ОГЛАВЛЕНИЕ

ТЕМ ВРЕМЕНЕМ НА НАС НАДВИГАЮТСЯ ТЕХНОЛОГИИ «ГЛУБОКИХ ФЕЙКОВ» (DEEP FAKE). Сейчас нейронные сети позволяют сгенерировать любое видео. Обучившись на некотором количестве настоящих видеозаписей с каким-то человеком, нейронная сеть создаст полностью фальшивое видео со звуком, неотличимое от настоящего, где заданный персонаж будет делать и говорить то, что нужно создателям фейка.

Использование этой технологии в промышленном масштабе (примерно в 2021–2022 годах) приведёт ко второму появлению на больших экранах популярных уже умерших актёров (или вообще несуществующих, синтезированных с нуля). Подобная «нежить», которую невозможно отличить от настоящих людей, заполонит экраны: с вами так будут общаться виртуальные помощники, сотрудники контакт-центров, продавцы, стюардессы, консультанты торгового зала, преподаватели и руководители.

Ну и, конечно, специалисты по компромату, шантажу, вымогательству и фишингу также начнут активно использовать эти великолепные возможности для создания иллюзий в составе своих сценариев вымогательства и разводки.

Машина времени уже включена

Как уже не раз было сказано выше, камеры позволяют анализировать не только отдельного стоящего рядом человека, но и искать лица в толпе, распознавать походку, фигуру.

Можно автоматически распознать **всех**, кто был на улице, в вагоне метро, на митинге, всех, кто был на каком-то событии (свадьбе, конференции и т. д.). Далее система распознавания может *атрибутировать* лица, то есть добавить личные данные (Ф. И. О., адрес, номер телефона и т. п.).

Эти данные не разовые, они *ретроспективные*, то есть накапливаются годами со всех сотен тысяч камер, установленных в каждом мегаполисе или городе-миллионнике.

Хранение данных сейчас обходится очень дёшево, так что в базах данных оседают полные сведения о том, кто куда ходил и что делал на улице, в общественных местах, в транспорте, — за каждый день, каждый час и каждую минуту в течение уже нескольких лет.

Если по каким-то причинам правоохранителям или спецслужбам, например, нужно посмотреть, что было в Петербурге 16 февраля в 14 часов 2019 года возле дальнего от центра входа в метро

на станции «Чёрная речка» или в Москве 22 апреля 2020 года в 17:30 у входа с Брянской улицы в торговый центр «Европейский», — пожалуйста, такие видеоданные есть, причём у многих владельцев камер (полиция, мэрия, администрация метро, владельцы ТЦ и т. п.).

По сути, создана машина времени для возврата в любой момент прошлого в любой точке пространства (пока в крупных городах).

Эта машина времени даёт её владельцам общую картину любого момента в прошлом, чёткую и объёмную, в цвете, в разрешении Full HD и, по сути, в 3D (потому что почти всегда и везде есть съёмка нужной сцены с нескольких камер), а в последнее время и со звуком. Камеры дают картинку с разных ракурсов, её можно «крутить», увеличивать, даже прослушивать звук.

Основные выводы относительно видеоследа

ВИДЕОСЛЕД СЕЙЧАС ВЫ ОСТАВЛЯЕТЕ ВСЕГДА. Нужно внимательно следить за тем, кто и как вас снимает, не давать шансов будущим насмешникам или шантажистам (не строить глупые рожи, не сниматься полураздетыми или пьяными, с бутылкой или «косяком» в руке, не выкрикивать глупости, оскорбления, матерщину на камеру, не сниматься в нехорошей компании, не обниматься с теми, кто потом вызовет раздражение подруги или друга).

И уж тем более нужно следить за тем, куда и зачем вы **САМИ** выкладываете свои фото и видео.

ПРИ РАЗБОРЕ ИНЦИДЕНТОВ ВИДЕОСЛЕД ИСПОЛЬЗУЮТ В ПЕРВУЮ ОЧЕРЕДЬ. Надо помнить, что сейчас в случае серьёзного конфликта, который привёл к приводу в полицию и/или возбуждению уголовного дела, судить о том, кто был зачинщиком конфликта, правоохранительные органы будут в основном не со слов свидетелей, а по видео с камер.

Тот, кто первый махнул рукой, толкнул, совершил агрессивное действие (что видно на видео), и будет, скорее всего, признан инициатором. А вот слова, оскорбления, угрозы, гримасы, издёвки, провоцирующие конфликт, останутся без внимания.

