DOI: 10.14515/monitoring.2023.3.2314

С. Г. Ушкин, Е. А. Коваль

АЛИСА, ТЫ СЛЕДИШЬ ЗА МНОЙ? ВОСПРИЯТИЕ КОНФИДЕНЦИАЛЬНОСТИ В НАРРАТИВАХ ПОЛЬЗОВАТЕЛЕЙ «УМНЫХ» КОЛОНОК

Правильная ссылка на статью:
Ушкин С. Г., Коваль Е. А. Алиса, ты следишь за мной? Восприятие конфиденциальности в нарративах пользователей «умных» колонок // Мониторинг общественного мнения: экономические и социальные перемены. 2023. № 3. С. 23—40. https://doi.org/10.14515/monitoring.2023.3.2314.
For citation:
Ushkin S. G., Koval E. A. (2023) Alice, Are You Following Me? Perception of Confidentiality in the Narratives of Smart Speaker Users. Monitoring *of Public Opinion: Economic and Social Changes.* No. 3. P. 23–40. https://doi.org/10.14515/monitoring.2023.3.2314. (In Russ.)

Получено: 24.09.2022. Принято к публикации: 15.03.2023.

DOI: 10.14515/monitoring.2023.3.2314

АЛИСА, ТЫ СЛЕДИШЬ ЗА МНОЙ? ВОСПРИЯТИЕ КОНФИДЕНЦИАЛЬНОСТИ В НАРРАТИВАХ ПОЛЬЗОВАТЕЛЕЙ «УМНЫХ» КОЛОНОК

ALICE, ARE YOU FOLLOWING ME? PERCEPTION OF CONFIDENTIALITY IN THE NARRATIVES OF SMART SPEAKER USERS

УШКИН Сергей Геннадьевич — кандидат социологических наук, ведущий научный сотрудник отдела мониторинга социальных процессов, Научный центр социально-экономического мониторинга, Саранск, Россия; исследовательский менеджер Всероссийского центра изучения общественного мнения, Москва, Россия
E-MAIL: ushkinsergey@gmail.com
https://orcid.org/0000-0003-4317-6615

КОВАЛЬ Екатерина Александровна — доктор философских наук, профессор кафедры уголовно-процессуального права и криминалистики, Средне-Волжский институт (филиал) Всероссийского государственного университета юстиции (РПА Минюста России), Саранск, Россия
E-MAIL: nwifesc@yandex.ru
https://orcid.org/0000-0003-0069-5335

Sergey G. USHKIN[1,2] — Cand. Sci. (Soc.), Leading Researcher at the Department for Monitoring Social Processes; Research Manager
E-MAIL: ushkinsergey@gmail.com
https://orcid.org/0000-0003-4317-6615

Ekaterina A. KOVAL[3] — Dr. Sci. (Philos.), Professor at the Department of Criminal Procedure Law and Criminalistics of the Middle Volga Institute (branch) of the All-Russian State University of Justice (RLA of the Ministry of Justice of Russia)
E-MAIL: nwifesc@yandex.ru
https://orcid.org/0000-0003-0069-5335

[1] Scientific Center for Socio-Economic Monitoring, Saransk, Russia
[2] Russian Public Opinion Research Center (VCIOM), Moscow, Russia
[3] Middle Volga Institute (branch) of the All-Russian State University of Justice (RLA of the Ministry of Justice of Russia), Saransk, Russia

Аннотация. «Умные» колонки завоевывают популярность во всем мире, и Россия — не исключение. Особенность «умных» колонок, привлекающая пользователей, заключается в интеграции в них голосовых помощников, общение с которыми происходит посредством вербальных команд. Тем не менее кажущаяся простота и удобство общения с «умными» колонками могут быть обманчивыми. Ряд научных статей, посвященных человекомашинному взаимодействию, поднимают проблему конфиденциальности информации, поскольку пользователь никоим образом

Abstract. “Smart” speakers are gaining popularity worldwide, and Russia is no exception. The feature of “smart” speakers that attracts users is the integration of voice assistants into them, communication with which takes place through verbal commands. Nevertheless, the apparent simplicity and convenience of communicating with “smart” speakers can be deceptive. Many scientific articles devoted to human-machine interaction raise the issue of information confidentiality since the user is in no way protected from penetration into his private life. In this context, we

