#CODEIB

КАК ИЗМЕРИТЬ ПОДВЕРЖЕННОСТЬ СОТРУДНИКОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ?

Карев Антон

инженер ИБ, журналист

Кто я ?

Темой ИБ интересуюсь 20 лет

Окончил физтех АлтГУ

Коплю интересные материалы по ИБ

Компоную их в экспертные статьи

Публикуюсь в:
- «Системный администратор»
- «Хакер»
- «Хабрахабр»

Когда просят – консультирую

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОФИ

Читаете «Системный администратор» ?

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПРОФИ

Обложки журналов с моими статьями

Мои статьи по СИ, в «Сисадмине»

Гарвардский взгляд на ИБ

Конспекты по социнженерии (3 части)

Гарвардский взгляд на Wisdom 2.0 (2 части)

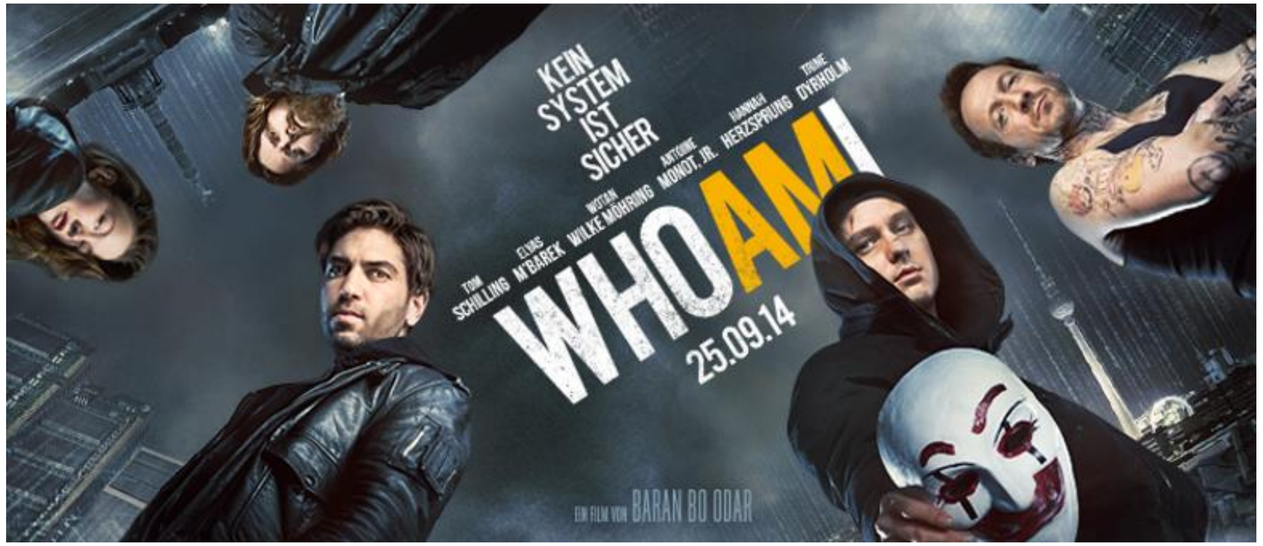
Какие первоисточники?
- публикации из SCOPUS (Harvard, MIT, DoD)
- остепенённые авторы (MD, PsyD, DBA)

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ
ПРОФИ

ВИДЕО-ФРАГМЕНТ ИЗ ФИЛЬМА «КТО Я»

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ПРОФИ

Показать видео-ролик
(2 минуты): clck.ru/FUW87



Природа человека и общие социальные тенденции

(подробнее в моей статье про СИ)

1

ИЛЛЮЗИЯ НЕУЯЗВИМОСТИ

Люди могут признавать, что преступления нередки, но при этом быть убеждёнными, что «меня-то они точно стороной обойдут».

2

ПСИХОЛОГИЧЕСКАЯ ЗАВИСИМОСТЬ ОТ СОБСТВЕННЫХ РЕШЕНИЙ

Люди могут сделать вывод, что «такой-то способ заработка эффективен», и отстаивать его вопреки доказательствам обратного.