Поэтому в случае развития конфликтной ситуации в общественном месте стоит прежде всего очень внимательно оглядеться и найти камеры вокруг. И вести себя соответственно — осмотрительно и сдержанно.

СОЦИАЛЬНЫЕ СЕТИ: ИДЕАЛЬНАЯ СРЕДА ДЛЯ ОСТАВЛЕНИЯ СЛЕДОВ

ЧТО ЗНАЮТ О НАС ПЛАТФОРМЫ: СОЦСЕТИ, МЕССЕНДЖЕРЫ, ВИДЕОХОСТИНГИ. Современный Интернет не просто россыпь миллионов сайтов и миллиардов страниц. В первую очередь это *платформы*. Платформа — это гигантский интернет-сервис, аккумулирующий десятки или сотни миллионов пользователей: «ВКонтакте», Facebook, Google, Mail.ru, YouTube, Twitter, «Яндекс». Платформы — это поисковики, социальные сети, публичные почты, фотохостинги, видеохостинги, мессенджеры и т. д.

Можно с уверенностью сказать, что 80–90 % времени в Интернете современный пользователь проводит не в «дикой» сети, не на сайтах мелких сайтовладельцев, а на тех или иных огромных цифровых платформах.

У платформ есть владельцы, которые заинтересованы в заработке на своей аудитории. Чем больше аудитория, тем больше денег на ней можно заработать. Именно поэтому большинство самых крупных платформ бесплатны — чтобы привлечь как можно большую аудиторию. Как уже говорилось выше, если вы используете бесплатный сервис, то товар — это вы.

На чём же зарабатывают владельцы платформ? На наших пользовательских данных — перепродаже или использовании их в рекламе.

А самые интимные и точные данные собирают о нас именно социальные сети — потому что мы сами их отдаём.

Раньше, в эпоху мессенджера ICQ и почтовых серверов POP3, логи (журналы) общения и переписки хранились только на компьютере у пользователя. И если он их не переносил с устройства на устройство при каждой смене компьютера, то они естественным образом иногда обнулялись. А сейчас в облаке, то есть в сетевых архивах на почтовых серверах и серверах мессенджеров, постоянно **хранится вся переписка**.

Поэтому при любой *компрометации облачного архива* (утечка, кража, нечаянная индексация поисковиком, хакерская атака, ошибка в правах доступа) он становится доступен практически всем. В результате за считаные секунды можно найти в поисковиках всё, что вы писали когда-либо в данном сервисе.

Можно найти, кого вы критиковали в разговорах с третьими лицами, с кем вы общались и кому назначали встречи, с кем и куда одновременно ездили по находящимся в почте билетам, все тексты и данные ваших документов, которые вы кому-то когда-то передавали.

Но если владельцы социальной сети всё-таки имеют свою внутреннюю политику обращения с персональными данными пользователей (хотя мы не всегда знаем, какую именно), имеют свои внутренние службы информационной безопасности и всё-таки придерживаются закона и опасаются контролирующих органов (Роскомнадзора, Федеральной антимонопольной службы, Министерства связи, Роспотребнадзора и прокуратуры), то **пользователи** социальной сети, все эти ваши «друзья», вообще ничем не ограничены в отношении ваших данных — ни этическими ограничениями, ни законом.

«Друзья»: без любви, уважения и обязательств

До сих пор у многих пользователей социальных сетей есть иллюзия, что они пишут для узкого круга друзей. Это огромное заблуждение.

Всё, что вы пишете и размещаете в социальных сетях, — дискуссии и комментарии, фото и видео на фотохостингах и видео в YouTube — видит, читает, пересылает и, возможно, сохраняет, как принято говорить у юристов, **неопределённый круг лиц** — «друзей», подписчиков, «френдов», «фолловеров» и т. п.

Facebook, например, вставляет ваши сообщения и комментарии в так называемые ленты не только ваших подписчиков и «друзей», но и кого угодно. То есть «рассыпает» их по публичному пространству по своему усмотрению.

Надо понимать, что даже ваши друзья и подписчики (люди, обычно мало вам знакомые, не испытывающие к вам дружеских чувств) не имеют никаких обязательств по сохранению в тайне ваших интимных сведений или нечаянных откровений.

