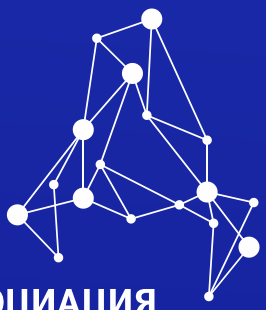


АССОЦИАЦИЯ
БОЛЬШИХ ДАННЫХ

ТЕХНОЛОГИИ ЗАЩИЩЕННОЙ ОБРАБОТКИ ДАННЫХ: ОТ ЗАЩИТЫ ДАННЫХ – К РАЗВИТИЮ ИИ, ПАРТНЕРСКИМ ОТНОШЕНИЯМ И ЭКОСИСТЕМНОЙ ЭКОНОМИКЕ

Москва
2024

СОДЕРЖАНИЕ

РЕЗЮМЕ

Доклад посвящен технологиям защищенной обработки данных (ТЗОД). Этот класс информационных технологий известен достаточно давно и применяется в самых разных сферах. Вместе с тем общее развитие техники и технологий в сочетании с их повсеместным использованием привело к экспоненциальному росту сосредоточенных в руках компаний и государства объемов информации о людях и, как следствие, к увеличению риска утечек персональных данных. Снизить эти риски и повысить доверие граждан к сбору, хранению и использованию такого рода информации как раз и призваны ТЗОД.

С юридической точки зрения ТЗОД — это лишь технические меры защиты. Вместе с тем в ряде ситуаций именно ТЗОД позволяют лучше защитить интересы людей и обеспечить надежное и эффективное соблюдение требований законодательства — в дополнение к таким привычным для юристов действиям, как оформление необходимых локальных документов, получение согласий на обработку персональных данных и заключение NDA. Кроме того, использование ТЗОД дает возможность продемонстрировать добросовестность поведения и благонадежность практик компании в отношении закрепленных в российской нормативной базе принципов обработки данных.

Повышение внимания к ТЗОД — мировая тенденция, поддерживаемая национальными регуляторами в области персональных данных и международными организациями. Развитие отечественных наработок в этой области усиливает позицию России как одной из ведущих технологических держав.

Применение перечисленных в докладе ТЗОД является перспективной, но не очень широко распространенной практикой, поэтому в докладе приводятся рекомендации для тех, кто только приступает к использованию ТЗОД. В частности, содержится анализ того, как выбрать подходящую технологию, каким компаниям для внедрения ТЗОД целесообразно вступать в партнерство, как сформировать эффективную проектную команду, какие сложности могут возникнуть, как их избежать или преодолеть.

В докладе приводится общий обзор ТЗОД и наиболее актуальных видов этих технологий: конфиденциальных вычислений и доверенных сред исполнения, защищенных многосторонних вычислений, федеративного обучения и синтетических данных.

Отдельное внимание в докладе уделено рискам, связанным с обработкой конфиденциальных данных. Изложенная риск-модель описывает варианты атак и предлагает меры по снижению рисков, в том числе за счет комбинированного использования компаниями нескольких ТЗОД.

Заключительная часть доклада посвящена перспективам развития ТЗОД и методикам их использования. Мы рассчитываем на то, что внедрение современных ТЗОД в России окажет важный положительный эффект как на общее состояние защищенности конфиденциальной информации граждан и компаний, так и на уровень экономического роста и развития страны.

ВВЕДЕНИЕ

Массовое проникновение технологий обработки данных практически во все сферы бизнеса привело к экспоненциальному росту объемов информационных потоков и массивов. Обратной стороной этой медали стало стремительное увеличение числа утечек конфиденциальных (в том числе персональных) данных.

Так, по данным компании InfoWatch, в 2023 году количество утечек конфиденциальной информации в мире увеличилось на 61,5% и составило 11 549 инцидентов, в результате которых было скомпрометировано как минимум 47,24 млрд записей персональных данных (ПДн), что в два с лишним раза (на 111,5%) больше, чем годом ранее. При этом, отмечают эксперты InfoWatch, даже такая большая цифра, по всей вероятности, является недооцененной.

В России в 2023 году, согласно данным InfoWatch, наблюдался резкий рост количества утекших персональных данных: их объем составил 1,12 млрд записей, что почти на 60% больше, чем в 2022 году (702 млн записей), причем в более чем 35% случаев прошлогодних утечек ПДн объем украденных данных остался неизвестен.

Роскомнадзор в 2023 году зафиксировал 168 утечек персональных данных, в результате которых в открытый доступ попало более 300 млн записей ПДн.

Несмотря на предпринимаемые усилия, по итогам первой половины 2024 года Россия заняла первое место в мире по количеству слитых в даркнет данных, опередив даже страны с гораздо большим населением, такие как Китай и Индия.

В ближайшие годы нас ожидает массовое внедрение технологий искусственного интеллекта (ИИ). Он будет активно проникать не только в коммерческие структуры и государственные органы, но и в повседневную жизнь граждан. Следовательно, рост объемов обрабатываемых данных ускорится, а сопутствующие риски для граждан, компаний и государства значительно возрастут.

На этом фоне ключевой становится проблема обеспечения дальнейшего развития экономики на основе данных при условии соблюдения приватности граждан и защиты данных. В частности, необходимо сделать безопасной и отвечающей интересам граждан совместную работу организаций, действующих в рамках различных экосистем и партнерских альянсов, в том числе в рамках развития ИИ. Актуальной задачей является поиск оптимального баланса между защитой данных и приватностью граждан с одной стороны и увеличением рисков несогласованного использования данных и возможных утечек с другой.

Ключом к решению этой задачи является применение технологий защищенной обработки данных (ТЗОД). Это относительно новый класс технологий и алгоритмов, защищающих данные на этапе их обработки (в англоязычных источниках для этих технологий используется термин Privacy-Enhancing Technologies, PET). С их помощью можно реализовать различные сценарии защиты данных при работе как внутри компании, так и в публичном облаке, а также при совместной работе с другими партнерами.

Благодаря контролю над данными ТЗОД открывают новые возможности при работе с данными, позволяют развивать новые бизнес-модели, внедрять инновации, решать многие другие задачи, которые требуют обеспечения безопасности данных и приватности пользователей. В то же время ТЗОД — это довольно сложные, не «коробочные» решения, их использование требует экспертизы в различных областях: в криптографии и защите информации, ИТ, законодательстве о персональных данных, аналитике данных и ИИ.

Эксперты прогнозируют бурный рост рынка ТЗОД. Так, компания Gartner относит эти технологии к наиболее значимым трендам и прогнозирует, что около 60% крупных предприятий будут использовать эти технологии к 2025 году. А организация Confidential Computing Consortium, в которую входят крупнейшие ИТ-компании и стартапы в области защиты данных, прогнозирует 30-кратный рост рынка конфиденциальных вычислений — до 50 млрд долл. к 2026 году и затем до 208 млрд долл. к 2032 году.

