# Идентификация и аутентификация при предоставлении госуслуг

Конявский В.А., д.т.н., проф.
Научный руководитель ФГУП ВНИИПВТИ
ФГУП КБПМ
ЗАО ОКБ САПР
Зав. Кафедрой «Защита информации» МФТИ,
проф. МИФИ и ВШЭ

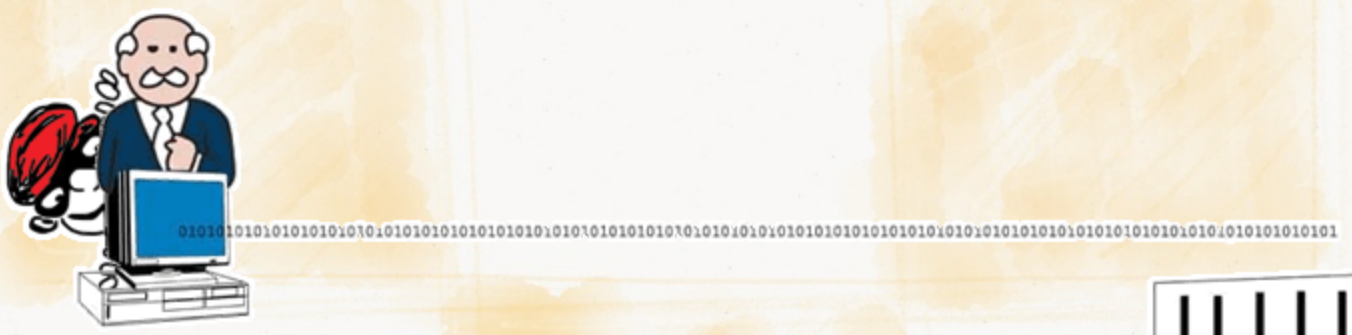




# Информационное взаимодействие при предоставлении госуслуг

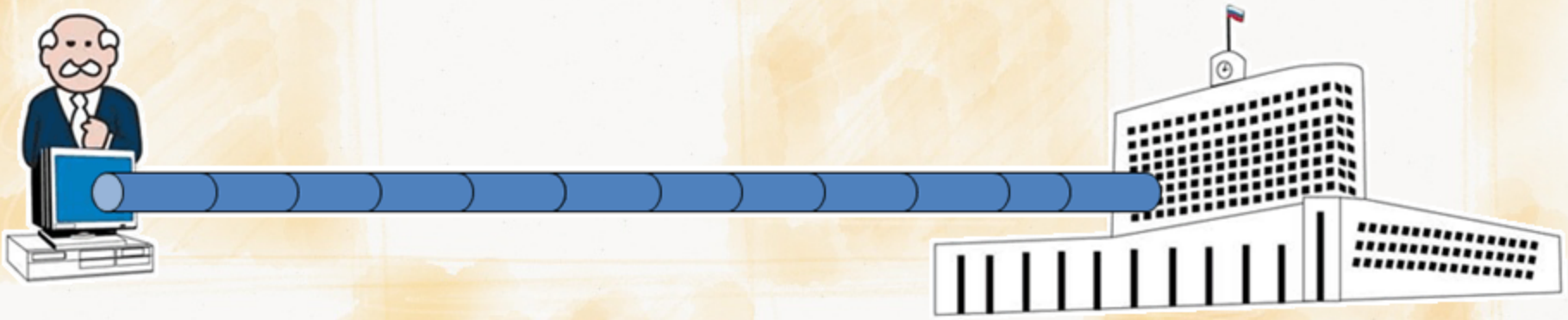
# Мы не одни
# Вредоносное ПО может быть везде

