

# MetaSociety Concept Paternity

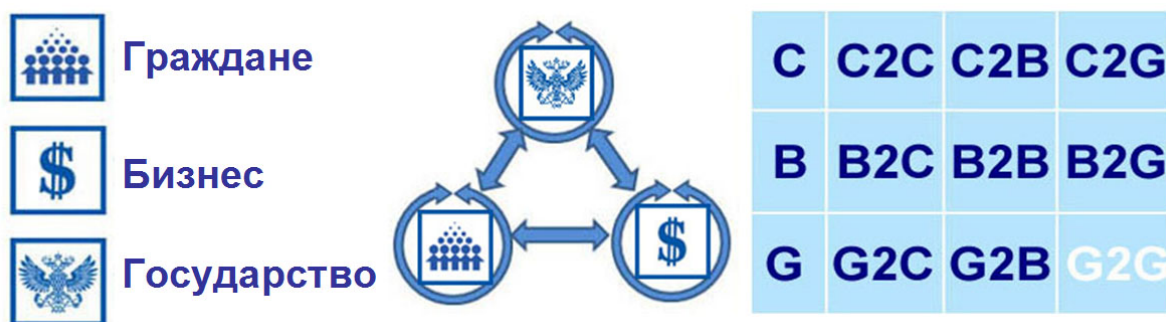
**MetaSociety** - концепция построения ИТ-системы обеспечения эффективного **социального взаимодействия** членов общества: **Social Interaction System (SIS)**.

Ориентация SIS на обеспечение **взаимодействия**, в отличие от многочисленных систем, ориентированных на **обмен информацией** (электронная почта, мессенжеры, социальные сети), предъявляет особые требования к системе коммуникаций, но и принципиально повышает ее значимость и функциональность.

## Структура общества

Жизнедеятельность общества состоит во **взаимодействии** членов общества, направленном на обеспечение личного, семейного, группового, корпоративного и общественного благополучия.

Общество можно рассматривать как совокупность трех групп взаимодействующих субъектов: **граждане** (физические лица), **бизнес** (юридические лица) и **государство** (государственные и муниципальные органы). Взаимодействие осуществляется как между группами, так и внутри групп.



Без создания условий для эффективного взаимодействия членов общества невозможно обеспечить его развитие, стабильность и процветание.

## Взаимодействие и коммуникации

Для полного и правильного понимания SIS нужно четко осознать принципиальную разницу между понятиями "коммуникации" и "взаимодействие".

Коммуникации мы рассматриваем как обмен сообщениями, данными, файлами. Последние десятилетия характерны резко возросшими возможностями электронных коммуникаций. Они стали глобальными, высокоскоростными, мультимедийными, экономичными, мобильными, общедоступными. Но практически все системы электронных коммуникаций индифферентны к семантике передаваемой информации.

Когда мы говорим о социальном взаимодействии, предполагается наличие некоторой реальной или кажущейся, осознаваемой или неосознанной цели взаимодействия, для достижения которой необходимо, в общем случае, совершить некоторое количество совместных взаимоувязанных действий.

При социальном взаимодействии на первый план выходит семантика передаваемой информации. Информационные коммуникации являются лишь медийной основой взаимодействия.

Виды действий определяются возможностями (функционалом) того или иного контрагента.

Поскольку цели, как правило, не достигаются одним действием, отдельные акты социального взаимодействия неким естественным образом увязываются в последовательности действий, происходящих в течение некоторого периода времени и затрагивающих некоторое количество участников.

Совокупность действий, направленных на достижение некоторой цели назовем процедурой социального взаимодействия (**Social Interaction Procedure - SIP**).

Очевидно, что многие процедуры являются стереотипными, типовыми. Они многократно повторяются разными участниками в разное время, в разных местах и разных обстоятельствах. Очевидно, что упорядочение, ускорение, гармонизация, обеспечение правомерности выполнения типовых SIP является важнейшей задачей общества и государства.

---

## Социальное взаимодействие

Будем рассматривать те виды социального взаимодействия, когда субъекты взаимодействия предполагают в итоге достижение некоторого, значимого для них результата.

Под **эффективностью взаимодействия** будем понимать достижение цели взаимодействия в возможно короткие сроки, с минимальными затратами,

минимальными рисками и бесконфликтно.

В процессе социального взаимодействия участники несут определенные затраты (как минимум - собственное время) и подвергаются определенным рискам (например, финансовых потерь).

Сам факт участия в процессе взаимодействия нескольких субъектов говорит о том, что между ними существует определенная взаимозависимость.

Факторами такой зависимости являются:

- полнота и достоверность полученной от партнеров информации
- корректность заключаемых партнерами соглашений
- честность партнеров
- выполнение партнерами своих обязательств.

Зависимость порождает взаимные обязательства и взаимную ответственность сторон за свои действия, поскольку в определенных ситуациях партнеру умышленно или невольно может быть нанесен ущерб.

Общество обязано создать надежные механизмы социального взаимодействия и обеспечить правовую защиту их участников. Для этого необходимы следующие компоненты:

- **законодательство** - свод правил и регламентов, обязательных для членов сообщества, включая институт их формирования и корректировки
- **фактография** - способ надежной регистрации происходящих в системе событий, документов, значимых действий участников сообщества
- **арбитраж** - система анализа конфликтов и принятия решений по мерам принуждения
- **система принуждения** - силовая система принуждения членов сообщества к исполнению законодательства на основании решения арбитража.
- **система коммуникаций** - совокупность систем информационного обмена участников сообщества

Информационная система, обеспечивающая социальное взаимодействие, должна предусматривать наличие этих структурных компонент, опираться на них и обеспечивать их совместное функционирование и развитие. Только так она может существенно повысить эффективность деловых усилий общества.

---

## Юридическая значимость коммуникаций

Взаимодействие членов сообщества осуществляется при посредстве различных систем коммуникаций. Осмысленное деловое взаимодействие возможно лишь, если обеспечена **юридическая значимость** коммуникаций.

Юридическая значимость проявляется в случае конфликта между участниками сообщества, который они не смогли или не захотели урегулировать самостоятельно. В таком случае стороны конфликта предъявляют всю имеющуюся фактографическую

информацию на рассмотрение в арбитраж, решения которого выносятся в соответствии с законодательством и обязательны для исполнения сторонами конфликта.

Членство в сообществе означает признание верховенства законодательства сообщества и обязательность исполнения решений арбитража.

Обязательность исполнения, юридическая сила, правовые последствия решений арбитража обеспечиваются созданной и поддерживаемой сообществом системой принуждения.

Функция системы юридически значимых коммуникаций состоит в предъявлении арбитражу фактографической информации, зарегистрированной системой, в не подлежащем сомнению виде.

Фактографическая информация должна включать согласованные сторонами документы и протоколы обмена, подтверждающие надлежащее информирование участников взаимодействия. Юридически должна быть обеспечена неотказуемость участников взаимодействия от подписанных ими документов, выполненных действий и принятых на себя обязательств.

---

## Требования к SIS

Чтобы обеспечить эффективное взаимодействие членов сообщества, SIS должна удовлетворять ряду требований.

1. SIS должна быть целостной системой. Любая фрагментация, особенно - при использовании разнородного инструментария, создает трудно преодолимые и ненужные проблемы.
  2. SIS должна обеспечивать юридическую значимость коммуникаций. Предоставляемые арбитражу документы должны иметь неопровержимые доказательства своей аутентичности.
  3. SIS должна обеспечивать возможность безбумажной реализации сложных видов взаимодействия.
  4. SIS должна обеспечить полную системную защиту персональных данных.
  5. SIS должна иметь простые и наглядные пользовательские интерфейсы.
  6. Схема владения и управления SIS должна обеспечивать максимально возможный уровень доверия участников сообщества.
  7. Базовые системные функции должны быть реализованы на инфраструктурном уровне.
-

## Моделирование как принцип построения SIS

Поскольку потенциально SIS должна обеспечивать информационное и алгоритмическое сопровождение любых видов взаимодействия для любых абонентов, главным принципом проектирования функционала системы принято последовательное и систематичное информационное **моделирование** общества и процессов, в нем происходящих.

Программная среда позволяет создавать информационные конструкции и процессы, не имеющие аналогов в реальном мире. Но опыт показывает, что такие решения не всегда хорошо стыкуются с реальными процессами, с трудом понимаются теми, кто с ними соприкасается.

Перенос коммуникаций, сопровождающих деятельность членов общества, в электронную среду с сохранением общей схемы процесса делает коммуникации более надежными, оперативными, комфортными, дешевыми, экологичными. При этом не возникает новых трудно разрешимых коллизий.

После накопления опыта будут произведены структурные преобразования, упрощающие схемы общественных процессов на основе интегрированной в SIS информации и процедур.

Важным результатом принятого метода является то, что при достаточно полном охвате общественных коммуникаций создается весьма полная, адекватная по структуре и синхронизированная во времени **информационная модель общества**. Это открывает много новых возможностей в совершенствовании управления обществом.

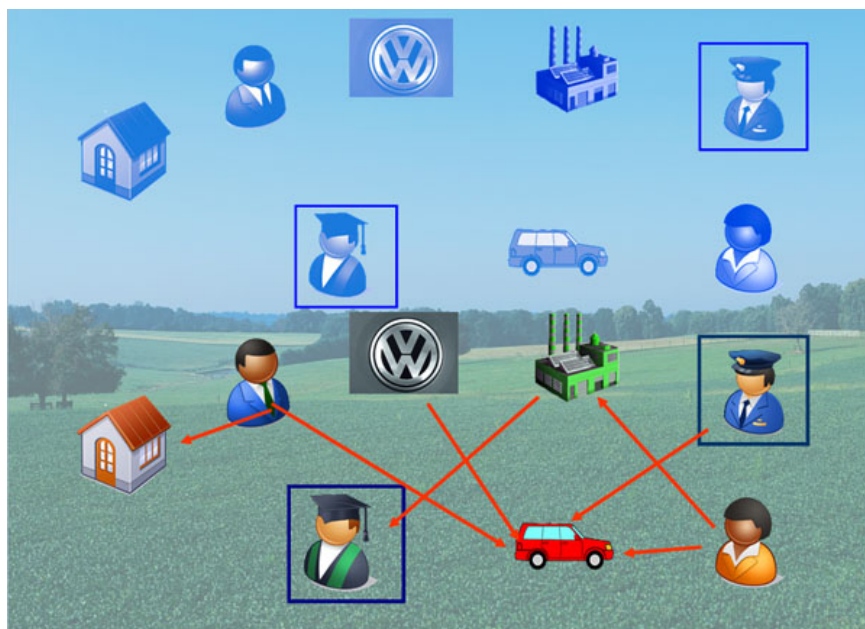
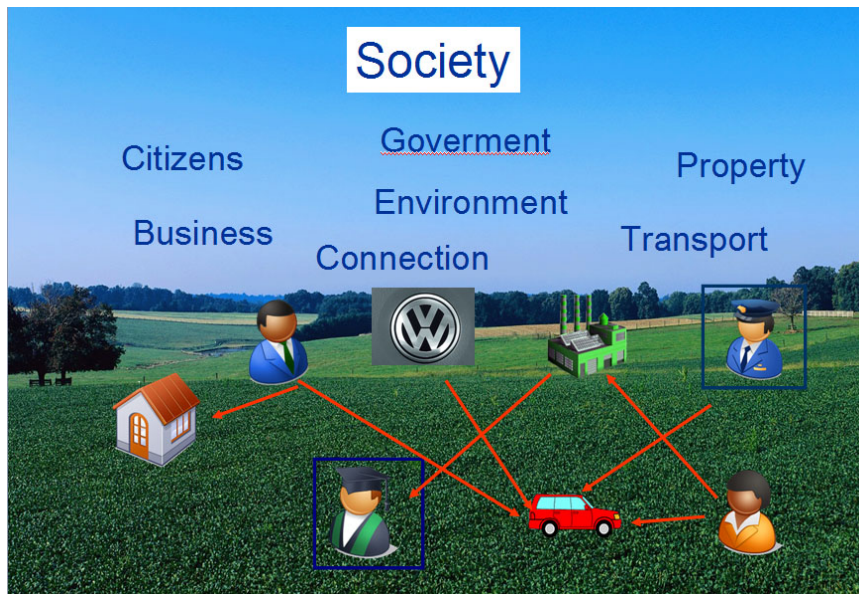
Такую модель уместно назвать **MetaSociety**.