Цель данного аналитического доклада — способствовать развитию ТЗОД как фундаментальных технологий для защиты данных и для дальнейшего развития экономики на основе данных. В докладе содержится обзор основных технологий, представлены примеры их применения, рассматриваются риски, дается юридическая интерпретация, а также приводятся рекомендации для тех, кто начинает работу с ТЗОД. Надеемся, что доклад позволит устранить пробелы в знаниях участников о работе с ТЗОД и предоставит единый базис для эффективного применения данных перспективных технологий.

ЧАСТЬ 1. ОБЗОР ТЕХНОЛОГИЙ ЗАЩИЩЕННОЙ ОБРАБОТКИ ДАННЫХ

Задача обеспечения сохранности данных при их совместной обработке не нова: эксперты занимаются ею на протяжении нескольких десятилетий. Так, специалисты по статистике и криптографии разработали различные методы анонимизации данных на источниках, позволяющие исключить возможность деанонимизации данных при их передаче и использовании. С ростом требований к детализации обрабатываемых данных и объемов данных, доступных в интернете, исключить деанонимизацию становилось все сложнее. Стали развиваться другие подходы, направленные на защиту данных при их обработке, в их числе — защищенные многосторонние вычисления (Secure Multi-Party Computation), доказательства с нулевым разглашением (Zero-Knowledge Proofs, ZKP), федеративное обучение, гомоморфное шифрование и, наконец, доверенные среды исполнения (Trusted Execution Environments, TEE/ДСИ).

Наиболее актуальные и популярные на сегодня методы защищенной обработки данных можно условно разделить на три группы[1]:

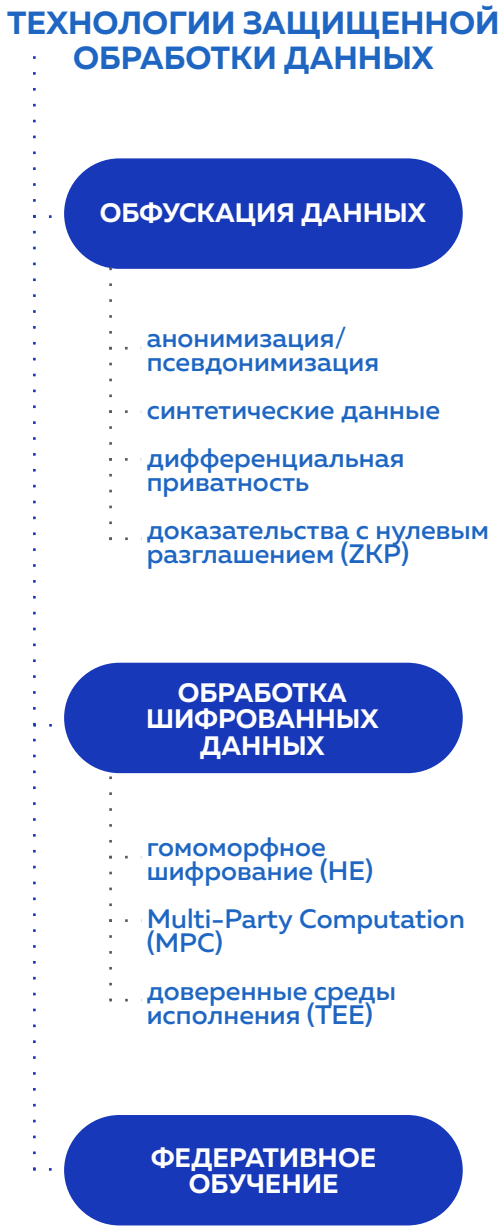
1. Методы обфускации (скрытия) данных.
Использование искаженных данных считается относительно безопасным — их обработка может происходить в открытом виде. К этой группе методов относят:

- методы анонимизации/псевдонимизации;
- методы генерации синтетических данных;
- методы дифференциальной приватности;
- доказательства с нулевым разглашением (ZKP).

2. Обработка шифрованных данных.
При использовании этих методов данные шифруются или преобразуются с использованием математических методов или аппаратной защиты:

- методы гомоморфного шифрования (Homomorphic Encryption, HE);
- методы защищенных многосторонних вычислений (Secure Multi-Party Computation, SMPC);
- доверенные среды исполнения (TEE) (для них также используется термин «конфиденциальные вычисления»).

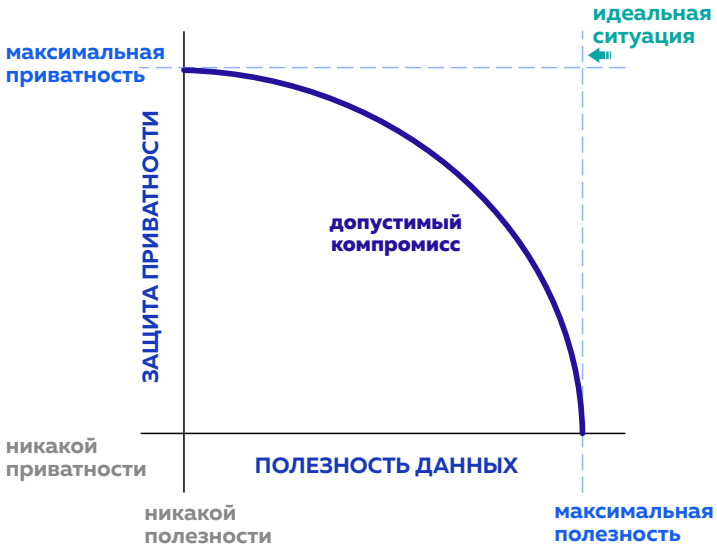
3. Федеративное обучение.
Обработка данных происходит на источниках, при этом между партнерами передаются не сами данные, а обученные на их основе модели.



[1] Использована классификация Организации экономического сотрудничества и развития

Методы обфускации (скрытия) исходных данных

Методы обфускации данных направлены на скрытие персональных данных и другой чувствительной информации при сохранении полезности данных для целей их обработки. Среди основных способов обфускации данных — исключение персональных идентификаторов, добавление в данные различного рандомизированного шума, перемешивание записей и пр. Для таких методов используется соотношение полезности и приватности (Utility vs Privacy): чем больше полезность данных, тем меньше приватность — выше возможность идентификации клиентов по составу данных. Высокого соотношения можно добиться, если при подготовке данных для конкретной задачи сохранять основные полезные для задачи распределения и свойства данных и зашумлять остальные, менее важные.



Для проверки возможности обратной деанонимизации данных (сохранения приватности) используют статистические методы k-anonymity, t-closeness и пр., суть которых — в определении степени неразличимости данных, то есть невозможности отнести данные к отдельному субъекту.[2]

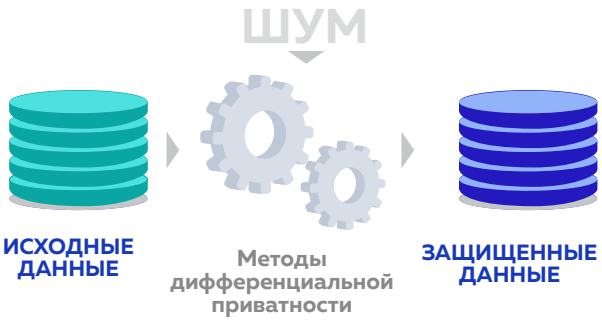
[2] См. например «Как обезличить персональные данные» / «Хабр» (habr.com)

Анонимизация данных — удаление идентифицирующих элементов из данных для исключения риска идентификации субъекта персональных данных (ПДн). В соответствии с определением, анонимизированные данные не считаются персональными, поскольку не могут быть отнесены к отдельному субъекту даже при использовании дополнительных данных. На практике полной анонимизации данных при сохранении их полезности добиться крайне сложно. С развитием ИИ и ростом доступных внешних данных (в том числе данных утечек) отдельные «анонимизированные» данные могут быть с высокой уверенностью отнесены обратно к субъектам ПДн.