DOI: 10.14515/monitoring.2023.3.2314

не защищен от проникновения в его частную жизнь. В этом контексте мы поставили перед собой задачу осмыслить повседневные практики человекомашинного взаимодействия, акцентируя внимание на социальной безопасности при взаимодействии с гаджетами. Для этого в марте 2022 г. мы провели 20 полуструктурированных интервью среди пользователей «умных» колонок в г. Саранске. В ходе исследования мы пытались выяснить, боятся ли российские пользователи «утечек» данных через «умные» колонки; на кого они возлагают ответственность за это; наконец, следуют ли они каким-либо мерам предосторожности при взаимодействии с устройствами. Полученные результаты свидетельствуют, что большинство информантов не видят существенных проблем в коммуникации с «умными» колонками, чаще всего рассматривая их как обычный бытовой прибор. Схема взаимодействия с ними заключается в даче простой вербальной команды («включить музыку», «поставить таймер» и т. д.), не требующей ведения последующего диалога. Коммуникация с девайсами становится рутиной, они воспринимаются как неотъемлемая часть домашней обстановки, позволяющая структурировать досуговые практики. В паре «комфорт — безопасность» пользователи, по всей видимости, выбирают первое: о проблемах с конфиденциальностью они предпочитают не задумываться, хотя в то же время стараются не общаться с устройствами на острые социально-политические темы.

Ключевые слова: голосовые помощники, искусственный интеллект, человекомашинное взаимодействие, искусственная социальность, конфиденциальность, «умные» колонки

have tasked ourselves with comprehending the everyday practices of human-machine interaction, focusing on social security when interacting with gadgets. To do this, in March 2022, we conducted 20 semi-structured interviews among users of “smart” speakers living in Saransk. In the course of the study, we tried to find out whether Russian users are afraid of “leaks” of data through “smart” speakers; whom they hold responsible for this; and finally, whether they follow any precautions when interacting with devices. The results indicate that most informants do not see significant problems in communication with “smart” speakers, most often considering them as ordinary household appliances. The scheme of interaction with them consists in giving a simple verbal command (“turn on the music”, “set the timer”, etc.), which does not require a subsequent dialogue. Communication with devices becomes routine. They are perceived as an integral part of the home environment, allowing one to structure leisure practices. In the “comfort — security” pair, users choose the first: they prefer not to think about privacy problems, but they try not to communicate with devices on acute socio-political topics.

Keywords: voice assistants, artificial intelligence, human-machine interaction, artificial sociality, confidentiality, “smart” speakers

DOI: 10.14515/monitoring.2023.3.2314

Введение

«Умные» колонки представляют собой устройства с интегрированными голосовыми помощниками, которые используют искусственный интеллект и обработку естественного языка для облегчения функциональных и гедонистических задач, таких как прослушивание музыки, установка напоминаний и получение информации из интернета [Lutz, Newlands, 2021: 147]. Их возможности из года в год расширяются, они становятся не просто объектами, но и субъектами взаимодействия, способными поддерживать диалоговую коммуникацию, а в отдельных случаях — предоставлять населению услуги по социальному обеспечению на дому [Hamblin, 2020: 117]. Более того, по замечаниям исследователей, в тех случаях, когда они вместе с другими «умными» устройствами (лампочками, розетками, пылесосами и т. д.) образуют общую экосистему, само домашнее пространство становится социальным, поскольку вынуждено реагировать на потребности жильцов, прежде всего через голосовые интерфейсы [Корбут, 2021: 198].

«Умные» колонки, приобретаемые как устройство-в-себе или как центр управления «умным» домом, быстро набирают популярность по всему миру. Например, в США, где подобные устройства появились одними из первых, по состоянию на первый квартал 2022 г. доля их пользователей достигла 35 % (в абсолютном выражении — 100 млн жителей от 18 лет и старше), а ежегодный прирост в пятилетней ретроспективе варьируется от 2 до 5 п.п[1]. В Великобритании «умные» колонки имеются у 50 % домохозяйств (то есть речь идет о примерно 34 млн человек всех возрастов), по сравнению с 2019 г. их доля увеличилась на 30 п.п[2]. Сведения о российских пользователях устройств представлены гораздо скуднее и опираются не на опросы населения, а преимущественно на раскрываемые данные ритейлеров. Так, на конец 2021 г. в России реализовано всего лишь порядка 4 млн гаджетов, и, по оценкам специалистов, рынок далек от насыщения[3]. Наиболее популярные устройства поставляются компанией «Яндекс», следом за ней с большим отставанием располагаются Сбер и VK. Каждая колонка располагает собственным голосовым помощником, который обладает присущими только ему «личностными характеристиками»[4]: Алиса от «Яндекса», Салют от «Сбера» и Маруся от VK.

