного кода

Вы боретесь не с шифровальщиками, вы защищаете свои деньги!

Борьба с вирусными эпидемиями

- Что такое вирус не с точки зрения ИБ?

- Чем характеризуется эпидемия?

Необходимость лечить и восстанавливать работоспособность большого количества пострадавших ПК

- К чему это приводит?

К затратам на процесс локализации пострадавших, их лечению и восстановлению в предатакованное состояние

- Что надо делать?

Внедрять средство защиты от вредоносного кода

**Вы боретесь не с
вирусами, вы
защищаете свои
деньги!**

Борьба с DDoS

- Что такое DDoS?

- Чем характеризуется DDoS?

Простоем сайта банка или Интернет-банка

- К чему приводит простой сайта?

К снижению лояльности клиентов и уменьшению числа операций, что приводит к потере денег

- Что надо делать?

Внедрять средство или сервис отражения DDoS-атак

Вы боретесь не с DDoS, вы защищаете свои деньги и лояльность клиентов!

Борьба со снижением простоев – самый простой способ перевести ИБ в деньги

- Простои могут быть

- У сотрудника

- У узла

- У процесса

- У приложения

- ...

- Простой всегда выражается в деньгах!

- Криптолокеры, эпидемии, DDoS, спам, ненужные для работы сайта, отсутствие SSO и т.п.

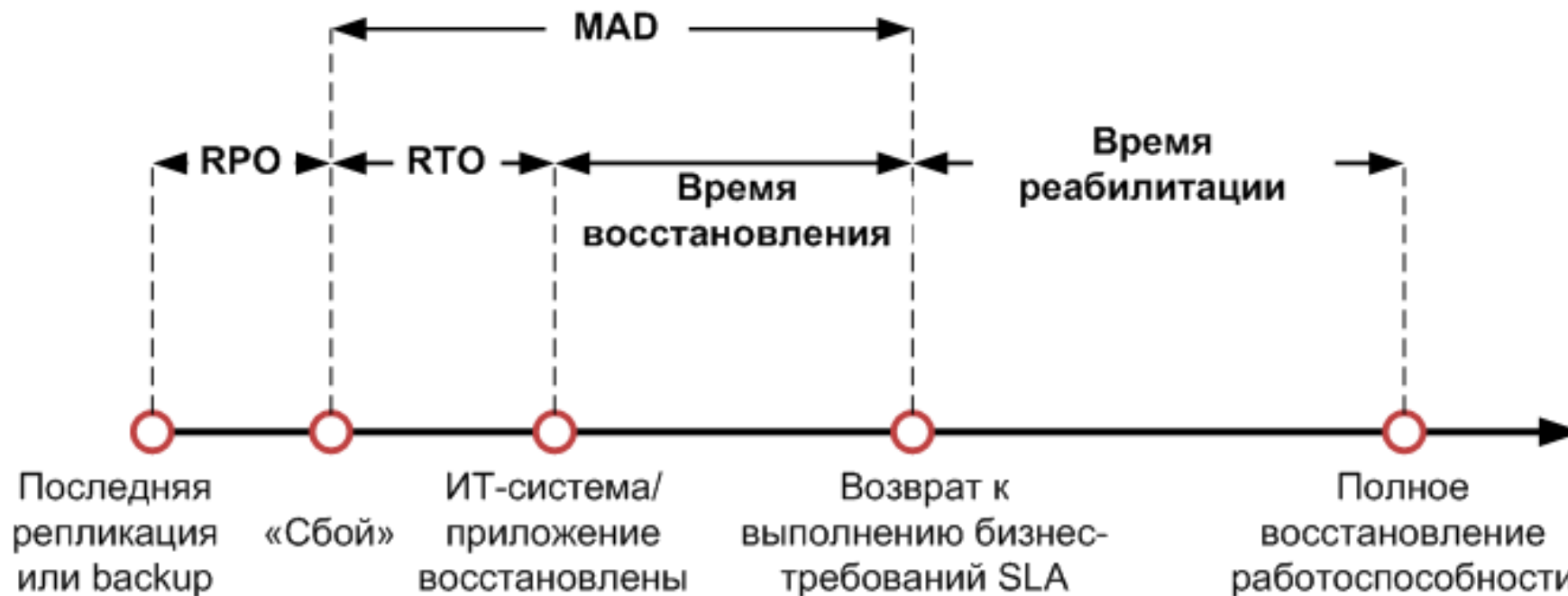
- Простой приводит к замедлению оформления кредитных договоров, замедлению осуществления транзакций, что приводит к снижению их числа и потерям денег

- Снижение времени простоя (обеспечение доступности) должна является одной из основных целей ИБ, т.к. она понятна бизнесу лучше конфиденциальности и целостности информации

Жизненный цикл сбоя (простоя)

- Степень влияния и составляющие цены «сбоя» меняется с течением времени

Эта иллюстрация может использоваться при оценке времени восстановления после атаки



RPO – Recovery Point Objectives, RTO – Recovery Time Objectives, MAD – Maximum Allowable Downtime

Как это все сложить вместе?

Преимущества – совокупная стоимость владения = ?

сокращение затрат и рост доходов

|

?

