СЕМИНАР
«АНТИКРИЗИСНАЯ СТРУКТУРНАЯ ОПТИМИЗАЦИЯ»
КОРПОРАТИВНОЕ МОШЕННИЧЕСТВО

МОСКВА

МИХАИЛ КРАПИВИН

- Старший советник в компании Alvarez&Marsal, лидер направления Global Forensic Services and Disputes в России
- Единственный официальный представитель Paul Ekman International в России, управляющий директор тренинговых программ PEI в России
- 15 лет опыта в области расследований, поиска активов и создания систем противодействия мошенничеству
- Единственный российский участник программы Behavioral Science в Лондонской Школе Экономики и Политических Наук

Контакты:
mikhail.krapivin@alvarezandmarsal.com
+ 7 903 725 49 73

СОДЕРЖАНИЕ

КЛЮЧЕВЫЕ ПРОБЛЕМЫ

- **ПСИХОЛОГИЯ: ТЕОРИЯ ПЕРСПЕКТИВ, МОТИВАЦИЯ (KAHNEMAN, VROOM)**
- Дорого
- Отсутствие системного понимания феномена мошенничества (наука о поведении, правовое регулирование, трасология и т.п.)
- Скрытая природа мошенничества
- Отсутствие парадигмы управления рисками мошенничества в привязке к конкретному сценарию мошенничества
- Разрыв между функциями HR, compliance, юридической службой и службой безопасности
- Статья 81 ТК РФ
- Инертность правоохранительных органов «(бизнес не может быть потерпевшим»)
- Сделки, заключенные под влиянием обмана - сложности
- Как собирать доказательства за пределами РФ?
- Вернуть и возместить: редкое требование

ЗАЧЕМ?

- Утрата активов, убытки, упущенная выгода
- Репутационные последствия
- **Заразно**
- **Всегда растет со временем, если вовремя не остановить**

СОДЕРЖАНИЕ

ЧТО ТАКОЕ МОШЕННИЧЕСТВО?

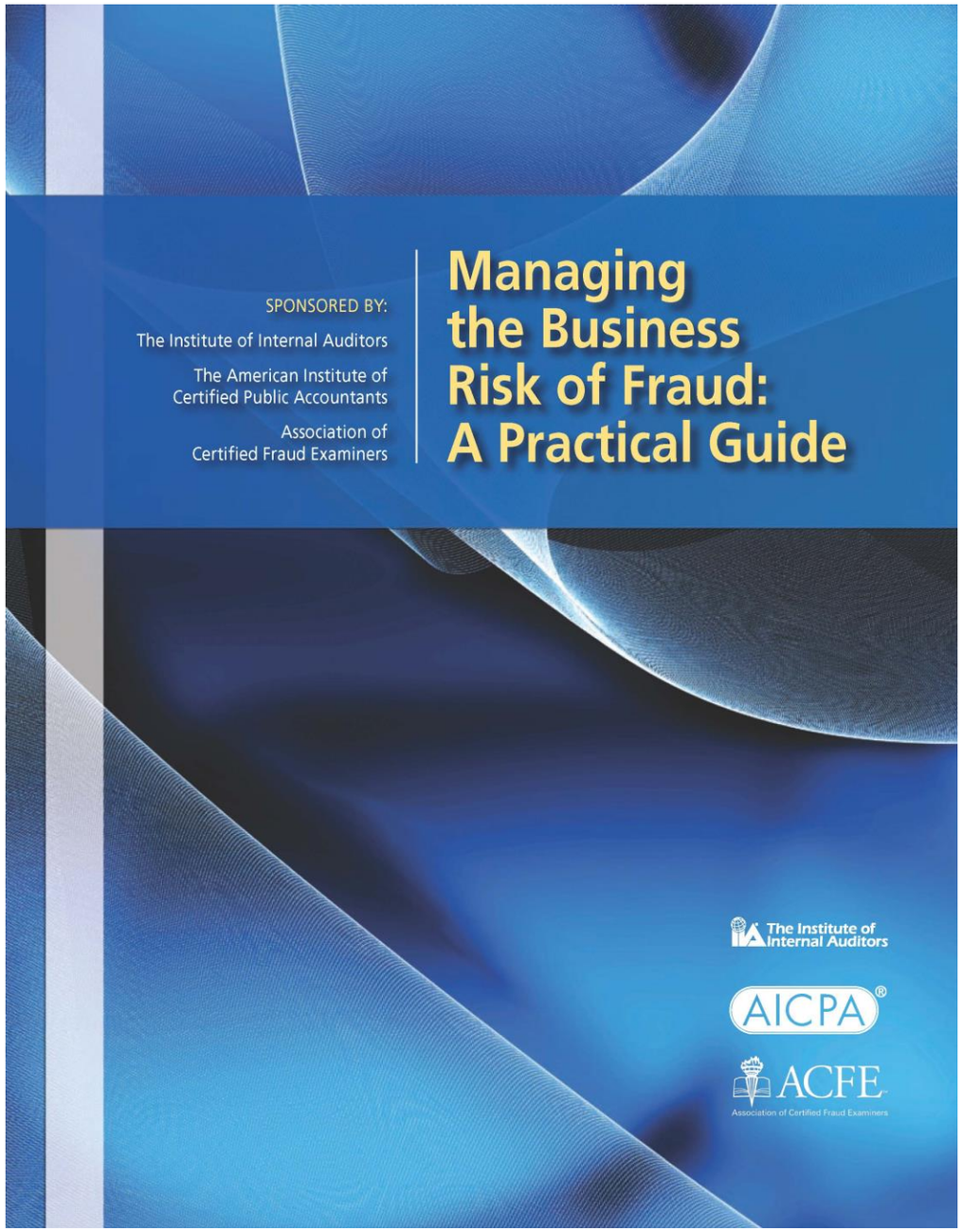
- Тесная связь с фидуациарными отношениями и доверием:
  - Статья 159 УК РФ «Хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием»
  - Статья 201 УК РФ «Использование лицом, выполняющим управленческие функции… своих полномочий вопреки законным интересам этой организации и в целях извлечения выгод и преимуществ для себя или других лиц либо нанесения вреда другим лицам или государства»
- Ключевой элемент – обман (сокрытие и умалчивание)
- Структура любой схемы:
  - Действие
  - Сокрытие
  - Конверсия

