|  |  |
| --- | --- |
| **Проект** | **Преобразование клиентской базы Сбербанка**  **в национальную платформу цифровизации** |

**Самое большое коммуникационное сообщество**

Клиентская база Сбербанка по России составляет более 110 миллионов физических лиц и более миллиона юридических лиц (по данным сайта sberbank.ru). Это подавляющая часть от всех экономически активных субъектов страны.

Каждый из этих субъектов имеет личный кабинет (ЛК) на сервере Сбербанка, документально идентифицирован, имеет счет и средства на счете, осуществляет те или иные финансовые операции.

**Формирование сервер-серверной среды**

В соответствии с концепцией "Аутентичный Интернет" (АИ), личные кабинеты преобразуются в Персональные Виртуальные Серверы (ПВС). Это чисто программная операция, не требующая ни дополнительного сбора данных, ни очных контактов с пользователями.

Сервер-серверная среда создает принципиально новое стратегическое качество коммуникационных систем – полную алгоритмизацию, роботизацию, регламентацию и протоколирование внутренних процессов взаимодействия серверов (читай – пользователей), исключение неуправляемого "человеческого фактора". Такая система позволяет реализовать любые схемы взаимодействия пользователей, является естественным носителем регламентов взаимодействия (аналогов "умных контрактов").

Протоколирование не означает систему типа "большого брата", так как полная регламентация подразумевает и полное регулирование доступа к информации, осмысленную схему как публикации, так и, если нужно, засекречивания или уничтожения той или иной информации.

Формирование ПВС не вызовет "ударного" скачка нагрузки на ЦОДы Сбербанка, так как преобразование ЛК в серверы может производиться постепенно, поэтапно – по регионам, по категориям пользователей, с пошаговым развитием функционала. Определенное время потребуется и пользователям, чтобы освоиться и активизироваться в новой среде.

**Сетевая идентификация**

В сервер-серверной среде каждый пользователь получает стационарную обезличенную сетевую идентификацию в виде IP-адреса своего персонального сервера.

Сбербанк становится естественным провайдером сетевой идентификации пользователей, хранителем информации о соответствии оффлайновых идентификаторов пользователя (ФИО, номер паспорта, номер телефона, адрес регистрации, биометрия, и т.п.) его сетевому идентификатору (IP). В дальнейшем удостоверенный провайдером (Сбербанком) обезличенный сетевой идентификатор является достаточным для проведения как платежных, так и любых других юридически значимых операций.

**Защита персональных идентификаторов**

Оффлайновые персональные идентификаторы хранятся провайдером вне сетевого доступа, что исключает их массовую утечку. В сетевом пространстве в подавляющем числе ситуаций оффлайновые персональные идентификаторы для электронных коммуникаций не нужны. Их отсутствие в сети является лучшей системной гарантией их безопасности.

Естественно, провайдер идентификации гарантирует определение оффлайновых идентификационных данных пользователя по его сетевым идентификаторам в определенных законом случаях и только представителям правоохранительных органо**в.**

**Взаимодействие с банком**

IP – единственный структурно подтвержденный (в отличие от логинов и паролей) сетевой параметр, пригодный для использования в качестве идентификатора, который практически невозможно подделать, украсть, модифицировать.

Контакт банка с клиентом в новой схеме осуществляется по самому надежному варианту – между двумя стационарными серверами. Пользователь владеет своим сервером, имеет инструменты для эффективного его контроля. Все сообщения ПВС являются юридически значимыми и неотказуемыми. Зоны ответственности пользователя и банка четко определены.

**Защищенные коммуникации**

Любой идентификатор, используемый постоянно и повсеместно, теряет конфиденциальность и открывает возможность нелегитимного агрегирования сетевой активности пользователей. В частности, недопустимо публичное использование IP-адреса ПВС. Иначе на этот адрес может быть организована, например, атака на сервер пользователя.

Провайдер идентификации обеспечивает защиту IP ПВС по технологии Multiport (патент автора). Эта технология предполагает генерацию уникального динамического идентификатора для каждого контакта пользователя. Таким образом блокируется СПАМ, пользователь имеет возможность разорвав контакт стать совершенно недоступным для нежелательного или далее не нужного корреспондента. IP-адрес известен только провайдеру идентификации.