---

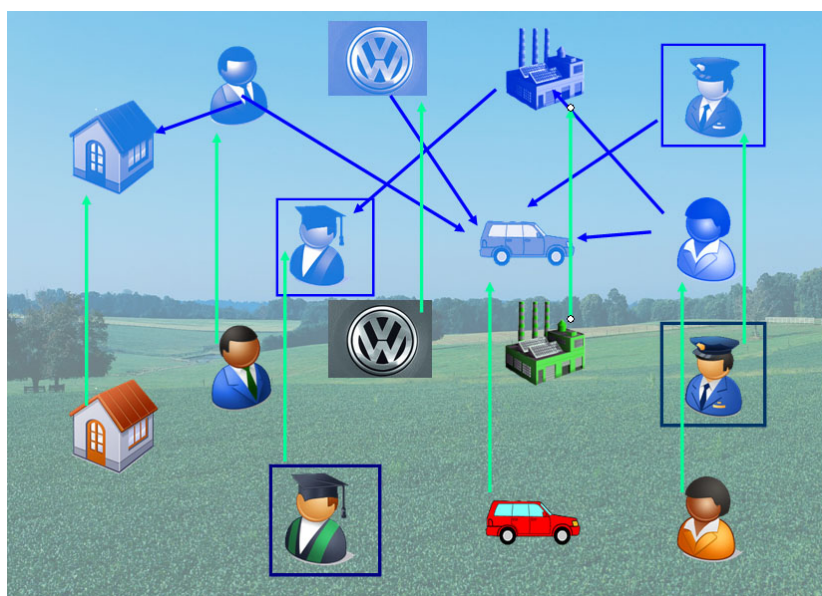
## Состав MetaSociety

Формируя SIS мы создаем информационную модель общества - MetaSociety. Существенными прототипами элементов такой модели являются:

- **участники коммуникаций** (физические лица, юридические лица, государственные структуры)
- **предметы**, являющиеся субъектами коммуникаций (недвижимость, транспортные средства и т.п.)
- существенные **элементы окружающей среды** (географическая информация, климатические данные и т.п.)
- **информационные связи** между элементами



В информационном пространстве последовательно и систематично создаются соответствующие модели.



Информационное взаимодействие прототипов заменяется информационным взаимодействием их моделей. Естественно, под управлением и под контролем участников коммуникаций.

---

## Модели и роботы

Понятие **модели** субъекта коммуникаций - важнейшее в SIS и определяет все прочие функции системы.

Под **субъектами коммуникаций** понимаются все виды сущностей, которые в той или иной форме участвуют в общественных коммуникациях. Это могут быть **активные участники**, которые осмысленно взаимодействуют с SIS (физические и юридические лица, государственные органы и т.п.), либо **пассивные**, являющиеся предметами, на которые направлена деятельность общества (здания, автомобили, домашние животные, энергетические установки и т.п.).

Модели в SIS являются **резидентными**. Это значит, что каждому субъекту соответствует одна и только одна модель. Второе свойство резидентности состоит в том, что модель создается однажды, сопровождает своего прототипа на протяжении всего периода его существования и далее навсегда остается в архивах SIS.

Субъекта, которому сопоставлена модель, будем называть ее **прототипом**.

Как любая модель, модель субъекта коммуникаций содержит, прежде всего, **информационное** описание прототипа. Это описание должно быть по возможности полным, универсальным. Оно создается не под решение какой-то конкретной частной задачи, а ориентировано на все виды взаимодействия, обеспечение которых может быть возложено на SIS.

Принципиальная особенность моделей SIS в том, что они являются не только информационными, но и **функциональными**. Это значит, что им могут быть заданы алгоритмы действий в зависимости от указаний прототипа, от входящих сообщений от контрагентов, от других факторов.

Учитывая функциональность моделей SIS, в отличие от информационных моделей типа "personal data store", в дальнейшем будем их называть "персональный **е-робот**". Учитывая, что е-робот может принимать, передавать, хранить информацию и выполнять программы, можно сказать, что каждому субъекту SIS сопоставлен некий специализированный виртуальный персональный сервер.

---

## Управление е-роботами

В MetaSociety предполагается, что каждый е-робот кому-то принадлежит и кем-то управляется.

Пассивные модели объектов недвижимости, транспорта и т.п. управляются их



владельцами. При смене владельца управление е-роботом передается новому владельцу. У бывшего владельца остается информационный архив за тот период, когда он владел и управлял соответствующим е-роботом.

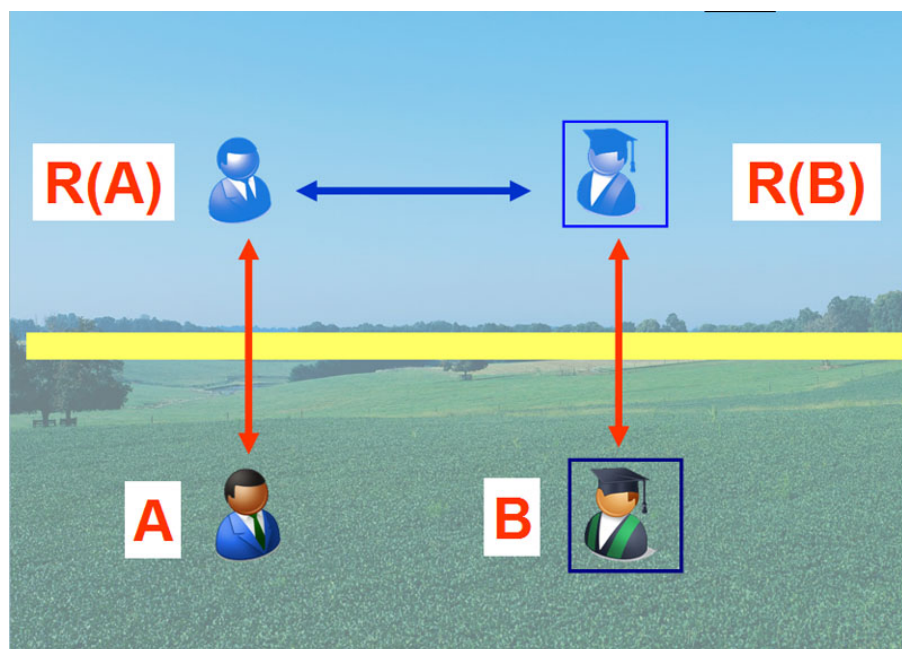
Модели юридических лиц и государственных структур управляются учредителями или лицами, ими уполномоченными.

Если говорить о физических лицах, то в ряде случаев управление е-роботом его прототипом невозможно или затруднительно. Речь идет о несовершеннолетних детях, престарелых, недееспособных. В этом случае, как и в реальном мире, выдается доверенность на управление или назначается опекун, который управляет е-роботом подопечного.

## Опосредованные коммуникации

Все деловые коммуникации между абонентами в SIS осуществляются при посредстве персональных роботов, которые имеются у каждого абонента.

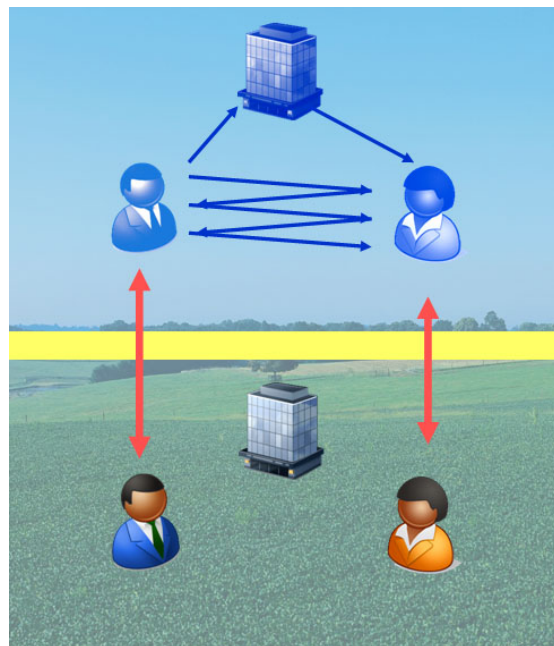
В сущности, каждый абонент, выходя в информационное пространство, имеет непосредственный контакт только со своим е-роботом.



Если абонент А хочет передать сообщение абоненту В, он дает соответствующую команду своему персональному роботу R(A), который передает сообщение персональному роботу адресата R(B), а тот уже доводит сообщение до сведения своего владельца. Или не доводит, а обрабатывает сам, если у него есть на то функционал и полномочия. В определенных ситуациях робот может сам инициировать обращение к своему прототипу-владельцу, либо к роботам контрагентов.



Такой двухуровневый протокол коммуникаций при посредничестве интеллектуальных и обладающих всей необходимой информацией е-роботов открывает неограниченные возможности для глубокой автоматизации делового взаимодействия, включая многостороннее взаимодействие и многошаговые процедуры.



В случае необходимости через роботов может быть организован речевой или видеоканал для прямого общения участников взаимодействия без нарушения конфиденциальности.

---

## Перераспределение рисков

Сравним риски, которые несут участники электронных коммуникаций при прямом и опосредованном взаимодействии.