└─→

> 0 – ИБ будет позитивно воспринята бизнесом

< 0 – ИБ будет негативно воспринята бизнесом

Центр затрат :-)

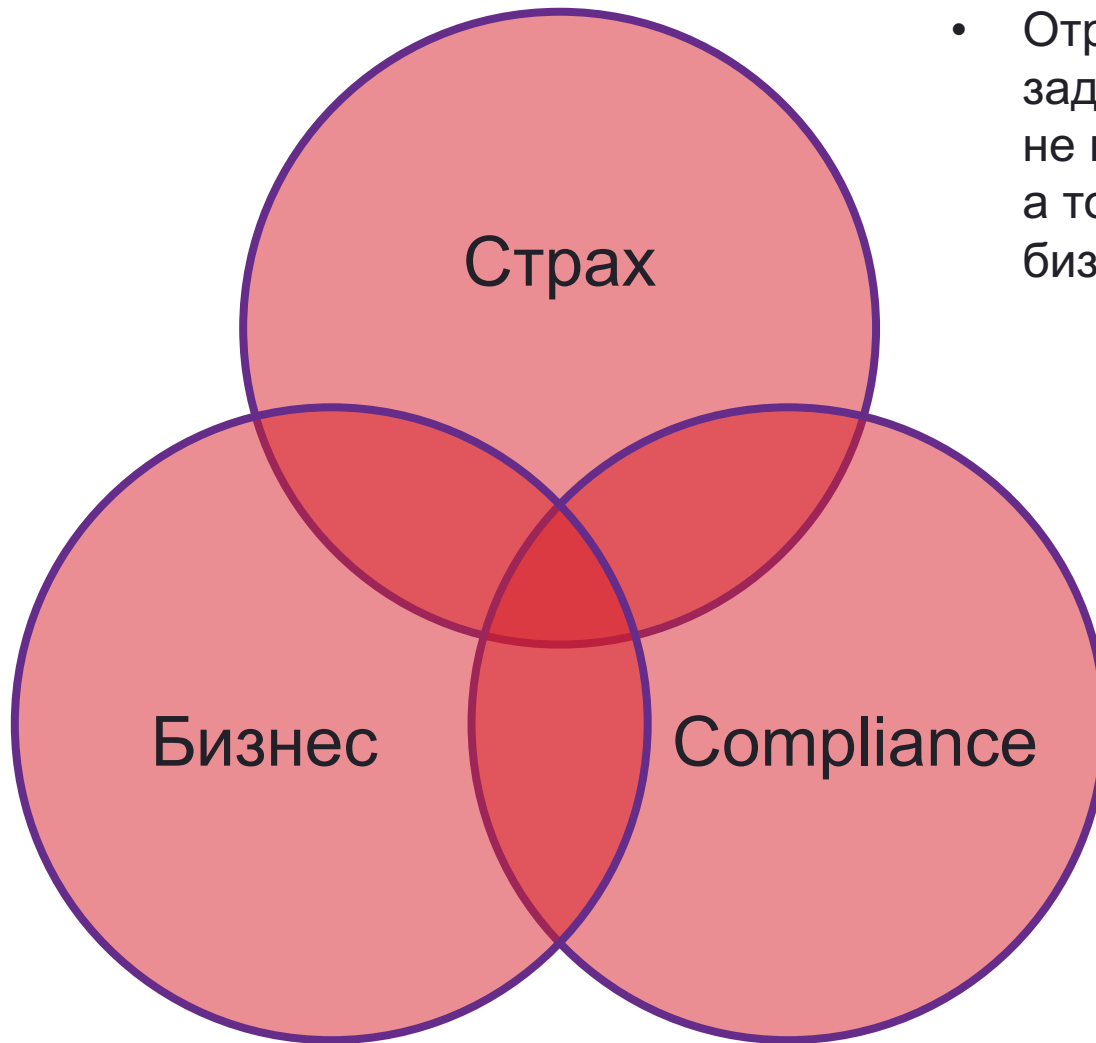
Какой же все-таки вклад ИБ делает в бизнес?

- Географическая экспансия
- Вынос точки продаж «в поля» (ближе к клиенту)
- Новый или более дешевый канал продаж
- Снижение арендной платы
- Оптимизация складских запасов и ускорение вывода продукта на рынок
- Оптимизация финансовых затрат (EBITDA, CapEx/OpEx, лизинг, амортизация...)
- Рост продуктивности сотрудников
- Уменьшение числа командировок и снижение рисков путешествий

Какой же все-таки вклад ИБ делает в бизнес?

- Сокращение затрат на Интернет
- Снижение ИТ-издержек на внутренний helpdesk
- Рост лояльности заказчиков
- Стандартизация
- Предотвращение увольнения сотрудников
- Обнаружение сговоров и конфликтов интересов
- Снижение простоев

А как же все-таки быть с угрозами и нормативкой?



- Отражение угроз является тоже бизнес-задачей, если мы будем рассматривать не мифические или навязанные угрозы, а то, что может нанести **реальный ущерб** бизнесу
- Выполнение нормативно-правовых актов тоже является задачей бизнеса, если их невыполнение влечет за собой штрафы, приостановление деятельности, дисквалификацию и иные риски, которые **подтверждены** правоприменительной практикой

Если вы готовы, то

- Поймите ваш бизнес (на чем он зарабатывает деньги)
- При финансовой оценке вопрос «ЗАЧЕМ что-то надо делать?» гораздо важнее вопроса «ЧТО надо делать?»
- Помните про декомпозицию
Целей, процессов, выгод и потерь
- Помните про целевую аудиторию, которой вы будете демонстрировать отдачу

Эффект наступит не сразу

Нет волшебных слов и
универсальных формул!

Изучайте свой бизнес и
учите бизнес-язык

Вы решаете не свои
проблемы, а задачи
бизнеса

Новый взгляд на ИБ с точки зрения бизнеса



Благодарю
за внимание

