От свеклы до финтеха и обратно

Конфиденциальные вычисления активно развиваются в финансовой сфере. Это наконец стало технологически возможным. Произошли регуляторные изменения, а на горизонте маячат колоссальные штрафы за утечку ПДн



Текст
ВАДИМ ФЕРЕНЕЦ,
ОБОЗРЕВАТЕЛЬ **«Б.О»**

Развитие финтеха сейчас в какой-то степени ограничено рамками действующего законодательства, сужающего круг технологий, доступных для использования широким кругом разработчиков банковских сервисов.

В 2018 году в интервью ТАСС **Ольга Скоробогатова,** на тот момент первый заместитель председателя Банка России, заявила: «Вопрос гражданской криптографии — это вопрос создания таких средств защиты, которые, с одной стороны, гарантируют гражданам и экономике безопасность, а с другой — позволяют быстро внедрять новые финансовые решения в стране».

Гражданская криптография (ГК) представляет собой набор методов и технологий, предназначенных для защиты информации и обеспечения конфиденциальности данных в приложениях, предназначенных для повседневного использования. В отличие от военной криптографии, которая используется для защиты секретных данных, ГК ориентирована на защиту личной и коммерческой информации.

Если уйти в сторону от классического шифрования информации, а также криптографии в блокчейне, то технологических новинок из этой сферы, полезных для финтеха, немало. Как правило, многие из них связаны с классом безопасных многосторонних вычислений (SMPC). Как бы ни был молод этот рынок, у него уже накопилась своя история.

Технологическая алхимия

В январе 2008 года первым крупномасштабным практическим кейсом применения SMPC стал аукцион датской сахарной свеклы. В связи с реформой политики на рынке сахара Европейского союза было решено провести электронный двойной аукцион для определения новой рыночной цены сахарной свеклы, где роль аукциониста играла компьютерная программа, реализующая безопасные многосторонние вычисления между местными фермерами и единственным в Дании переработчиком сахарной свеклы компанией Danisco.

Что было важно обеспечить? Поскольку заявки фермеров могли раскрыть их индивидуальное экономическое положение, а также особенности применяемой ими агротехники, необходимо было



сделать так, чтобы Danisco даже гипотетически не могла использовать эти данные в своих интересах. Эксперимент был признан удачным, а технология пошла «в народ».

В ходе сессии «Технологическая алхимия: конфиденциальные вычисления и обмен данными» в рамках Finopolis 2024, организатором которой выступил фонд «Сколково», поддерживающий несколько отечественных стартапов из этой сферы, можно было понять, как далеко проник в бизнес-среду этот раздел криптографии, а также ознакомиться с отечественными кейсами. Один из них был сфокусирован на построении скоринговой межбанковской инфраструктуры на дебетовых счетах. К проекту подключились уже шесть банков, которые могут совместно использовать данные друг друга, кратно увеличивая их аналитический потенциал.

«При этом банки не обмениваются данными между собой, не консолидируют их у третьих сторон и неукоснительно следуют всем коммерческим и регуляторным ограничениям», — рассказал **Петр Емельянов,** генеральный директор финтех-компании Bloomtech.

Сначала доверие, потом бизнес

Директор монетизации данных Т-Банка **Евгений Исупов** добавил: «Сегодня регулятором в лице Банка России отрегулирован лишь обмен данными с бюро кредитных историй. Но и другой информации предостаточно, и ей нужно каким-то образом обмениваться. Тут возникает задача создать между разными участниками программируемое доверие, раз никакого другого пока создать не удается».

Как оказалось, отечественные банкиры сегодня не доверяют ни одному третьему лицу в этой щекотливой сфере. Ровно такая же ситуация сложилась в 2008 году и в Дании. Поэтому между этими двумя событиями много общего, включая технологию, которая легла в основу решения проблемы.