В случае прямого взаимодействия абонент А контактирует через интернет со своим контрагентом, предполагая, что это абонент В. Абонент А применяет доступные ему методы аутентификации абонента В: логин, пароль, методы риск-менеджмента. Все подтверждения аутентификации являются косвенными и не дают 100% гарантии аутентичности. Решение о достоверности проведенной аутентификации принимает абонент А, соответственно он и несет риски потерь. Если окажется, что под видом абонента В действовал злоумышленник, то абонент В не будет нести ответственности за потери абонента А, а злоумышленника, возможно, найти не удастся. Существенно, что при прямом взаимодействии абонентов злоумышленник не ограничен в применяемом инструментарии.

В случае опосредованного взаимодействия абонентов А и В при посредстве роботов R(A) и R(B), действия которых являются юридически значимыми, риски принципиально перераспределяются.

Взаимодействие роботов происходит по схеме, аналогичной схеме host to host и под управлением централизованной системы управления взаимодействием SIS. Надежность идентификации в таком случае максимальна. Если робот R(A) получает некоторое обязательство от робота R(B), то это обязательство юридически значимо, неотказуемо и интересы абонента А находятся под защитой всей правоохранительной

системы.

Даже если абонент В каким-то образом был обманут, и его робот выполнил нежелательное действие, риски потерь несет абонент В.

Формально - потому что использование SIS предполагает юридически зафиксированное признание любым абонентом юридической значимости действий своего робота.

По существу - потому что любой абонент имеет возможность полного контроля за действиями своего робота. Даже если злоумышленник сможет каким-то образом дать команду роботу R(B) помимо воли абонента В, от абонента В будет по независимым каналам запрошено подтверждение действий его робота. И если робот все-таки выполнил нежелательное действие, то это может произойти только в случае недопустимой халатности абонента В.

Возможно возникновение инцидентов по вине SIS или из-за ошибки в программе робота R(B). Такие инциденты решаются в рамках обычной юридической практики на основании соглашений абонента В с администрацией SIS и фирмой, разработавшей программу для робота. Принципиально важно, что ни в какой ситуации эти риски не касаются абонента А.

---

## Программируемый робот

е-робот в MetaSociety - не просто механический ретранслятор сообщений. Он обладает функциональностью и может, например, анализировать потоки входящих сообщений и по некоторым предпринимать самостоятельные действия (в соответствии с регламентом, который задан его владельцем).

Например, если входящее сообщение - счет за отопление квартиры, владелец может запрограммировать своего е-робота, чтобы он эти счета оплачивал автоматически, не требуя подтверждения, а лишь информируя, что получен счет и платеж произведен. А может быть - и не информируя, поскольку в данном случае требование оплаты безальтернативное. На усмотрение владельца. Но при этом робота можно запрограммировать и на то, чтобы он проверил соответствие суммы счета договору с компанией, что это не счет, случайно выставленный повторно и т.п.

Пользователя нужно обеспечить не программой, которая позволит ему оплатить полученный счет, а системой, которая полностью возьмет на себя поддержание отношений с тем или иным сервисом. Это вполне реально, поскольку такое взаимодействие обычно четко регламентировано контрактом и законами.

Для такого программирования должен быть создан **Interaction Procedure Language (IPL)** - язык описания процедур взаимодействия. Создание библиотек описаний типовых процедур взаимодействия абонентов на строгом формальном языке программирования будет огромным шагом в упорядочении законодательства и всякого

рода регламентов. Передача управления взаимодействиям компьютерной системе позволит минимизировать "человеческий фактор", приводящий к нечеткому их исполнению либо злоупотреблениям.

Есть еще один интересный аргумент в пользу персональных е-роботов. Концепция MetaSociety предполагает, что робот имеет ограниченную функциональность. Он может делать только то, чему его научили.

И если при непосредственном выходе на тот или иной сервер человек соответствующего опыта и ориентации может этот сайт "хакнуть", то при общении через роботов это принципиально невозможно.

Если обратиться к концепции LifeManagement, упоминаемые в ней controlled push и informed pull - тоже функция персонального робота.

---

## Императив

Коммуникации в SIS ориентированы на деловое взаимодействие. Это значит, что сообщения в системе как правило несут в себе некий импульс к действию: пожелание, просьбу, приказ, поручение.

Чтобы выделить этот импульс из неформализованного текста сообщения и сделать его понятным е-роботам, в сообщения SIS вводится соответствующий структурный элемент - **императив**.

Императив может содержать одну или несколько строк IPL (языка описания коммуникационных процедур), указывающих на действие, ожидаемое от получателя сообщения.

Примеры императивов:

- "Ожидаю ответа в течение трех дней"
- "Ожидаю ответа ASAP"
- "Прошу подписать прилагаемый документ"

Как минимум, использование императивов даст каждому абоненту полную картину состояния его деловых коммуникаций: список полученных отработанных и не отработанных императивов, список направленных им самим императивов, отработанных или не отработанных партнерами.

Роботы смогут на основании императивов выполнять определенные действия самостоятельно. Например, напомнить контрагенту или своему прототипу о невыполненном в срок императиве.

По мере развития IPL роботы смогут выполнять многошаговые многосторонние процедуры любой сложности.

---

## Надлежащее извещение

Одним из ключевых моментов, обеспечивающих юридическую значимость коммуникаций, является надлежащее извещение (proper notice).

Например, при проведении судебного заседания принципиально важно, были ли участники судебного процесса надлежащим образом оповещены о времени и месте заседания. Нарушения процедуры надлежащего извещения является безусловной причиной для отмены решения суда, вынесенного в отсутствие не надлежащим образом извещенного участника.

В принципе, для любого сообщения или документа важно, был ли он своевременно и без искажений доставлен адресату. Как ни странно, при невероятном современном развитии средств коммуникаций, проблему надлежащего извещения нельзя считать решенной.

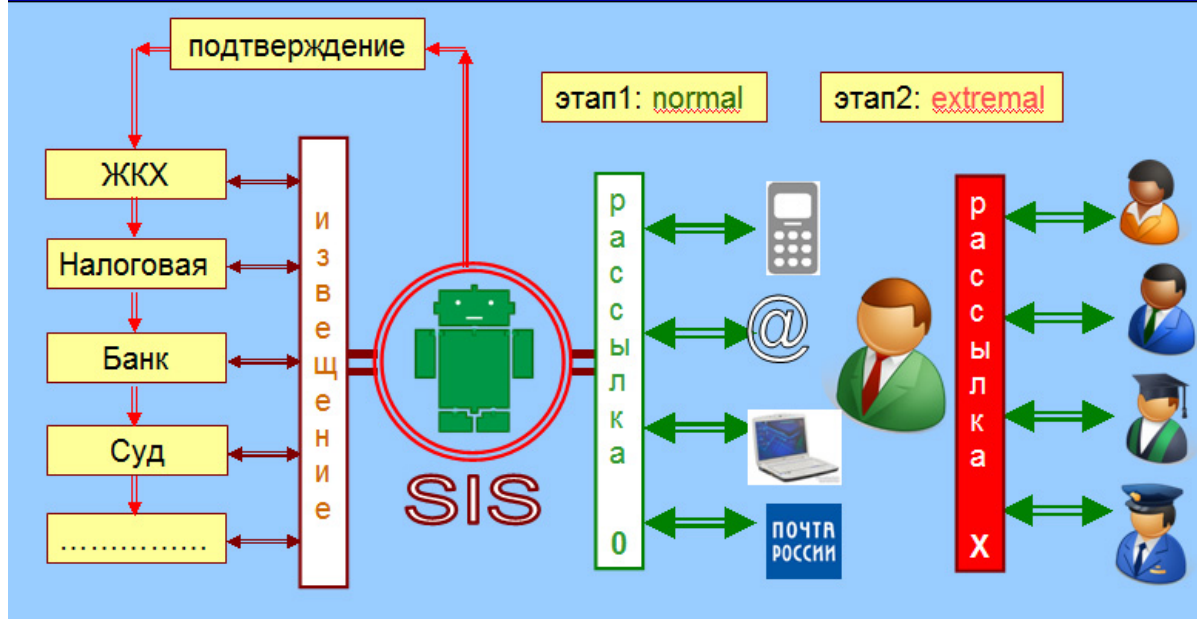
Основная причина в том, что гражданам навязывается некая единая для всех технология надлежащего извещения. Но у людей самые разные и динамически меняющиеся жизненные обстоятельства, и никакое единое решение не может быть приемлемым для всех.

С помощью е-роботов проблема надлежащего извещения решается наилучшим образом.

Извещающей стороне достаточно послать извещение е-роботу извещаемого абонента. Робот даст подтверждение в получении и у извещающей стороны будет юридически значимое доказательство выполнения ею своей обязанности по надлежащему извещению.

Далее е-робот займется оповещением своего владельца о полученном сообщении. При этом он будет действовать в соответствии с заранее заданным владельцем алгоритмом, используя все доступные каналы связи.

# Надлежащее извещение средствами SIS



Для начала е-робот может послать email и SMS. Если владелец не отреагировал в течение заданного времени, сообщения повторяются. Список каналов может быть расширен: звонок на резервный телефон, сообщение в Skype, Facebook, ICQ и т.д.

Отсутствие ответа на повторные обращения может свидетельствовать о какой-то нештатной ситуации с владельцем робота: потеря связи, попадание в больницу, арест, похищение, смерть. В зависимости от статуса извещателя и важности сообщения, сценарием на определенном этапе может быть предусмотрено оповещение родственников, коллег, друзей, правоохранительных органов.

Таким образом будет сделан максимум возможного, чтобы доставить сообщение абоненту.

Сценарии извещения в зависимости от типов сообщений определяет сам пользователь. В любой момент он может изменить эти сценарии. Например, в случае командировки, отъезда на отдых, болезни.

Граждане должны понимать, что в надлежащем извещении прежде всего заинтересованы они сами. В случае неполучения важного извещения, страдающей стороной скорее всего окажутся они сами.

Обязанность поддерживать канал связи с государственными органами вообще нужно считать гражданской обязанностью каждого гражданина. Нельзя вынуждать государство предпринимать чрезвычайные усилия для связи с гражданином. SIS предоставляет канал такой связи - экономичный, оперативный, ориентированный на пользователя (user centric), юридически значимый.

---

## Идентификация в MetaSociety

В информационном пространстве MetaSociety взаимодействие происходит между е-роботами, которые являются резидентными представителями своих прототипов-владельцев. Роботы действуют под полным контролем своих владельцев и их действия юридически значимы. Т.е. действия е-робота с точки зрения законодательства приравниваются к действиям его владельца.

Поскольку между абонентами SIS и е-роботами есть взаимно однозначное соответствие, для контрагента не имеют значения идентификационные персональные данные физического лица, владеющего и управляющего е-роботом, с которым контрагент осуществляет деловое взаимодействие. При обращении в арбитраж ему достаточно предъявить идентификационные данные е-робота.

Идентификация в цифровом информационном пространстве производится своими специфическими методами, она значительно более надежна, чем идентификация в реальном мире.

Соответствие е-робота и его прототипа формируется уполномоченной регистрационной службой при первичной регистрации абонента. Эти данные строго конфиденциальны, хранятся в уполномоченной регистрационной службе вне SIS. Только она и только по мотивированному запросу правоохранительных органов может раскрыть идентификационные данные владельца е-робота.