Принцип работы «умных» колонок заключается в том, что говорящий должен произнести «побудительное» слово (например, «Алиса», «Маруся» и т. д.), которое выведет гаджет из спящего режима и позволит ему обнаружить голосовую команду и соответствующим образом на нее отреагировать, направив запрос на удаленный сервер. Мониторинг речевых триггеров ведется в постоянном режиме,

[1] The Smart Audio Report. URL: https://www.nationalpublicmedia.com/uploads/2022/06/The-Smart-Audio-Report-Spring-2022.pdf (дата обращения: 19.08.2022).

[2] Media Nations 2021: UC. URL: https://www.ofcom.org.uk/__data/assets/pdf_file/0023/222890/media-nations-report-2021.pdf (дата обращения: 19.08.2022).

[3] Рынок умных колонок и голосовых ассистентов в России и мире: ежегодное исследование Just AI. URL: https://just-ai.com/blog/rynok-umnyh-kolonok-i-golosovyh-assistentov-v-rossii-i-mire-ezhegodnoe-issledovanie-just-ai (дата обращения: 19.08.2022).

[4] Термин «личностные характеристики» в отношении «умных» колонок находит все большее употребление в работах западных исследователей, в первую очередь тех из них, кто занимается разработкой решений для голосовых помощников [Poushneh, 2021]. В некотором смысле он обладает перформативностью, поскольку приближает нас к образу устройства, где размываются границы между искусственной и не-искусственной социальностью.

DOI: 10.14515/monitoring.2023.3.2314

для этого задействованы встроенные микрофоны, улавливающие изменения окружающей среды без доступа к интернету. Некоторые модели позволяют их отключить, в таком случае активация команд будет происходить после нажатия специальной физической кнопки на корпусе устройства. При этом «умные» колонки зачастую используются в приватных пространствах (дом, квартира, комната). Это одна из основных причин, по которым проблема потенциальных утечек конфиденциальной информации все больше укореняется в научном и публичном дискурсе [Lau, Zimmerman, Schaub, 2018].

Но осознают ли сами пользователи потенциальную опасность «умных» колонок? Результаты исследований зарубежных коллег носят амбивалентный характер, и, по всей видимости, зависят от методики их проведения, целей и задач. Например, масштабная работа по анализу 4 500 отзывов о работе линейки «умных» колонок Echo, собранных на Amazon, не выявила актуализации темы конфиденциальности [Maccario, Naldi, 2022]. Люди демонстрируют свое положительное отношение к устройствам, о проблемах, связанных с использованием персональных данных, упоминают не более 3 % от всей выборки.

Результаты направленных качественных исследований свидетельствуют о том, что пользователи могут испытывать недоверие к «умным» колонкам и тревогу по поводу конфиденциальности, полагая, что получить их персональные данные и иную приватную информацию могут не только производители гаджетов, но и домочадцы, соседи, гости и т. д. [Huang, Obada-Obieh, Beznosov, 2020]. Те, кто попадает в «поле зрения» колонки, тоже испытывают определенное беспокойство. [Marky et al., 2020]. Ситуацию осложняет то, что пользователи, как правило, плохо понимают, где хранятся их данные, как обрабатываются и куда передаются[5] [Hyang et al., 2020].

В других работах упоминается «парадокс конфиденциальности», возникающий тогда, когда пользователи (сайтов, гаджетов и т. д.) практически не прилагают усилий для защиты своих персональных данных, поскольку получаемая выгода перевешивает потенциальные потери [Gerber, Gerber, Volkamer, 2018; Kowalczuk, 2018]. Недавние исследования подтверждают и усиливают этот тезис. В частности, сравнение поведенческих моделей пользователей и не-пользователей «умных колонок» указывает на то, что первая группа практически не задумывается о возможных рисках, пока получает определенные преимущества, в то время как вторая, во всяком случае декларативно, сосредоточена на большем контроле конфиденциальности [O'Maonaigh, Saxena, 2021].

