Либерально-демократические ценности / Journal of liberal democratic values https://liberal-journal.ru

2019, №3–4, Том 3 / 2019, No 3–4, Vol 3 https://liberal-journal.ru/issue-3-4-2019.html

URL статьи: https://liberal-journal.ru/PDF/02PLLD319.pdf

Ссылка для цитирования этой статьи:
Медведева Е.И. Использование персональных данных: правовой и этический аспекты // Либерально-демократические ценности, 2019 №3–4, https://liberal-journal.ru/PDF/02PLLD319.pdf (доступ свободный). Загл. с экрана. Яз. рус., англ.

For citation:
Medvedeva E.I. (2019). Use of personal data: legal and ethical aspects. *Journal of liberal democratic values*, [online] 3–4(3). Available at: https://liberal-journal.ru/PDF/02PLLD319.pdf (in Russian)

УДК 327.7

ГРНТИ 11.25.25

Медведева Екатерина Игоревна
ФГБОУ ВО «Санкт-Петербургский государственный университет», Санкт-Петербург, Россия
E-mail: ketmermaid@gmail.com

Использование персональных данных: правовой и этический аспекты

Аннотация. В статье автор рассматривает правовой и этический аспекты безопасности пользовательских данных владельцев гаджетов. Этот вопрос актуален с точки зрения мировой политики, поскольку из-за быстрого развития технологий и роста транснациональных корпораций законодательное регулирование этой сферы отстает от технических возможностей мобильных устройств и искусственного интеллекта. Это обстоятельство обращает наше внимание на корпоративную этику популярных брендов, продукты которых собирают данные о своих владельцах.

В своей работе автор опирался на монографию К. Дэвиса, посвященную этике работы с базами данных. Статья построена на анализе документов – пользовательских соглашений о конфиденциальности и законодательных актов. Автор исследует различные угрозы безопасности персональных данных, возникающие при использовании современных средств связи, и на их основе делает выводы о конфликтах, которые могут вспыхнуть в мировом политическом поле.

Как видно по результатам исследования, корпоративная этика компаний-гигантов допускает манипулирование данными пользователей: фирмы используют их для недобросовестной рекламы, продают третьим лицам и государствам. В связи с этим для мировой политики остро встает вопрос о новом законодательстве в сфере информационных технологий.

Кроме того, корпорации приобретают огромное политическое влияние в мире за счет массива персональных данных. Они угрожают нарушить «баланс интересов» стран, в связи с чем мы снова акцентируем внимание на необходимости изменений в национальном и международном законодательстве для защиты прав человека и сохранения международной стабильности.

Ключевые слова: глобальные проблемы; баланс интересов; информационная безопасность; корпоративная этика; персональные данные; автоматическая обработка данных; этика данных

По данным исследовательского центра Пью (Вашингтон) [1] 50 % американцев считают, что их персональные данные за последние пять лет стали менее защищены. По данным исследования Оксфордского университета [2] американцы связывают друг с другом кибератаки, цифровое манипулирование и угрозу конфиденциальности, как проблемы, затрагивающие большое количество людей, с которыми властям трудно бороться.

Свое бессилие против роста влияния транснациональных корпораций, связанных с IT-технологиями, осознают и национальные власти, что будет видно на примерах ниже. Чувство уязвимости у пользователей и затянувшееся бездействие государств и надгосударственных образований создают напряженную атмосферу на глобальном политическом поле. Угроза информационной безопасности – новый вызов мировой политике, и пока этот вызов не принят, единственное, что препятствует манипуляциям с личными данными – этические кодексы самих корпораций.

Проблему этики работы с данными для больших корпораций, занимающихся технологиями, поднимает в своей книге К. Дэвис. По его мнению конфликт возникает, в следствие того, что бизнес стремится к коммерческой выгоде, а этика воспринимается с точки зрения философии, как нечто директивное и сугубо теоретическое [3, p. 52], то есть накладывает излишние ограничения на развитие компаний.