Такой принцип системно решает проблему защиты персональных данных в информационном пространстве - их там просто нет.

---

## Доверие е-роботу

На первый взгляд может показаться, что признать действия е-робота юридически значимыми для его владельца - неоправданный риск и несколько противоестественно.

На самом деле есть много аргументов за то, что схема работы через е-робота более эффективна и безопасна, чем прямое ручное управление всеми операциями в электронной среде самим абонентом.

1. Робот не спит, не употребляет алкоголь, не болеет, не впадает в депрессию, никогда ничего не забывает.
2. Робот использует типовые, массово опробованные процедуры, поэтому реакция робота на возникающие в компьютерной среде ситуации точнее, чем человека.



3. Контрагент, ведущий общение с абонентом через робота ограничен в формах и степени воздействия на абонента регламентом нормальных деловых отношений.

4. Тот факт, что взаимодействие при посредстве роботов является юридически значимым, заставляет партнеров вести сугубо корректный диалог. Попытки обмана, угроз, шантажа в такой схеме бессмысленны, так как они могут вызвать соответствующие негативные правовые последствия.

5. Главное: для операций, которые абонент считает для себя ответственными, в SIS обеспечивается полная подконтрольность робота своему владельцу. Перед проведением таких операций е-робот информирует владельца и получает от него подтверждение или запрет. Для этого используется альтернативный канал связи. Например, мобильный телефон.

Такая схема позволяет предотвратить нежелательные последствия даже в случае чьего-то неправомерного доступа к е-роботу. Сам же факт попытки неправомерного доступа будет немедленно зафиксирован и будут предприняты адекватные меры.

Признание абонентом юридической значимости действий своего е-робота и неотказуемости должно быть закреплено письменно в некотором базовом соглашении об условиях работы абонента в системе юридически значимых коммуникаций.

---

## Нужны ли персональные данные в деловых отношениях?

Чтобы поддерживать деловые отношения, система коммуникаций должна обеспечивать юридическую значимость документов и сообщений. Зачем нужна юридическая значимость? Юридическая значимость проявляется только в одной ситуации: при обращении к суду в случае возникновения конфликта, который стороны не смогли или не захотели урегулировать в досудебном порядке.

**Вопрос:** в какой деловой ситуации абоненту А может потребоваться физическая идентификация абонента В?

**Ответ:** ни в какой!

Если в процессе общения через роботов возникший конфликт не будет урегулирован, есть только один законный путь дальнейших действий: обращение в суд. При этом истец, абонент А, представляет электронные документы и протоколы обмена сообщениями с абонентом В по спорному вопросу.

Если взаимодействие сторон происходило полностью через SIS, представленные материалы могут полностью описывать ситуацию и арбитраж может быть проведен так же при посредстве SIS.

Предположим, суд решил, что абонент В должен выплатить штрафные санкции абоненту А. И он их выплатил. Конфликт исчерпан, физическая идентификация

абонента В не потребовалась.

И только если абонент В отказывается выполнять решение суда, или суд приговаривает его к наказанию в виде тюремного заключения, требуется розыск и физическая идентификация абонента В.

Но розыск - отнюдь не функция абонента А. Право на розыск, идентификацию, принуждение и наказание имеют только государственные правоохранительные органы. Соответственно, судебный пристав или полицейский должны обратиться в регистрационную службу со ссылкой на решение суда. Там они получают идентификационные данные физического лица, владеющего роботом В.

**Следствие №1.** Идентификационные персональные данные в сетевом пространстве не нужны. Они должны храниться вне сети в уполномоченной регистрационной службе.

**Следствие №2.** Регистрационной службой SIS должна быть государственная, либо уполномоченная государством структура. Это нужно, чтобы достоверность идентификации *в дальнейшем* не подвергалась сомнению судом (государственной структурой).

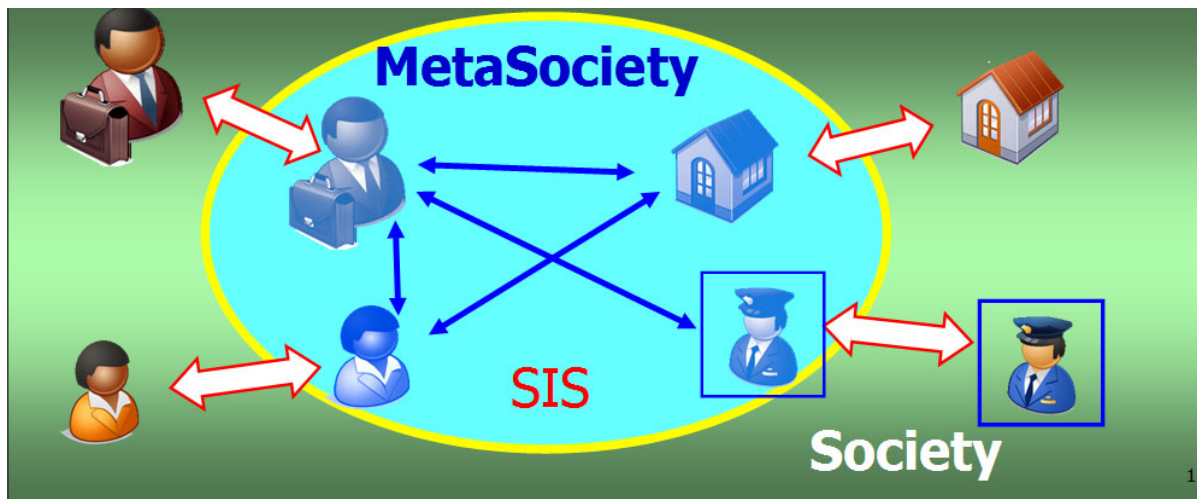
Представление о том, что участие государства в регистрационном процессе приведет к тотальному контролю государства над коммуникациями в SIS, сугубо неверно. Это будет показано позже.

---

## Первичная идентификация

Концепция MetaSociety предполагает, что каждому физическому и юридическому лицу сопоставлен виртуальный сервер (e-Robot), и все взаимодействие абонентов производится через их личных роботов. Абонентам обеспечен полный контроль за действиями роботов, и, соответственно, на них возложена полная, в том числе и юридическая ответственность за их действия.

Роботы являются информационными и функциональными моделями своих владельцев-прототипов. Совокупность этих моделей де-факто создает информационную модель общества - MetaSociety.



MetaSociety - целостная, полностью программируемая вычислительная среда. Роботы в ней надежно идентифицируются специфическими сетевыми методами. Нет никакой необходимости использовать для идентификации роботов офф-лайновые идентификационные признаки владельцев: имена, даты рождения, номер паспорта, биометрические данные. Естественно, что соответствие роботов и их владельцев надежно зафиксировано, но это делается вне сетевого пространства.

Сопоставление роботов своим прототипам проводится неким специальным идентифицирующим органом (Identifying Authority) на входе в SIS.

Identifying Authority выполняет три операции:

1. Первичная идентификация. Проводится на основе общепринятых офф-лайновых идентификационных документов (паспорт, водительские права...) и, в случае необходимости, биометрия.

Прежде всего проверяется подлинность документов и их принадлежность абоненту. Далее абоненту выдается первичный электронный паспорт, представляющий собой обезличенный уникальный цифровой код (Primary Electronic Passport - PEPass). На основании PEPass абонент регистрируется в SIS и ему сопоставляется персональный e-Robot. В дальнейшем для выполнения конкретных операций робот получает целевые динамические электронные паспорта (DEPass).

Идентифицирующий орган сохраняет протокол о факте выдачи PEPass и всю информацию, необходимую для офф-лайновой идентификации абонента. Протокол и необходимая дополнительная информация хранятся вне сетевого пространства, возможно даже просто в виде папки с бумажными документами. Таким образом обеспечивается 100% гарантия от утечки персональных данных в сетевом пространстве: их там просто нет! (Privacy by Design, не так ли?)

2. Восстановление аутентичности. Производится по заявке абонента в случае утраты им доступа к его e-Robot.

3. Реидентификация. Обращение в Identifying Authority - единственный способ определить офф-лайновую идентификацию абонента по его PEPass. Эта операция производится в исключительных случаях: по заявке родственников в случае смерти абонента и по решению суда в криминальных ситуациях. Учитывая юридическую значимость действий роботов, в среде MetaSociety нет необходимости использовать

офф-лайнные идентификационные параметры абонента.

Identifying authority несет полную ответственность за достоверность первичной и обратной идентификации, за сохранность информации и за ее раскрытие только в определенных законом случаях.

Пример взаимодействия гражданина и налоговой инспекции.

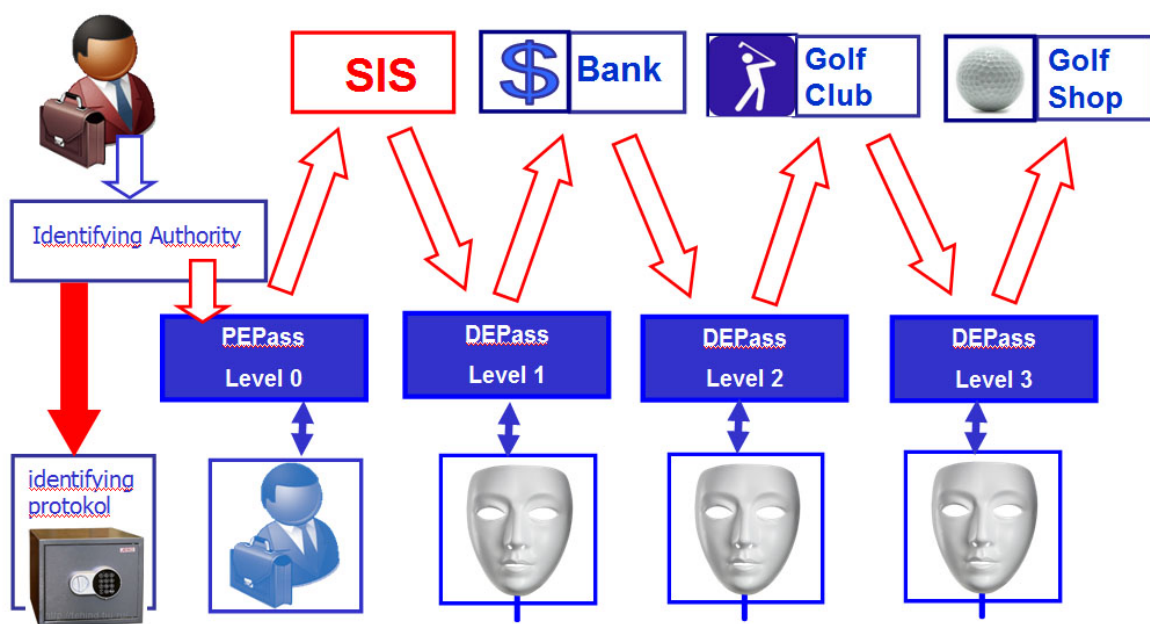
Гражданин с DEPass=5FQ8XTJ владеет квартирой DEPass=ТЗЕСГМУ и должен заплатить налог \$1527 до 25.04.2014 г.