- Количество вариантов базовых схем на уровне бизнес-процессов конечно
- Деньги, штуки, ценный воздух
- **Обладая знанием природы недобросовестных действий, риск их возникновения на уровне бизнес-процесса можно оценить**

СОДЕРЖАНИЕ

СИСТЕМА ПРОТИВОДЕЙСТВИЯ МОШЕННИЧЕСТВУ

- Выявление
- Расследование и реагирование
- Предотвращение



СОДЕРЖАНИЕ

ВЫЯВЛЕНИЕ

- Мошенничество скрыто (обман)
- Мошенничество не всегда материально
- Классический аудит плохо справляется с задачей (одного профессионального скепсиса мало, нужны знания)
- Иголку случайной выборкой можно найти только случайно
- Решение:
  - Понимание бизнес-процесса
  - Понимание того, что вообще может произойти (знание базовых схем и их признаков). Расходы: конфликт интересов, деловая коррупция, прямой вывод денежных средств, сговор поставщиков, «мертвые души», переплаты сотрудникам
  - Оценка рисков мошенничества на уровне бизнес-процесса (профили риска)
  - Формирование профиля данных под профиль риска
  - Формирование экспертной выборки
  - Forensic Data Mining (да, 6000 контрагентов, если нужно)
  - Документарная проверка

- Решение должно быть системным:
  - Мониторинг рисков мошенничества
  - Проактивные регулярные форензик-аудиты в привязке к рискам мошенничества
  - Горячая линия
  - И т.д.

ФОРЕНЗИК-ПРОВЕРКА РАСХОДОВ (1/2)

Формирование экспертной выборки для проверки

Предлагаемые решения

В отличие от классического аудита в рамках форензик-проверки изначально устанавливается перечень транзакций, которые необходимо детально проанализировать форензик-методами:

- Интервью с представителями компании с целью детального понимания бизнес-процессов, связанных с расходованием денежных средств, общий анализ структуры расходов;
- Сплошной анализ контрагентов компании:
  - выявление признаков конфликта интересов (юридический и/или фактический контроль контрагента сотрудниками компании или их родственниками);
  - выявление контрагентов-посредников и неблагонадежных контрагентов;
  - выявление групп контрагентов, связанных между собой;
  - выявление контрагентов, созданных специально для конкретного договора; и т.д.
- Анализ данных о расходовании денежных средств методами Forensic Data Mining с целью выявления подозрительных закономерностей и аномалий;
- Сопоставление данных реестра контрагентов в бухгалтерской системе с данными системы банк-клиент, выявление расхождений;
- Экспертное дополнение выборки для детального анализа (напр., крупные расходы, CAPEX, группы связанных транзакций на сумму меньше установленного предела в рамках конкурентных процедур, и т.д.)

Как правило, при расходовании денежных средств возможны следующие варианты злоупотреблений, ведущие к невыполнению бизнес-планов: конфликт интересов сотрудников, деловая коррупция, недобросовестные действия контрагентов, прямое хищение денежных средств с расчетных счетов компании с последующим сокрытием в бухгалтерском учете

ФОРЕНЗИК-ПРОВЕРКА РАСХОДОВ(2/2)

Предлагаемые решения

Документарная проверка

Детальный анализ операций, попавших в экспертную выборку:

- Документарная проверка (документация конкурентных процедур, анализ договоров, учетных реестров, данных о движении денежных средств и первичных документов) с целью установления случаев злоупотреблений и калькуляции размера возможного ущерба.
- Выявление случаев завышения цен и стоимости ТМЦ/работ/услуг путем сравнения с рыночными ценами/иными предложениями (если это возможно).
- Выявление признаков бестоварных поставок путем сопоставления данных оприходования/списания ТМЦ и данных о расходовании денежных средств.

Анализ расчетов с персоналом

В том случае, если расходы на персонал составляют значительную часть расходов:

- Методами Forensic Data Mining:
  - Выявление «мертвых душ»;
  - Выявление признаков переплат персоналу.
- Проверка экспертной выборки персонала на предмет случаев непотизма.