Известно множество случаев, когда «френды» использовали откровенное общение в социальных сетях для того, чтобы организовать травлю, высмеять, переслать комментарии или фото третьим лицам и т. п.

> **ПРИМЕР.** В Рунете есть целое движение «разоблачителей», которые вступают в социальных сетях в переписку с наивными и не очень разборчивыми в знакомствах девушками (под фальшивыми именами, естественно), обещая свидания с видными и богатыми парнями или работу моделью. Они постепенно убеждают девушек прислать откровенные фото, а затем выкладывают их в Сеть на специальных сайтах — «досках позора»

(один из них, уже заблокированный Роскомнадзором, — CheckYou, он же Checkgirls, и др.). Это делается либо для привлечения посетителей на такие сайты (доступ платный), либо вообще для шантажа фигуранток (требование денег за то, чтобы снять фотографии с сайта).

Более того, это верно и для закрытых групп или постов «только для друзей», ведь если «друзей» у вас в закрытом списке или группе больше 30–40 человек, наверняка половину из них вы даже не знаете.

«Подзамочные» записи на самом деле публичны

Обычно круг подписанных на «подзамочные» сообщения или на закрытую группу всё равно широк и включает людей, как минимум равнодушных к вам, а часто и враждебных. Вы не можете близко знать десятки или сотни подписчиков закрытой группы или иметь с ними гарантированно хорошие, доверительные отношения.

Это значит, что любое неосторожное высказывание или нескромное фото, опубликованное, казалось бы, в закрытом сообществе, «под замком», имеет все шансы на публикацию где угодно недружественными «друзьями».

Разглашать и глумиться не запрещено

За вынос «из-под замка» и вообще за практически любую травлю и глумление не полагается никакого наказания или даже общественного порицания, и многие это делают специально, с удовольствием, чтобы потом пообсуждать, заработать себе лайки и расширить аудиторию, получить психологическое преимущество над кем-то.

Никакого этического кодекса пользователя социальной сети, моральных ограничений в отношении нарушения приватности в Сети сейчас не существует.

Социальные сети также не следят за этим.

Так что на самом деле не существует никаких закрытых «подзамочных» постов или комментариев. Надо понимать, что всё сказанное в Сети хотя бы для трёх или пяти «друзей» — «под замком» или нет — опубликовано, по сути, для всех и рано или поздно может стать общим достоянием.

ОБЩЕНИЕ В МЕССЕНДЖЕРАХ И ЛОГИ

Общение в мессенджерах происходит либо в группах и чатах, либо один на один. Что касается группового общения в мессенджерах — здесь всё понятно: группы обычно большие, подписан на них кто угодно, риск выноса на публику любого высказывания высокий, как и в обычных социальных сетях.

Что касается общения один на один, которое кажется абсолютно конфиденциальным, то оно тоже не гарантирует неразглашения. В Сети можно найти огромное количество скриншотов переписки, которые выложены «бывшим парнем», или «бывшей девушкой», или младшим братом бывшей девушки, добравшимся до её смартфона, и т. д.

Мессенджер хранит так называемые логи вашей переписки, то есть журналы всех ваших сообщений. Как минимум они хранятся на вашем устройстве, в клиентском модуле мессенджера (а также на серверах сервиса).

Эти журналы могут быть украдены как вашими родными, знакомыми, получившими доступ к смартфону, так и какими-то шпионскими приложениями, которые вы нечаянно установили на смартфон.

Надо ещё понимать, что сама платформа мессенджера — Facebook, Telegram или WhatsApp — «видит» всю вашу переписку. Несмотря на любые заверения владельцев мессенджеров, что переписка зашифрована, недоступна центральному серверу, для вашей же безопасности стоит предполагать, что они всё же хранят логи на своих серверах и могут выдать их по запросу правоохранительных органов или слить по своему усмотрению[1].

Сказанное означает, что переписка в мессенджере не защищена так же, как публичная, поэтому не стоит сообщать в ней интимные подробности, пересылать «голые» фото, планировать правонарушения или угрожать кому-то.

---

[1] Более того, в Российской Федерации с 2019 года владельцы мессенджеров по закону обязаны хранить логи переписки и идентифицировать пользователей.

РАЗМЕЩЕНИЕ СОБСТВЕННЫХ ФОТО И ВИДЕО

Нет ничего более информативного, чем картинка. Лучше один раз увидеть, чем сто раз услышать или прочесть. В социальных медиа это нехитрое правило тем более работает, поскольку в приоритете — скорость размещения информации. На описание того, где он находится и что по этому поводу испытывает, пользователь затратит куда больше сил и времени, чем на публикацию селфи.