**Беспарольная среда**

Поскольку все серверы имеют единый источник идентификации, пользователи могут взаимодействовать без использования логинов и паролей, используя лишь динамическую паспортизацию. При этом они уверены, что все участники коммуникаций прошли должную идентификацию и в случае юридически значимого конфликта они могут быть персонифицированы перед правоохранительными органами.

Соответственно, для осуществления платежей не потребуется передавать третьему лицу номера карт, счетов, номера телефонов и прочие персональные атрибуты.

**Персональные роботы**

ПВС отличается от персональных архивов данных тем, что кроме данных включает программные модули. В частности – персональных платежных роботов, которые смогут автоматизировать все многочисленные повторяющиеся платежи в самом удобном для пользователя варианте: оплата ЖКХ, связи, кредитов и т.п.

Персональные роботы могут быть разработаны банком, независимыми ИТ-разработчиками или самими пользователями**.**

**Банковская экосистема**

В результате перечисленных мероприятий мы получаем высокозащищенное комфортное пространство для взаимодействия клиентов банка, физических и юридических лиц. В этом пространстве отсутствует трекинг, фишинг, СПАМ, гарантированно и полностью защищены персональные данные.

Подобная сетевая структура в сопоставлении с социальными сетями должна иметь в несколько раз большую капитализацию в расчете на одного абонента, так как абоненты экосистемы имеют документальную идентификацию, счета, деньги на счетах и реальные платежные операции. Можно предположить, что при имеющейся клиентской базе экосистема Сбербанка будет стоить не менее $20 миллиардов.

**Национальный провайдер**

Построенная экосистема банка структурно открыта для подключения других банков и платежных систем с правом или без права первичной идентификации.

Таким образом экосистема Сбербанка должна преобразоваться в единую национальную систему делового взаимодействия, включая все финансовые транзакции населения и бизнеса страны.

**Национальная платформа цифровизации**

Переход к выпуску и распространению Персональных Автономных Серверов (ПАС), которые будут устанавливаться на территории пользователя, позволит построить мощнейшую хорошо защищенную и устойчивую национальную сервер-серверную платформу, которая станет естественной основой для программы цифровизации экономики и управления государств**ом.**

Каждый персональный сервер по сути – информационная и функциональная модель своего владельца. Платформа в целом будет де факто экономической моделью страны с беспрецедентно точной полнотой, статистикой, оперативностью.

В сущности, это единственное концептуальное решение, которое создает инновационную технологическую базу для призывов к цифровизации экономики, в настоящий момент не имеющих осмысленного содержания.

**Радикальные решения АИ**

1. Устранение сетевого неравенства – предоставление серверов физическим лицам, пользователям Интернета
2. Формирование гомогенной сервер-серверной среды коммуникаций с неограниченными возможностями регламентации, автоматизации, протоколирования, управления доступом
3. Использование в сетевом пространстве обезличенной сетевой идентификации вместо персонифицированной оффлайновой, что гарантирует конфиденциальность персональных данных
4. Защита контактов абонента путем предоставления отдельного уникального идентификатора для каждого его корреспондента
5. Использование персонального прокси-сервера для мобильных устройств, обеспечивающего оптимальное сочетание мобильности и стационарности
6. Ликвидация необходимости использования в публичном пространстве уязвимой аутентификации посредством логинов и паролей
7. Решение проблемы надлежащего уведомления
8. Блокировка трекинга, фишинга, СПАМа, фрода, скимминга
9. Разработка централизованной альтернативы блокчейну

**Драматические последствия внедрения АИ**

Внедрение АИ будет иметь драматические последствия для многих ИТ-секторов.

1. Заканчивается эпоха НТТР, HTML, сайты останутся только для неответственных приложений развлекательного характера
2. Финтех-проекты финансового посредничества будут невостребованы
3. В связи с блокировкой трекинга трудные времена наступят у Google, Apple, Facebook и подобных сервисов, торгующих информацией о сетевой активности пользователей
4. Рекламная индустрия перейдет на прямое взаимодействие с пользователями
5. В связи с появлением у пользователей стационарных коммуникационных центров отпадет потребность в многочисленных мессенджерах
6. Будет ликвидирована самая архаичная коммуникационная технология – телефонная нумерация. В связи с этим функцией операторов мобильной связи останется лишь мобильный доступ к Интернету
7. Уйдет из обсуждения тема применения блокчейна и его клонов для задач, не связанных непосредственно с криптовалютными спекуляциями.
8. Финансовые потери от кибермошенничества сократятся на два порядка