Деперсонализация (псевдонимизация, обезличивание) — значительно более легкая форма анонимизации, предполагающая исключение только идентифицирующих атрибутов клиентов без изменения других полей данных. Тем не менее клиент может быть идентифицирован по оставшимся атрибутам с использованием дополнительных наборов данных. Следовательно, деперсонализированные данные остаются персональными. Метод используется для снижения рисков обработки персональных данных внутри организаций, а также при внешней обработке совместно с другими ТЗОД.

Дифференциальная приватность (Differential Privacy) — более сильная форма защиты данных, при которой в данные добавляется дополнительный шум. Это позволяет скрыть детали по отдельным субъектам и тем самым осложнить возможность их обратной идентификации, сохранив при этом полезность датасетов для обработки. Шум, добавляемый в данные, называется бюджетом приватности. Шум может добавляться глобально (после агрегации данных) или локально каждым поставщиком данных. Глобальная модель более точная, но при этом сторонам приходится доверять агрегатору. Глобальная модель была, например, использована для публикации итогов переписи населения в США в 2020 году. Локальные модели используются, в частности, для передачи статистики с устройств пользователей: случайный шум добавляется при подготовке данных на каждом устройстве и взаимно нивелируется при агрегации.

ЧАСТЬ 1. ОБЗОР ТЕХНОЛОГИЙ ЗАЩИЩЕННОЙ ОБРАБОТКИ ДАННЫХ



Синтетические данные — это новые, генерируемые, «искусственные» данные, статистически повторяющие основную структуру и математические распределения в исходных данных. Синтетические данные создаются с использованием моделей, обученных на реальных данных. Результаты вычислений на основе синтетических данных должны быть близки к результатам на основе реальных.

Сложность использования синтетических данных зависит от того, какие именно свойства они должны повторять и с какой степенью достоверности. Также сложность бывает вызвана необходимостью контроля за раскрытием атрибутирующих свойств ПДн.

Популярность синтетических данных растет благодаря их генерации с использованием ИИ (по прогнозам Gartner[3], к 2030 году синтетические данные вытеснят реальные данные в моделях ИИ). Однако совместная (в рамках экосистем и альянсов) обработка синтетических данных затруднена, так как необходимо сопоставлять данные между строками разных партнеров и сохранять кросс-партнерские свойства распределений в данных, что невозможно при независимой генерации данных на стороне каждого партнера.

Среди преимуществ технологий обфускации данных следует отметить относительную простоту реализации, отсутствие необходимости в специальном оборудовании или иных инструментах, отсутствие замедления алгоритмов при работе с данными и управляемый уровень приватности данных.

Недостатками этих технологий являются не стопроцентный уровень приватности (следовательно, сохраняется риск деперсонализации и утечки данных), потенциальное снижение точности работы моделей в результате внесенных в данные искажений, а также имеющаяся в некоторых реализациях возможность для обработчика получить доступ к исходным данным.

[3] Is Synthetic Data the Future of AI?» (gartner.com).

Доказательство с нулевым разглашением

Доказательство с нулевым разглашением (Zero Knowledge Proofs, ZKP) — особый тип защищенной обработки данных. Суть его применения заключается в том, что при использовании данных раскрывается ровно столько информации, сколько нужно для конкретной задачи, избыточное раскрытие не допускается. Например, предоставляется информация о том, что возраст пользователя более 18 лет, но не раскрывается точная дата рождения, или даются сведения о том, что доход более X тыс. руб., но не сообщаются точные суммы дохода.

Классический пример демонстрации технологии — пещера Алибабы. Это пещера в форме кольца, посередине которой находится дверь, открываемая кодовым словом. Пегги хочет доказать Виктору, что она знает кодовое слово для открытия двери, но при этом не хочет называть это слово. Виктор остается перед пещерой, Пегги заходит внутрь через один из входов и должна выйти, используя путь, который назовет Виктор. Действие повторяется несколько раз для достижения требуемого уровня уверенности Виктора.

Так как Виктор случайным образом называет выход, то вероятность того, что Пегги знает код при правильном выходе первый раз, — 50%. Второй раз — 75%, для 10 повторений — 99,99% (1 – 1/(2 [10])) и т. д.

Практические реализации технологии, как правило, подразумевают наличие третьей стороны, которой будут доверять другие участники. Например, предъявление паспорта для подтверждения возраста решает задачу возрастного контроля, но оставляет у проверяющей стороны большое количество избыточной чувствительной информации. В случае использования ZKP пользователь может запустить приложение или веб-сервис третьей стороны, загрузить в него подтверждающие документы, сервис распознает в них дату рождения и по запросу пользователя выдаст шифр, который может быть использован для подтверждения его возраста в других сервисах.

Хотя в данный момент технология ZKP находится на ранних этапах бизнес-применения, тем не менее она активно применяется в таких новых направлениях, как, например, оптимизации работы блокчейн-сетей. Кроме того, ее планируется использовать в системах управления цифровыми идентификаторами и в хранилищах персональных данных (Personal Data Store).

Подробную информацию о ZKP можно найти по ссылкам [4,5].

[4] ZKProof Community Reference

[5] Пример реализации подтверждения возраста в ZKP — Zero-knowledge Proof: Proving age with hash chains (asecuritysite.com).

Гомоморфное шифрование

Рассмотренные выше методы предполагают искажение данных и их обработку в открытом виде. В этом случае хранение и передача данных могут быть защищены техническими средствами (путем шифрования диска и каналов передачи данных), но во время обработки данные, хотя и искаженные, будут доступны обработчику, провайдеру инфраструктуры и прочим участникам процесса. Методы обработки шифрованных данных позволяют сделать такой вариант использования защищенным, избежать раскрытия данных. В отличие от методов обфускации данных, исходные данные не искажаются, а скрываются с помощью шифрования.

Гомоморфное шифрование (Homomorphic Encryption) основано на математических принципах сохранения формы данных при преобразованиях. Например, на этом принципе основывается одна из первых реализаций шифрования с публичным ключом RSA:
если c(x)=(x^e)(mod n) — алгоритм зашифрования,
m1 — первое сообщение,
m2 — второе сообщение,
c1 = (m1^e) (mod n) — шифр от m1
и c2 = (m2^e) (mod n), то произведение двух шифров будет эквивалентно шифру от произведения: c1*c2 = c(m1*m2). Таким образом, операция умножения сообщений может быть выполнена на шифрованных данных. Впрочем, это простейший вариант, а для реальных задач требуются сложные и ресурсоемкие схемы преобразования данных, разрабатываемые отдельно для каждой задачи.