На вашем фото, а уж тем более на видео, вы даёте любому наблюдателю огромный массив образной, невербальной (то есть несловесной) информации о себе и своём окружении, такой как внешний вид, настроение, состояние здоровья, комплекция, стиль одежды, домашняя обстановка, любимые бренды, марка машины, место нахождения и т. п. Этих данных хватит на то, чтобы довольно чётко охарактеризовать ваши интересы и пристрастия, а в ряде случаев и установить вашу личность.

Какие данные можно автоматически извлекать из ваших фото, подробно описано в подразделе «Что можно узнать по выложенным фото и видео» далее в книге.

ПОСЕЩЕНИЯ САЙТОВ И СМИ

По всему Интернету разбросаны миллиарды фрагментов следящего кода от десятков наблюдателей, они есть практически на каждой веб-странице. Когда вы перемещаетесь по сайтам (смотрите новости, читаете анекдоты, просматриваете демотиваторы или видеоролики, заходите на форумы и в социальные сети), вы как бы задеваете **тысячи маленьких колокольчиков**, аккуратно развешанных повсюду.

Это «пикселы» (картинки размером 1 × 1 пиксел) интернет-счётчиков, коды авторизации в комментариях и на форумах через аккаунт в социальной сети, коды рекламных систем, запоминающие ваши посещения страниц, и т. п.

Когда вы заходите на какой-то сайт, то, кроме его содержания (контента), скачиваете к себе на смартфон или ноутбук ещё несколько десятков невидимых для вас следящих фрагментов программного

кода, так называемых пикселов от счётчиков. Это счётчики посещений от порталов наподобие LiveInternet, системы статистики Google Analytics и «Яндекс.Метрика» и др.

В среднем на каждой странице популярного сайта сейчас находится больше 50 таких следящих кодов.

Google, Facebook, Twitter и другие гигантские цифровые платформы собирают свои большие данные о пользователях сайта с любого фрагмента своего кода, установленного на сайте. Сюда относятся:

- код рекламной системы;
- средства авторизации через аккаунт социальной сети;
- бесплатная поисковая строка;
- внешние сервисы поддержки комментариев (наподобие DISQUS);
- обменные новостные блоки (тизерные новостные сети наподобие «Яндекс.Дзен» или «МаркетГид») и т. п.

Эти коды передают данные о вашем посещении страницы на центральный сервер интернет-сервиса. Чем больше сервис, тем больше у него таких кодов и тем больше различных данных. Чем шире линейка сервисов у интернет-гиганта, тем больше у него разнообразных данных о вас, которые можно сводить между собой для анализа.

> Google, например, сводит данные о вашем посещении конкретной страницы с данными поисковой системы, где вы делаете поисковые запросы, а также с данными вашего ящика электронной почты на Gmail, данными рекламной системы AdSense (где и какую рекламу вам показывали), данными геопозиционирования, платёжной системы Google и операционной системы Android на вашем смартфоне.
>
> В результате Google затем «видит» посетителей сайтов по всему Интернету — везде, где установлены реклама Google и сервисы его партнёров. И знает почти всё об их пристрастиях и интересах.
>
> Та же история со счётчиком «Яндекс.Метрика» — его данные о ваших посещениях сайтов затем сводятся с вашими поисковыми запросами в «Яндексе», с данными из его почты, с данными его рекламной сети (РСЯ), с данными о пользовании картами и такси и т. д.

Пометив пользователя сайта, присвоив ему «вектор интересов», крупные платформы потом «видят» этого пользователя везде:

в аккаунтах социальной сети, на других сайтах, в поиске, могут показывать рекламу («догоняя» его по всему Интернету), другие сообщения, создавать для него так называемый *информационный пузырь* в социальных сетях и новостных агрегаторах.

КОДЫ СОЦИАЛЬНЫХ ПЛАТФОРМ НА СТОРОННИХ САЙТАХ

Социальные платформы Facebook и «ВКонтакте» тоже «видят» не только ваше поведение, фото и тексты в **своих** социальных сетях. Они встроили миллиарды своих кодов на «чужих» сайтах и в «чужих» приложениях.

