**Государство и чиновники в цифровом пространстве**

*Что можно и нельзя*

*Конфиденциально*

*Игорь Ашманов 29.10.2015*

**Введение**

Все современные интернет-сервисы, мобильные приложения и сами мобильные телефоны, программное обеспечение для настольных компьютеров и ноутбуков собирают так называемые Большие Данные о пользователях. Эти данные дают своим владельцам огромный политический и коммерческий рычаг.

**Что выкачивают.** С мобильных устройств, браузеров, антивирусов, социальных сетей, выложенных фотографий собираются данные о местоположении, тексты CMC, голосовая запись звонков, тексты постов и комментариев, списки друзей, геокоординаты перемещений, фото, документы, логи звонков и всех совершенных контактов, данные из адресных книг, отпечатки пальцев, физиологические данные из смарт-часов, браслетов: о пульсе, фазах бодрствования и сна, физической нагрузке.

**Как анализируют и что полезного извлекают.** Анализ Больших данных построен на сопоставлении потоков данных из разных источников, а также на изучении истории поведения и транзакций пользователя (ретроспективы). Это позволяет сводить данные из разных сервисов (почта, мобильная связь, хранение файлов, поисковые машины, карты, рекламная система, платёжные системы) воедино, восстанавливать истинные ФИО пользователя, распознавать тематические предпочтения, увлечения, политическую позицию, круг друзей и знакомств, посты и должности, уровень достатка, покупки, места отдыха, посещаемые сайты и места в городе, тайные пристрастия и т.п.

Например, всего по четырём привычным GPS-точкам в городе однозначно идентифицируется любой человек; по данным за несколько дней о времени выхода в Интернет и времени написания постов в ВК или ФБ однозначно раскрывается анонимный ник в соцсети. И так далее.

**Зачем.** В первую очередь с целью слежки. Слежка используется для общего анализа ситуации в стране или организации, а также для получения **рычага влияния** на конкретного пользователя. Связи с нужными людьми, любовные интрижки, посещение порносайтов, жизнь не по средствам, связь с коррупционерами и криминалитетом, фальшивый диплом, кумовство и семейственность в карьере, денежные проблемы, что угодно скользкое или просто полезное может быть легко выловлено из этих данных и использовано для вербовки, шантажа, влияния.

**Кто в зоне риска.** Последние скандалы с почтой Хиллари Клинтон и директора ЦРУ Бреннана показывают, что даже высокопоставленные государственные служащие и руководители разведки с разными целями, но практически неизбежно заводят себе адреса на публичных почтах, а потом, рано или поздно, по небрежности или второпях, пересылают и хранят там секретные документы. А любую публичную почту рано или поздно взламывают, это не очень трудно для опытного хакера, владеющего социотехникой и технологиями взлома.

В нашей стране ситуация ещё сложнее: большинство публичных интернет-сервисов, компьютерных и мобильных платформ в нашей стране - американские. Американские ИТ-компании обязаны согласно закону Patriot Act 2001 сохранять и передавать все данные в американские спецслужбы (АНБ и др.). Мы не знаем, как именно были сделаны последние громкие взломы почты и социальных аккаунтов государственных деятелей и политиков в нашей стране, но нельзя исключить, что в том числе с помощью самих американских технологических платформ.

Российские чиновники, руководители, бизнесмены, элита довольно бездумно пользуются этими ИТ-сервисами, тем более, что они очень удобны, а также создают иллюзию защищённости от «своих», внутри страны.

Айфон / Android, аккаунт в ФБ, Twitter, Whatsup, Viber, браузер Chrome, Windows 10 и т.п. есть практически у каждого. В зоне риска - все.

**За кем следят.** У неискушённых пользователей есть иллюзия, что «слушают» не всех. Что слушать и анализировать всех сложно и дорого, а конкретно он, обычный пользователь, не может быть никому интересен.

На самом деле, хранение данных сейчас очень дёшево, и Большие Данные уже несколько лет **собираются о каждом пользователе,** потому что неизвестно, кем будет сегодняшний студент через 10-15 лет или куда через 3 года продвинется сегодняшний чиновник невысокого ранга, с кем или «под кем» он будет работать.

Наличие маркеров - болевых точек, точек интереса - определяется автоматически, процедурами массовой обработки данных. Анализ данных сейчас тоже дёшев.