В общем случае владелец данных на своей стороне шифрует их с использованием собственного приватного ключа и передает их обработчику вместе с публичным ключом. Обработчик выполняет на шифрованных данных необходимые вычисления, но при этом итоговый расшифрованный результат может быть получен только с применением приватного ключа

владельца данных. После расшифровки результат будет идентичен результату, полученному при выполнении обработки на базе исходных данных.

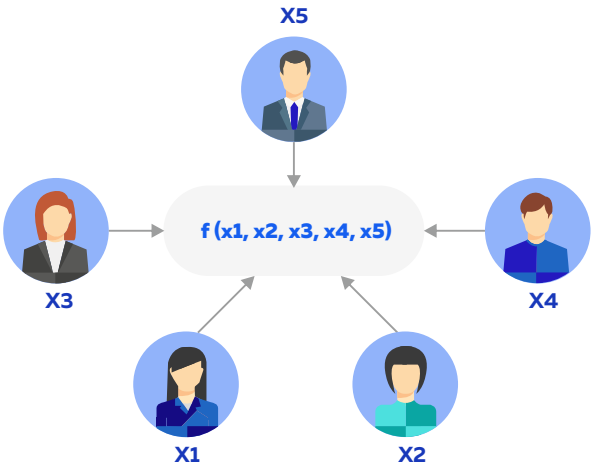
Преимуществами гомоморфного шифрования являются сохранение приватности, защита входных данных партнеров (другие участники процесса не могут получить доступ к исходным данным), защита модели (нет необходимости передавать модель между участниками, при этом обучение и инференс моделей происходят на шифрованных данных) и квантовая криптостойкость (используются алгоритмы криптографии на решетках, которые относятся к квантовостойким).

Среди недостатков — сложность реализации схем гомоморфного шифрования, отсутствие проверки достоверности расчетов и входных данных, сильное замедление расчетов (может достигать тысяч раз) и существенные требования к вычислительным ресурсам (для обработки шифрованной информации потребуется увеличить требуемый объем оперативной памяти до значений, превышающих исходные в десятки, сотни, а то и в тысячи раз).

Защищенные многосторонние вычисления

Методы защищенных многосторонних вычислений (Secure Multi-Party Computation, SMPC) позволяют сторонам производить совместную обработку общих данных, не раскрывая исходные данные друг другу. Большинство реализаций SMPC используют криптографический протокол разделения секретов (Secret Sharing). Основная идея — в том, чтобы разделить вычисления на небольшие части, дать каждому участнику выполнить отдельный набор действий с этими частями, а затем объединить результаты.

Простой классический пример для демонстрации подхода — поиск суммы или среднего значения нескольких (n) чисел, которые находятся у каждого из партнеров, не раскрывающих эти числа друг другу. Для этого каждый партнер делит число на n частей случайным образом и передает каждому другому одну из частей. Затем каждый на своей стороне считает сумму и объявляет итог. Значения суммируются и делятся на количество участников.



Для реальных задач требуются дизайн и тестирование криптографического протокола для каждого отдельного кейса. Задача протокола — произвести нужные вычисления так, чтобы стороны не раскрыли данные друг друга. Протокол требует интенсивного обмена чувствительными данными, поэтому для его реализации необходимы высокая пропускная способность и защищенность сети.

MPC сегодня применяется для аналитики объединенных данных в отраслях, где приватность особенно критична (например, финансы и медицина), а также в антифрод-решениях на основе обработки данных множества партнеров.

Среди преимуществ технологии MPC для машинного обучения и ИИ — сохранение приватности и защита входных данных партнеров, возможность масштабирования протокола на большое количество участников и защищенного обучения моделей на чувствительных данных без раскрытия самих исходных данных. В числе основных недостатков MPC — сложность разработки, тестирования и запуска MPC-протоколов, возможность утечек данных в результате сговора участников или уязвимости протокола, высокая ресурсоемкость вычислений (в десятки и сотни раз больше по сравнению с запуском без MPC) и резкий рост нагрузки на сеть.

Пересечение множеств без их раскрытия (Private Set Intersection, PSI)

Одна из наиболее популярных задач совместной работы с данными — определение общих элементов между несколькими партнерами без раскрытия полных множеств друг другу. Как правило, задача сводится к поиску множества общих (пересекающихся) элементов или к другой сводной аналитике на основе этих данных (например, оценке средних продаж по общим клиентам).

Одной из практических реализаций PSI является использование фильтров Блума. В целом фильтры Блума полезны для быстрого выявления пересечения множеств без их раскрытия. Фильтр Блума — вероятностная структура данных, допускающая ложноположительные срабатывания, при этом позволяющая делать безопасные пересечения множеств без их раскрытия. Пересекая фильтры Блума, можно находить общие элементы множеств без раскрытия остальных. Путем подбора параметров фильтра Блума можно добиться требуемого процента точности — процента ложных срабатываний, элементов, которых на самом деле не было в списке.

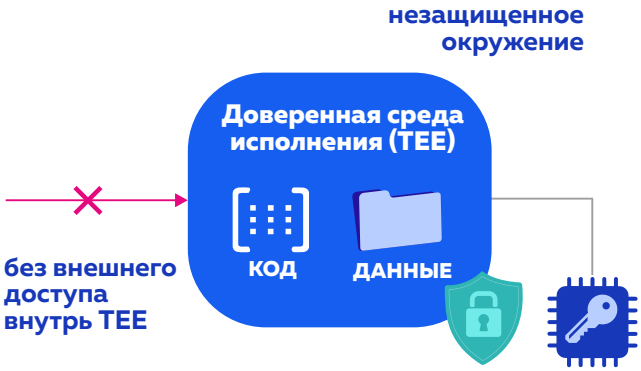
Получение информации без раскрытия выборки (Private Information Retrieval, PIR)

Нередко возникает необходимость скрыть от партнера — поставщика данных, какие именно его данные интересуют получателя. Такая задача возникает, например, в инвестиционной деятельности, где запрос информации от крупных фондов по отдельным компаниям может свидетельствовать об особом интересе к этим компаниям и способен вызвать волну спекуляций их ценными бумагами и другие нежелательные последствия.

Задача, как правило, решается путем запроса избыточного объема данных либо, в крайнем случае, полных баз данных. Однако эти объемы могут быть очень большими, при этом отдающая сторона не всегда готова делиться данными в таких количествах. Инструменты для такого рода обмена минимизируют объем избыточных передаваемых данных, сохраняя, тем не менее, конфиденциальность исходных запросов. Сегодня существует множество реализаций протокола для различных баз данных, эти реализации обладают различными характеристиками производительности и защиты данных[7].

Конфиденциальные вычисления и доверенные среды исполнения

Технология доверенных сред исполнения (Trusted Execution Environment, TEE/ДСИ) основана на использовании изолированных и шифрованных областей памяти, в которых выполняется конфиденциальная обработка данных. Защита информации обеспечивается с использованием секретного аппаратного ключа, как правило, встроенного в процессор при его производстве[7].



