DOI: 10.34773/EU.2022.3.27

Анализ политик конфиденциальности и управления цифровыми двойниками

Analysis of Privacy Policies and Management of Digital Twins

Л. РОЗАНОВА, М. КОРНЕЕВА

Розанова Лариса Федоровна, канд. техн. наук, доцент кафедры цифровой экономики и коммуникации Института экономики, финансов и бизнеса Башкирского государственного университета.
E-mail: rozanova_lara@mail.ru
Корнеева Мария Станиславовна, магистрант кафедры вычислительной математики и кибернетики Уфимского государственного авиационного технического университета.
E-mail: mariakorneevaa@gmail.com

В статье приведены результаты анализа политик конфиденциальности нескольких крупных корпораций, таких как Google, Meta (Facebook, Instagram, WhatsApp), Apple, на серверах которых хранятся цифровые двойники пользователей этих систем. Показано, что информацию, хранящуюся в цифровых двойниках, люди добровольно отдают в силу удобства использования продуктов этих компаний, не задумываясь о том, для чего и куда дубликаты частных данных попадут. Приведены возможные способы и механизмы их использования заинтересованными фирмами и лицами, а также мероприятия для сохранения конфиденциальности, что чрезвычайно важно в условиях развития искусственного интеллекта.
***Ключевые слова**: цифровой двойник, конфиденциальность, пользовательские данные, Google, Apple, Facebook, Instagram, WhatsApp.*

In this paper, we studied the privacy policies of several large corporations, such as Google, Meta (Facebook, Instagram, WhatsApp), Apple, on whose servers our digital counterparts are stored. A digital double refers to user data that is stored on company servers. The information stored in digital doubles is voluntarily given by users when using the products of these companies. A reflection on the topic of people's irresponsibility in relation to their private information is given. Conclusions are drawn on the topic of privacy in the modern digital world, as well as on the management of digital doubles.
***Key words**: digital twin, privacy, user data, Google, Apple, Facebook, Instagram, WhatsApp.*

Основные положения

1. Создавая профиль в той или иной социальной сети и заполняя его, люди создают своего цифрового двойника.
2. Цифровой двойник – это данные о пользователе, которые хранятся на серверах компаний.
3. Конфиденциальность – это сохранность и секретность информации.
4. Информацию, хранящуюся в цифровых двойниках, пользователи добровольно отдают при использовании продуктов этих компаний.
5. Пользователи безответственно относятся к своей частной информации.

Введение

В статье 3 Всеобщей декларации прав человека говорится, что каждый человек имеет право на жизнь, свободу и личную неприкосновенность [11].

В современном мире, в котором всё больше и больше применяются цифровые технологии, сохранить конфиденциальность частной жизни становится всё сложнее.

Многие вещи, такие как камеры наблюдения на улицах, системы электронных платежей и отправление геолокации операторами сотовой связи кажутся нам обыденными. IT всё больше и больше интегрируется в частную жизнь, появляются новые «умные» устройства, интегрируемые в цифровые экосистемы. Цифровые экосистемы, с одной стороны, служат для удобства и комфорта, а с другой стороны – вмешиваются в частную жизнь, собирая и обрабатывая данные о людях.

Из вышесказанного вытекают два важных вопроса.

Первый: возможно ли сейчас сохранить свою конфиденциальность, имея цифрового двойника? И второй: может ли человек полностью управлять своим цифровым двойником?

Чтобы получить ответы на поставленные вопросы, необходимо ознакомиться с политикой конфиденциальности компаний, которые предоставляют онлайн-услуги, и сделать необходимые выводы о правилах использования, хранения и защиты персональных данных.

В статье приведены результаты анализа политик конфиденциальности нескольких крупных корпораций, таких как Google, Meta (Facebook, Instagram, WhatsApp), Apple, на серверах которых хранятся цифровые двойники пользователей этих систем.

Методы

В ходе работы использованы методы анализа, систематизации и обобщения информации.

Результаты

Активной интеграции «умных» устройств в обычную жизнь способствовала пандемия COVID, из-за которой наш мир очень сильно поменялся. Раньше у человека была просто страничка на Facebook, где он изредка поддерживал связь со своими друзьями, изредка менял фотографии, вёл не очень активную интернет-жизнь, выставляя ограниченное количество информации о себе и отдавая предпочтение личному общению. Сейчас, спустя два года жизни в условиях пандемии, люди стали использовать интернет-ресурсы более активно.