Следящих интересует даже не конкретный пользователь сейчас, а *процент конверсии информации во влияние -* на кого из всей массы за годы слежки удастся насобирать компромат, сведения о связях и т.п. и начать влиять.

Поэтому соблюдать **информационную гигиену** должен каждый. *]А* особенно - служащий госаппарата, политик, руководитель, известный человек в любой области, то есть все, кто уже сейчас попадает в группу риска и являются целями слежки и влияния.

**Информационная гигиена**

1. Совсем недопустимо

*Личные коммуникационные средства на службе*

**Мобильные телефоны, смартфоны, планшеты.** Пересылают CIVIC, голос, фото без ведома пользователя, в скрытом режиме. Голосовой трафик «пишется» весь без исключения.

Нельзя использовать или держать включёнными на столе на закрытых совещаниях, в кабинетах, на переговорах. Нельзя использовать смартфоны для ведения служебных разговоров, пересылки документов, приёма и отправки служебной почты. Нужно понимать, что некоторые модели смартфонов **активны и в выключенном состоянии.**

***Альтернатива:*** собственные почтовые сервера учреждения, городские телефоны, «бабушкофоны» (простые кнопочные мобильные телефоны), корпоративные защищенные мобильные телефоны, файрволы для смартфонов, защищенные здания, средства «глушения» в переговорных и кабинетах.

**Носимые устройства (умные часы, фитнес-браслеты).** Передают «в центр» («облако») биометрические данные: пульс, нагрузку, количество шагов вместе с географическим положением, номерами телефонов, логами звонков, именами сетей WIFI и прочими «обычными» утечками. Категорически нельзя использовать государственным служащим.

**Настольные компьютеры, ноутбуки.** Последние версии операционных систем в стандартной конфигурации (IOS, Windows, особенно Windows 10) передают «в центр» очень много информации, вплоть до всех нажатий клавиш. Западные антивирусы имеют фоновый, скрытый доступ ко всему компьютеру.

***Альтернатива:*** пока не распространились отечественные ПК и ОС, нужно устанавливать (с помощью системных администраторов) жёсткие настройки ОС, запрещающие отправку данных наружу, устанавливать исключительно отечественные антивирусы и файрволы (Касперского, Доктор Веб), использовать служебные почтовые серверы и отечественные средства документооборота (например, 1С, Битрикс, ЭОС).

Нужно запланировать переход учреждения на отечественные продукты и системы, в том числе сертифицированное в РФ свободно распространяемое программное обеспечение (СПО - Linux и др.), а также установку систем борьбы с утечками (DLP).

**Поисковые машины.** Поисковые машины сохраняют все запросы пользователя, а также все сайты, по которым он кликнул в поисковой выдаче. По этим данным легко определить предпочтения и сиюминутные потребности пользователя, его планы на покупки, поездки, встречи. Поскольку у всех поисковых машин есть также свои публичные почты, рекламные сети, коды счётчиков, новостные агрегаторы, мобильные платформы, платёжные системы, карты и другие сервисы, в том числе собственные социальные сети и поиск по блогам, то очень ценная информация о поисковых запросах сопоставляется и тесно увязывается с остальной личной информацией. Нельзя использовать зарубежные поисковики в служебных целях, с рабочих устройств, и крайне нежелательно - в личных целях.

**Альтернатива;** отечественные поисковики Яндекс, Спутник, поиск [IVlail.ru](http://IVlail.ru).

**Социальные сети и блоги.** Все посты и комментарии в социальных сетях сохраняются, индексируются и анализируются (включая даже «посты-призраки», то есть набранные и стёртые без публикации посты и комментарии). У большинства пользователей по их постам можно выяснить абсолютно всё о них, семье, друзьях, коллегах.

Для руководителей практически любого ранга это недопустимый риск. Как утечек, так и необдуманных высказываний, личных данных, на основе которых можно построить информационную атаку, а также кражи аккаунта или подмены данных.

***Альтернатива.*** Единственным исключением можно считать официальные аккаунты в соцсетях, которые ведут пиарщики (или лично сам чиновник, но выкладывая официальную, взвешенную публичную информацию).