Такие представления об этике не лишены основания. Так, в словаре по культурологии Б.И. Кононенко, этика определяется, во-первых, как философское учение о морали, изучающее условия возникновения морали, ее сущность, понятийные и императивные формы, и во-вторых, как система норм поведения нравственного человека, какой-либо общественной или профессиональной группы[1].

Однако, мы убеждены, что говорить об этике в бизнесе необходимо и особенно об этике поведения компаний, которые в силу специфики своего продукта – смартфонов, планшетов, умных часов – собирают огромное количество персональных данных каждую минуту. Назначение этих гаджетов заключается в сборе, обработке, сопоставлении и представлении больших объемов информации, обладателями которой неизбежно становятся IT-компании, как, например, гиганты Apple и Samsung. В связи с этим остро встает проблема информационной безопасности и защиты персональных данных. Поэтому все наиболее актуальной темой политических и научных дискуссий становится этическая проблема: не нарушает ли использование пользовательской информации, получаемой корпорациями, основные гражданские, политические и социальные права.

Для иллюстрации рассмотрим скандал с Apple, произошедший в апреле 2011: общественности сообщили [4], что iPhone регулярно записывали данные о перемещениях своих владельцев в закрытый файл, доступ к которому мог получить кто угодно через синхронизацию с устройством. Использование этой технологии отслеживания было этическим выбором разработчиков Apple, и этот выбор имел реальные последствия для безопасности и личной свободы пользователей.

В августе того же года владельцев смартфонов ждал новый удар: мобильное приложение Facebook без согласия выгружало данные из телефонной книги, в результате чего имена и номера телефонов оказывались в социальной сети, даже если человек не указывал его в своем аккаунте[2]. После скандала Facebook анонсировала возможность отключить автоматическую

[1] Большой толковый словарь по культурологии. Кононенко Б.И. 2003 [Электронный ресурс]. Код доступа: https://dic.academic.ru/dic.nsf/enc_culture/2623/Этика, свободный на 10.11.2019.

[2] Facebook сохранил у себя все номера из мобильных телефонов пользователей // Habr [Электронный ресурс]. Режим доступа: https://habr.com/ru/post/126162/, свободный на 20.11.2019.

Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

выгрузку данных, однако этический вопрос, почему они не сделали этого сразу при создании функции, остается открытым.

В 2015 приватность пользователей нарушила программа Google Photos [5]. Было обнаружено, что даже после удаления она продолжает скрытно от владельца устройства сохранять его фотографии в облаке. Google, получившая на просторах интернета прозвище «корпорация добра», посоветовала юзерам отключить в настройках синхронизацию и сочла скандал исчерпанным. Это было лишь начало разрушения «доброго» имиджа компании: в мае 2018 из корпоративного кодекса компании пропала ключевая фраза, бывшая девизом организации, – «не будь злом». Несколькими месяцами позже Google скрыла брешь в системе безопасности своей социальной сети Google+, и тогда же развернулся скандал с поисковиком Dragonfly, подверженном цензуре [6].

Эта история началась в 2010 году, когда Google были вынуждены покинуть китайский рынок, так как руководство фирмы отказалось нарушать право на свободу слова граждан Китая, цензурируя поисковую выдачу. И спустя 8 лет в прессу попала информация о том, что уже несколько лет Google секретно даже от властей США ведет разработку поисковика Dragonfly с жесткой цензурой по заказу китайского правительства. Зачем фирме рисковать своей репутацией и отношениями с властями страны, где зарегистрирован Google и в чьей юрисдикции он находится? Руководство компании объяснило это перспективой выйти на богатейший китайский рынок с миллиардом новых пользователей. Попытки власти США каким-то образом надавить на корпорацию провалились: на слушания в Сенате по обвинению в нарушении прав пользователей представители Google не явились.

Транснациональные корпорации стали полноправными акторами на политической арене. Их интересы могут идти вразрез с внешнеполитическими интересами стран, на территории которых они зарегистрированы, что может привести к национальному кризису. Подчеркнем, что международное законодательство в сфере информационной безопасности и национальные органы, курирующие эту сферу, не готовы к резкому росту влияния неправительственных организаций.