3

АФФЕКТИВНОЕ ОБЯЗАТЕЛЬСТВО

Люди могут вживаться в какую-то роль и принимать ценности, для того, чтобы чувствовать общность с какой-то группой.

4

ПРИВЛЕКАТЕЛЬНОСТЬ И ДОВЕРИЕ

Люди доверяют тем, кого любят, и любят тех, кому доверяют.

5

«ТИМУРОВСКОЕ» ВОСПИТАНИЕ

Люди восприимчивы к СИ в значительной степени потому, что в детстве их учили быть надёжными, послушными, добрыми и т.д.

6

СТРЕМЛЕНИЕ БЫТЬ ПОЛ ЕЗНЫМ

Эта склонность укоренилась в нас с тех пор, когда нас просили «помочь с работой на дворе», «помочь маме донести сумку».

Особенности социального взаимодействия в Интернет-пространстве

1

ИНТЕРНЕТ РАСКРЕПОЩЯЕТ
В Интернете черты характера обостряются и ускоряются.

2

СЕТЕВЫЕ ТРОЛЛИ ВНУТРИ НАС
В силу раскрепощающего воздействия Интернета, порой даже очень хорошие люди проявляют качества сетевых троллей.

3

ХАЙТЕК ВЫТЕСНЯЕТ ЖИВОЕ ОБЩЕНИЕ
Инженеры может быть и не стремились к этому сознательно, но подсознательно – определённо. Ведь им труднее управлять.

4

ПОБОЧНЫЕ ЭФФЕКТЫ ВЫТЕСНЕНИЯ ЖИВОГО ОБЩЕНИЯ
Люди становятся менее терпимыми, в том числе к альтернативным точкам зрения, более зависимыми, более антогонистичными.

5

ЛЮДИ ВСЕГДА ИРРАЦИОНАЛЬНЫ
Хотя мы можем считать себя рационалами, по факту все решения принимаются иррационально.

6

СЛЕПАЯ ВЕРА В ИИ
По мере развития систем ИИ, мы вскоре можем перейти черту, - если уже не перешли её, - когда для использования ИИ нам нужно будет совершить прыжок веры.

Измеряем уровень подверженности СИ (УПСИ)

Идеальная атмосфера рабочего места:

- руководители «влияют» (авторитет)
- сотрудники «самоактуализованы»

Гарвардский тест ДАРМ, диагностирует эту атмосферу (Х) по 12 показателям:
los.hbs.edu

УПСИ = 1 – Х

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОФИ

12 показателей ДАРМ

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ПРОФИ

	Контрольные показатели				
	1	2	3	4	5
Атмосфера, располагающая к образованию					
• Психологическая безопасность	31–66	67–75	76	77–86	87–100
• Дружба контрастных взглядов	14–56	57–63	64	65–79	80–100
• Открытость к новым идеям	38–80	81–89	90	91–95	96–100
• Время для рефлексии	14–35	36–49	50	51–64	65–100
В целом по этой части	31–61	62–70	71	72–79	80–90
Конкретизированные образовательные процессы					
• Экспериментирование	18–53	54–70	71	72–82	83–100
• Сбор информации	23–70	71–79	80	81–89	90–100
• Анализ информации	19–56	57–70	71	72–86	87–100
• Передача информации	34–60	61–70	71	72–84	85–100
• Учебные мероприятия	26–68	69–79	80	81–89	90–100
В целом по этой части	31–62	63–73	74	75–82	83–97
Заинтересованность лиц принимающих решения (ЛПР)					
В целом по этой части	33–66	67–75	76	77–82	83–100

В ЧЁМ СЛОЖНОСТЬ ?