**Устройства с геомодулями.** Следят за перемещениями все устройства и сервисы, фиксирующие геокоординаты. Все телефоны с lOS/Android/Win могут фиксировать перемещения. Это же касается сервисов: фотохостингов, видеохостингов, Твиттера, ФБ, в которые пользователь выходит со смартфона. При этом координаты передаются без спроса, в скрытом режиме (даже если пользователь сообразил найти и выключить соответствующую галочку в настройках). Если факт посещения каких-то мест не нужно разглашать, то такие телефоны просто нельзя носить с собой.

**Умные телевизоры.** Последние поколения телевизоров (в том числе Samsung, LG) требуют соединения с Интернетом и передают наружу дальше больше информации, чем смартфоны. В частности, в каждом таком телевизоре есть камера хорошего качества, распознающая людей и движения (так как есть функция управления жестами) с нескольких метров. Данные с камеры тоже передаются наружу. Выключить эту функцию фактически нельзя (проверки показывают, что снимание соответствующей «галочки» в настройках не прекращает поток данных наружу). Сейчас умные телевизоры есть практически в каждом офисе и квартире.

***Альтернатива:***отключить доступ в Интернет в телевизоре, закрыть камеру, не скачивать приложений на телевизор.

**Сервисы публикации фото и видео.** Геокоординаты места съёмки фиксируются в некоторых фотофайлах, при выкладывании их в соцсетях и фотосервисах нужно про это помнить. Надо помнить также, что сейчас качество и скорость массовых технологий распознавания таковы, что все лица (а также, возможно, здания и пейзажи) на фото будут гарантированно быстро распознаны и семантически проиндексированы.

**Развлекательные сайты на службе.** Нельзя использовать никаких служебных устройств (смартфонов, компьютеров, планшетов) для просмотра развлекательных сайтов, порно, скачивания пиратской музыки и т.п. - порносайты и пиратские сайты любят «подсадить» своим посетителям троянские программы. Нельзя открывать даже очень интересные спам-письма в электронной почте, по той же причине.

**Любые неизвестные мобильные приложения.** Известно много случаев, когда вроде бы безобидное андроид-приложение шпионило за владельцем (например, известный случай с приложением "фонарик"). Это же касается некоторых игр. Ничего неизвестного не следует ставить на телефон.

Кроме того, любые приложения, где, например, есть рекламный код AdMob. Этот код не подчиняется ограничениям. Каждому пользователю он присваивает ID, собирает по нему всю доступную на телефоне информацию и передаёт в Google. Таким образом, даже если приложение устанавливается из официального магазина, не требует никаких разрешений, но в нем есть AdMob, то через него происходит утечка всех тех же данных.

**Внутренняя служебная коммуникация**

**Публичные почты, мессенджеры и сервисы хранения файлов** все без исключения сейчас мониторят и автоматически анализируют содержание писем и файлов. Это можно видеть, например, по тому, что Google показывает в Gmail рекламу в соответствии с содержанию письма. При этом данные сервисы не гарантируют бесперебойного доступа: может оказаться, что зарубежный сервис недоступен в разгар работы, и на это никак нельзя повлиять.

Нельзя использовать публичные почты (Gmail, Yahoo, AOL и пр.) для хранения и пересылки служебных документов, переписки. Нельзя использовать публичные сервисы хранения документов (Dropbox), мессенджеры (Viber, Telegram, Whatsup), зарубежные файловые хостинги ([Megaupload.com](http://Megaupload.com)) для служебной переписки и документации.

**Социальные сети.** Категорически нельзя вести служебную переписку и работу через социальные сети ФБ, Твиттер, Linkedin и другие, по тем же причинам: негарантированный доступ и утечка данных.

**Средства документооборота.** Нельзя использовать в работе «облачные» средства документооборота, CRM, управления проектами от Google (Google Docs), Microsoft, Sales Force **и** других западных поставщиков, календари (Google Calendar и т.п.).

Нельзя использовать «облачные» версии Microsoft Word, Excel, Power Point и тому подобные «облачные» средства обработки документов, в которых все данные проходят через сервера в США и Европе (впрочем, если сервера этих сервисов согласно новым законам РФ и будут установлены в России, это не снизит риска утечек в АНБ по американским законам).