С тех пор несколько изменились драйверы, двигающие инвесторами: в современной России в условиях жесткой конкуренции между финансистами буквально за каждого клиента в ход пошла обработка клиентских данных, содержащих персональные данные и сведения, подпадающие под законодательство о банковской тайне. При этом над бизнесом нависает реальная угроза радикального повышения штрафов за утечку персональных данных, причиной которой являются уязвимости в классических базах данных, а также в решениях по их защите. Вот и пригодился опыт датских фермеров и экспертов «Сколково» в области ГК.

В отличие от технологии криптоанклава, предложенной банком ВТБ в кооперации с учеными из МФТИ и предназначенной для безопасного объединения больших данных с помощью аппаратной доверенной среды выполнения, технология SMPC позволяет на новом уровне решить пресловутую задачу доверия, ведь, как ни крути, у криптоанклава существует оператор в лице ВТБ.

Новая бизнес-суть

«Финтех созрел до того, чтобы обсуждать категорию “данные как актив”, которая может нести в себе некую материальную ценность, а также быть способной увеличивать капитализацию компании», — заявил **Максим Травин,** директор департамента централизованного управления данными Росбанка, в сентябре 2024 года в ходе панельной дискуссии «Современные технологии, методы прогнозирования и анализа в бизнесе» на международном форуме Kazan Digital Week 2024.

Тогда эксперт не стал углубляться ни в бизнес-модели, ни в технологии, однако намекнул: «Многое из сказанного происходит за кадром для тех, кто смотрит на финтех снаружи». И вот через месяц, безусловно, находящийся «внутри финтеха» фонд «Сколково», приоткрыл некоторые тайны венчурных инвесторов, а также инновационных центров крупнейших банков.

Итак, базовый технологический компонент для безопасной работы с чувствительными данными, пусть с определенными ограничениями, о которых предупреждают эксперты компании «КриптоПро», найден и протестирован. Он, как отмечали эксперты в рамках сессии «Технологическая алхимия… », дает практическую возможность создания некоей среды доверия для практически неограниченного круга участников финансового рынка. А вот какие в связи с этим открываются бизнес-перспективы?

По словам Евгения Исупова, Т-Банк начал совместно с дочерней компанией Альфа-Банка и другими крупными игроками пилотный проект, связанный с BNPL-сервисами. Благодаря использованию SMPC-криптопротокола можно оценивать платежную нагрузку, не раскрывая и не передавая сами клиентские данные.

Технологическая суть, понятно, не раскрывается, но, вероятно, используется гомоморфное шифрование, которое позволяет пользователям выполнять вычисления с зашифрованными данными без их предварительного дешифрования. Тем не менее достоверно известно об интересе фонда «Сколково» и других инвесторов к стартапам, создающим на базе этого вида шифрования площадки для электронного голосования, системы борьбы с мошенничеством и социальной инженерией, аналитические медицинские и HR-решения.

О перспективах

«За последние 10 лет во всем мире проинвестировано примерно 800 млн долларов в SMPC. В основном это США, Израиль и Европа», — поделился статистикой технический директор и соучредитель КБ «ТехноСкор» **Сергей Вельц.** А руководитель блока информационных технологий ВЭБ.РФ **Тимур Малин** отметил: «Между технологией и ее внедрением наблюдается огромная пропасть, хотя интерес к ней, безусловно, налицо». Есть нюансы, связанные с регуляторикой, затрудняющей коммерциализацию инноваций и быстрое внедрение разработок в бизнес.

Однако любой венчурный инвестор, связанный с криптографией, помнит, как в 1969 году руководство шифровальной службы Великобритании не приняло шифр RSA в качестве рабочего инструмента из-за «сложности», и он был опубликован в открытой печати только в 1983 году. А вот в 1982 году была создана компания RSA Data Security Inc с многомиллиардными оборотами сегодня. Однако изобретатели шифра RSA не получили ни цента, поскольку основателями компании были совсем другие люди. Поэтому все надеются, что в России подобного казуса не случится. Б.О