Обычно корпоративная кибербезопасность интересна только безопасникам

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОФИ

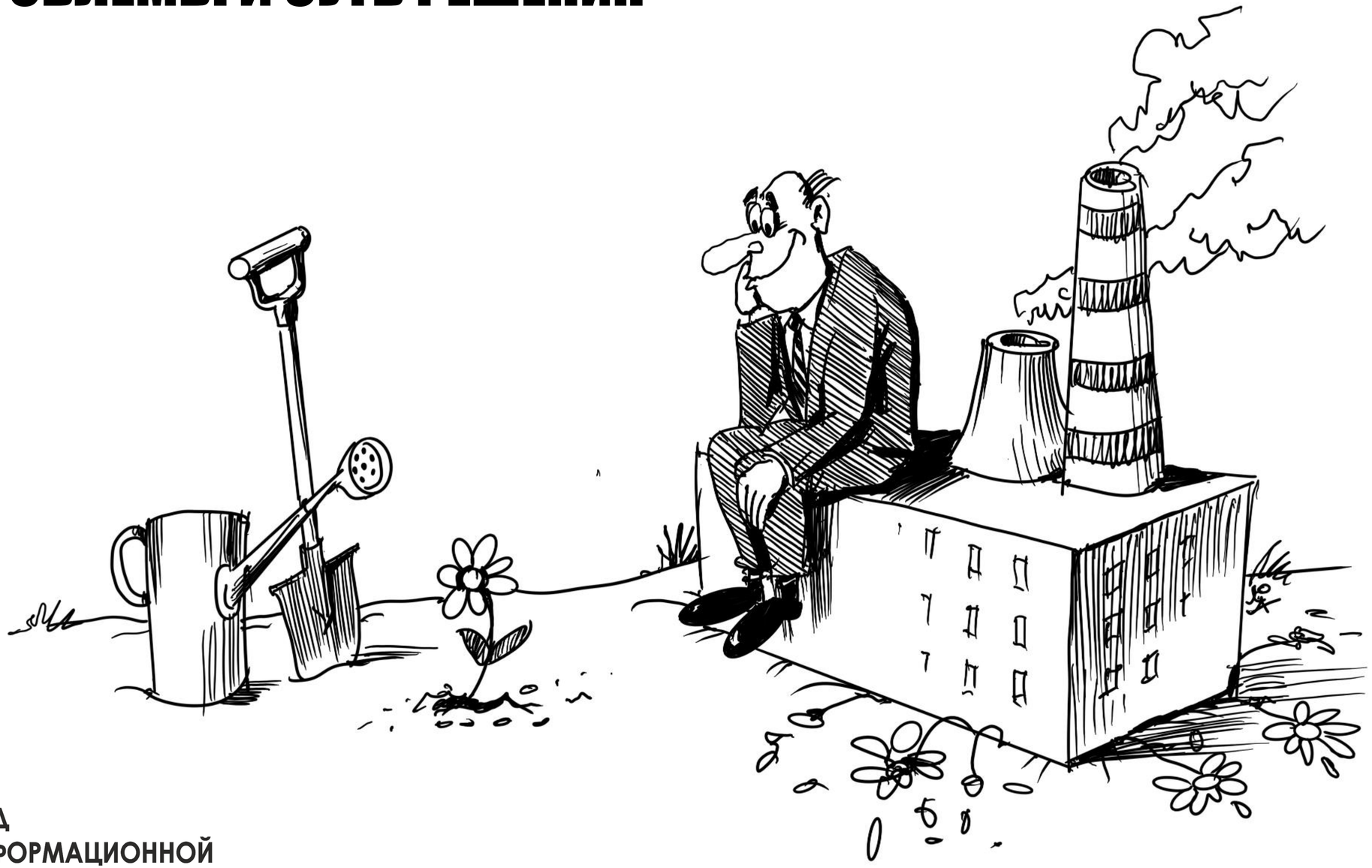
РУКОВОДИТЕЛЬ:
«Не хочу тратить время и деньги»

СОТРУДНИКИ:
«Вы достали уже со своими тренингами!»

ИНСТРУМЕНТ
безосновательный, потому что:
«Есть ложь, есть наглая ложь, а есть статистика» (Уинстон Черчилль)

ГАРВАРДСКИЙ УНИВЕРСИТЕТ
«Это же американский чужак!»