# Вредоносное ПО может быть везде

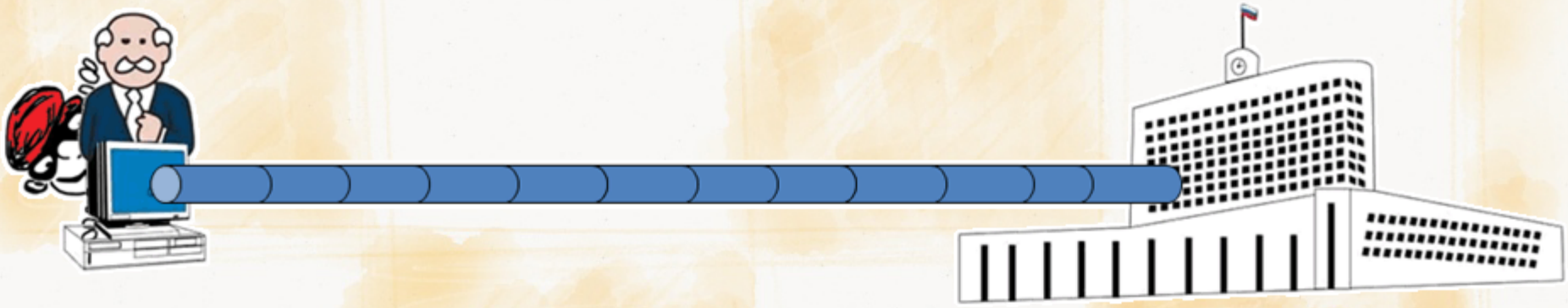


# Вредоносное ПО может быть везде

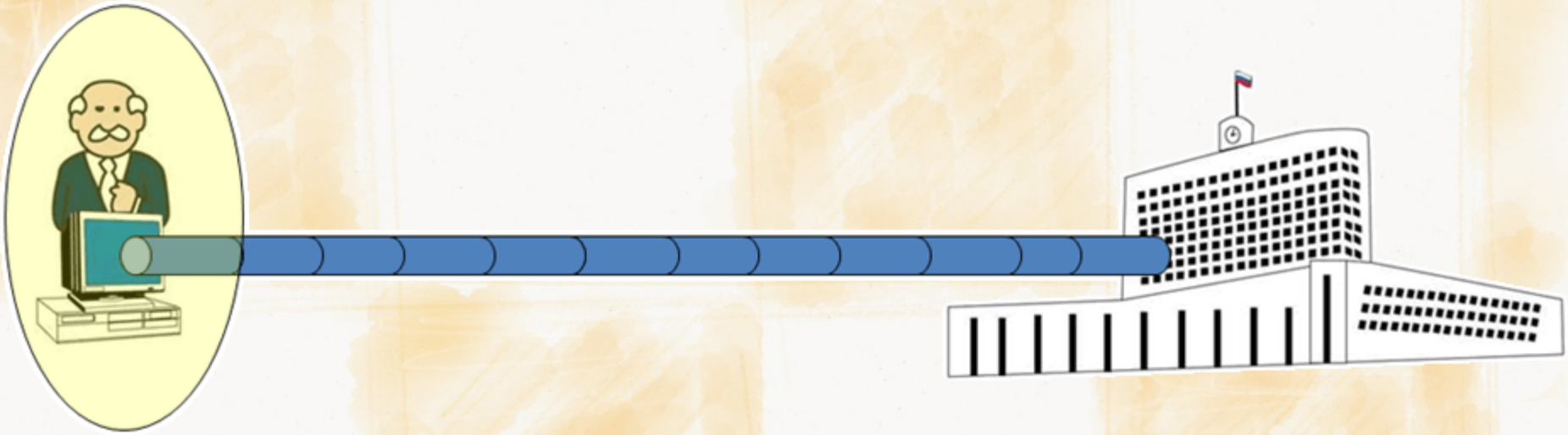
# Можно защищать канал



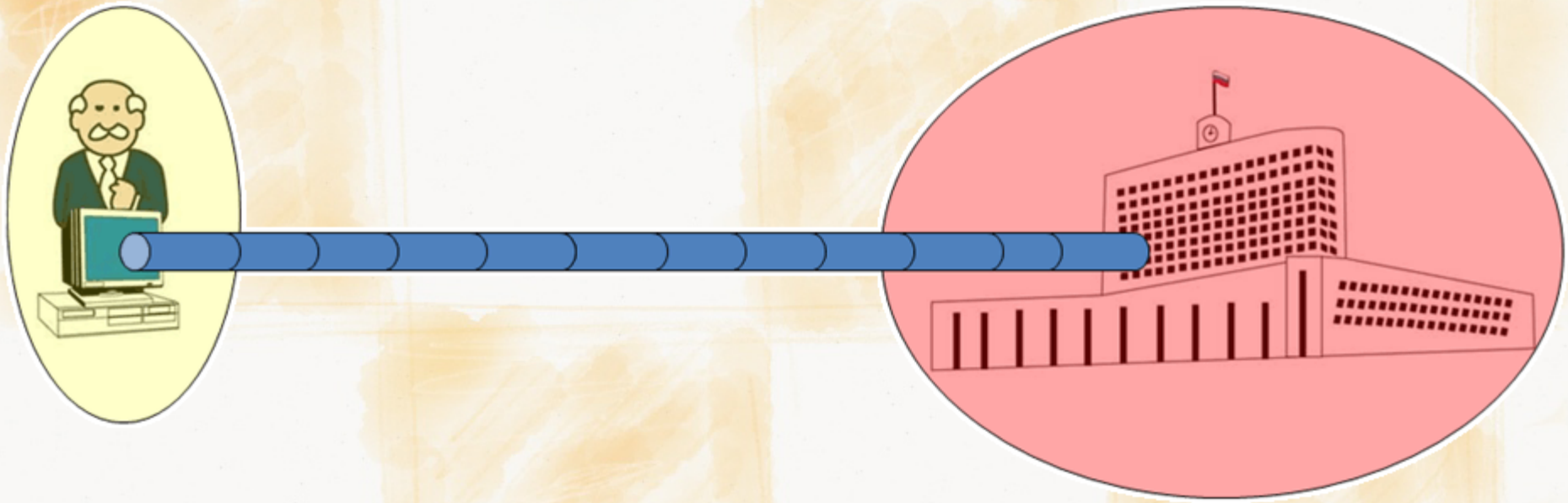
# Достаточно ли этого?



# Нужна доверенная среда у клиента



# Нужна доверенная среда в ЦОД



# Аксиомы доверенного взаимодействия

1. Платежные документы подписываются ЭП

2. Подпись ставится с помощью СЭП

3. СЭП требует доверенной среды

# Все врут

1. Применение токенов обеспечивает достаточный уровень защищенности

2. Квалифицированная ЭП может быть получена в недоверенной среде

3. Если стоит ЭП, то документу можно доверять

4. Главный приоритет – удобство клиента, а безопасность – его проблема

# Доверенная среда (СФК) создана, если:

На проверенном компьютере используется:

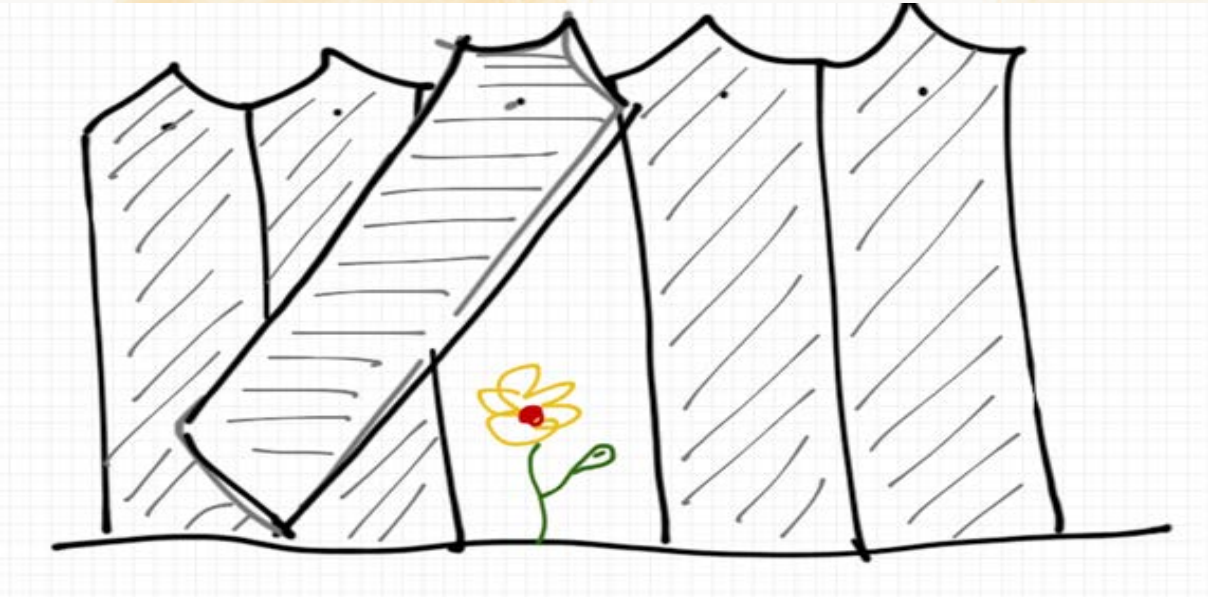
- проверенная ОС
- проверенное ПО
- проверенные данные

# Доверенная среда (СФК) поддерживается, если обеспечивается:

1. Контроль запуска задач и процессов
2. Взаимное невлияние задач
3. Защита от перехвата управления
4. Защита ИТ как последовательности операций

Нарушение доверенности среды возникает при ошибках реализации пунктов 1-4

# Дыры в заборе может и не быть

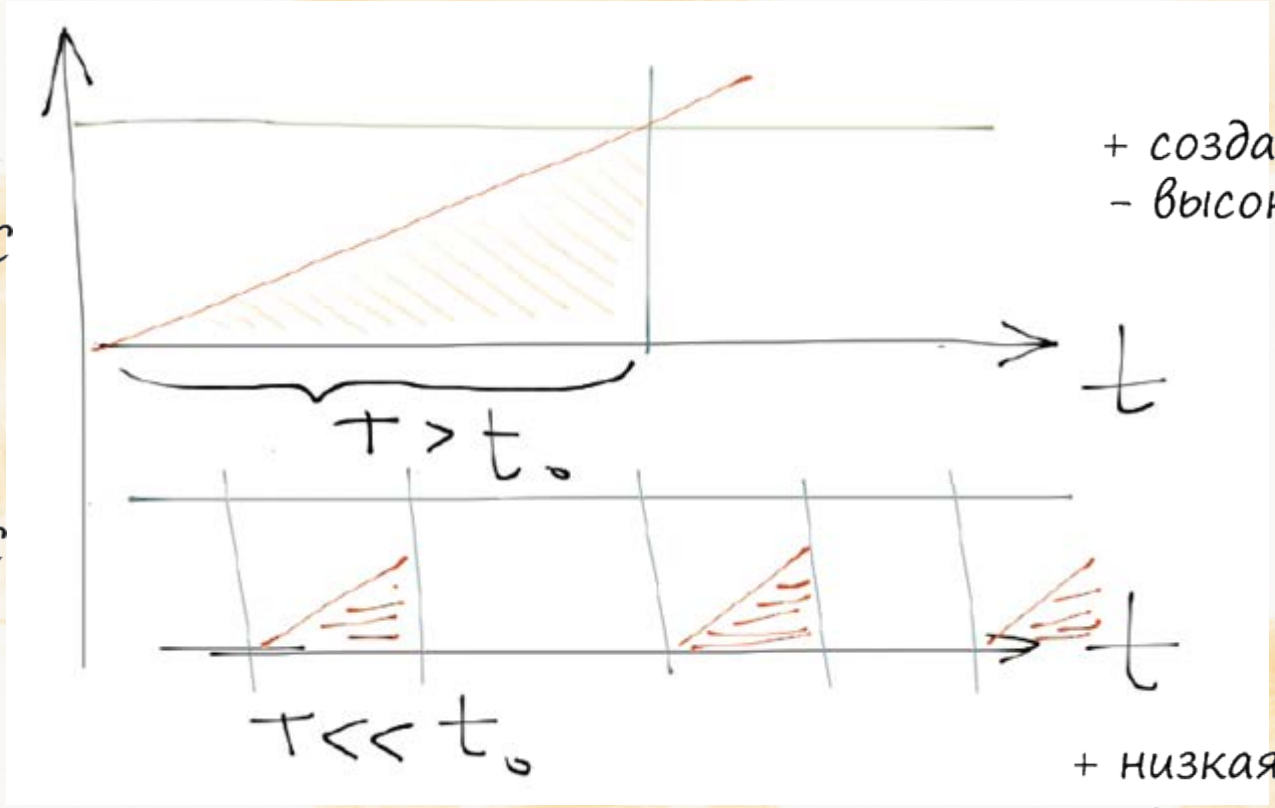


Если:

1. Клиенту обеспечить ненастраиваемый ДСС
2. Управление безопасностью поручить профессионалам