Более того, соображения безопасности — вторая по популярности причина отказа от покупки «умной» колонки среди потребителей в США после высокой стоимости гаджетов [Barbosa, Zhang, Wang, 2020]. Согласно общенациональному репрезентативному опросу интернет-пользователей в Великобритании, опасения по поводу рисков конфиденциальности перевешивают преимущества «умного» дома, заявляемые производителями [Cannizzaro et al., 2020].

[5] Abdi N., Ramokapane K. M., Such J. M. (2019). More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. In: *Proceedings of the Fifteenth Symposium on Usable Privacy and Security*. Santa Clara, CA: USENIX Association. P. 451—466. URL: https://www.usenix.org/conference/soups2019/presentation/abdi (дата обращения: 23.06.2023).

DOI: 10.14515/monitoring.2023.3.2314

Показательно, что дискуссии пользователей социальных сетей вокруг вопросов кибербезопасности и приватности, не являющихся экспертами в них, выявляет устойчиво высокие опасения по поводу бесконтрольного сбора данных «умными» устройствами и передачи их третьим лицам (государственные органы, бизнес) [Pattnaik, Li, Nurse, 2023]. Впрочем, здесь стоит говорить о наличии другого парадокса: говоря о защите личной жизни, авторы сообщений не только сделали публичными свои позиции, но и имплицитно дали возможность эти позиции исследовать (поскольку эти данные открыты для третьих лиц). Между тем беспокойство по поводу сохранения конфиденциальности при использовании «умных» устройств обострилось в период пандемии, которая спровоцировала ускоренное развитие дистанционных форм обучения и труда. Вместе с ними выросли и запросы на экспертную помощь, которую неквалифицированным пользователям удается получить не всегда, что влечет за собой разочарование как в устройствах, так и в их производителях. Попытаемся обобщить основные претензии пользователей и не-пользователей подобных устройств в контексте конфиденциальности передаваемых данных, обозначенные в научной литературе (см., например, [Chalhoub, Flechais, 2020; Mhaidli et al., 2020; Pattnaik, Li, Nurse, 2023] и др.).

Первая заключается в наличии потенциальной возможности «умных» колонок мониторить все разговоры внутри дома, начиная от того, что мы говорим на кухне, и заканчивая тем, что воспроизводится телевизором. Известны случаи, когда доступ третьих лиц к таким данным оказывал непосредственное влияние не только на личную жизнь пользователей, но и на их карьеру [Jayatilleke, Thelijjagoda, Pathirana, 2019].

Вторая связана с прослушиванием разговоров, осуществляемых посредством встроенных в интерфейс устройства аудио- или видеозвонков. Протокол передачи данных, как правило, не защищен, существуют уязвимости, которые могут быть использованы злоумышленниками.

Третья вытекает из того, что все голосовые команды передаются на удаленный сервер и хранятся на нем в течение длительного времени: обычно разработчики голосовых помощников набирают специальный штат, который прослушивает их для последующего улучшения распознавания речи. В ряде случаев анализируемая информация не обезличивается, и к ней остаются привязанными история предыдущих запросов, IP-адреса, геолокация и даже платежные карты.

В соответствии с вышесказанным можно выделить несколько основных групп, заинтересованных в утечках пользовательских данных. Во-первых, это сами компании, производящие «умные» колонки и/или работающие с голосовыми помощниками, которые могут использовать полученную информацию как для повышения качества работы своих устройств, так и для передачи третьим лицам (например, чтобы в дальнейшем предоставлять таргетинговую рекламу). Во-вторых, это злоумышленники, чей интерес в первую очередь выражен в краже персональных данных, вплоть до записанных образцов голоса (он может быть использован для подтверждения финансовых операций). В-третьих, это органы правопорядка, которым важен не только доступ к разговорам потенциальных субъектов правонарушения, но и к истории их запросов, содержащих параданные, способные помочь раскрытию преступления (что пользователь искал в интернете, какие заказы делал в интернет-магазинах, осуществлял ли вызов такси и т. д.).