Куда еще устройства выгружают персональные данные? По словам главы ФБР Дж. Коми, всем лучше заклеивать объективы камер на ноутбуках и телефонах, так как наблюдать за пользователем могут спецслужбы [7]. И не только они, но и продвинутые хакеры [8]. Так, в апреле 2016 года, неизвестный получил доступ к компьютерам нескольких сотен пользователей и транслировал их жизнь на YouTube, как реалити-шоу. А в 2011 американский хакер сделал фотографии незнакомых девушек через веб-камеры и шантажировал их[3].

Если говорить о создании видео-роликов, рекламирующих гаджеты и другие товары, то в его основе лежит анализ огромной базы персональных данных, которую собирают о нас наши мобильные устройства. В ходе эмпирического анализа в нашем исследовании мы убедились, что каждый ролик ориентирован на конкретную целевую аудиторию, а их последовательность имеет свою хронологическую стратегию на несколько лет вперед. Маркетологи прибегали к сбору информации о пользователях на всех этапах рекламной деятельности, пользуясь статистикой для разработки сценариев, а далее – доступными базами данных о пользователях, чтобы не пустить рекламный бюджет на ветер на этапе продвижения. Использование личной информации в коммерческих целях определяет суть этической проблемы в сфере информационной безопасности.

[3] Hacker gets 6-year sentence for ‘sextortion’ // CBS News, 2 September 2011. Режим доступа: https://www.cbsnews.com/news/hacker-gets-6-year-sentence-for-sextortion/, свободный на 20.11.2019.

Смартфон записывает данные о наших запросах в поисковике и приложениях, знает, что у пользователей есть дети и домашние животные, по геопозиции определяет, как часто они путешествуют, и добираются ли на работу на машине или ходят пешком. Вся эта информация доступна и становится крючками, на которые клиентов ловят маркетологи. В этих условиях все более сложным становится вопрос приватности.

Смартфоны собирают данные о наших запросах в поисковиках и интересах, предлагая потом релевантный контент. Например, приложение iTunes можно приучить показывать только ту музыку, что тебе понравится. В последние годы смартфоны с функцией Touch ID и Face ID начали узнавать владельцев по отпечаткам пальцев и лицам. Куда биометрическая информация может попасть в случае нарушения безопасности их хранения?

На этих примерах мы видим, что крупные бренды становятся владельцами баз данных, содержащих персональную информацию, которую можно использовать с безграничным количеством целей, далеко не всегда в интересах ее владельцев. Все чаще мы наблюдаем примеры, как личная конфиденциальная информация, содержащаяся в устройстве, играет против своего правообладателя. Ежегодно происходят скандалы связанные с утечками данных и их недостаточной защищенностью, в связи с чем рушатся репутации компаний и их сотрудников. Законодательство, о чем пойдет речь ниже, не в состоянии предусмотреть темпы развития всех технических новшеств по работе с данными, поэтому положения актов, регулирующих сферу информационной безопасности, носят общий характер.

В России в области безопасной передачи данных действуют федеральные законы 2006 года ФЗ-149 «Об информации, информационных технологиях и защите информации» [4] и ФЗ-152 «О персональных данных» [5], также ратифицирована международная конвенция о «защите физических лиц при автоматизированной обработке данных»[6].

Они определяют способы передачи и хранения информации, а также накладывают ограничения на этот процесс в целях защиты прав человека и государства. Однако указанные нормативные акты не адаптированы к быстро меняющемуся миру гаджетов, технические возможности которых с каждым годом позволяют собирать все больше самой разнообразной информации о пользователях.

Политики делают попытки угнаться за техническим прогрессом. Например, 5 ноября 2019 года в первом чтении Государственная Дума приняла закон о предустановке российского программного обеспечения на смартфоны, компьютеры и смарт-ТВ [9]: мессенджеров, карт, поисковиков и др. По официальной версии это более удобно для российских пользователей и дает преимущество российским IT-компаниями в конкуренции с западными. Однако это можно рассмотреть и как ограничение: навязывание софта для тех, кто в нем не нуждается. Аналогичную двоякую ситуацию можно констатировать в части закона «о суверенном интернете» от 1 мая 2019 года[7]. Учитывая, что смартфон является базой данных о пользователе, то такие меры могут лишь привести к увеличению числа тех, кто может собирать эти данные.