# Доверенная среда

ДВС




ДСС

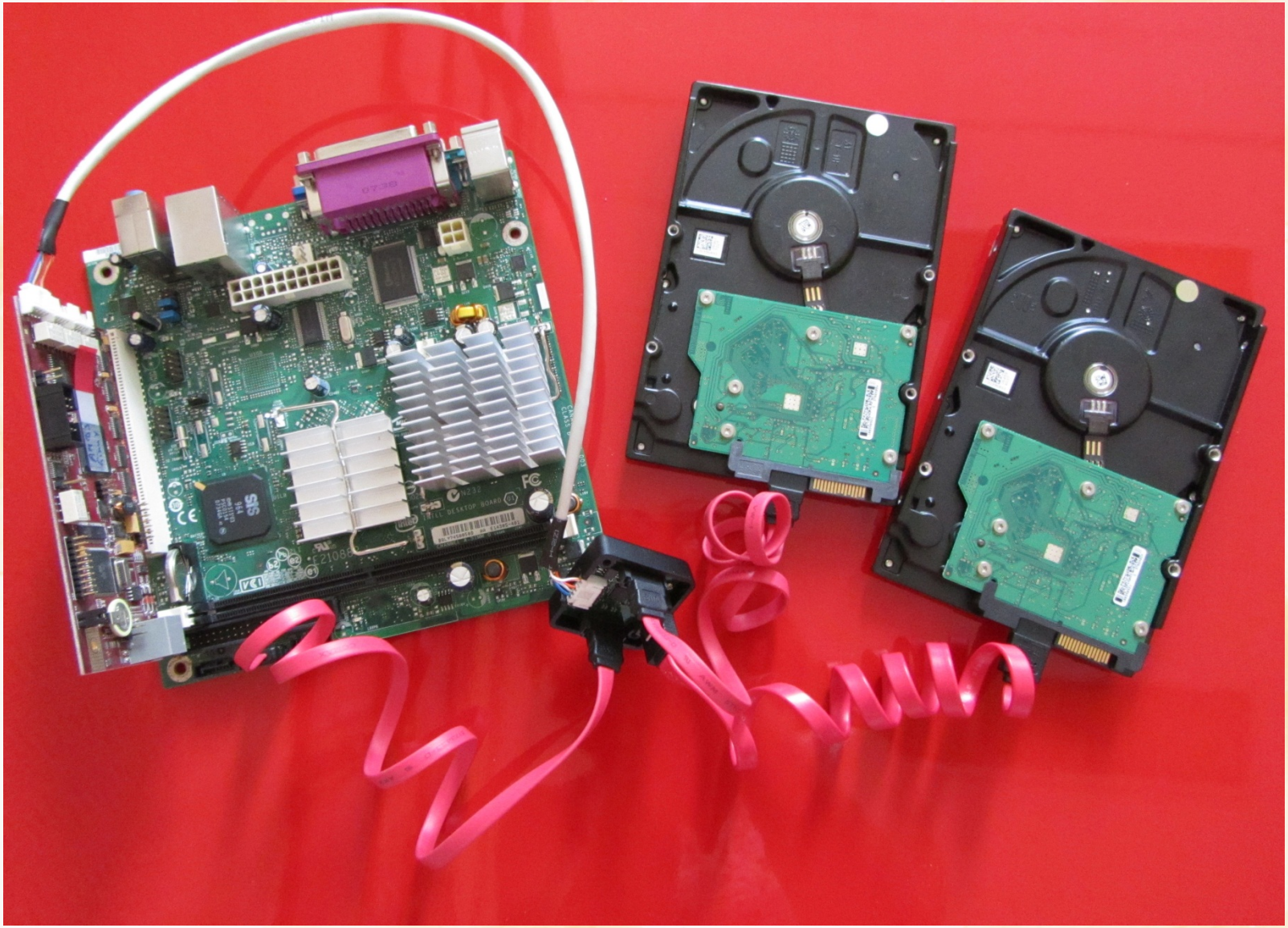
+ создается однократно
– высокая цена

+ низкая цена
– многократное создание

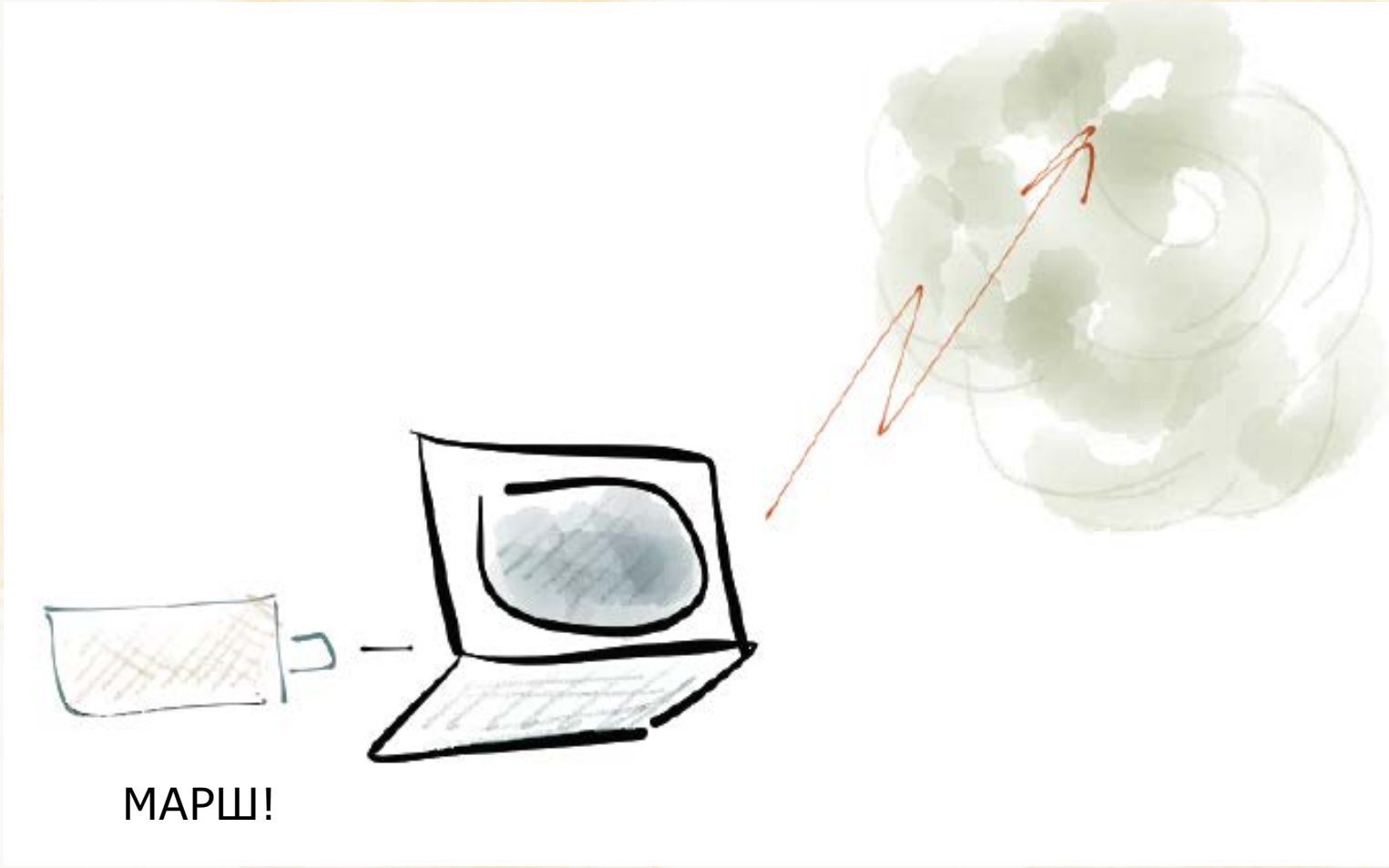