При использовании технологии создается своего рода цифровой сейф, который обеспечивает конфиденциальную обработку данных, защищая исходные данные и модель от несанкционированного доступа и выдавая вовне лишь результаты обработки.

[6] Private Information Retrieval and Its Applications: An Introduction, Open Problems, Future Directions

[7] A Technical Analysis of Confidential Computing | Confidential Computing Consortium.

ЧАСТЬ 1. ОБЗОР ТЕХНОЛОГИЙ ЗАЩИЩЕННОЙ ОБРАБОТКИ ДАННЫХ

Современные реализации TEE позволяют не только защитить обрабатываемые данные от просмотра и изменения, но и удостовериться в том, что исполняются лишь те вычисления, которые были согласованы партнерами. Таким образом, данные не могут быть просмотрены, изменены или скопированы, при этом у участников сохраняется контроль над тем, как именно используются их данные. Код внутри TEE также защищен, что позволяет сохранить интеллектуальную собственность партнеров (поскольку у них по-прежнему остается возможность контроля кода до его помещения в TEE и исходящих из TEE данных).

TEE можно объединять в доверенные сети, создавая различные конфигурации конфиденциальных вычислительных кластеров.

На сегодня TEE поддерживаются большинством крупнейших производителей процессоров, в том числе Intel, AMD, NVIDIA, Huawei, ARM. Технологии TEE свободно доступны и на российском рынке. В основе большинства реализаций TEE — встроенный в процессор ключ и дополнительный набор инструкций процессора. Такой подход исключает возможность удаленно «выключить» TEE. Благодаря локальной аттестации TEE можно работать без обращений к серверу производителя, что позволяет добиться полной автономности использования технологии.

TEE обладают целым рядом преимуществ:

·Широкая доступность готовых коммерческих решений на рынке — это наиболее широко применяемая, коммерческая технология защищенной обработки данных.

·Надежная, сквозная защита данных: данные могут быть защищены на всех этапах работы с ними — при хранении, передаче и обработке.

·Безопасность: данные и код остаются защищенными от внешнего доступа, даже если основная система скомпрометирована.

·Целостность кода и данных: данные и код защищены от изменений.

·Аттестация: возможность проверки подлинности TEE (того, что данные загружаются именно в конфиденциальную доверенную среду) и подлинности итоговых результатов вычислений (того, что они получены именно из используемой TEE-среды).

·Низкая дополнительная вычислительная нагрузка: происходит замедление на 10–20%, а не в десятки, сотни и тысячи раз, как при использовании многих других технологий.

·Не требуется адаптация кода приложений, запускаемых в среде TEE.

Впрочем, технология TEE не лишена недостатков:

·Требуются процессоры специальных серий или иное специальное оборудование (как в случае с Huawei Qingtian).

·В некоторых ранних реализациях TEE имеются ограничения на доступные объемы вычислительных ресурсов.

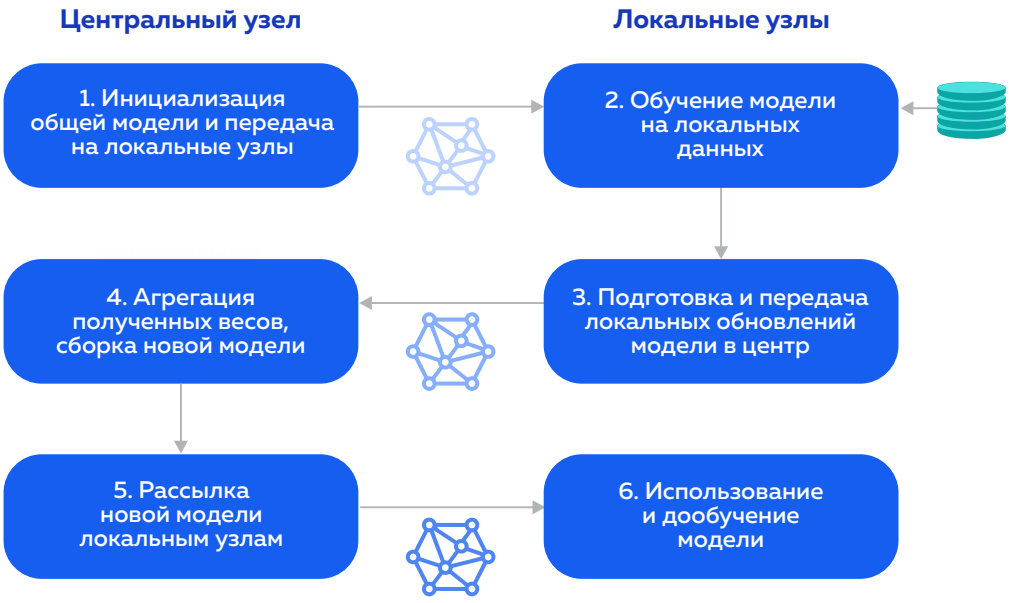
·Необходимо доверять производителю оборудования в отношении защиты данных.

Технология TEE позволяет решать самые разные задачи — от простого выявления пересечения клиентских баз до глубокого машинного обучения. Она широко используется для переноса чувствительных данных и расчетов в публичные облака, для защиты данных внутри организаций и для совместной работы с данными в партнерских альянсах и экосистемах. Подробнее технология TEE с примерами и особенностями применения рассмотрена во второй части доклада.

Федеративное обучение

Технология федеративного обучения (Federated Learning) позволяет сторонам обучать модели машинного обучения на локальных данных, избегая передачи самих данных. Например, веса модели могут параллельно рассчитываться у каждого из участников и затем агрегироваться на центральном узле. Классический пример — дообучение моделей программ-ассистентов на смартфонах, распознавание лиц и пр.

СХЕМА РАБОТЫ ФЕДЕРАТИВНОГО ОБУЧЕНИЯ



Существуют централизованные и децентрализованные модели федеративного обучения. В централизованном варианте обученная модель от каждой стороны передается на центральный узел, где происходит агрегация полученных моделей. В децентрализованном варианте модели передаются и агрегируются между узлами иным образом, без центрального узла.

Главными преимуществами федеративного обучения являются сохранение приватности и защита входных данных партнеров, а также возможность использовать параллельные вычисления, позволяющие перераспределять нагрузку между множеством параллельно работающих процессов.

В качестве главного недостатка этого подхода можно отметить отсутствие защиты модели вычислений: скрипт и обучаемая модель (включая весовые характеристики и параметры градиентов для каждого шага расчета) передаются всем партнерам, в результате чего каждый узел получает доступ ко всем параметрам модели. Среди других недостатков — возможность утечки данных вместе с передаваемыми весами моделей, а также необходимость доверять узлам, так как локальная работа модели и передаваемые параметры могут быть скомпрометированы.

Федеративное обучение рекомендуется использовать совместно с другими технологиями защиты данных — например, с дифференциальной приватностью и TEE. Наиболее широко федеративное обучение используется в масштабных B2C-приложениях, в которых дообучение относительно типовых моделей происходит параллельно на миллионах устройств.