[4] 149-ФЗ Об информации, информационных технологиях и защите информации. 27 июля 2006. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный на 20.11.2019.

[5] 152-ФЗ О персональных данных. 27 июля 2006. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/, свободный на 20.11.2019.

[6] Конвенция о «защите физических лиц при автоматизированной обработке данных. 28 января1981. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_121499/, свободный на 20.11.2019.

[7] Как будет действовать закон о «суверенном интернете»? // Государственная дума, 1 мая 2019. Режим доступа: http://duma.gov.ru/news/44676/, свободный на 20.11.2019.

Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

Неспособность законодательства предусмотреть все детали ведет нас к вопросу о необходимости создания этической политики, которая сможет быть применима на всех уровнях и транслироваться в действиях компании, ее рекламе и пользовательских соглашениях.

Чтобы побудить потребителя к приобретению товара реклама, в зависимости от целевой аудитории, транслирует различные ценности. Именно здесь и возникает пространство для манипуляции. Как показывает наше исследование, в 30 % случаев проводником ценностей бренда становится реклама, построенная на мифологических образах и сюжетах. Она демонстрирует полную клиентоориентированность бренда. Так, скрытый миф воздействует на эмоциональное состояние покупателя, заслоняя собой вопрос о безопасности.

Рассмотрим для примера рекламу Apple. Они представляют функцию iCloud – возможность хранения данных и копирования их на все ваши устройства под слоганом «Автоматически. Везде. iCloud» [8]. Функция представлена с использованием дихотомии «удобство – неудобство»: все книги, музыка и фотографии появляются, играючи, сразу на всех ваших устройствах. Ценность, транслируемую Apple в этом ролике, можно сформулировать так: «Мы заботимся о клиентах, поэтому сделали хранение и передачу данных легким и секундным делом».

После покупки устройство непременно предлагает пользователю принять «Политику конфиденциальности», где прописаны нюансы хранения, передачи и других операций с данными. Содержащиеся в этом документе этические принципы компании, безусловно, находятся в рамках общих положений законов, но могут сильно отличаться от той позиции безграничной заботы о пользователе, что была представлена в рекламе.

Было проведено исследование [3, pp. 29–39] «Политики конфиденциальности» у топ-50 компаний Fortune на 2012 год (куда входят и компании, производящие смартфоны, например, Apple и Microsoft), где их сравнили по определенным позициям. Из интересных нам результатов:

- 40 из 50 будут передавать данные третьим лицам, включая поставщиков и грузоотправителей. Только 2 из 50 документов содержат пункт о том, что компания сохранит личные данные в тайне. Оставшиеся 8 умолчали об этом, оставив решение вопроса на свое усмотрение.
- 33 из 50 сообщили, что пользователь может контролировать использование своих данных в целевой рекламе. 31 из 33 документов объяснили, как отказаться от задействования своих данных для рекламы, и только 17 направили на сайт для автоматического отказа без лишних процедур.
- 34 из 50 заявили, что не будут продавать личные данных. Хотя остальные открыто о продаже тоже не заявили.

Как мы видим по результатам исследования, ценность безграничной заботы о данных пользователя, показанная в рекламе, может разительно отличаться от положений, содержащихся в «Политике конфиденциальности».

Кроме то, компании имеют возможность по собственному усмотрению корректировать интерпретацию ключевых понятий нормативных актов. Согласно российскому законодательству персональные данные – это любая информация, относящаяся прямо или косвенно определенному или определяемому физическому лицу. В соглашении же, которое принимает пользователь устройства, это определение может быть изменено. Например, у

[8] Youtube, реклама Apple iCloud. Режим доступа: https://www.youtube.com/watch?v=vK5DjoGLk-0, свободный на 16.11.2019.