# Доверенная среда. Реализация

1. ПЭВМ с постоянной поддержкой ДСС
2. ПЭВМ с сеансовой поддержкой ДСС
3. ТК с сеансовой поддержкой ДСС

# ПЭВМ с ДСС



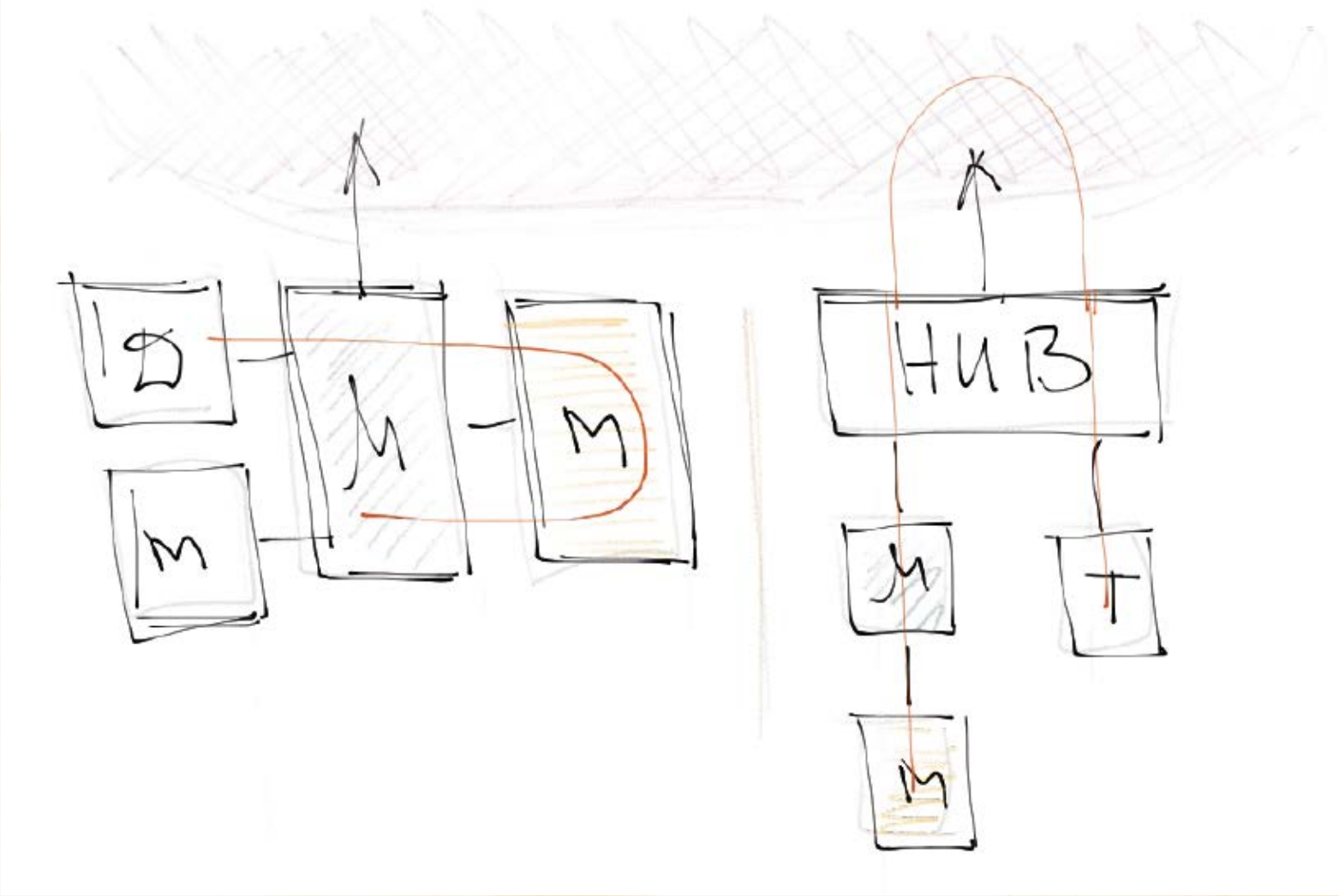
# ТК с ДСС



МАРШ!