Например, это коды авторизации, позволяющие вам зайти на форум, в блог, просмотреть комментарии в интернет-СМИ без регистрации и ввода пароля, а просто через ваш существующий аккаунт в Facebook или «ВКонтакте». С помощью этих кодов социальные платформы следят за действиями пользователя на сайте или в приложении. Обычно пользователь даёт разрешение на такую «слежку», нажимая кнопку «Согласен» при первом посещении страницы.

Но так бывает далеко не всегда: некоторые сайты считают, что сам факт использования сайта уже означает согласие на сбор данных.

По данным организации «Электронный фронтир» (Electronic Frontier Foundation), отслеживающие коды Facebook установлены на 30 % из 10 000 самых популярных сайтов (https://www.eff.org/deeplinks/2019/01/guided-tour-data-facebook-uses-target-ads).

Можно предположить, что доля в трафике, то есть в показах или посещениях пользователей, на популярных сайтах у кодов Facebook ещё выше, заведомо больше половины. Иначе говоря, Facebook «видит» больше половины популярного Интернета, что практически равно **всей** аудитории Сети, которая так или иначе время от времени заходит на эту «половину».

Так что всякий раз, когда вы на каком-то форуме, в СМИ, в блоге выбираете «зайти через Facebook», эта социальная платформа

получает данные о том, на каком сайте вы находитесь и что там делаете.

В результате нескольких скандалов с утечками данных, под давлением возмущённых пользователей, интернет-СМИ и конгресса США в 2017–2018 годах компания Facebook в 2020 году выпустила инструмент, который дал пользователям возможность удалять информацию, собранную кодами этой соцсети со сторонних сайтов.

В январе 2020 года на сайте Facebook в настройках учётной записи появилась вкладка «Действия вне Facebook» (Off-Facebook Activity). Там можно посмотреть, что именно «видит» платформа, когда вы пользуетесь сайтом или приложением, где есть код Facebook.

- Открытие приложения или сайта.
- Вход через Facebook.
- Просмотр веб-страниц и другого контента.
- Поиск товаров.
- Добавление товара в корзину.
- Совершение покупки.
- Совершение благотворительного пожертвования.

«Данные об этих действиях мы получаем от компаний и организаций, которые используют вход через Facebook, — говорится на сайте Facebook. — Компании и организации могут пользоваться услугами сторонних поставщиков данных или маркетинговых агентств, чтобы анализировать взаимодействия клиентов со своими приложениями и сайтами. Иногда третьи стороны используют наши инструменты для бизнеса, чтобы отправлять нам данные о ваших действиях от лица компании или организации, с которой они сотрудничают».

Обратите внимание на упоминание «сторонних поставщиков» и «третьих сторон»: оно означает, что Facebook не только получает данные пользователей от своих партнёров по всему Интернету, но и **передаёт и продаёт их «третьим сторонам»**.

Примерно те же данные получает о ваших перемещениях и платформа «ВКонтакте», а также множество других, более мелких игроков.

Ещё раз повторим: **социальные, поисковые и рекламные платформы «видят» вас на любых сайтах, а не только на сайтах самих платформ**.

ПОИСКОВЫЕ ЗАПРОСЫ

Поисковые запросы — главное богатство поисковых систем, таких как «Яндекс» и Google. Они никогда не удаляются, долгие годы хранятся вместе с данными о пользователе, времени запроса, «соседними» запросами и т. п.

Все поисковые запросы автоматически классифицируются по тематикам и потребностям пользователя («интентам») — это довольно точный и детальный анализ.

Поисковик анализирует не только сами запросы, но и поисковые сессии, то есть то, какие ещё запросы делал пользователь в течение некоторого времени «вокруг» анализируемого запроса. Клики пользователя по сайтам (результатам поиска) по данному поисковому запросу также навсегда сохраняются в базе данных поисковика.

Используя дополнительно анализ данных своих кодов контекстной рекламы, расставленных по множеству сайтов, поисковик может очень точно выяснить ваши интересы.

По вашим запросам поисковик может определить не только ваше желание купить какую-то вещь или услугу, но и наличие у вас беременности, болезней, проблем в семье и т. п. Он может выявить у вас интерес к порно, наркотикам, «снюсам» или пиратскому кино, понять политические предпочтения или сексуальные привычки.