Google персональная информация[9] – это данные, которые вас идентифицируют (имя, e-mail, адрес, платежные данные) и другая информация, связанная с гугл-аккаунтом. Apple указывает, какие персональные и неперсональные данные она собирает, и как использует те и другие[10]. Важно отметить, что местоположение, они относят к неперсональным данным (хотя точно идентифицировать человека по этому параметру возможно, с чем и связан скандал 2012 года), а также они могут получить информацию о друзьях пользователя, если их смартфоны каким-то образом сообщились.

Исследователи ставят множественность этих определений под сомнение [3, p. 39]: любая информация о пользователе хранится вместе идентифицирующей его информацией, даже если весь этот блок имеет кодовое имя. Его можно расшифровать, что поставит безопасность под угрозу. Даже если какие-то данные собираются для рекламы или для владельцев приложений, набор их может оказаться уникальным, а пользователь – вычисляемым.

Почему пользователи так легко принимают эту политику? Потому что большинство даже не читали ее. По статистике 76 рабочих дней в год уходило бы на чтение всех политик конфиденциальности, которые в среднем принимает современный человек. Единицы обладают достаточным терпением и способностью разобраться во всех правовых нюансах, а 1/3 пользователей, согласно исследованию, нет дела, как используются компаниями их персональные данные [10]. Можно выделить две причины, по которой мы так безрассудно поступаем с нашими данными, доверяя их устройствам и брендам:

- Во-первых, мало компаний, которые делают свои соглашения читаемыми и доступными пользователю. Это является проявлением их стратегии в отношении к клиентам, где прибыль ставится выше честности. Намного проще в рекламе создать образ дружественного к пользователям бренда и предложить запутанное соглашение, которое никто не будет читать.
- Во-вторых, сами пользователи уже поддались на посыл рекламных роликов и приобрели устройство. Юридические формальности – последнее, что волнует человека, затянутого в сети «общества потребления» и поглощенного покупкой самой вещи и «магии» в ней сокрытой [11, с. 208]. Теперь смартфон узнает его лицо и автоматически разблокируется. Потребитель присваивает образ, созданный рекламой, что сродни верованию в знаки и ритуалы у древних людей. Не удивительно, что инновационные товары продаются за счет использования мифов в рекламе.

В целом, как мы видим, в рекламе бренды легко могут манипулировать пользователем, поэтому вопрос этики звучит так остро. Если реклама призвана усыплять бдительность потребителя и нарочито транслирует обманчивые ценности компании, то изучение рекламных кампаний становится необходимым для распознания недобросовестного поведения IT-бизнеса.

В заключение мы выделим основные проблемы:

- национальное и международное законодательство в сфере информационной безопасности не успевает реагировать на расширение перечня собираемых компаниями данных. Таким образом, этика корпораций практически не ограничена, что дает возможность для нарушения личной безопасности граждан

[9] Google Privacy Policy // Google Privacy&Terms. Режим доступа: https://policies.google.com/privacy?hl=en-US, свободный на 20.11.2019.

[10] Apple Privacy Policy // Apple, 29 August 2019. Режим доступа: https://www.apple.com/legal/privacy/en-ww/, свободный на 20.11.2019.

Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

и манипуляций с персональными данными, в том числе и в рекламе за счет использования мифологических сюжетов;

- транснациональные корпорации приобретают политическое влияние за счет обладания массивами персональных данных и возможностью манипулировать ими. Корпоративная этика фирм в данной ситуации может служить гарантом сохранения «баланса интересов» стран;
- возникает угроза столкновения национальных интересов при операциях с данными пользователей, которые производят корпорации. Это связано с двумя особенностями их работы: во-первых, с трансграничной передачей данных и разными законодательствами по их обработке на территории каждой страны, и, во-вторых, с нахождением самой корпорации под юрисдикцией одного государства, где она зарегистрирована, и осуществлением ее деятельности в другой стране, законы которой отличаются от принятых в страны регистрации фирмы.

Процесс быстрого роста числа гаджетов, собирающих данные, и роста их технических возможностей может стать новым глобальным вызовом мировой политике. Найти «баланс интересов» в мировом сообществе без создания подробной международной правовой базы невозможно, и пока это не сделано, бренды-производители только усугубляют конфликт, нарушая этику работы с данными пользователей.