С объявлением в самом начале пандемии локдауна, который предписывал жителям многих стран сидеть дома и общаться лично только с членами своей семьи, люди ушли в онлайн и начали активно пользоваться доступными цифровыми технологиями. Например, более активно использовать доставку продуктов и вещей, применять бесконтактные способы оплаты, использовать сервисы видео-звонков и онлайн-кинотеатры. Общение в интернете теперь – довольно обычное и привычное явление для огромного количества людей.

Многие компании перешли на удаленный формат работы, в том числе в формате онлайн, там, где позволяли бизнес-процессы. Для этого сотрудники были вынуждены создать себе аккаунты на платформах видеоконференций и электронной почты, заполненные частной информацией.

Однако винить только пандемию в снижении частной конфиденциальности не стоит. С каждым годом люди сами начинают всё больше «доверять» новым технологиям, чаще всего абсолютно слепо. Личные фотографии, биометрические данные (отпечатки пальцев, распознавание лиц), данные своих банковских карт для бесконтактной оплаты покупок, данные геолокации (своей и даже своих близких) – всю эту информацию люди добровольно отдают в руки глобальных корпораций.

Заполняя профиль в той или иной социальной сети, люди создают своего цифрового двойника. Связывая свои профили друг с другом, как, например, Facebook и Instagram, каждый человек все больше насыщает цифрового двойника информацией.

Если буквально два года назад, когда социальные сети для многих были формальностью, аккаунт был лишь цифровой тенью, то сейчас, когда многое перешло в онлайн, это уже полноценный цифровой двойник, использование которого чревато риском потери конфиденциальности.

Согласно определению, данному в проекте «Энциклопедия» Ксенией Карповой [9], «цифровой двойник (digital doubles или digital twin) – это виртуальная модель любых объектов, систем, людей, процессов и сред. Цифровой двойник отслеживает прошлое и предсказывает будущее».

Конфиденциальность – это сохранность и секретность информации. Наши данные сейчас как никогда нуждаются в сохранности и секретности. Однако, регистрируясь и принимая политику конфиденциальности разных приложений, социальных сетей, компаний, мало кто читает, на что он соглашается. Так, по данным опроса, проведенного Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций, «только 20 % опрошенных при посещении сайтов читают пользовательское соглашение и политику

конфиденциальности» и «40,3% пользователей читают соглашения выборочно, а 39,5 % вообще не обращают внимания на документы, определяющие политику сайта в области обработки персональных данных» [1].

В политике использования данных социальных сетей Facebook и Instagram от компании Meta сказано, что им необходимо обрабатывать информацию о пользователях для предоставления своих продуктов [4; 6].

Всю информацию о пользователе компания Meta хранит в его цифровом двойнике. Собранная информация помогает компании взаимодействовать со своими пользователями, проводить и поддерживать исследования, а также внедрять новшества, касающиеся вопросов социально-экономического обеспечения и благополучия, здравоохранения, технического прогресса, общественных интересов.

Компания Meta предоставляет обобщенную статистику, которая позволяет анализировать взаимодействие пользователей с публикациями и объявлениями различных людей и компаний, предоставляет информацию о пользователях рекламодателям, партнерам по измерениям, партнерам, предлагающие товары и услуги в продуктах компании Meta, поставщикам товаров и услуг, исследователям и ученым, а также правоохранительным органам, и другим органам по официальным запросам.

Любой пользователь продукции компании Meta имеет право на доступ к своим данным, а также на их исправление, перенос и удаление. Данные о пользователе хранятся до тех пор, пока компания не перестанет в них нуждаться для предоставление своих сервисов и продуктов или пока пользователь самостоятельно не удалит свой аккаунт – в зависимости от того, какое событие наступит раньше. Срок хранения данных определяется в индивидуальном порядке в зависимости от таких факторов, как характер данных, цель их сбора и обработки, а также соответствующие причины их хранения в интересах соблюдения закона или обеспечения работы.

При удалении аккаунта по запросу пользователя компания Meta удаляет всё, что пользователь публиковал.

Как написано в политике конфиденциальности WhatsApp [7], им необходимо получать и накапливать ту информацию, которая будет обеспечивать функционирование предоставляемых услуг, совершенствовать, анализировать, корректировать, поддерживать и продвигать эти услуги.