СУТЬ ПРОБЛЕМЫ и СУТЬ РЕШЕНИЯ

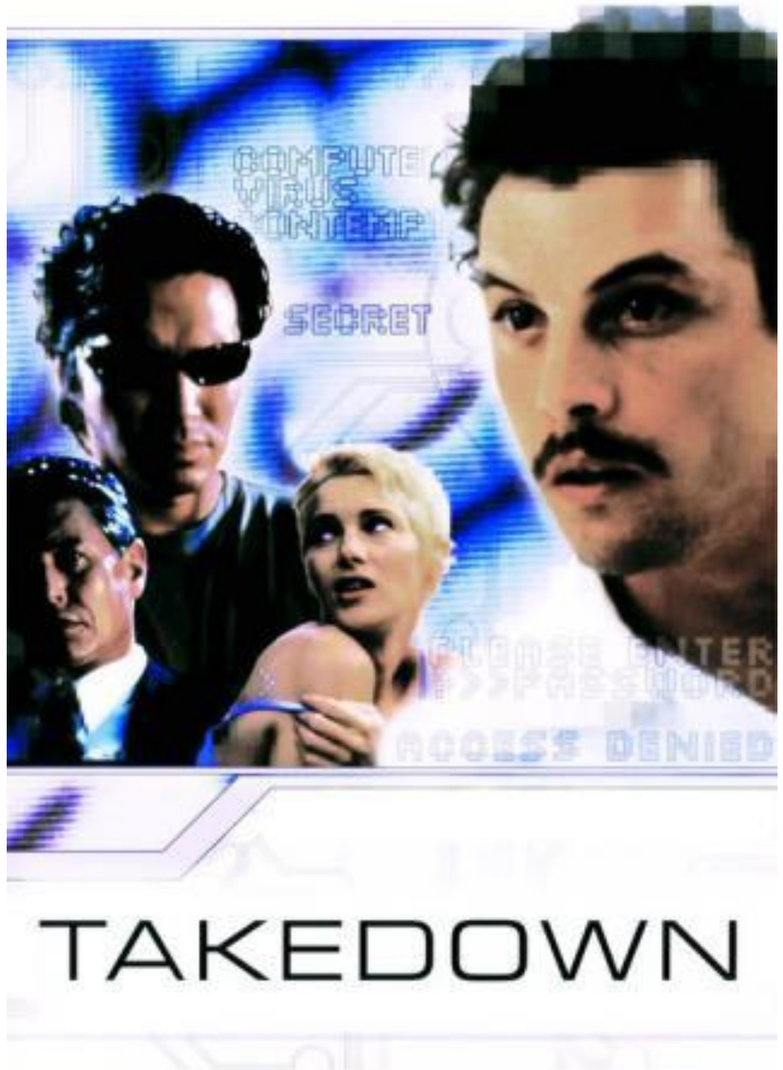


КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ
ПРОФИ

БОНУС: ФРАГМЕНТ ИЗ ФИЛЬМА «ВЗЛОМ»

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОФИ

Показать видео-ролик (6 минут): https://clck.ru/FUXTH



КАК ИЗМЕРИТЬ ПОДВЕРЖЕННОСТЬ СОТРУДНИКОВ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ?

1

ПОЙМИТЕ, ЧТО СИ ПОДВЕРЖЕНЫ ВСЕ
Никто не застрахован от обмана. Можно снизить шансы злодея на успех, но не полностью исключить их. Нужно учитывать этот момент при управлении рисками.

2

ПОСМОТРИТЕ ФИЛЬМ «КТО Я»
Здесь в игровой форме разобраны очень глубокие принципы социальной инженерии.

3

ПОСМОТРИТЕ ФИЛЬМ «ВЗЛОМ»
Это классика. Наблюдая за развитием событий фильма, вы увидите, как социальную инженерию использовал тот, кто её придумал, – Кевин Митник.

4

ЧИТАЙТЕ 6 МОИХ СТАТЕЙ ПО СИ
В них вы найдёте всё, что вам нужно по СИ. В докладе я представил примерно 3% от информации, изложенной в них.

5

ИЗМЕРЯЙТЕ УПСИ КОСВЕННО
Никто не хочет тратиться непосредственно на измерение ИБ, тем более на измерение психологической её части.

6

ГАРВАРДСКИЙ ТЕСТ «ДАРМ» – РЕШЕНИЕ
Разрабатывался не для измерения СИ, а для более актуальных для руководителя задач. Но он косвенно замеряет УПСИ.

#CODEIB

СПАСИБО ЗА ВНИМАНИЕ

anton.barnaul.1984@mail.ru
+7 929 391 03 14

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