В основном это используется, конечно, для того, чтобы создавать навязчивую, своевременную, неотразимую рекламу, но любые «нехорошие» или «чувствительные» интересы, проявленные в запросах (порно, извращения, наркотики), тоже фиксируются навсегда. В дальнейшем они могут быть использованы следствием, шантажистами, коллекторами — кем угодно, кто «дотянулся» до этих данных неформально (например, через сотрудников поисковика) или формально (по запросу суда, прокуратуры).

ПОКУПКИ

За вашими покупками в Сети следит огромное количество наблюдателей, потому что это касается денег: они стараются понять ваши потребительские запросы, чтобы потом «втюхать» ещё один (а лучше не один) товар и услугу. А деньги создают самую сильную мотивацию для слежки.

Журналы ваших поисков товаров и сделанных покупок ведут сами магазины, рекламные сети, поисковые машины, в которых вы делаете «потребительские» (так называемые *транзакционные*) запросы. Все эти игроки рекламного рынка помечают вас (ваш браузер, устройство и т. п.) и потом «догоняют» рекламой по всему Интернету. Более того, они перепродают вас друг другу.

Каждый ваш переход на другую страницу *монетизируется*.

> Это называется умной рекламой[1], хотя все мы знаем примеры нелепого и глупого поведения рекламных сетей, когда после покупки холодильника или телевизора нас несколько недель преследуют рекламой таких же товаров, хотя мы точно не собираемся в ближайшие годы покупать второй экземпляр этой дорогой техники долговременного пользования.
>
> Мы ищем «горнолыжный курорт на озере Банное на Урале» — и потом две недели на каждом шагу нам предлагают банные полотенца. С семантикой в рекламных сетях пока не всегда хорошо.

Тем не менее часто данные о потребителе релевантны, содержательны, живут годами, их перепродают, присоединяют в базах данных к идентификаторам его смартфона, ноутбука, смартфонов детей и жены и т. д. Их заносят в так называемые рекомендательные системы магазинов и интернет-порталов, чтобы предложить «похожие товары» или «товары, которые ищут вместе с этим товаром».

Хорошо ли быть объектом пристального изучения продавцов? Нам кажется, что не очень — это риск увеличения потока навязчивой рекламы или спровоцированных умной рекламой *импульсных покупок* какой-нибудь ерунды.

МОБИЛЬНЫЕ ОПЕРАТОРЫ

Мобильные операторы, предоставляющие нам доступ к мобильной связи и Интернету, — такие же внимательные наблюдатели за нашим поведением и игроки рынка персональных данных и умной

---

[1] Современное название этих технологий — RTB (Real-Time Bidding) или «Программатик». Их цель — мгновенный аукцион рекламодателей за право показать пользователю свою рекламу на том сайте, где его опознали. Данные о пользователе передаются по всей Сети, и на каждой веб-странице — на сайте, в магазине, в СМИ, на форуме — работает рекламный аукцион в борьбе за его внимание.

таргетированной рекламы, как и другие цифровые платформы и «экосистемы» (только они ещё берут с нас деньги, в отличие от социальных сетей и поисковиков). Чтобы не пересказывать, что они делают с данными, своими словами, приведём рекламное письмо от компании МТС, которое получили по электронной почте в октябре 2020 года, с подробным и открытым описанием того, какую информацию МТС собирает о своих клиентах и что может предложить рекламодателю и рекламному агентству.

Письмо говорит само за себя (орфография и лексика сохранены, убраны только Ф. И. О. менеджера).

FROM: ********* ******

SENT: Thursday, October 22, 2020 5:31 PM

SUBJECT:отПАОМТС. Индивидуальное коммерческое предложение.

Добрый день!

Я эксперт отдела продаж в ПАО МТС.

Хочу предложить Вам сотрудничество и рассмотреть один из наших инструментов)

Наша компания активно трансформируется из «телеком» оператора, в IT компанию с собственной продуктовой разработкой. Большим шагом на пути к этому стало создание в 2017 году центра по обработке «больших данных» (BigData).

Теперь мы фиксируем и анализируем всю информацию о наших абонентах — **звонки, SMS, посещение сайтов, геолокацию, финансовую активность и пр.**

МТС — лидер отрасли с базой абонентов в 60 млн человек (в Москве доля МТС 41 %) которые ежедневно генерируют терабайты данных для анализа.

Наши знания могут помочь Вам эффективнее находить Ваших потенциальных клиентов.

В результате анализа данных о наших абонентов мы строим готовые сегменты целевых аудиторий, на основе теории вероятности и машинного обучения.