***Альтернатива:*** собственные внутренние служебные сервисы документооборота, отечественное ПО для документооборота (например, 1С, Bitrix, Галактика и пр.), в крайних случаях, когда речь не идет об информации ограниченного распространения, почта и «облачные» средства коллективной работы и хранения документов от Яндекса, ВКонтакте, [Mail.ru](http://Mail.ru), Bitrix.

**Социальное окружение.** Очень важно понимать также, что поведение окружающих и их недостаточная цифровая гигиена может свести на «нет» все усилия человека по защите государственных данных, персональной информации и личной жизни. Бесконтрольное использование смартфонов и приложений сотрудниками и подчинёнными, членами семьи и друзьями, может привести ко всем перечисленным утечкам и проблемам. Все устройства «видят» друг друга, умеют обмениваться информацией. Достаточно одного человека в переговорной комнате или ресторане, смартфон которого работает в стандартном режиме слежки, и все усилия остальных пяти присутствующих по защите своей информации можно считать бесполезными. Если блокировать, сдавать секретарю или убирать в сумку смартфоны - то у всех.

Необходимо обеспечить контроль маршрутов прохождения трафика и места обработки данных. Как на уровне офиса, компании, города, так и на уровне региона. Любое устройство с «зашитыми» недекларированными функциями по слежению не сможет передать собранное, если администратор следит за маршрутами и состоянием фаерволов. Обработка данных должна осуществляться в профессиональных, сертифицированных и проверенных дата-центрах, лучше государственных компаний. Нужен контроль инженерной инфраструктуры.

**Официальная коммуникация с населением**

**Социальные сети.** Нельзя использовать западные социальные сети (Facebook, Twitter) для создания средств официальной коммуникации с гражданами (прием обращений граждан через социальные сети). Кроме утечек и взломов, есть негарантированность доступа (опасность выключения сервиса в неурочное время), а также риск «угона» аккаунта и подмены данных на стороне самой платформы.

***Альтернатива:*** собственные сайты, сервисы общения с населением ([gorod.mos.ru](http://gorod.mos.ru), [open.tatarstan.ru](http://open.tatarstan.ru), <http://dem.nso.ru>) Также официальные федеральные ресурсы (Российская Общественная Инициатива [ROI.ru](http://ROI.ru)). Также можно использовать отечественные сервисы для опросов, комментирования, обратной связи (например. Довольный гражданин, Witology и др.), группы в ВКонтакте.

**Счётчики на официальных сайтах.** Нельзя устанавливать внешние зарубежные счётчики на государственные сайты, в первую очередь - Google Analytics. Эти системы статистики передают данные на центральный сервер сервиса, который в случае GA сводит данные с данными поисковой системы, почты, рекламы, социальной сети, платёжной системы и «видит» затем ваших посетителей по всему Интернету - везде, где установлена реклама Google и сервисы его партнёров.

Например, если на государственном сайте установлена GA, то Google сможет в будущем при желании каждому посетителю госсайта послать письмо о чём-нибудь в его аккаунт на Gmail или сообщение на его телефон под управлением Android.

***Альтернатива:*** собственные системы анализа статистики сайта, на рабочих местах чиновников - использование браузеров, которые позволяют заблокировать внешние средства мониторинга и статистики (Спутник Браузер). Использование отечественных систем статистики допустимо при наличии документов (договор с поставщиком ПО, лицензионное соглашение), регламентирующих сбор информации о пользователях с официальных сайтов: Яндекс.Метрика, Openstat, Bitrix, Liveinternet и др. При наличии в собираемой информации персональных данных пользователей оператор информационной системы должен быть зарегистрирован в Роскомнадзоре как оператор персональных данных.

**Коды зарубежных систем на официальных сайтах.** Google, FB, Twitter и другие зарубежные системы собирают свои Большие Данные о пользователях сайта с любого кусочка своего кода, установленного на сайте. А потом они «видят» этого пользователя везде: в аккаунтах социальной сети, на других сайтах, в поиске и т.п., могут показывать ему рекламу («догоняя» его по всему Интернету), другие сообщения, подбирать для него «информационный пузырь». Сюда относится:

* код рекламной системы,
* средства авторизации через аккаунт социальной сети,
* бесплатная поисковая строка,
* система комментариев (наподобие DISQUS),
* обменные новостные блоки и т.п.

Нельзя устанавливать на официальные сайты никакого чужого кода, в том числе рекламного.