Завершение проверки

- По результатам проверки:
- Подготовка черновой версии отчета;
- Форензик-интервью с лицами, подозревающимися в недобросовестных действиях, оценка достоверности пояснений этих лиц;
- Формирование финальной версии отчета и его презентация.

СОДЕРЖАНИЕ

РАССЛЕДОВАНИЕ И РЕАГИРОВАНИЕ

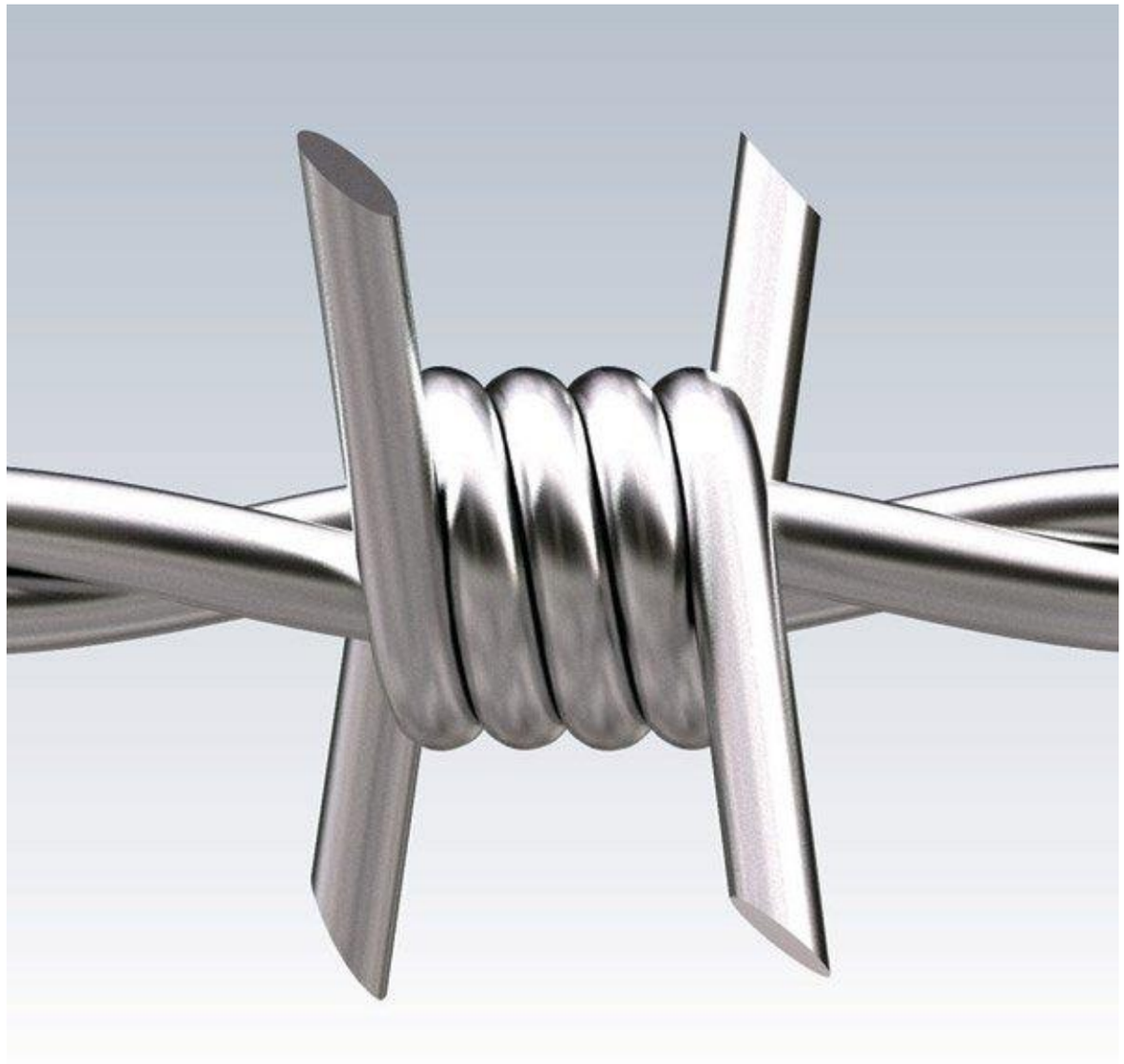
- Уже готовы:
  - Система дисциплинарной и материальной ответственности
  - Протокол реагирования, связанный с картой рисков мошенничества, проработанный с юристами
- Постоянно помним о конечной цели:
  - Прекратить отношения
  - Привлечь к уголовной ответственности
  - **Возместить ущерб/вернуть активы**
- Ст. 81, 193 и 247 ТК РФ – полностью применимы к расследованию корпоративного мошенничества
- Не забываем об объяснениях
- Понимаем, что нам нужно доказать по статьям 159,165, 201 и 204 УК РФ. Обязательно правильно фиксируем размер ущерба

- Используем правильные инструменты:
  - Судебная бухгалтерия
  - Корпоративная разведка
  - Компьютерная криминалистика
  - Экспертизы
- Устанавливаем, где находятся выведенные активы и как до них можно дотянуться