Сравнение методов защищенной обработки данных

Каждая из рассмотренных технологий имеет свои достоинства и недостатки, которые определяют их зоны применения. Эти характеристики отражены в сводной таблице.

	Доверенные среды исполнения (TEE)	Гомоморфное шифрование	Защищенные многосторонние вычисления	Федеративное обучение	Методы обфускации данных (дифференциальная приватность)
Принцип работы	Позволяет проводить аналитику и вычисления на основе данных в безопасной, изолированной области	Обеспечивает возможность проводить аналитику и вычисления на основе зашифрованных данных без их расшифровки	Благодаря разделению на фрагменты позволяет множеству партнеров проводить вычисления на основе общих данных, без раскрытия данных друг другу	Позволяет обучать модели на множестве узлов без передачи самих данных	Позволяет раскрывать и совместно обрабатывать данные без раскрытия чувствительной информации по отдельным субъектам
Какие данные и от кого защищаются	Все данные, помещенные в полностью изолированную среду, без какого-либо внешнего доступа	Обрабатываемые данные защищаются от стороны, выполняющей вычисления	Обрабатываемые данные защищаются от доступа других сторон, участвующих в совместной обработке	Данные, на которых происходит обучение, защищаются от стороны, выполняющей обучение моделей, и от других узлов	Чувствительные данные по отдельным субъектам, для которых проводится аналитика, защищаются от всех участников процесса обработки
Основные кейсы использования	Безопасные вычисления на внешних серверах Безопасные совместные вычисления Безопасные вычисления внутри компаний	Безопасный аутсорсинг вычислений на основе чувствительных данных Безопасный доступ к чувствительным данным	Совместная аналитика на основе чувствительных данных, проводимая несколькими партнерами	Обучение моделей на распределенных данных (без их объединения)	Предотвращение доступа к персональным данным при обработке и публикации статистики и аналитики
На каких этапах защищает данные	При хранении При обработке Результат (возможно, с использованием дополнительных контролей выхода)	При хранении При обработке Результат	При хранении При обработке Результат	При хранении При обработке Результат	При хранении При обработке Результат (с ограничениями)
Преимущества	Широко доступны коммерческие решения Без потери информации Без необходимости переработки моделей Аттестация вычислительных сред Минимальная дополнительная вычислительная нагрузка (10–20%)	Могут работать без потери информации Полное гомоморфное шифрование может поддержать сложные вычисления	Без необходимости в специальном оборудовании Без третьей стороны, которой нужно доверять	Минимальные потери информации	Управляемый уровень потери информации Уровень приватности может быть достоверно оценен Минимальная дополнительная вычислительная нагрузка

продолжение таблицы на следующей странице

	Доверенные среды исполнения (TEE)	Гомоморфное шифрование	Защищенные многосторонние вычисления	Федеративное обучение	Методы обфускации данных (дифференциальная приватность)
Текущие ограничения и недостатки	Ограничения на доступные ресурсы в некоторых ранних реализациях	Огромная дополнительная вычислительная нагрузка (увеличение вычислительных ресурсов на 1000% и более) Не все вычисления могут быть реализованы Необходимость разработки моделей для каждого кейса	Огромная дополнительная нагрузка на вычислительные мощности (увеличение вычислительных ресурсов на 1000% и более) и на сеть между партнерами Сложная разработка и проверка протокола для каждого кейса	Риски утечки данных вместе с моделями Инверсия моделей и утечки данных партнеров Атаки могут использовать уязвимости реализации	Точность анализа и моделей находится в обратной зависимости от степени защиты данных Требует высокого уровня экспертизы для оценки и управления уровнем приватности
Уровень готовности технологии	Коммерческое использование, широкое применение	Коммерческое использование, узкоспециализированное применение	Отдельные реализации в промышленной эксплуатации, более сложные — в пилотных	Коммерческое использование, широкое применение	Коммерческое использование
Требуемые специальные ресурсы и компетенции	Оборудование с поддержкой TEE	Специалисты для разработки криптографических протоколов для каждого конкретного кейса	Специалисты для разработки криптографического протокола для каждого конкретного кейса Широкие и защищенные каналы передачи данных	Компетенции в области распределенных вычислений и управления распределенной сетью	Специалисты для оценки и управления параметрами приватности, разработки производных протоколов защиты данных

ТЗОД с точки зрения законодательства РФ

Использование ТЗОД позволяет обеспечить повышенный уровень защиты персональных данных, закладывая эти гарантии на уровне архитектуры информационных систем или моделей взаимодействия участников. Применяя ТЗОД, можно, не теряя эффективности, снизить объем обрабатываемых персональных данных или уменьшить перечень лиц, имеющих к ним доступ. Кроме того, использование ТЗОД оператором обработки данных может повысить доверие к нему со стороны субъектов ПДн.

Законодательство РФ не регулирует ТЗОД сами по себе, поэтому с юридической точки зрения следует рассматривать каждый случай их применения в отдельности. Использование ТЗОД относится к лучшим практикам — в частности, в области обработки персональных данных (так называемая проектируемая конфиденциальность, Privacy by design). Но необходимо учитывать, что в большинстве случаев использование ТЗОД не приводит к изменению статуса обрабатываемой информации как «персональных данных», поэтому важно продолжать соблюдать требования действующего законодательства в этой сфере. Также нельзя исключать вероятность сбоя или взлома ТЗОД, важно заранее оценивать риски их внедрения и принимать меры по их снижению.

При реализации международных проектов или проектов, в которых данные могут передаваться за рубеж, важно учитывать, что юридическая квалификация ТЗОД и последствий их применения может отличаться от страны к стране.

ТЗОД в мире

Современный цифровой ландшафт в большинстве стран продолжает активно развиваться, что делает потребность в надежных и адаптируемых безопасных технологиях обработки данных все более насущной. Государственные субъекты, негосударственные и международные организации все больше поднимают вопрос о целесообразности или необходимости применения ТЗОД для защиты данных.

Организация Объединенных Наций в 2023 году подготовила Руководство ООН по технологиям повышения конфиденциальности для официальной статистики[8], в котором основное внимание уделено анализу и распространению конфиденциальных данных. В нем среди прочего предлагаются рекомендации по проведению анализа без открытой передачи данных, объединению данных между сторонами, имеющими конфликт интересов, и по обеспечению гарантий правильности использования данных с учетом правовых требований. Согласно Руководству, ТЗОД помогают обеспечить безопасный жизненный цикл данных начиная от конфиденциальности их ввода до конфиденциальности вывода, выступая гарантом доверия субъектов данных. Также приводятся примеры использования ТЗОД из опыта стран — членов ООН.