***Альтернатива:***использование браузеров, блокирующих внешние средства мониторинга и статистики (Спутник Браузер). Использование отечественных встраиваемых кодов в страницу сайта допустимо при наличии документов (договор с поставщиком ПО, лицензионное соглашение) регламентирующих сбор информации о пользователях с официальных сайтов. Если собираются персональных данные граждан РФ, поставщик информационной системы должен быть зарегистрирован в Роскомнадзоре как оператор персональных данных.

**Системы управления сайтами и хостинги.** Не следует использовать для официальных сайтов зарубежные системы управления сайтами, в том числе «облачные» конструкторы сайтов. Категорически нельзя размещать официальные сайты на зарубежных хостингах. Не очень желательно использование «открытых» систем управления сайтом наподобие Drupal, WordPress, Joomla и т.п.

***Альтернатива:***отечественные системы управления сайтом (Bitrix, UMI CMS и др.), отечественные хостинги и дата-центры.

В Приложении к данному документу мы даём каталог отечественных интернет-сервисов и корпоративного и клиентского ПО, которые мы рекомендуем применять вместо указанных выше зарубежных сервисов и ПО.

2. Нежелательно

**Использование зарубежных публичных почт и мессенджеров для личной переписки.** Все публичные почты наподобие Yahoo, Gmail и мессенджеры наподобие Whatsup, Telegram, Viber легко идентифицируют реальные ФИО своих пользователей, даже при регистрации под анонимными пиками, и безусловно мониторятаккаунты всех госслужащих.

Кроме того, большинство пользователей в силу забывчивости или в спешке обязательно рано или поздно, время от времени, посылают служебные документы через личную почту.

**Социальные сети и фотохостинги для личных блогов и фото.** Социальные сети постоянно анализируют привычки пристрастия пользователей, их круг знакомств. При этом они настраивают ленту новостей по неким закрытым алгоритмам, создавая вокруг пользователя так называемый **«информационный пузырь»,** то есть создают для пользователя особую, специальную информационную реальность.

При этом ФБ, Youtube, Twitter активно, не скрываясь, участвуют в идуш,ей сейчас информационной войне. И не на нашей стороне. Например, Твиттер ежедневно присылает в почту приглашения прочесть новые твиты - как правило, исключительно нашей «оппозиции», контролируемой американцами (Навального, Яшина, Адагамова и т.п.). Этим же занимается служба новостей MSN, которая встроена в Windows и делает автоматическую подборку новостей.

Нужно помнить также о возможности *информационных атак* на основе данных из соцсетей: вызываюш,ие фотографии в Фейсбуке на фоне пальм и Бентли могут быть использованы против вас лично и против власти, даже если пальмы пластиковые, а Бентли -чужой.

***Альтернатива*** - отечественные социальные сети ВК, ОК, Мой Мир или ведение аккаунта пресс-секретарём (предпочтительно).

**Кредитные карты зарубежных платёжных систем.** Нужно понимать, что кроме взятия процента со всего «карточного» оборота страны. Visa, Mastercard и другие зарубежные системы также накапливают чрезвычайно ценные и чувствительные данные о всех покупках, встречах в ресторанах, поездках, перелётах и т.п. наших граждан, причём со всеми данными о Ф1/10, номерах телефонов, местоположении магазинов и банкоматов и т.п. При этом Visa, Mastercard, American Express и прочие платёжные системы также находятся в сфере действия закона Patriot Act.

Для чиновников среднего и высокого ранга отдавать эти данные за рубеж - недопустимо.

Для исправления, в частности, этой ситуации принят федеральный закон о Национальной

Платёжной Системе. С 1 октября 2015 и Мастеркард, и Виза работают через НПС. Однако, вопрос их доступа к данным транзакций пока неясен.

Карты, привезённые с Запада, использовать в РФ нельзя по тем же причинам. Использование китайской Union Pay тоже нежелательно. Использование российских карт за рубежом приводит к прохождению данных через зарубежные центры обработки, то есть к утечкам данных. Никогда нельзя совершать никаких платежей через Интернет и смартфон (банк-клиент), поскольку данные точно так же передаются через смартфон и браузер.

***Альтернатива*** *-* отечественные дебетовые карты наподобие ПроЮОи другие, выпускаемые отечественными банками, или наличные. В смартфоне при покупках и важных поездках всегда должны быть выключены Wi-Fi, Bluetooth и GPS.