Компания WhatsApp хранит информацию о пользователях столько, сколько необходимо для своих целей. Срок хранения определяется в индивидуальном порядке в зависимости от таких факторов, как характер информации, цель её сбора и обработки и соответствующие юридические или операционные потребности в её хранения.

Пользователь может самостоятельно управлять своими данными, изменять их, а также удалять или ограничивать доступ к ним. При удалении аккаунта в WhatsApp пользователем все данные об этом пользователе будут удалены.

Компания Google собирает пользовательские данные для того, чтобы их сервисы были более удобными [5]. Google собирает пользовательские данные для обеспечения работы функций в сервисах Google, для поддержки и оптимизации сервисов Google, для разработки новых сервисов, для оценки эффективности, для поддержки связи с пользователями, а также для обеспечения безопасности компании Google, пользователей и других лиц.

Пользователь Google может потребовать от Google удалить контент из конкретного сервиса, а также собственноручно полностью удалить свой аккаунт.

Apple использует персональные данные для обеспечения работы своих служб, обработки транзакций пользователей, связи с пользователями, обеспечения безопасности, борьбы с мошенничеством и соблюдения законодательства. С согласия пользователя компания может использовать персональные данные в других целях [3].

Компания Apple использует персональные данные в случае, если для этого есть законные основания. В зависимости от обстоятельств, Apple может действовать, исходя из согласия пользователя, или того факта, что обработка необходима для исполнения договора с пользователем, защиты пользовательских жизненно важных интересов или интересов других лиц, или же для

соблюдения требований законодательства. Также могут обрабатываться персональные данные пользователя, если в компании полагают, что действуют в своих законных интересах или интересах других лиц, при этом учитывая интересы, права и ожидания пользователя.

Обсуждение

Как выяснилось в результате исследования, компании часто используют собранные пользовательские данные в своих целях, передают эти данные другим компаниям по разрешению пользователя, своим партнерам, а также по запросам государственных органов. Кому и куда будут переданы пользовательские данные, сам пользователь не знает.

В политиках конфиденциальности говорится лишь о том, что пользовательские данные передаются, но куда именно – не написано. Возможно, информация о том, куда передаются пользовательские данные, где-то указана, но чтобы её найти, нужно очень постараться. Станет ли это делать обычный пользователь, который очень хочет как можно скорее воспользоваться гаджетом/сервисом/услугой? Скорее всего, нет. Это подтверждается исследованиями [1; 2].

Многие пользователи используют данные сервисы бездумно. Люди не читают политику конфиденциальности, не глядя, соглашаются на нее, не читают сообщение об использовании их личных данных, которое появляется при регистрации на том или ином ресурсе. Люди стремятся быстрее начать пользоваться сервисом, и воспринимают такие информационные сообщения как что-то отнимающее время, ненужное. Тем самым они относятся безответственно к своей безопасности и безопасности своих личных данных.

Большинство пользователей данных сервисов не могут оценить, какой объемом персональных данных находится в распоряжении компаний и как этот факт может влиять на их жизнь.

Изучая последние разработки американских специалистов, можно сказать, что есть приложения, позволяющие выявить тех, кто следит за пользователем. Идея авторов подобных разработок заключается в том, чтобы показать компании, которые следят за онлайн-жизнью пользователей [10]. Это знание может показать пользователям, как используется их информация, а также привлечь внимание к различным случаям нарушения неприкосновенности частной жизни.

Как и кем может быть использован наш цифровой двойник? Сейчас об этом можно только догадываться.

Одно дело, если эта информация будет использована в благих целях – для предотвращения и раскрытия преступлений, поимки преступников.

Другое дело, когда ее использование будет нарушать границы частной жизни в угоду чьим-либо интересам – политическим, коммерческим, личным.

Но тут встает другой вопрос: «Могут ли интересы общественной безопасности стоять выше личного интереса?». Используя разные ресурсы, делясь своей личной информацией, большинство людей хотят сохранить свои данные в безопасности, а передача их от одного ресурса к другому увеличивает риски потери конфиденциальности.

Также никто не исключает возможности взлома пользовательского аккаунта злоумышленниками извне, ровно как никто не исключает возможности утечки данных с серверов той или иной компании. В современном мире это встречается довольно часто. Поэтому каждый пользователь сам должен следить за контентом, который он транслирует.