Ситуации:

1. Налог уплачен. Реидентификация не нужна.
2. Налог к нужной дате не уплачен. Через SIS отправляется надлежащее извещение о необходимости уплаты налога и пени. Гражданин оплачивает налог и пени. Реидентификация не нужна.
3. Налог к нужной дате не уплачен. На извещения гражданин не реагирует. DEPass вместе с материалами о нарушении передается в суд. Далее, по запросу суда проводится реидентификация. Офф-лайнные идентификационные данные передаются службе судебных приставов, которые осуществляют розыск гражданина и принуждение к выполнению своих обязательств.

Интересно, что налоговой инспекции при электронном взаимодействии офф-лайнные идентификационные данные гражданина не нужны даже в случае конфликта, поскольку функции розыска и принуждения не входят в ее права и обязанности.

Конфиденциальность операций в сети обеспечивается возможностью многоуровневого формирования DEPass.



В приведенном примере SIS выдает роботу DEPass level 1, по которому абонент открывает аккаунт в электронном банке. Банк выдает роботу DEPass level 2,

представляющий собой по сути виртуальную кредитную карту. С этой картой абонент регистрируется в гольф-клубе и получает DEPass level 3 - членскую карточку клуба, по которой абонент может получить, например, скидку в специализированном магазине.

Каждый DEPass issuer имеет информацию только об использовании выданных им паспортов, и не может отслеживать применение паспортов следующего уровня. Это, в частности, является механизмом, предотвращающим тотальный контроль государства над операциями абонентов в SIS.

Если в операциях с DEPass level 3 произошел криминальный эпизод, требующий офф-лайн идентификации абонента, на основании решения суда раскручивается в обратном направлении цепочка Golf Club - Bank - SIS и PEPass предъявляется в Identifying Authority.

В данной схеме Identifying Authority не обязательно государственная структура. Это может быть и специальный отдел в крупной фирме, который псевдонимизирует новых абонентов, предотвращая возможность утечки их персональных данных из подразделений фирмы.

Но есть и свои аргументы в пользу построения единой национальной системы идентификации в электронном пространстве с участием государства.

---

## Электронные паспорта

Для идентификации субъектов коммуникаций в SIS вводится понятие **Динамического Электронного Паспорта (DEPass)**.

DEPass - это просто уникальный обезличенный неструктурированный код, которому сопоставлен набор атрибутов, определяющих его статус.

Набор атрибутов может быть переменным. Например, с помощью атрибутов можно задать:

- срок действия паспорта (постоянный, временный)
- кратность (многократный, разовый)
- назначение (зона действия вплоть до конкретного адресата)
- лимит ответственности (предельная сумма, гарантированная к расчетам по этому паспорту)

Поскольку процедура выдачи электронного паспорта несравнимо дешевле и быстрее выдачи обычных паспортов, абонент SIS может получить неограниченное количество DEPass.

Например, если абонент покупает что-то в определенном магазине и хочет накапливать скидки, он использует постоянный DEPass для этого магазина. Если он

покупает лекарства и не хочет, чтобы кто-то мог обобщить эти данные, он использует разовые DEPass.

Ограничение кратности использования DEPass, срока действия (например, одна минута - для совершения одной конкретной операции), точная адресность делают бессмысленным хищение паспортов.

DEPass может быть первичным (выданным государственным органом) и вторичным (выданным другими участниками SIS для использования в сфере их контроля).

Пример: банк, на основании первичного паспорта выдает клиенту кредитную карту - по сути это вторичный паспорт, имеющий определенную узкую зону применения. Клиент, оплачивая кредитной картой членство в спортивном клубе получает паспорт от клуба, предоставляющий клиенту определенные права.

Наличие вторичных паспортов снимает вопрос о полном контроле государства над SIS. Государственные органы участвуют в системе только на входе (первичная идентификация) и на выходе (определение по предъявленному DEPass физической идентификации абонента).

Все промежуточные операции не могут контролироваться непосредственно, но могут быть раскрыты по решению суда.

---

## Псевдонимизация

Электронный паспорт - это просто некий уникальный безликий и неструктурированный код. Это лучший формат для общения в информационном пространстве между роботами, но он абсолютно не подходит для человеческого общения.

Поскольку за роботами находятся люди, необходимо иметь какую-то форму обращения друг другу в переписке или непосредственном контакте, не раскрывающую идентификационных данных партнеров.

Такая форма в интернете давно освоена. Это nickname или псевдонимы.

SIS дает возможность в случае необходимости сопоставить тому или иному DEPass некий, пригодный для человеческого общения псевдоним. При этом не требуется глобальной уникальности псевдонима. Главное - он не должен дублировать псевдонимы контрагентов, участвующих в общении. Таким образом псевдоним не является полным идентификатором абонента и имеет ограниченную зону действия, определяемую абонентом по своему усмотрению.

Один абонент для разных своих электронных паспортов может использовать разные псевдонимы.

Поскольку многие процессы взаимодействия являются смешанными, т.е. происходят



попеременно и в информационном пространстве и в реальном, допускается использование псевдонимов и при непосредственном контакте.

Например, использование псевдонима вполне уместно при контакте с врачом. Лечение ни коим образом не зависит от фамилии пациента. Врачу важно знать о наличии страхового полиса и иметь доступ к медицинским документам пациента. Это наилучшим образом обеспечит электронный паспорт, не публикуя идентификационные данные владельца.

---

## Идентификация в реальном мире

При наличии юридически значимой информационной модели общества MetaSociety виртуальная информация становится приоритетной по сравнению со всякого рода документами на бумажных носителях. Это мотивировано тем, что фальсифицировать информацию, зафиксированную в базе данных сложной структуры, защищенную многочисленными логическими связями, протоколированием любых изменений много сложнее, чем любые физические носители.

При идентификации в реальном мире необходимо выполнить следующие шаги:

1. Идентифицируемый тем или иным способом должен сообщить свой DEPass идентифицирующему.
2. Идентифицирующий запрашивает у SIS подтверждение валидности полученного DEPass.
3. SIS проверяет полномочия идентифицирующего и подтверждает или не подтверждает валидность DEPass.
4. Если проверки 2 и 3 прошли успешно, проверяется принадлежность указанного DEPass идентифицируемому.
5. Если проверка 4 прошла успешно, идентифицирующий запрашивает у SIS необходимые ему сведения о статусе и полномочиях идентифицируемого.

Способ сообщения DEPass в зависимости от обстоятельств может быть любым. Код на чипе пластиковой идентификационной карты, QR-код на визитке или просто распечатанный на принтере, код, записанный в мобильном телефоне, сокращенный код или псевдоним, который может быть сообщен устно. Возможна косвенная идентификация. Например, по регистрационному номеру автомобиля можно через центральный сервер выйти на статусы его владельца, если у идентифицирующего есть соответствующие права.

Наиболее тонкий момент - проверка принадлежности кода идентифицируемому лицу.

Способы проверки могут быть следующими:

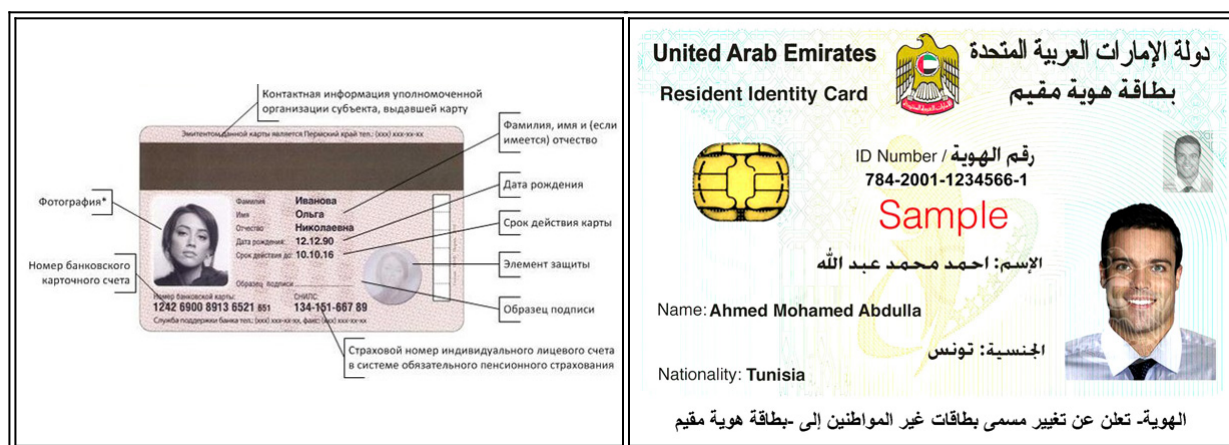
- сличение с фотографиями, полученными от центрального сервера
- ввод пин-кода
- ответ на контрольный вопрос, переданный с центрального сервера
- биометрическая проверка по данным с центрального сервера.

Если принадлежность кода подтверждена, идентифицирующий запрашивает у центрального сервера необходимые ему сведения об идентифицируемом лице. Это могут быть различные статусы (совершеннолетний, пенсионер, инвалид), права (на посещение данного объекта, на скидку в данном магазине, на получение посылки или товара на складе и т.п.). Данные сообщаются в пределах прав, которыми обладает идентифицирующий.

Следует обратить внимание, что идентифицирующий не получает собственно идентификационных данных проверяемого лица. Сами по себе фамилия и имя, дата и место рождения не имеют значения для определения статуса проверяемого и принятия решения. Все реально необходимые статусы сообщит центральный сервер на основании данных, связанных с предъявленным DEPass. Идентификационные данные могут получать только правоохранительные органы по специальному запросу и не по сети, а в регистрационной службе.

## ID-карты

Популярный способ идентификации - различного рода пластиковые идентификационные карты с чипом. Учитывая массовую распространенность банковских пластиковых карт, ID-карты можно считать одним из вполне приемлемых способов идентификации.



Однако, в своих конкретных реализациях проекты ID-карт обычно представляют собой эклектическую смесь атрибутов он-лайновой и офф-лайновой идентификации, не обеспечивающую ни конфиденциальности персональных данных, ни полной замены паспорта. Защита таких карт эквивалентна защите чиповых банковских карт с использованием традиционного пин-кода.

Системный недостаток идентификации по применяемым ID-картам - ориентация на долговременное и многократное использование неких постоянных идентификаторов для разных применений. Принципиально это открывает возможность нелегитимной интеграции данных по операциям владельца.

Нанесение на поверхность карты имени владельца, даты его рождения, номеров банковских карт и страхового полиса, образца подписи, снижает уровень конфиденциальности персональных данных владельца, не принося никаких дополнительных возможностей в электронной идентификации.