СОДЕРЖАНИЕ

ПРЕДОТВРАЩЕНИЕ

- Оценка рисков мошенничества (на уровне всего предприятия, на уровне бизнес-процесса, на уровне сценария мошенничества)
- Мониторинг рисков мошенничества и работа с накапливаемой статистикой
- Системы внутреннего контроля (hard)
- Проверка контрагентов и персонала при формировании отношений
- Отслеживание поведенческих индикаторов мошенничества
- Система работы с персоналом (soft): корректировка поведения
  - Compliance-тренинги
  - Кодексы этики
  - Контроль конфликта интересов
  - Внутренние коммуникации по результатам расследования инцидентов



ТРАДИЦИОННАЯ ПАРАДИГМА: GARY BECKER

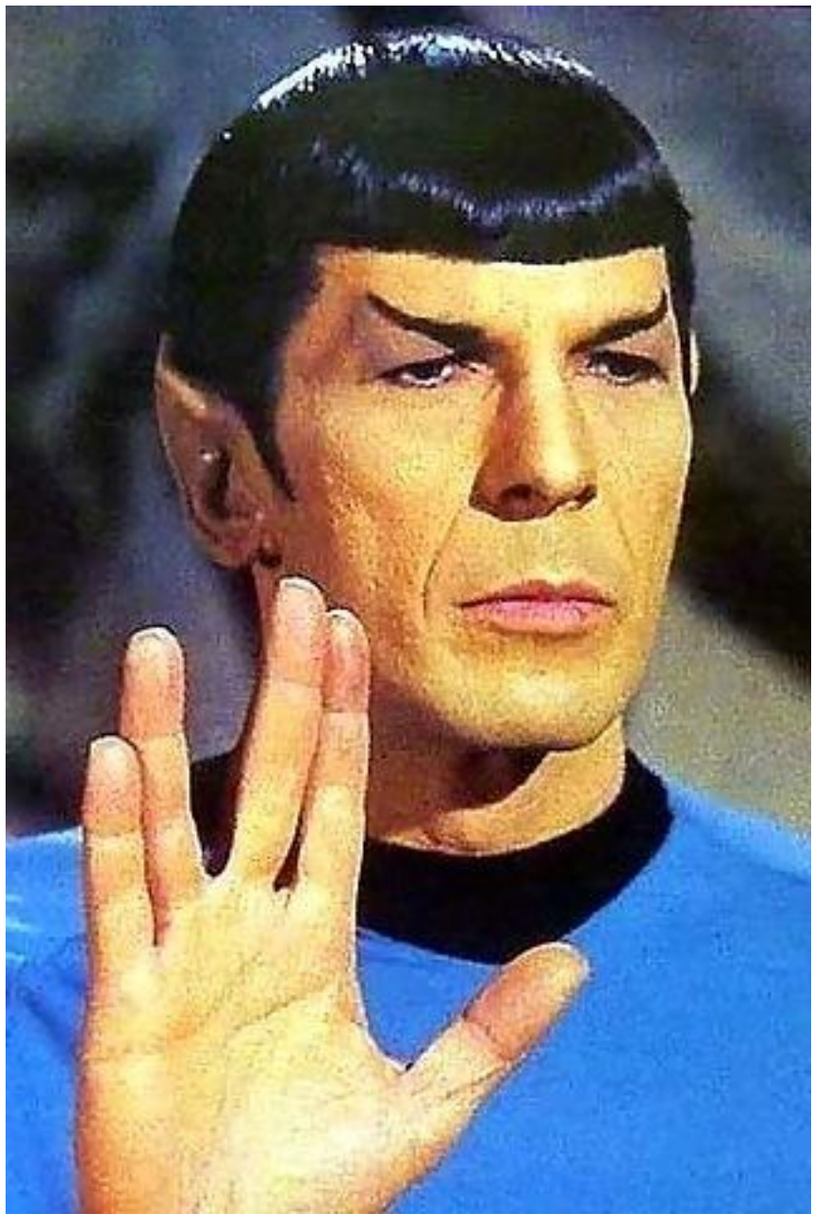
SMORC (SIMPLE MODEL OF RATIONAL CRIME):

- История одной парковки
- Возможная выгода
- Оценка риска поимки
- Масштаб наказания

- Ловим лучше (расход на систему выявления и расследования)
- Увеличиваем масштаб наказания

HOMO ECONOMICUS

- Неограниченные когнитивные возможности
- Нет затрат на вычислительные процессы
- Стабильные предпочтения, которые не зависят от контекста
- Полное знание будущих предпочтений, включая эмоциональные реакции
- Неограниченная сила воли и самоконтроль
- Цель: увеличить полезность для себя
- Тщательное исследование возможных последствий