Отвечая на вопрос «Возможно ли сейчас сохранить свою конфиденциальность, имея цифрового двойника?», можно ответить с большой степенью ответственности, что сейчас это невозможно. Однако можно контролировать контент, который поступает на серверы данных сервисов. Думать перед тем, как делиться фотографией с подписчиками в социальных сетях. Ограничивать доступ к своей личной информации. С умом выбирать собеседников.

Может ли человек полностью управлять своим цифровым двойником?

Опираясь на результаты исследования, можно сказать, что полностью управлять своим цифровым двойником у пользователя не получится. Сам пользователь не знает, кому и куда будут переданы его пользовательские данные. Никто не даёт никаких гарантий, что после удаления

профиля в данных сервисах цифровой двойник пользователя и в самом деле удалится. Поэтому к выкладываемому на всеобщее обозрение контенту просто необходимо подходить с умом.

Заключение

Как же ответить на поставленные в статье вопросы:

1. Возможно ли сейчас сохранить свою конфиденциальность, имея цифрового двойника?

2. Может ли человек полностью управлять своим цифровым двойником?

Ответом будет: скорее нет, чем да. Каким бы безопасным не казался сервис, никогда не следует исключать возможности утечки данных пользовательского аккаунта (цифрового двойника) с серверов сервиса вследствие действий сотрудников сервиса [8] или стороннего взлома с целью кражи.

Что же делать пользователю, чтобы постараться сохранить свою конфиденциальность?

Во-первых, следует ответственно относиться к правилам использования его личных данных другими сервисами, компаниями, корпорациями, которым пользователь дает доступ к этой информации.

Во-вторых, обдуманно относиться к контенту, который пользователь размещает у себя в профиле, а также задуматься в том, что все данные, которые выложены в профиле, могут быть использованы другими людьми.

В-третьих, необходимо осознание того, что пользователь покупает различные электронные гаджеты для своего комфорта, и платит за это не только деньгами, но и своими персональными данными. Никто ведь не будет спорить, что социальные сети, гаджеты от Apple и сервисы от Google – это удобно и комфортно в использовании, однако они собирают персональные данные пользователя.

В дополнение к изложенному, для защиты персональных данных пользователей – раз уж Интернет охватывает весь мир – логичным было бы принять международные правила, регулирующие порядок обращения с цифровыми персональными данными. Сделать это нужно для защиты частной информации о наших цифровых двойниках, так как цифровые персональные данные в современном мире – это уже часть личности человека.

Литература

1. Данные тестирования: лишь каждый пятый студент при посещении сайтов читает пользовательское соглашение [Электронный ресурс]. URL: https://rkn.gov.ru/news/rsoc/news68102.htm

2. Никто не читает политику конфиденциальности – вот как это исправить [Электронный ресурс]. URL: https://rus.sciences-world.com/nobody-reads-privacy-policies-heres-how-fix-that-16696

3. Политика конфиденциальности, применимая к пользователям Apple в России [Электронный ресурс]. URL: https://www.apple.com/ru/legal/privacy/ru/

4. Политика конфиденциальности Facebook [Электронный ресурс]. URL: https://www.facebook.com/privacy/explanation

5. Политика конфиденциальности Google [Электронный ресурс]. URL: https://policies.google.com/privacy

6. Политика конфиденциальности Instagram [Электронный ресурс]. URL: https://help.instagram.com/519522125107875

7. Политика конфиденциальности WhatsApp [Электронный ресурс]. URL: https://www.whatsapp.com/legal/privacy-policy

8. СМИ: в сеть слили данные 1,5 млрд пользователей Facebook [Электронный ресурс]. URL: https://www.gazeta.ru/tech/news/2021/10/04/n_16637869.shtml

9. Что такое цифровые двойники. Объясняем простыми словами [Электронный ресурс]. URL: https://secretmag.ru/enciklopediya/chto-takoe-cifrovye-dvoiniki-obyasnyaem-prostymi-slovami.htm

10. Privacy apps to help fight back against companies that track you [Электронный ресурс]. URL: https://www.newscientist.com/article/mg22830492-300-privacy-apps-to-help-fight-back-against-companies-that-track-you/

11. Universal Declaration of Human Rights [Электронный ресурс]. URL: https://www.un.org/en/about-us/universal-declaration-of-human-rights