В концепции MetaSociety чиповая пластиковая карта рассматривается как один из возможных способов идентификации. В памяти чипа предусматривается возможность записи большого количества DEPass для различных ситуаций применения.



На поверхности ID-карты нет необходимости размещать какую-либо текстовую информацию. Нужно лишь принять меры, чтобы владелец мог отличить свою карту от лежащей рядом чужой. Для этого достаточно придать каждой карте индивидуальный дизайн.



Хорошим отличительным признаком ID-карты может быть фотография владельца. Но эта фотография служит только для того, чтобы владелец мог отличить свою карту от чужой. Верификация предъявителя карты должна проводиться по изображениям, переданным по каналам связи в соответствии с DEPass, считанным с чипа карты.

Процесс идентификации:

1. Человек предъявляет ID-карту
2. ID-карта вставляется в считыватель
3. Идентифицирующий получает разрешенный для него DEPass

4. По DEPass прежде всего определяется и выводится идентифицирующему фото владельца карты
5. Идентифицирующий подтверждает системе, что перед ним находится именно владелец ID-карты
6. Идентифицирующий получает необходимые и доступные ему данные.

Среди этих данных не будет офф-лайн-овых идентификационных данных: фамилии, имени, адреса проживания и т.п.

Например, он получит подтверждение, что перед ним пенсионер, имеющий право на скидку проезд, или человек, обладающий действующими водительскими правами категории "B".

Аналогичные функции по хранению DEPass может выполнять и мобильный телефон.

---

## Персонализация интерфейсов

В качестве одного из очевидных удобств работы через персонального е-робота можно назвать персонализацию интерфейсов.

Сейчас, обращаясь к различным сетевым сервисам, абонент вынужден осваивать разнородные по стилю, качеству, логике, дизайну интерфейсы. Общение через персональных роботов нивелирует все это многообразие. Пользователь общается с информационным пространством в едином, индивидуально настроенном, привычном, хорошо освоенном интерфейсе.

Это не просто комфорт. Это технология, которая позволит дать как простые и понятные интерфейсы непрофессиональным пользователям, так и функционально развитые интерфейсы профессионалам.

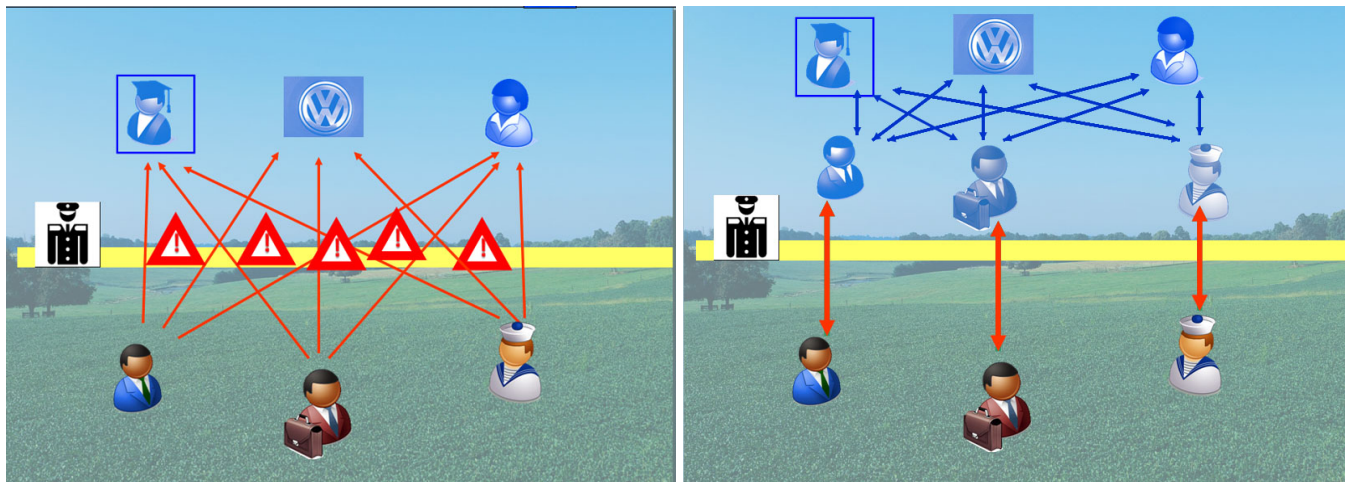
---

## Проблема аутентификации

Аутентификация в среде стационарных роботов-серверов существенно проще и надежнее, чем аутентификация динамически подключающихся абонентов. Все основные риски и опасности возникают на границах информационных систем.

Организовать надежный доступ одного абонента к одному собственному серверу - принципиально и многократно более простая задача, чем доступ любого абонента к любому серверу (сервису).





Помимо системного упрощения доступа (1:1 вместо n:m), появляются широчайшие технические возможности персонализировать алгоритмы доступа абонента к своему е-роботу и, главное, возможность возложить выбор схемы доступа и оперативное управление ею на самого пользователя.

Пользователь сможет выбрать наиболее понятный и психологически приемлемый для него набор "замочков", самостоятельно выбирать неизбежный компромисс между удобством доступа и надежностью защиты, определять разные уровни защиты в зависимости от проводимых операций.

Сегодня пользователю навязывается схема доступа тем сервисом, к которому он обращается. Выбор средств весьма ограничен. Учитывая многообразие вкусов пользователей, их привычек, уровня владения компьютером, различия в их технических средствах, каналах доступа, жизненных обстоятельств, достичь высокой степени удовлетворенности пользователей каким-то одним компромиссным решением принципиально невозможно.

И не нужно! Удовлетворенность пользователя средствами защиты доступа - вопрос не столько технический, сколько психологический. Поэтому очень важно, что в нашем варианте схему защиты выбирает сам клиент, в соответствии со своими представлениями, опасениями, предрассудками, образом жизни, степенью ответственности проводимых операций.

Можно представить множество оригинальных и нетрадиционных вариантов аутентификации абонента и доступа его к собственному серверу. Должен появиться рынок средств доступа. Квалифицированный пользователь может использовать индивидуальное программирование.

Тут уместно напомнить главный принцип концепции MetaSociety: моделирование объектов и процессов реального мира.



Близкая аналогия доступа к серверу - замки на дверях наших квартир. Вы кому-то можете высказать недовольство защитой вашей квартиры? Нет, потому что вы сами из широчайшего набора замков выбрали подходящую себе комбинацию. Вы сами выбрали естественный для вас компромисс между сложностью открывания и надежностью защиты, в любой момент можете поставить дополнительный замок или перестать пользоваться одним из имеющихся.

С точки зрения киберпреступности совершенно разная мотивация - взломать защиту, которую используют миллионы абонентов или заниматься индивидуальным подбором "ключей" к каждому из них.

---

## Доверие к SIS

Для централизованной системы коммуникаций крайне важно доверие абонентов.

По большому счету нельзя доверять по отдельности никому - ни государству, ни бизнесу, ни частному лицу.

SIS - программная система. Т.е. можно реализовать любые алгоритмы доступа. Публичная информация будет публичной, конфиденциальная - строго конфиденциальной, информация, которая должна раскрываться по решению суда, будет раскрываться только по решению суда.

Вопрос только в том, чтобы программа не содержала так называемых "недекларированных возможностей". Методы проверки программ на отсутствие недекларированных возможностей существуют. Вопрос только в их корректном применении.

Максимально возможные гарантии корректности работы системы может дать **Наблюдательный Совет**, включающий регулярно сменяемых представителей общественности, бизнеса и государства. Акции SIS должны быть распределены в равных долях между частными лицами, бизнесом и государством.

Система должна быть написана в открытом коде.

---

## Анонимность и аутентичность

Коммуникации в интернете по существу анонимны. Послать в банк email с поручением выполнить платеж в 50\$ невозможно, поскольку канал не обеспечивает юридически значимые коммуникации.



С другой стороны, если некто разошлет письма с экстремистскими призывами, он будет вычислен и наказан.

Получается, что юридической значимости коммуникаций в интернете недостаточно, чтобы распорядиться суммой в 50\$, но достаточно, чтобы отправить человека в тюрьму.

Концепция SIS обеспечивает реально полную анонимность в отношении идентификационных персональных данных абонента, но одновременно придает его коммуникациям полную аутентичность.

Рассмотрим работу защитных механизмов SIS на примере социологического опроса, выборов или референдума.

Каждому гражданину соответствует одна и только одна резидентная модель в информационном пространстве. Она не содержит идентификационных данных, но содержит все необходимые статусные данные.

Если говорим о социологическом опросе, то к результату голосования могут быть приложены данные о поле, возрасте голосующих, образовании, пенсии, инвалидности, регионе проживания. Эти данные не дают возможности идентифицировать абонента, но обеспечивают абсолютную объективность собранных данных.

Если говорим о выборах или референдуме, то при голосовании юридически значимо подтверждается, что голосующий гражданин данной страны, совершеннолетний и не лишен гражданских прав. Этого достаточно, чтобы результаты его голосования признать юридически значимыми.

Тайна голосования обеспечивается многоуровневостью электронных паспортов в SIS.

Для участия в выборах выдается специальный DEPass, причем выдается не государственной регистрационной службой, а избирательным комитетом, находящимся под полным общественным контролем. Избирательный DEPass выдается таким образом, что его обратная дешифровка технически невозможна.

Это полная аналогия выданного избирательного бюллетеня. Если человеку выдан бюллетень, это означает, что документы человека проверены и его право участвовать в выборах подтверждено. Он может проголосовать или не проголосовать. Но в случае голосования его голос должен быть учтен.

И так же как по избирательному бюллетеню, по избирательному DEPass нельзя восстановить имя голосующего.

Возможно, это наиболее важное свойство SIS. Оно делает возможным проведение оперативных, малозатратных, предельно достоверных и юридически значимых оценок общественного мнения по тем или иным вопросам жизни общества, действий правительства, проектов решений законодателей.

---

## Платформа SIS

В качестве функциональной платформы SIS используется формат социальной сети.

Социальные сети сегодня - весьма совершенный коммуникационный механизм, доказавший свою востребованность обществом. Главное, что привнесли социальные сети в электронные коммуникации - это резидентность абонента.

Страница пользователя в социальной сети существует постоянно, на ней можно накапливать документы и разного рода пользовательскую информацию (почти personal data store).

Другое важное свойство социальных сетей - полный контроль абонента над своими контактами, возможность протоколирования диалогов и долговременного хранения протоколов обмена сообщениями и документами.

И, наконец, возможность создания производных структур: закрытых и открытых групп и сообществ. На основе этого механизма создаются производные модели юридических лиц и государственных ведомств.

Эти традиционные механизмы адаптируются под задачи SIS и дополняются средствами, обеспечивающими юридическую значимость коммуникаций.

---

## Физические лица

В терминологии социальных сетей модель физического лица представляет собой некий базовый аккаунт и несколько дополнительных страниц, соответствующих различным ролям абонента.