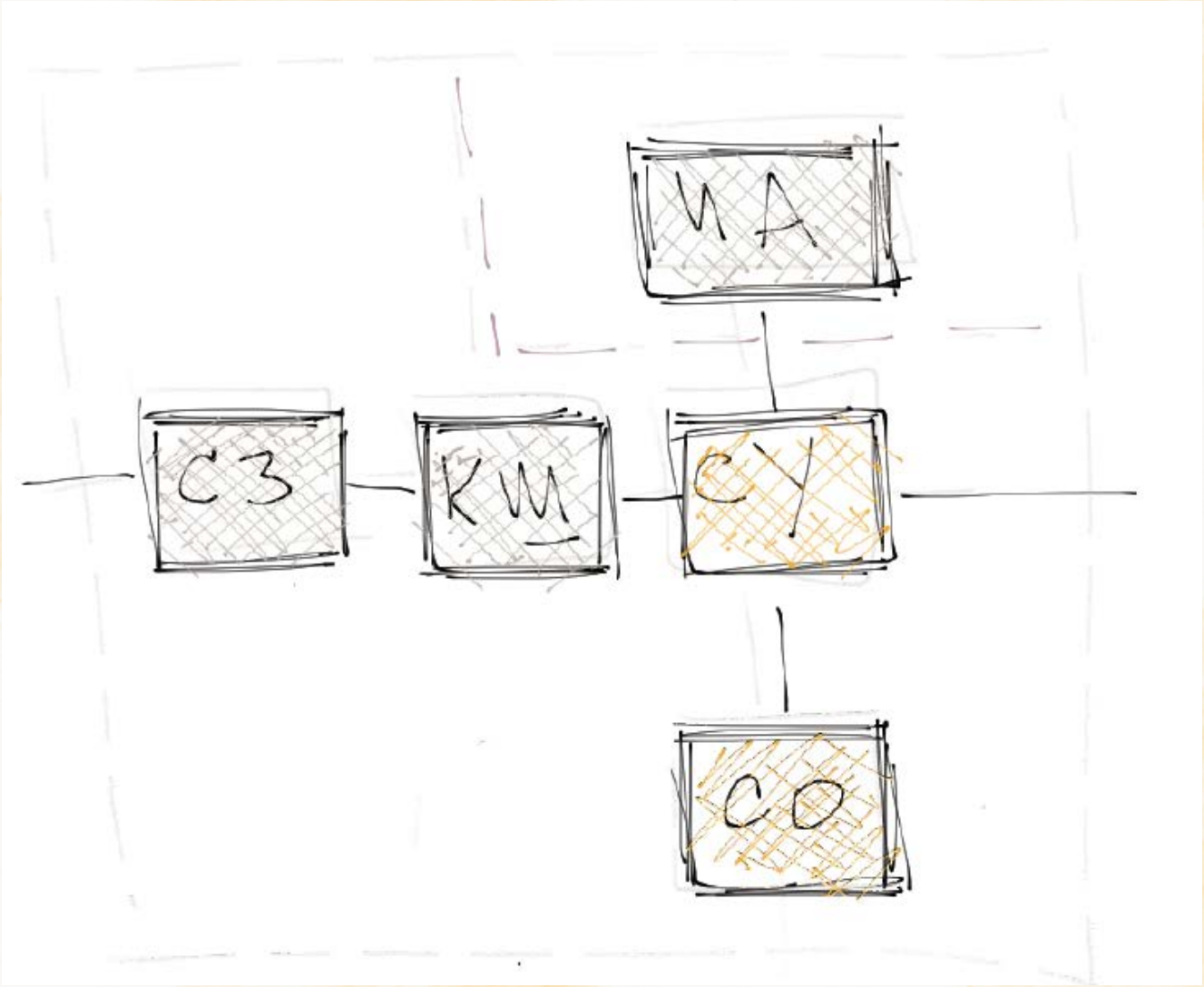
# МАРШ! Управление памятью

# МАРШ! Архитектура аппаратных средств

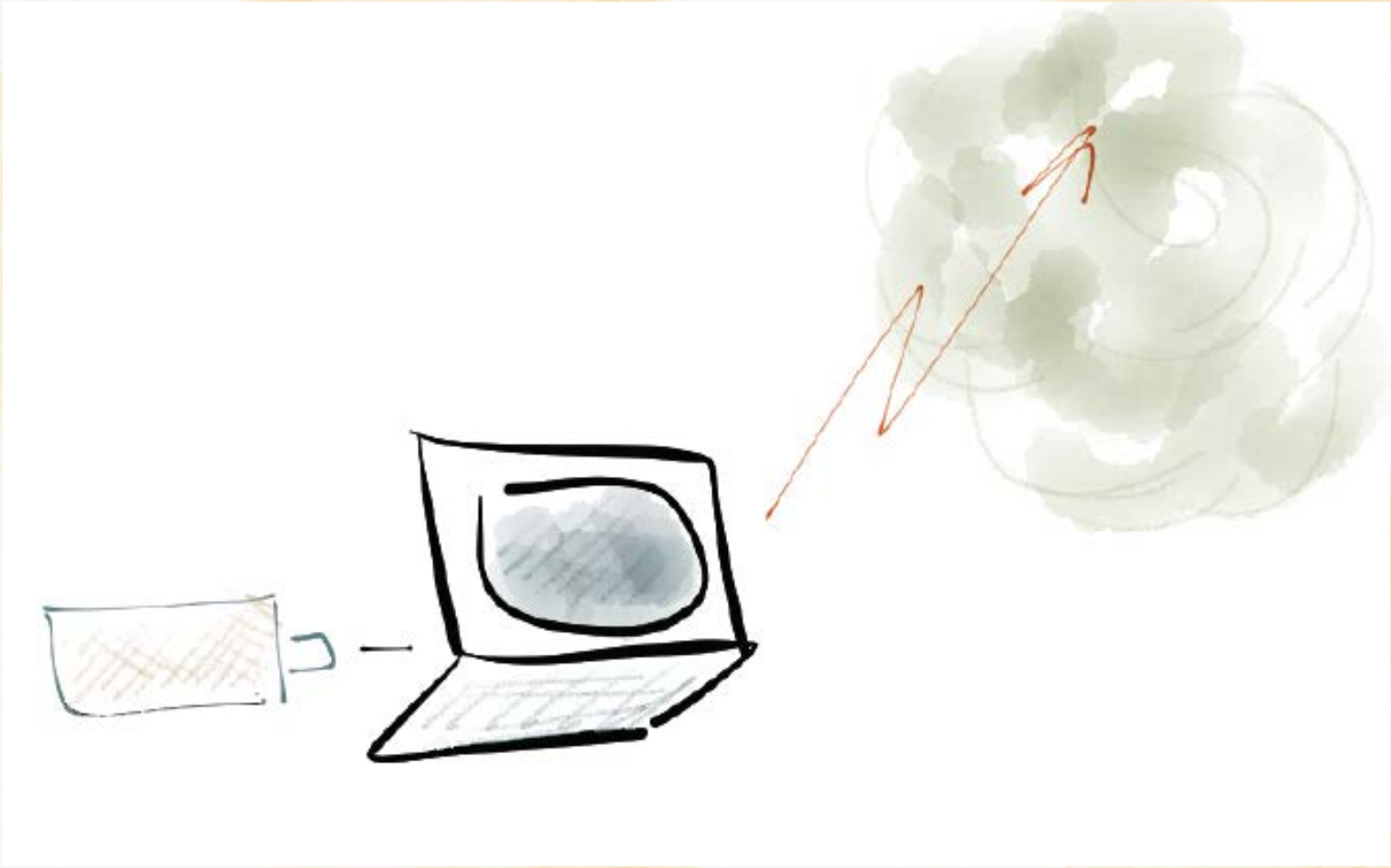


# МАРШ! Взаимодействие с системой

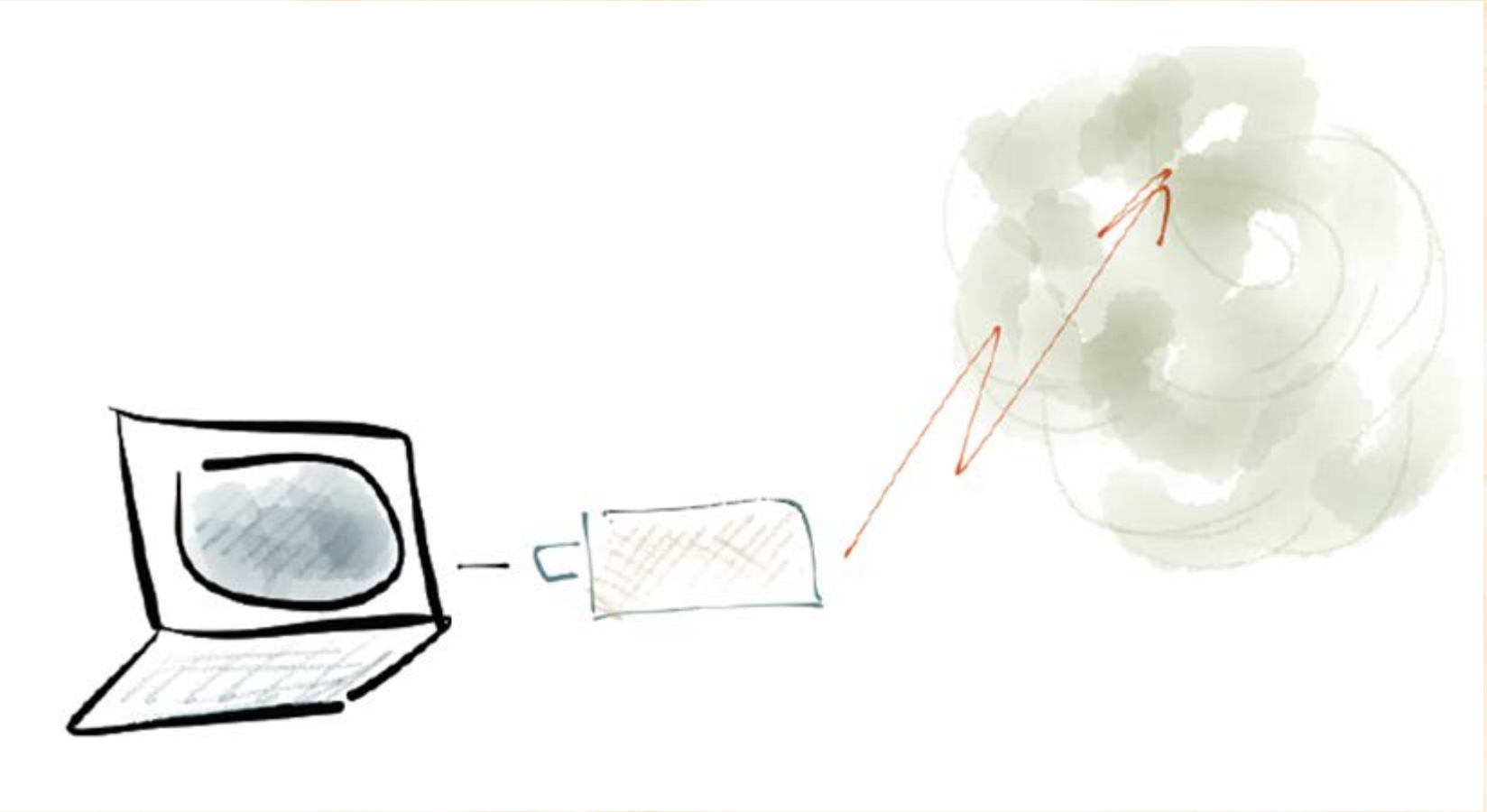
# МАРШ! Сервер ДСС



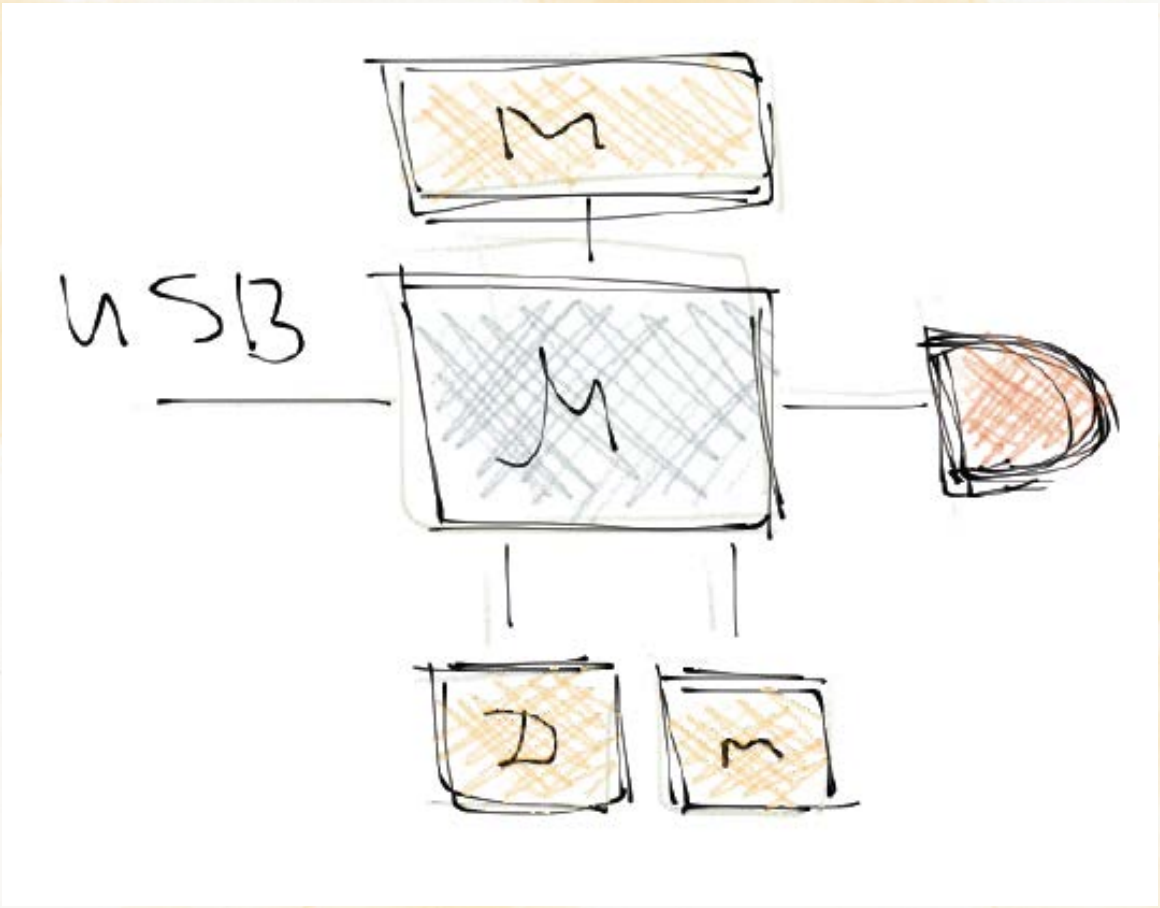
# Использование МАРШ! v1.0



# Использование МАРШ! v2.0



# МАРШ!
# Архитектура аппаратных средств



# Почему МАРШ! – это «серебряная пуля»?

1. Состояние критичных компонентов зафиксировано
2. Вирусы блокированы
3. Ключи неизвлекаемые
4. Перехват управления невозможен
5. Управление отчуждено от Клиента

Вопросы нам жить не мешают, –
ответы мешают

(Н. Матвеева)

# Можно ли ослабить требования?

Можно.

Достаточно поддерживать доверенность источника сообщений (информация имеет направление)

# Какие карты можно применять для идентификации?

Любые.

Как смарт-карты, так и карты с магнитной полоской

(нет необходимости выпускать для каждого проекта свою карту)

# Можно ли обеспечить надежную аутентификацию за счет использования карт?

Нет. Только карт недостаточно. Необходимо создать и поддерживать доверенную среду.

# Нужно ли шифровать канал?

Нет.

Достаточно шифровать часть данных.

Конявский Валерий Аркадьевич
001@pvti.ru

Вопросы?