Пользуясь тем, что пользовательские соглашения никто не читает, компании активно собирают данные о пользователях, чтобы эффективно использовать их для совершенствования рекламных стратегий. Это пример явной манипуляции, поэтому вопрос об этике и ужесточении законодательства на национальных уровнях и в международном масштабе так актуален.

Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

ЛИТЕРАТУРА

1. Smith A. Americans and Cybersecurity // Pew Research Centre, 26 January 2017. [Электронный ресурс]. Режим доступа: https://www.pewresearch.org/internet/2017/01/26/1-americans-experiences-with-data-security/, (свободный 20.11.2019).
2. Zhang B., Dafoe A. Artificial Intelligence: American Attitudes and Trends // Center for the Governance of AI, Future of Humanity Institut, University of Oxford, January 2019 [Электронный ресурс]. Режим доступа: https://governanceai.github.io/US-Public-Opinion-Report-Jan-2019/, (свободный 20.11.2019).
3. Davis K. Ethics of Big Data [Текст]. Sebastopol: O'Reilly, 2012. 82 p.
4. Горяинов Н. iPhone следит за своим владельцем // iphones.ru, 20 апреля 2011 [Электронный ресурс]. Режим доступа: https://www.iphones.ru/iNotes/135674, (свободный 20.11.2019).
5. Kumar M. Google Photo App Uploads Your Images to Cloud, Even After Uninstalling // The Hacker News, 13 July 2015 [Электронный ресурс]. Режим доступа: https://thehackernews.com/2015/07/google-photo-app-sync.html, (свободный 20.11.2019).
6. Герасюкова М. Корпорация зла: как Google предала идеалы // Газета.ru, 13 октября 2018 [Электронный ресурс]. Режим доступа: https://www.gazeta.ru/tech/2018/10/12/12018853/google_evil.shtml, (свободный 16.11.2019).
7. Hattem J. FBI Director: Cover up your webcam // The Hill, 14 September 2016 [Электронный ресурс]. Режим доступа: https://thehill.com/policy/national-security/295933-fbi-director-cover-up-your-webcam, (свободный 20.11.2019).
8. Лихачев Н. Пользователь «Двача» превратил в шоу наблюдение за людьми через веб-камеры их взломанных компьютеров // Блогплатформа TJ, 27 апреля 2016 [Электронный ресурс]. Режим доступа: https://tjournal.ru/flood/27199-polzovatel-dvacha-prevratil-v-shou-nablyudenie-za-lyudmi-cherez-veb-kamery-ih-vzlomannyh-kompyuterov, (свободный 16.11.2019).
9. Герасюкова М. Запрет на продажи: все смартфоны получат российский софт // Газета.ru, 5 ноября 2019 [Электронный ресурс]. Режим доступа: https://www.gazeta.ru/tech/2019/11/05/12796460/russian_soft.shtml, (свободный 16.11.2019).
10. Boyon N., Wallard H. Ignorance and Distrust Prevail about What Companies and Governments Do with Personal Data // Ipsos, 25 January 2019 [Электронный ресурс]. Режим доступа: https://www.ipsos.com/en/ignorance-and-distrust-prevail-about-what-companies-and-governments-do-personal-data, (свободный 16.11.2019).
11. Бодрийяр Ж. Общество потребления. Его мифы и структуры [Текст]. М.: Культурная революция, Республика, 2006. 269 с. (в пер.).

Medvedeva Ekaterina Igorevna
Saint-Petersburg state university, Saint-Petersburg, Russia
E-mail: ketmermaid@gmail.com

Use of personal data: legal and ethical aspects

Abstract. The author of the article considers legal and ethical aspects of gadget owners' user-data security. The issue is relevant because of the fast-growing global corporations and technologies. Due to such a rapid development, the legislative regulation of cyber security lags behind the technical capabilities of mobile devices and artificial intelligence. This fact draws our attention to the corporate ethics of popular brands whose products collect information about their owners.