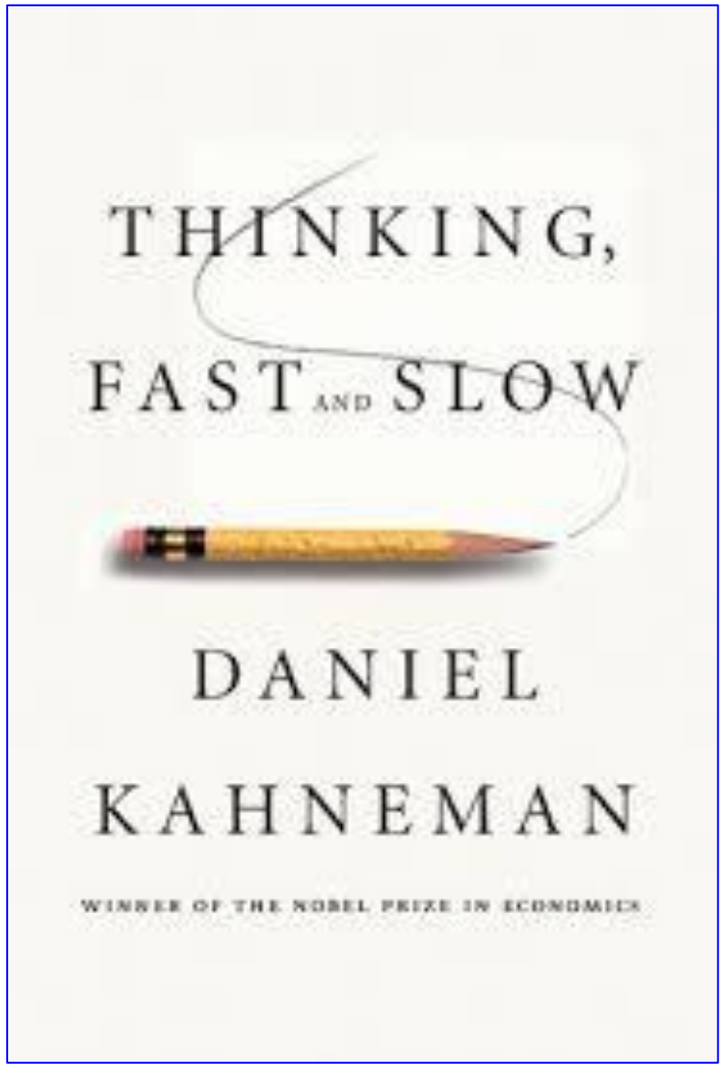


Источник: Dr. Paul Dolan, LSE

РАЦИОНАЛЬНОСТЬ И ПОВЕДЕНИЕ

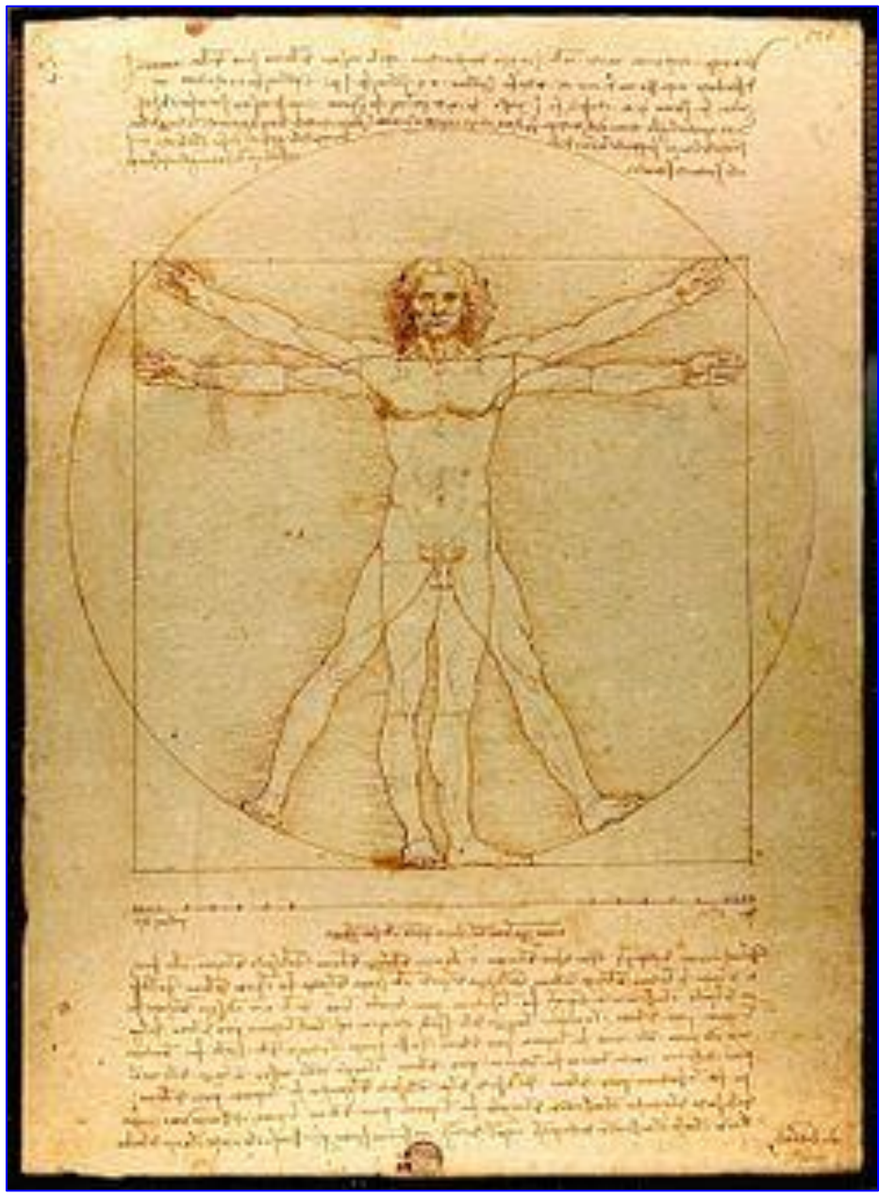
Наша рациональность ограничена:

- Наша рациональность ограничена (Herbert Simon, Daniel Kahneman & Amos Tversky)
- Дуалистичность когнитивных процессов (Система 1 и Система 2)
- Sustein & Thaler («подталкивание»)
- Behavioral Insights Team (UK)
- Executive Order (US) – Sept.15, 2015
- Поведенческая наука - наука о том, что мы делаем и как мы можем это изменить (понимание поведения, предсказание поведения, влияние на поведение)
- Behavioral forensics



BEHAVIORAL FORENSICS: ОБЛАСТИ ПРИМЕНЕНИЯ

- **Мошенничество и коррупция – деяния ЧЕЛОВЕКА.**
- <u>После</u>: Думай как преступник, чтобы поймать преступника
- <u>До:</u> Ответ на вопрос «почему происходит недобросовестное поведение»: разрабатываем более совершенные систем предотвращения и расследования
- <u>Всегда:</u> Как улучшить решения, принимаемые специалистами в области корпоративного контроля?



КЛЮЧЕВЫЕ СООБРАЖЕНИЯ

- Возможные мотивы?
  - Жадность
  - Самооценка/статус
  - Месть
  - Удовольствие
  - Справедливость
  - Сбитые моральные ориентиры
- Всегда ли это рациональное поведение?
- Всегда ли мотивы осознаваемы?
- Как влияет контекст?
- Хищники и коллеги

- **Автоматическая система 1**
- **Эмоции**

ФАКТОРЫ, ВЛИЯЮЩИЕ НА НЕЧЕСТНОСТЬ

Рационализация

Конфликт интересов

Креативность

1+ нарушение

Усталость

Источник: Dan Ariely

желание быть честным vs
желание заработать

Обещание

Выгода других

Сумма $

Подпись

Поведение других

Вероятность поимки (рациональная оценка)