3. Допустимо с ограничениями

Допустимо использовать **отечественные** публичные сервисы для личных нужд и для служебных нужд (как резервный канал).

Естественно, секретные и ДСП-документы в любом случае не должны пересылаться или храниться в публичных сервисах. Эти сервисы легко взламываются третьими лицами, а их системные администраторы не имеют допуска секретности и соответствующего уровня ответственности. В любом случае чиновники высокого уровня не должны использовать никаких зарубежных «облачных» сервисов и публичных почт даже для личных надобностей.

Итак, допустимо с предосторожностями:

* Использование отечественных публичных почт и сервисов документооборота для личной переписки.
* Установка отечественных внешних счётчиков на государственные сайты (описано выше).
* Использование отечественных файл-хостингов и публичных средств документооборота (наподобие Yandex.Disk, Облачный офис, Bitrix и т.п.)

Гигиена отношений с западными компаниями в регионах РФ

Крупные западные компании ведут активную административную и политическую деятельность на территории РФ по привлечению пользователей в свои сервисы, продаже своих продуктов и т.п., в том числе:

**Обучение госслужащих.** Приход западных компаний в регион для целей обучения госслужащих пользованию их средствами коммуникации и прочим ПО. Это категорически недопустимо, поскольку приводит к распространению в госорганах ровно тех платформ и технологии, о которых мы пишем выше.

**Работа с молодёжью.** Приход Google и других западных компаний в регион для пропаганды своих брендов среди детей и подростков. Конкурсы на лучшую картинку для названия Google («дудла»), различные олимпиады, креативные задания, научные проекты для детей, и т.п. Это способ вовлечения в использование зарубежных сервисов с ранней юности, продвижение брендов как «добрых», удобных, полезных, «своих».

**Рекрутирование ценных специалистов.** Приход западных компаний в регион для рекрутирования программистов и инженеров как в местных центрах разработки, так и вывоза в США и Европу.

***Пример:***так называемый «пароход Цукерберга». Приезд руководства Фейсбука в Москву и

Петербург, семинары для студентов матвузов с рассказами о том, как прекрасно работать

на ФБ в США, летняя стажировка в ФБ для студентов Мехмата МГУ, ВМиК в США.

Результат: кто-то вообще не вернулся со стажировки, десятки студентов после защиты

диплома сразу уехали в США.

При этом руководство факультетов зачастую бездумно способствует этому, считая, что

помогают своим выпускникам лучше устроиться.

Отечественным компаниям очень трудно конкурировать с этой утечкой мозгов, особенно в связи с падением курса рубля по отношению к доллару. Ни в коем случае нельзя способствовать таким рекрутинговым походам иностранцев в регионы.

**Работа со СМИ.** Большие рекламные бюджеты, стимулирование СМИ для открытия «представительств» в Фейсбуке и Твиттере. Результат - СМИ активно пиарят Фейсбук и Твиттер в прайм-тайм, за свои деньги, в своих передачах и статьях.

**Благотворительная и общественная деятельность.** Западные компании в регионах РФ запускают много благотворительных проектов в целях пропаганды своих сервисов и втягивают государственные организации и чиновников в сотрудничество в этих благотворительных и общественных проектах. Пример: использование сервисов и денег Гугла для создания проекта о ветеранах Отечественной войны весной этого года.

При этом власти регионов, вузов, школ обычно охотно идут навстречу, так как у западных компаний много денег, отлично проработанные, готовые маркетинговые и проектные решения, энергичный персонал, убедительные культурные и этические обоснования предлагаемой деятельности. Это огромные транснациональные корпорации с большим опытом «захвата территорий».

Всё это - вредная и нежелательная активность с бутафорским фасадом, в особенности рекрутирование программистов и работа с детьми и подростками. Не следует помогать в этом зарубежным компаниям , участвовать в их инициативах, сотрудничать.

Надо понимать, что практически всё, что могут предложить Google и Facebook на территории (полезное ПО, лекции, обучение, конференции, проекты, благотворительность), могут также предложить отечественные компании наподобие Яндекса, [Mail.ru](http://Mail.ru), ВКонтакте, Лаборатории Касперского-без ненужных вредных эффектов. С ними и нужно сотрудничать.