На уровне государств можно отметить Национальную стратегию США на 2023 год по развитию обмена данными и аналитики с сохранением конфиденциальности[9], направленную на развитие и ускорение внедрения ТЗОД, наращивание экспертного потенциала и содействие международному сотрудничеству, а также вышедшую в 2023 году в Китае Белую книгу блокчейна[10], где упоминается применение TEE при использовании блокчейна. Хорошо проработанные рекомендации по использованию ТЗОД выпустил также регулятор Великобритании (ICO).[11]

Европейское агентство по сетевой и информационной безопасности (The European Union Agency for Cybersecurity) в ходе своей работы регулярно публикует отчеты и обзоры, посвященные ТЗОД, — например, подготовленные в 2016 и 2017 годах обзоры «Матрица элементов управления PET» ("PETs controls matrix") и «Инструмент по управлению знаниями и оценке зрелости технологий повышения конфиденциальности» ("A tool on Privacy Enhancing Technologies (PETs) knowledge management and maturity assessment"), которые описывают систематический подход к оценке инструментов конфиденциальности и зрелости применяемых технологий[12]. Организация экономического сотрудничества и развития также выпустила в 2023 году обзор различных ТЗОД.[13]

Применять ТЗОД рекомендует и Международная организация по стандартизации (ISO) — в частности, в стандартах ISO 12812–1:2017 «Основные банковские операции. Мобильные финансовые услуги» ("Core banking — Mobile financial services") и ISO/IEC 27553–1:2022 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Требования безопасности и конфиденциальности для аутентификации с использованием биометрии на мобильных устройствах» ("Information security, cybersecurity and privacy protection — Security and privacy requirements for authentication using biometrics on mobile devices").

Исследования в области ТЗОД проводятся и в научной сфере. Так, согласно исследованию, проведенному в Канаде[14] , внедрение ТЗОД малыми и средними предприятиями обусловлено технологическими, экологическими, организационными и управленческими факторами. Было обнаружено, что намерение внедрить ТЗОД оказывает положительное влияние на эффективность деятельности компаний.

Сегодня ТЗОД используются за рубежом на финансовом рынке, в сфере медицинских услуг, в государственном управлении и ряде других областей. Этот опыт можно и нужно учитывать при разработке отечественных решений.

8 The United Nations Guide on Privacy-Enhancing Technologies for Official Statistics.

9 National Strategy to Advance Privacy-Preserving Data Sharing and Analytics.

10 White Paper on Blockchain (2023) |China Academy of Information and Communications Technology.

11 Privacy-enhancing technologies (PETs) | ICO.

12 PETs controls matrix - A systematic approach for assessing online and mobile privacy tools ENISA (europa.eu); —Privacy Enhancing Technologies: Evolution and State of the Art ENISA (europa.eu).

13 Emerging privacy-enhancing technologies | OECD.

14 Privacy enhancing technology adoption and its impact on SMEs performance | Semantic Scholar.

Рекомендации по началу использования ТЗОД

Для выбора наиболее подходящей технологии защищенной обработки данных можно использовать приведенную выше таблицу сравнения технологий. В ней перечислены типовые сценарии использования технологии, указаны риски и ограничения технологии, требуемые ресурсы и квалификация. Подробнее с выбранной технологией можно ознакомиться в соответствующих частях доклада.

Для реализации сценариев совместной работы с данными можно использовать следующий фреймворк. На первом шаге партнеры (в приведенном примере это банк и ретейлер) описывают свои данные, на основе чего формируются сценарии-кандидаты на основе общих данных, интересные каждой из сторон. На втором шаге каждый сценарий прорабатывается с учетом требований к данным, инструментам, ожидаемым результатам, рискам и средствам управления ими.

ШАГ 1. Совместный поиск возможностей дата-партнерств

	БАНК	РЕТЕЙЛЕР
Уникальные ценные данные	Транзакционные данные по всем мерчантам (онлайн и офлайн) Точные персональные данные Данные о доходе и финансовом состоянии клиентов История кредитования, рисковые оценки	Содержание чеков: данные о покупках конкретных товаров и категорий Аналитические данные о составе семьи, детях, домашних животных и пр. Данные о ценовой чувствительности и склонности к промопредложениям Ретейл-медиа площадка и данные
Потребности/ гэпы в данных	Содержание покупок, т.к. просто по типу мерчанта и размеру чека сложно делать какие-то выводы о клиенте для персонализации предложений Данные о доходах/остатках на счетах могут быть неполными, т.к. клиенты пользуются также другими банками Фактические адреса проживания клиентов часто отличаются от прописки	Видят только свои покупки - могут не видеть целые категории потребления, покупаемые в других сетях Данные о доходах клиентов
Возможности партнерств	Развитие кешбэк-сервисов: рекомендации категорий для кешбэка, актуальных для конкретного клиента на основе данных ретейлера Уточнение модели дохода клиентов на основе поведенческого профиля ретейлера Развитие lifestyle-продуктов банка на основе данных ретейлера Таргетированные размещения в ретейл-медиа сетях ретейлера	Аналитика «доли в кошельке» ретейлера по клиентам банка Аналитика для развития онлайн-канала

ШАГ 2. Проработка кейса дата-партнерств

Кейс 1. Развитие кешбэк-сервисов банка на основе данных ретейла

Компания, разработчик, модели	БАНК(+)	РЕТЕЙЛЕР
Мэтчинг данных	Мэтчинг по номеру телефона (хэшировано) с использованием фильтров Блума Только клиенты банка с согласиями на обработку	
Требуемые данные	Текущая модель и данные для кешбэк-сервисов	Покупки по категориям в рублях, штуках помесячно Доля продаж по промо в категориях
Гипотеза	Прирост качества модели на X% Повышение конверсии на Y%	
Способ проверки	Проведение тестовой кампании Проверка на ретроданных	
Риски	Утечка данных Обработка без соответствующих согласий	
Инструменты снижения рисков	Конфиденциальные вычисления PSI для пересечения аудиторий Проверка согласий пользователя Расчет в контуре банка Тестирование на ограниченной выборке	

Наши рекомендации по практической реализации кейсов следующие:

1. Не стоит ожидать, что эффект будет достигнут с первого раза, необходимо рассчитывать на три-пять итераций.

2. В проекте над кейсом должна работать команда, включающая представителей каждого из партнеров. Это позволит использовать отраслевые знания и накопленный опыт работы с данными каждого участника.

3. Разрабатывать модели на основе общих данных может любая из сторон. Тем не менее рекомендуется вовлекать в нее специалистов каждой стороны, поскольку здесь важно знание нюансов как самих данных, так и методов их применения.

4. Следует использовать ограниченную песочницу, позволяющую проводить быстрые и безопасные эксперименты с обезличенными данными.

5. До начала реализации кейсов нужно обсудить с юридической службой аспекты необходимой юридической конструкции для запуска в случае успеха теста, а со службой информационной безопасности — целевые инструменты защиты данных.

6. После достижения и подтверждения эффекта можно внедрять целевые решения для технического обмена данными, юридические решения и средства защиты информации. Полезно определить целевые SLA для данных каждого из партнеров.

7. Необходимо проводить регулярный мониторинг качества работы моделей на общих данных и использовать общую среду экспериментов для анализа отклонения и развития моделей.