Морал. напоминания

Культура

Надзор

Нечестность +

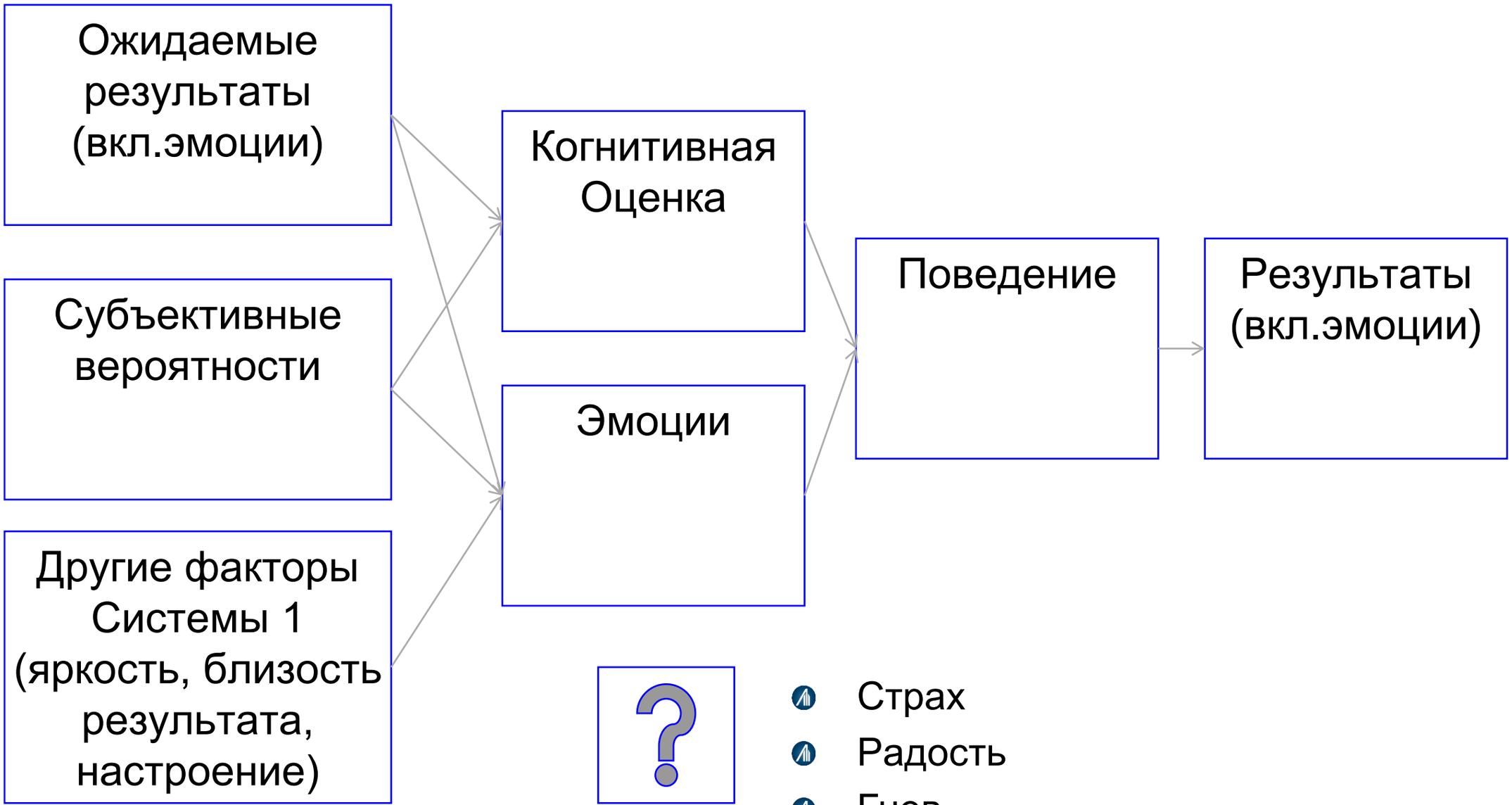
0

Нечестность -

Не-деньги

РИСК КАК ЭМОЦИИ

Источник: Lowenstein et al. (2001)



- Страх
- Радость
- Гнев
- Стыд
- …

ЭМОЦИИ ПРИ НЕДОБРОСОВЕСТНЫХ ДЕЙСТВИЯХ

- Эмоции присутствуют во всех элементах недобросовестных действий
  - Присутствуют при оценке риска и принятии решения
  - Присутствуют при действии
  - Присутствуют при рационализации
  - Используются для сокрытия
  - Используются для убеждения что-то сделать (жертва, соучастник)

- Развитый эмоциональный интеллект – мощный инструмент для противодействия недобросовестным действия при межличностной коммуникации

Жертва

Нарушитель

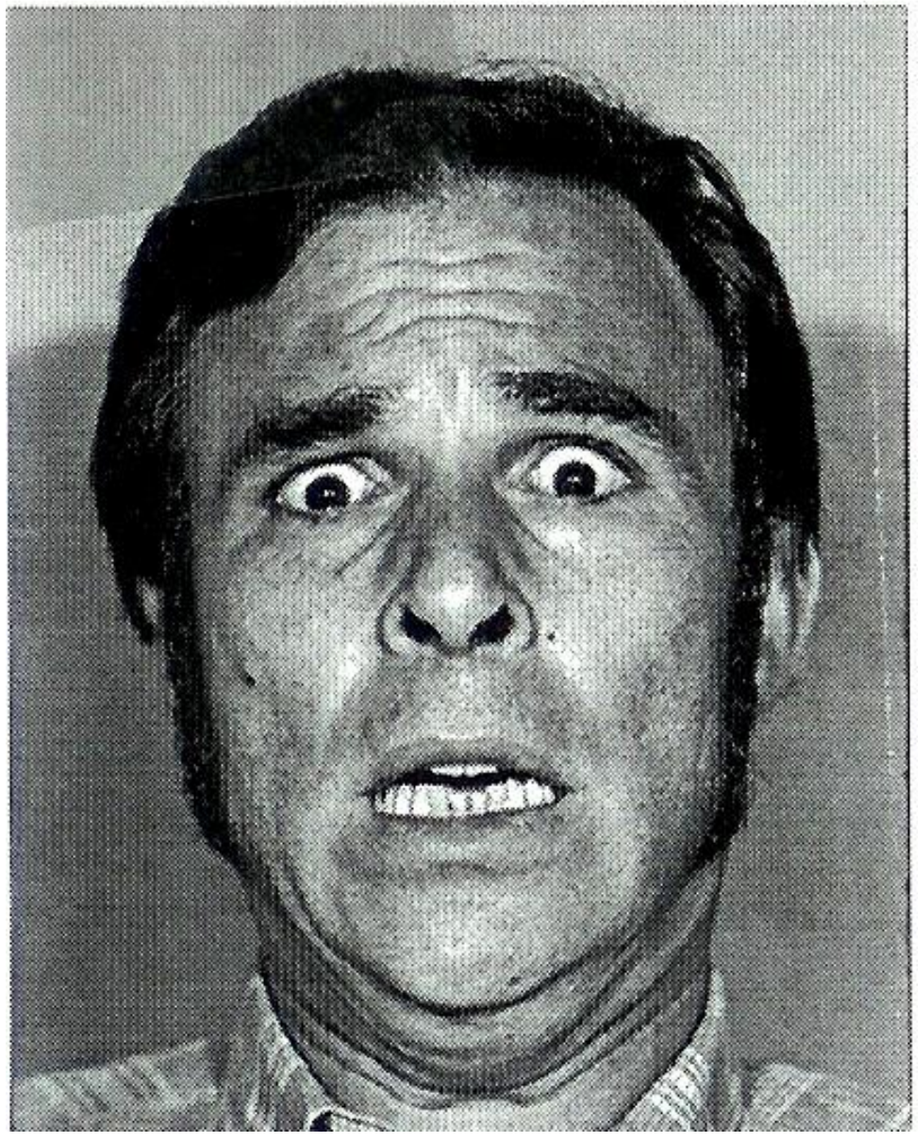
Соучастник

ИТАК, ПОВЕДЕНИЕ ВО МНОГОМ ОПРЕДЕЛЯЕТСЯ СИСТЕМОЙ 1 И ЭМОЦИЯМИ…ЧТО ДЕЛАЕМ МЫ?