Базовая страница доступна только самому абоненту и содержит информацию, предназначенную только для него самого.

Дополнительные страницы доступны только указанному в них кругу контактов: семья, друзья, коллеги, партнеры. На разных страницах абонент может использовать различные псевдонимы.

Если человек занимается некоторой публичной деятельностью (коммерческой, политической, религиозной, просветительской), он может создать публичные страницы, доступ к которым будет открыт для всех.

В каких-то ролях человек может опубликовать и свои реальные идентификационные данные - мы не можем ему это запретить. Но это не нарушит конфиденциальность других его ролей.

---

## Юридические лица

Юридическое лицо по сути - некоторое соглашение физических лиц, которое регистрируется государством, дает этим лицам определенные права и накладывает определенные обязательства.

Юридическая значимость коммуникаций в SIS позволяет абонентам не отходя от компьютера заключить соглашение об образовании юридического лица, после чего роботы выполнят все остальные процедуры регистрации в налоговом ведомстве, пенсионном фонде и т.д. - вплоть до открытия счета в банке.

*При государственной регистрации новому юридическому лицу будет выдан электронный паспорт и создан соответствующий е-робот, управлять которым будут уполномоченные учредителями лица. Учредители и персонал предприятия могут образовывать структуры, подобные группам в социальных сетях.*

Далее учредители могут либо самостоятельно программировать е-робота нового юридического лица, либо использовать типовые проверенные разработки: робот-кафе, робот-магазин, робот-аптека.

---

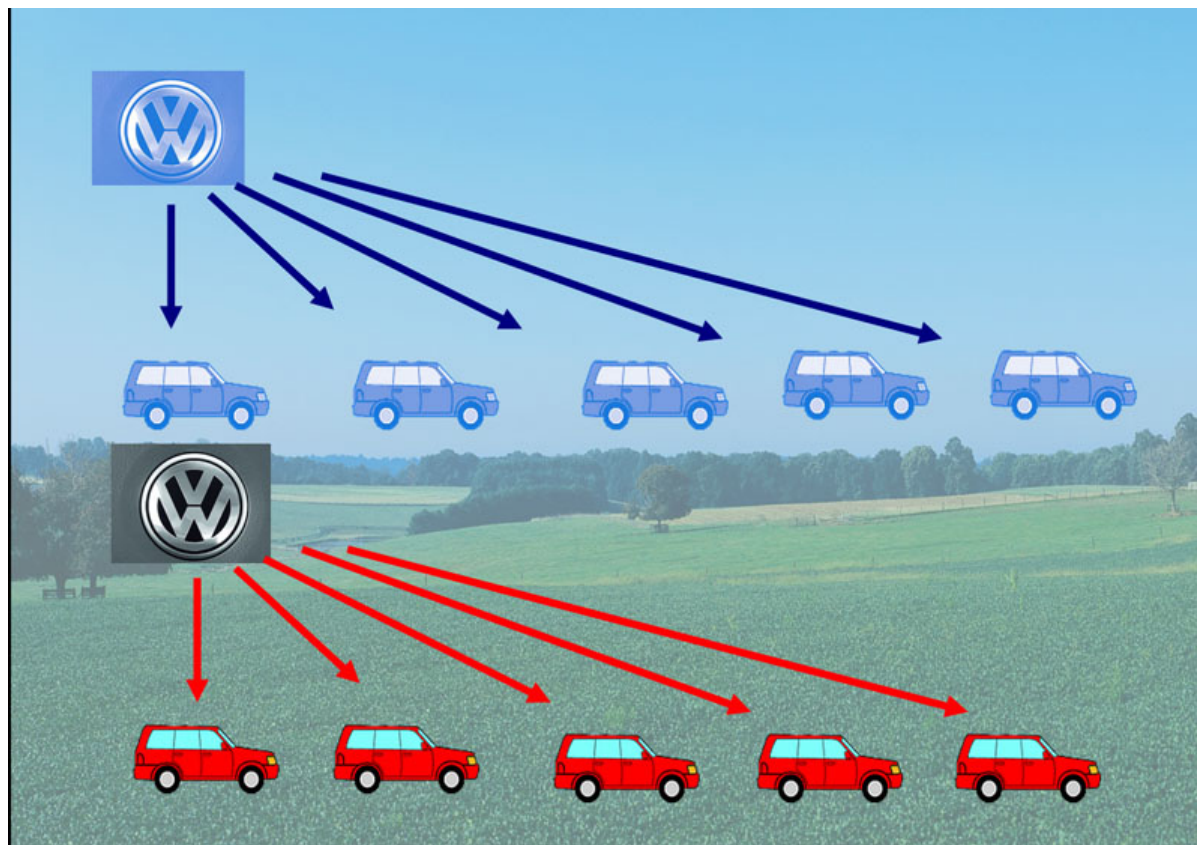
## Пассивные модели

Полноценная модель общества должна включать многочисленные объекты, которые окружают человека. Недвижимость, транспорт, бытовые приборы, энергетические установки, компьютеры, медицинские комплексы и т.д. - все они являются важными участниками социального взаимодействия. Мы их производим, эксплуатируем, проводим сервисное обслуживание и ремонт, покупаем и продаем.

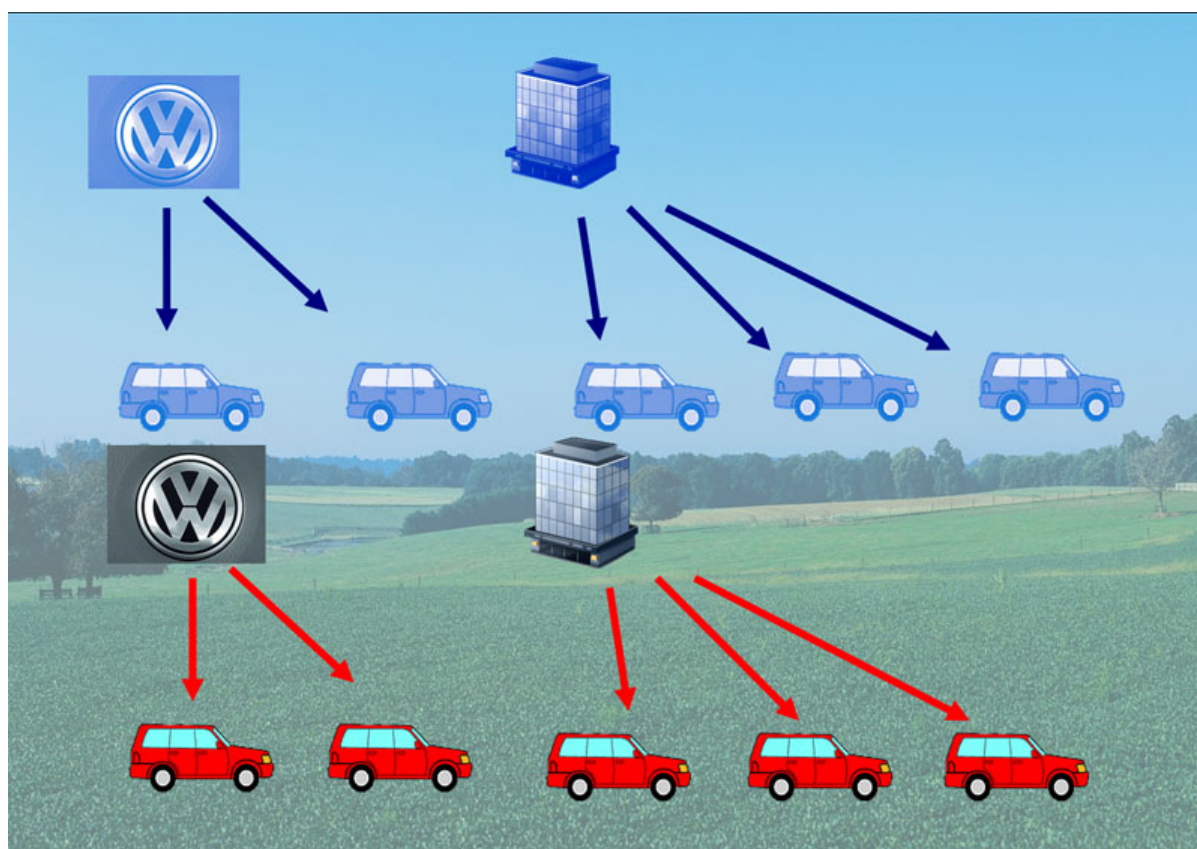
Наличие и доступность полноценных и актуальных информационных моделей окружающих нас предметов существенно повысят эффективность общественных коммуникаций (social interaction).

Такие модели первоначально должны создаваться производителем соответствующих объектов и содержать точную техническую спецификацию каждого конкретного экземпляра. Например, автомобили одной марки, выпущенные на одном и том же конвейере могут отличаться друг от друга, так как в конструкцию вносятся изменения, используются различные комплектующие детали, учитываются индивидуальные пожелания заказчиков.

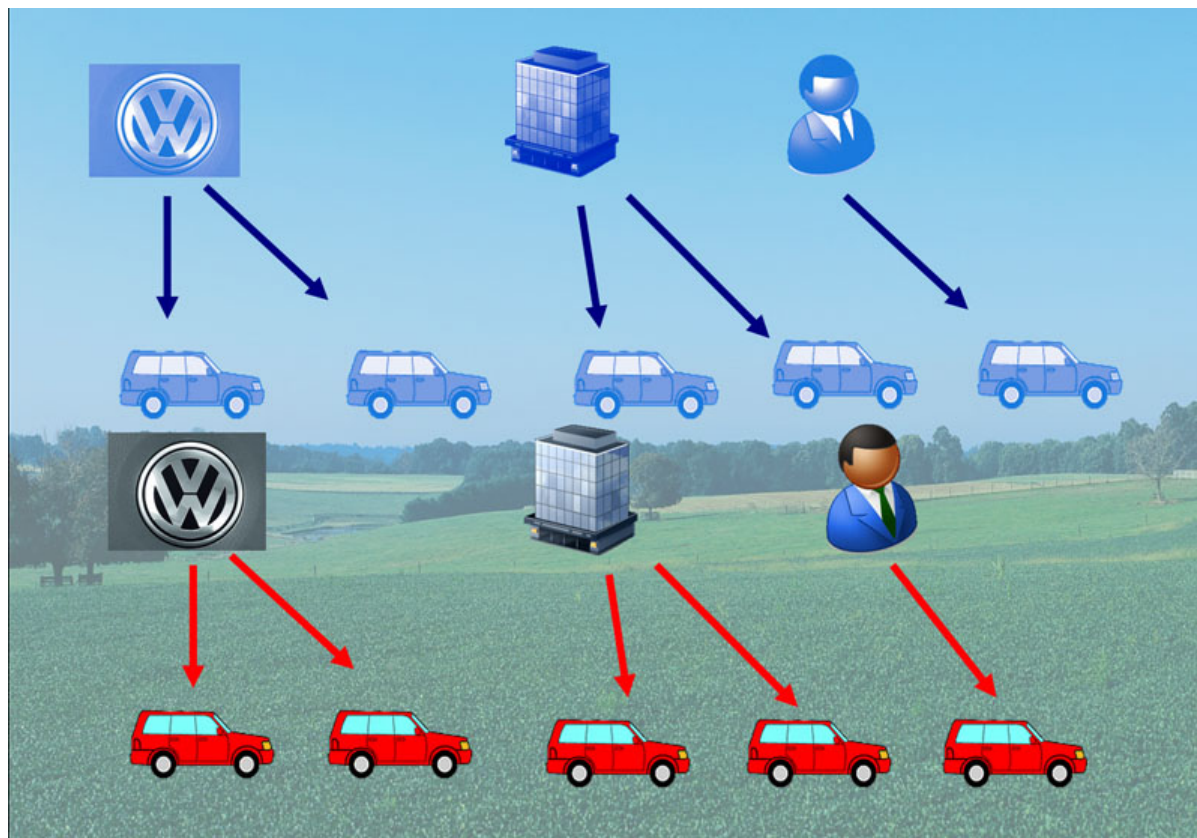
Образно можно сказать, что параллельно и синхронно с заводом, который выпускает автомобили, виртуальная модель завода должна выпускать информационные модели этих автомобилей.