ЧАСТЬ 1. ОБЗОР ТЕХНОЛОГИЙ ЗАЩИЩЕННОЙ ОБРАБОТКИ ДАННЫХ

Общая риск-модель

В эпоху больших данных защита конфиденциальной информации не может быть оценена «двоично» — либо данные защищены абсолютно, либо вообще не защищены. Более правильный подход состоит в том, чтобы оценивать вероятность успешной атаки, в результате которой конфиденциальные данные будут раскрыты третьим лицам.

Риск деобезличивания (повторной идентификации) оценивается как вероятность успешной атаки. Такой количественный показатель риска является относительным (поскольку зависит от предположений, сделанных при расчете), тем не менее он позволяет оценить эффективность предлагаемой защиты и перейти от декларативной безопасности данных к фактической.

Общий риск, связанный с обработкой конфиденциальных данных, представляет собой произведение двух составляющих — контекстного риска (то есть риска среды, в которой данные собираются, управляются и передаются) и риска данных (риска раскрытия конфиденциальной информации, непосредственно связанного с самим набором данных).

Минимизировать риск данных, как и контекстного риска, до нулевых значений нельзя, поскольку существуют неконтролируемые события, наступление которых может оцениваться только вероятностно. Кроме того, при повышении уровня защищенности данных эти данные становятся бесполезными, а полностью полезные данные оказываются незащищенными.

ТЕКУЩАЯ РИСК-МЕТОДИКА АССОЦИАЦИИ БОЛЬШИХ ДАННЫХ

Свой вариант риск-модели предлагает Ассоциация больших данных. Разработанная нами риск-модель позволяет оценить вероятность повторной идентификации (соотнесения записи в обезличенном наборе с конкретным физическим лицом) при обработке обезличенных данных и, основываясь на этом, принять решение об используемых средствах защиты и способах обработки данных.

Построение безопасной системы обработки обезличенных данных с использованием риск-модели требует ясного понимания целей бизнес-кейса. Схема защиты, как и адаптированная риск-модель (фактически составляющая часть модели угроз), должна строиться в расчете на конкретный сценарий использования данных.

Основной подход к количественной оценке вероятности повторной идентификации заключается в разложении на множители вероятности контекстных рисков и вероятности по рискам данных. Модель включает в себя отдельные формулы для каждого семейства методов: организационных и оперативно-технических, криптографических, методов псевдонимизации, классического обезличивания (анонимизации), конфиденциальных вычислений, статистических методов и машинного обучения. Предложенная модель может стать основой риск-ориентированного регулирования обезличенных данных в России.

Перспективы развития ТЗОД

ТЗОД, в частности конфиденциальные вычисления, призваны защитить данные компаний и пользователей, что позволит значительно снизить риски их использования в условиях развития новых технологий, таких как ИИ, блокчейн, облачные вычисления, а также будет способствовать совместной работе компаний, государственных и научных организаций.

С использованием ТЗОД обработка данных как внутри компаний, так и за их пределами станет более защищенной, и, как следствие, уменьшится количество утечек данных.

Применение ТЗОД сделает более безопасным использование ИИ в крупных компаниях, что откроет новый этап развития генеративного ИИ с использованием массивов чувствительных корпоративных данных.

Вычисления в облаках станут защищенными, и компании смогут продолжить перенос данных и расчетов в облачные сервисы, таким образом повышая скорость разработки и масштабирования решений и снижая затраты.

Использование ТЗОД будет способствовать сотрудничеству различных организаций, в том числе в целях улучшения инновационной деятельности, совершенствования государственных сервисов, развития медицинской сферы, снижения мошенничества, а также решению других важнейших задач на основе данных.

Благодаря сохранению контроля над данными компании смогут создавать различные альянсы, монетизировать свои данные и улучшать клиентский опыт.

Применение ТЗОД позволит работать с данными как с активом и будет способствовать развитию рынка данных и сервисов на их основе.

Технологии защищенной обработки данных — недостающий элемент для решения задач защиты данных, развития цивилизованного рынка данных, становления новых форм кооперации и внедрения новых технологий. Их широкое распространение имеет огромный экономический потенциал и является стратегически важным для дальнейшего развития экономики на основе данных.

Об авторах доклада

АЛЕКСЕЙ НЕЙМАН
Исполнительный директор
Ассоциации больших данных.
Head of FIT Academy of Russia.
Master of Data Science.
CDMP, PMP

АЛЕКСЕЙ МУНТЯН
Генеральный директор Privacy Advocates.
Внешний Data Protection Officer
в нескольких транснациональных холдингах.
Соучредитель в Regional Privacy
Professionals Association - RPPA.pro
Сопредседатель Privacy & Legal Innovation
и кластера РАЭК

АРТЁМ АЛЕКСЕЕВ
Управляющий партнер
Aggregion

ДЕНИС БЕЗРУКОВ
CTO & co-founder of Aggregion.
Co-founder of SuperProtocol

АЛЕКСАНДР ПАРТИН
Адвокат, Партнер
Privacy Advocates.
Соучредитель РППА.Офис.
Сопредседатель
Privacy & Legal Innovation
кластера РАЭК.
CIPP/E, CIPM

ЮЛИЯ ПОСТОЛ
Юрист.
Специалист по праву
цифровых платформ,
персональным данным
и управлению ИИ.
Магистр НИУ ВШЭ

ВАЛЕРИЙ ХВАТОВ
Специалист по кибербезопасности
и распределенным вычислениям.
CTO DGT Network

Редакторы доклада

ЖАННА ПОКРОВСКАЯ
Руководитель пресс-службы
Ассоциации больших данных

АЛИЯ ТРУНАЕВА
PR-менеджер
Ассоциации больших данных

Ассоциация больших данных

Основная цель Ассоциации больших данных — создание условий для развития технологий и продуктов в сфере больших данных в России.

Сегодня членами АБД являются: Яндекс, VK, Сбербанк, Газпромбанк, Т-Банк, Россельхозбанк, МегаФон, Ростелеком, билайн, МТС, Аналитический центр при Правительстве РФ, Банк ВТБ, Авито и Центр стратегических разработок.

Подробнее об АБД и наших проектах можно узнать в Альманахе.

Privacy Advocates

С 2008 года помогаем клиентам в обеспечении комплаенса по персональным данным, проактивном управлении privacy-рисками и эффективном прохождении надзорных проверок, в том числе по утечкам данных. Специализируемся на аутсорсинге функций лица, ответственного за обработку персональных данных (DPO).

Основа нашей команды – компетентные и опытные privacy-специалисты различных компаний.

Aggregion

С 2019 года разрабатываем решения в области конфиденциальных вычислений и распределенной обработки данных.

Среди клиентов — крупнейшие телеком-операторы, банки, ритейлеры и экосистемы.

Основной продукт компании — платформа децентрализованных конфиденциальных вычислений. Платформа позволяет автоматизировать весь цикл работы с данными, делая совместную работу с данными и конфиденциальные вычисления доступными для широкого применения. Платформа получила престижные награды от Microsoft, Intel и других вендоров.

АССОЦИАЦИЯ БОЛЬШИХ ДАННЫХ

www.rubda.ru

Адрес: Москва,
Пресненская набережная, 10с2

+7 (495) 252-72-60
info@rubda.ru