- Как правило, основные эмоции, которые контрольная система стремимся вызвать у человека – страх и стыд/вину.

- «Это законно?» vs «Это надлежащее поведение?»

- Tom Tyler: Compliance – инструментальная (боязнь наказание) и нормативная перспектива (суперэго)

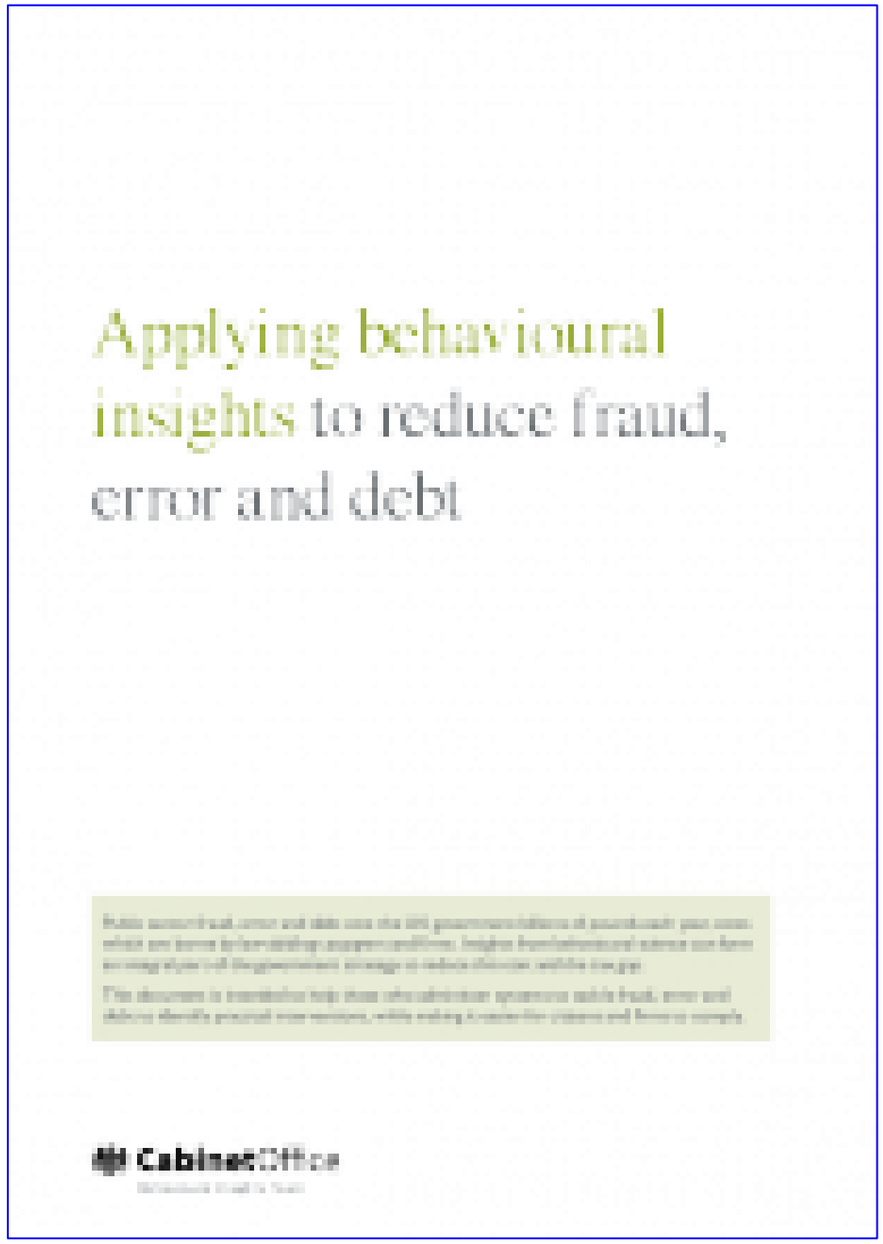


ИТАК, ПОВЕДЕНИЕ ВО МНОГОМ ОПРЕДЕЛЯЕТСЯ СИСТЕМОЙ 1 И ЭМОЦИЯМИ…ЧТО ДЕЛАЕМ МЫ?

- Возможные направления для размышления:
  - Эмоциональный дизайн compliance-тренингов: яркие, эмоциональные элементы, направленные на создание новых конструктивных триггеров
  - Подход Nudge: архитектура решений (iNcentives, Understand Mappings, Defaults, Give Feedback, Expect Error, Structure Complex Choices)
  - Подход Mindspace: Messenger, Incentives, Norms, Defaults, Salience, Priming, Affect, Commitments, Ego

ПРИМЕР: РАБОТА BEHAVIORAL INSIGHTS TEAM (РЕЗУЛЬТАТ + 30%)

- **Важность оценки возможностей для недобросовестных действий – цельная система и ее окружающая среда**
- Семь уроков:
  - Если просишь осуществить действие – это должно быть просто сделать
  - Привлеки внимание
  - Личное обращение
  - **Напомни о честности в ключевые моменты**
  - Сравни с другими
  - Награди правильное поведение
  - Подчеркни риск и последствия нечестности – без угроз



ALVAREZ & MARSAL