The author refers to a monograph of Cord Davis on the ethics of big data. Current article is based on the analysis of user confidentiality agreements and legislative acts. The research goes through various threats to personal data security caused within modern means of communication. The text is concluded with the conflicts might be erupted in the global political field. As a result we prove, the business integrity of global companies allows data manipulation. Brands could use them for unfair advertising or sell to third parties and states. Considering this, the issue of a new law in cyber security sphere is demanded. Moreover, transnational corporations acquire political leverage by collecting huge amount of personal data. It is a threat to upset the balance of political forces and this is a call for another argument in cyber security legislation.

Keywords: artificial intelligence; cybersecurity; ethics of big data; global political problems; business integrity; personal data; balance of political power; automated data processing

REFERENCES

1. Smith A. Americans and Cybersecurity // Pew Research Centre, 26 January 2017. [Ehlektronnyy resurs]. Rezhim dostupa: https://www.pewresearch.org/internet/2017/01/26/1-americans-experiences-with-data-security/, (svobodnyy 20.11.2019).
2. Zhang B., Dafoe A. Artificial Intelligence: American Attitudes and Trends // Center for the Governance of AI, Future of Humanity Institut, University of Oxford, January 2019 [Ehlektronnyy resurs]. Rezhim dostupa: https://governanceai.github.io/US-Public-Opinion-Report-Jan-2019/, (svobodnyy 20.11.2019).
3. Davis K. Ethics of Big Data [Tekst]. Sebastopol: O'Reilly, 2012. 82 p.
4. Goryainov N. iPhone sledit za svoim vladel′tsem // iphones.ru, 20 aprelya 2011 [Ehlektronnyy resurs]. Rezhim dostupa: https://www.iphones.ru/iNotes/135674, (svobodnyy 20.11.2019).
5. Kumar M. Google Photo App Uploads Your Images to Cloud, Even After Uninstalling // The Hacker News, 13 July 2015 [Ehlektronnyy resurs]. Rezhim dostupa: https://thehackernews.com/2015/07/google-photo-app-sync.html, (svobodnyy 20.11.2019).
6. Gerasyukova M. Korporatsiya zla: kak Google predala idealy // Gazeta.ru, 13 oktyabrya 2018 [Ehlektronnyy resurs]. Rezhim dostupa: https://www.gazeta.ru/tech/2018/10/12/12018853/google_evil.shtml, (svobodnyy 16.11.2019).
7. Hattem J. FBI Director: Cover up your webcam // The Hill, 14 September 2016 [Ehlektronnyy resurs]. Rezhim dostupa: https://thehill.com/policy/national-security/295933-fbi-director-cover-up-your-webcam, (svobodnyy 20.11.2019).
8. Likhachev N. Pol′zovatel′ «Dvacha» prevratil v shou nablyudenie za lyud′mi cherez veb-kamery ikh vzlomannykh komp′yuterov // Blogplatforma TJ, 27 aprelya 2016 [Ehlektronnyy resurs]. Rezhim dostupa: https://tjournal.ru/flood/27199-polzovatel-dvacha-prevratil-v-shou-nablyudenie-za-lyudmi-cherez-veb-kamery-ih-vzlomannyh-kompyuterov, (svobodnyy 16.11.2019).
9. Gerasyukova M. Zapret na prodazhi: vse smartfony poluchat rossiyskiy soft // Gazeta.ru, 5 noyabrya 2019 [Ehlektronnyy resurs]. Rezhim dostupa: https://www.gazeta.ru/tech/2019/11/05/12796460/russian_soft.shtml, (svobodnyy 16.11.2019).
10. Boyon N., Wallard H. Ignorance and Distrust Prevail about What Companies and Governments Do with Personal Data // Ipsos, 25 January 2019 [Ehlektronnyy resurs]. Rezhim dostupa: https://www.ipsos.com/en/ignorance-and-distrust-prevail-about-what-companies-and-governments-do-personal-data, (svobodnyy 16.11.2019).
11. Bodriyyar Zh. Obshchestvo potrebleniya. Ego mify i struktury [Tekst]. M.: Kul′turnaya revolyutsiya, Respublika, 2006. 269 s. (v per.).

Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com