Когда автомобили передаются дилеру для продажи, ему же передается и управление информационными моделями этих автомобилей.



Покупатель вместе с автомобилем получит и право/обязанность поддерживать его информационную модель. В этой модели будут накапливаться сведения о проведенных ремонтах, замене деталей, авариях автомобиля.



Робот, сопоставленный автомобилю, своевременно напомнит о необходимости проведения технического обслуживания. Производитель будет иметь оперативную и полную информацию об эксплуатации своих автомобилей, о поломках тех или иных узлов, что позволит ему улучшать качество автомобилей и повышать их безопасность. При этом конфиденциальность владельца не будет нарушена.

Продажа автомобиля будет заключаться, помимо его визуального осмотра, в поручении продавца и покупателя своим е-роботам произвести сделку по согласованной цене. Далее все вопросы расчетов, регистрации и передачи доступа к информационной модели автомобиля роботы проведут без вмешательства человека.

---

## Социальный автопортрет

Сочетание анонимности и аутентичности, предлагаемое концепцией MetaSociety, открывает принципиально важные новые возможности в управлении обществом.

Если смотреть в суть вещей, то основными критериями состояния общества должны быть не общепринятые экономические показатели, не объем инвестиций, и даже не рост зарплаты. Исследования устойчиво показывают, что максимальный процент людей, считающих себя счастливыми, регистрируется далеко не в самых экономически сильных государствах.

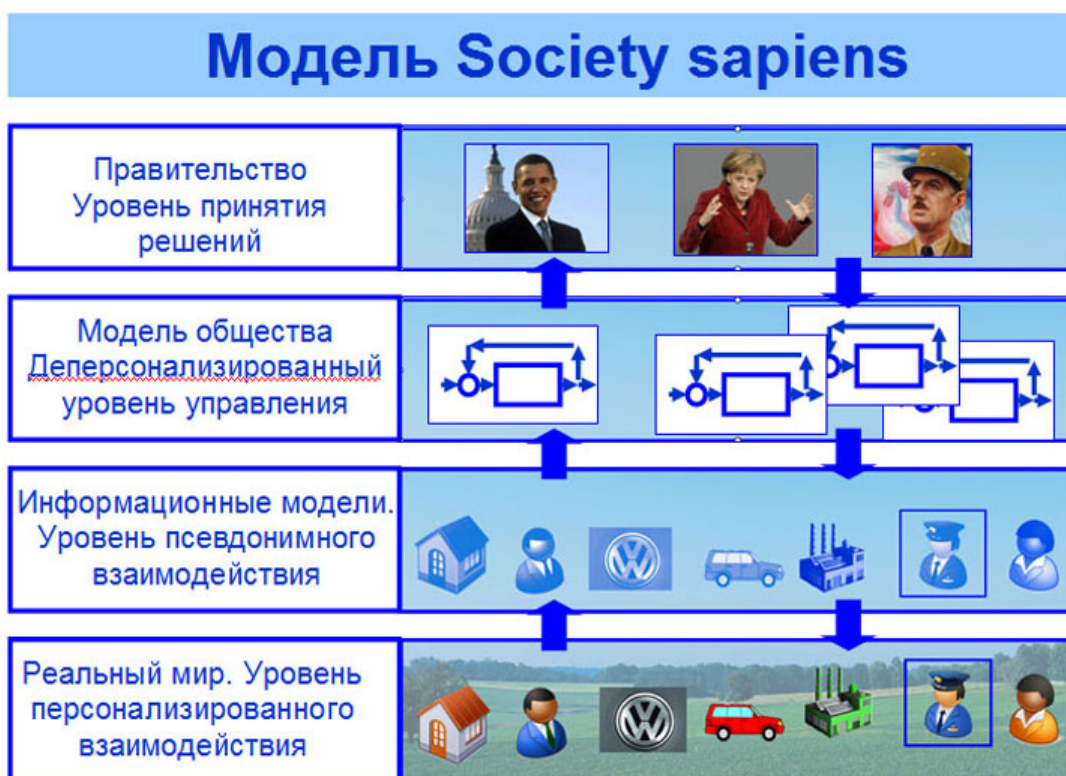
Ведущим критерием состояния общества должна быть социальная удовлетворенность



населения качеством собственной жизни. В основу такого критерия может быть положена "Пирамида потребностей Маслоу": физиологические потребности, безопасность, принадлежность к социальной группе, любовь, уважение, познание, эстетика, самоактуализация.

Управлять можно только тем, что можно измерить. SIS обладает уникальными возможностями оценки социальных параметров состояния общества.

В процессе социального взаимодействия при посредстве SIS естественным образом формируется и поддерживается социальный автопортрет каждого члена общества. Эта информация будет одновременно аутентичной, анонимной, объективной и оперативной.



Это позволяет переориентировать систему государственного управления с финансово-экономических критериев на более важные социальные. Статистическая обработка социологических автопортретов обеспечит органы управления необходимой информацией, дифференцированной по регионам и социальным группам населения.

Социологическая информация и выраженные через SIS волеизъявления граждан являются юридически значимыми, поэтому они могут и должны быть закреплены законодательно как основание для принятия тех или иных управленческих решений. В частности, существенное отклонение социологических показателей ниже определенного порога должно рассматриваться законодательством как безусловная причина отставки правительства либо отдельных министров.

Сегодня высказать свое мнение правительству можно только так:





И получить примерно такой ответ:



SIS - единственный путь избавиться от остающейся до сих пор основной формы диалога общества с государством в форме митингов, восстаний, организации беспорядков, при которых критерием значимости является нанесенный ущерб и количество человеческих жертв.

---

## Секреты интенсивного развития

Когда-то Билл Гейтс сказал: "Если бы автомобиль прогрессировал так же быстро, как компьютер, "Роллс-Ройс" стоил бы сейчас меньше доллара, а на литре бензина можно было бы проехать тысячу километров".

В чем секрет? Почему эта столь сложные отрасли как компьютеры и программирование столь беспрецедентно интенсивно развиваются?

Секретов два.

Первый секрет заключается в том, что в этих сферах возможна очень четкая фиксация достигнутых результатов. Однажды разработанный, проверенный, отлаженный процесс может воспроизводиться многократно, повсеместно и аутентично.

Секрет второй в том, что в компьютерной сфере оказалось возможным постоянное наращивание уровня компонент, из которых строились новые технические и программные конструкции. В компьютерной технике это повышение степени интеграции чипов. Программирование прошло путь от машинных команд через подпрограммы, функции, процедуры, алгоритмические языки к мощным технологиям объектного программирования.

Если же взять социальное взаимодействие, то его принципы, стиль и технологии за последние несколько тысяч лет принципиально не изменились. Каков бы ни был изучен и описан некий общественный процесс, он реализуется людьми, которые неизбежно привносят в него "человеческий фактор": недостаточную компетентность, лень, психологическую неустойчивость, корысть, коррупцию, криминальность. Хорошо работающий процесс может рухнуть при смене одного человека. В разных регионах один и тот же общественный процесс может быть реализован на совершенно разных уровнях.

Фактически большинство общественных процессов теоретически хорошо регламентированы различными законами, инструкциями, контрактами. Каждый закон, каждая инструкция, каждый контракт - это некоторая программа, фиксирующая логику процесса. Проблема в том, что эти законы, инструкции, контракты написаны на мало пригодном для этого естественном языке. В результате возможна их логическая неполнота, различные интерпретации формулировок. В сочетании с "человеческим фактором" при исполнении этих процедур, качество функционирования всей системы социального взаимодействия весьма невысоко.

В реальных процессах большинство шагов жестко регламентированы и лишь в отдельных ситуациях необходимо волевое эмпирическое решение человека. Например, выбор желаемого соотношения между ценой и качеством услуги или изделия.

SIS дает возможность изначально проектировать общественные процессы как профессионально запрограммированные процедуры взаимодействия роботов, которые в отдельных ситуациях обращаются к человеку для принятия волевых решений. Такие процедуры должны создаваться не в процессе политических баталий, а разрабатываться учеными - экономистами, социологами, фиксироваться в программном коде IPL (Interaction Procedure Language).

Создание и накопление отлаженных процедур социального взаимодействия позволит привнести в жизнедеятельность общества те факторы, которые обеспечили столь интенсивное развитие компьютерных технологий.

---

## Цена вопроса

Архитектурно SIS представляет собой специализированную социальную сеть. Разработка социальных сетей глобального масштаба - уже хорошо освоенный интернет-сообществом этап. Такие проекты максимально быстро набирают капитализацию. И это даже при условии, что сегодня социальные сети не обеспечивают юридически значимый документооборот и не выполняют финансовые транзакции.

Поскольку SIS должна прежде всего взять на себя платежные функции (налоги, коммунальные платежи, интернет-торговля), монетизация проекта не представляет проблемы.

Юридически значимые коммуникации, связанные с бизнесом, так же относятся к числу операций, за которые пользователи охотно заплатят.

Создание SIS логично было бы проводить как развитие какой-то из существующих систем, в которой уже есть много абонентов, осуществляющих платежи.

Это может быть аудитория крупного оператора мобильной связи, налоговое ведомство, система сбора коммунальных платежей. В сущности, нужно лишь придать государственный статус идентификации в такой сети и перейти на обезличенные коммуникации внутри сети.

Далее вопрос сводится к разработке процедур для различных видов социального взаимодействия. Интернет-сообщество с этим справится блестяще.

Если для обычных социальных сетей оценка капитализации примерно 100\$ на абонента, то для SIS с учетом значимости выполняемых операций эта оценка должна быть выше.

---

<http://metasociety.com>

[info@metasociety.com](mailto:info@metasociety.com)

**MetaSociety Copyright © 2014**