DOI: 10.14515/monitoring.2023.3.2314

Боятся ли российские пользователи «утечек» данных через «умные» колонки? На кого они возлагают ответственность за это? Следуют ли они каким-либо мерам предосторожности при взаимодействии с устройствами? На эти и другие вопросы пытаются ответить авторы настоящей статьи. Важно отметить, что мы сознательно отказались от обсуждения некоторых важных тем (например, детальное описание практик использования голосовых помощников, коммуникативные сбои в человекомашинных взаимодействиях и реакции на них, перспективы человекомашинного взаимодействия), поскольку затрагивали их в нашей предыдущей работе [Ушкин, Коваль, Яськин, 2022].

Дизайн и методы исследования

Эмпирическую базу исследования составили 20 полуструктурированных глубинных интервью с пользователями «умных» колонок, взаимодействующих с ними с различной степенью интенсивности. Среди участников исследования семь мужчин и четырнадцать женщин, их возраст варьируется от 21 года до 50 лет[6]. Рекрутинг информантов осуществлялся через сильные и слабые социальные связи интервьюеров. Трудности возникли с достижимостью возрастных и одиноких людей, которые пользовались бы голосовыми помощниками. Это — одно из ключевых ограничений исследования.

Сбор данных выполнен в марте 2022 г. в гибридном формате: одиннадцать интервью осуществлены очно, шесть — посредством телефонного общения, три — посредством обмена голосовыми или текстовыми сообщениями в виртуальных социальных сетях и мессенджерах. В первых двух случаях они продолжались от 15 до 50 мин., в третьем — достигали трех дней (ввиду повышенной занятости информанты отвечали в удобное для них время).

Предполагалось, что среди информантов, имеющих детей (13 человек), интервью будет проведено в диадах (родитель — ребенок). Только два из них осуществлены подобным способом, и они сводились преимущественно к фиксации непосредственного взаимодействия ребенка и «умной» колонки «здесь и сейчас». Дети мало участвовали в разговоре, и это становится общим местом для диадных интервью [Чередеева, Савинская 2018: 443]. Поэтому они остались родительским нарративом и мало отличались от того, что сообщили о практиках коммуникации своих детей и голосового помощника другие информанты.

Результаты

Подавляющее большинство информантов прямо или косвенно указывают на то, что «умные» колонки стали для них неотъемлемым элементом домашней социальности, а повседневные взаимодействия с ними рутинизировались. В первую очередь это произошло ввиду естественности коммуникации с устройством, которое обрабатывает поступающие запросы и дает обратную реакцию на них. Только один опрошенный заявил, что использование гаджета представляет для него своего рода таинство, поскольку для этого необходимо совершить ряд подготовительных операций (включение телевизора, запуск приложения). Наибо-

[6] Основные социально-демографические характеристики информантов и способы их интервьюирования приведены в Приложении.

DOI: 10.14515/monitoring.2023.3.2314

лее востребованными функциями пользователи называют прослушивание музыкального контента, получение ответов на интересующие вопросы, установку таймеров и будильников, управление «умным» домом или отдельными его устройствами; в продвинутых версиях популярным времяпрепровождением становится просмотр видеоконтента.

Да, к ней быстро привыкаешь. «На автомате» включаю. Например, музыку фоном ставлю и делаю домашние дела. (Инф. 7)

Работает она исправно, жалоб нет. И да — колонка уже стала привычным устройством, как сотовый телефон. (Инф. 20)

Существенным расширением функционала «умных» колонок служат запросы детей, которые, используя устройство, не только познают мир, но и перенимают поведенческие и речевые паттерны. Отмечается рост интереса к обучению, поскольку взаимодействие с устройством у ребенка вызывает неподдельный интерес, а также улучшение коммуникативных навыков и устранение возрастных дефектов речи.

Мы сейчас просто на том этапе, когда учим ребенка, чтобы максимально правильно формулировать мысли, сначала подумать, а потом сказать. Но сейчас она стала уже думать, потому что иногда это бывает просто поток всего, а сейчас стали замечать, что у нас случаются и «проблески» — сначала подумает, а потом задаст [вопрос]. *Или начинает неправильно задавать, формулировать свой вопрос, запрос, сама осекается, а потом уже все делает правильно. То есть быть более конкретной.* (Инф. 6)

Вот, например, у него [ребенка] *недавно по окружающему миру был вопрос, ну, про планеты Солнечной системы, мы в книге изучали. Соответственно, я прошел потом в гостиную, и я ему через эту умную колонку также задал такой запрос, и ему там тоже наглядно рассказали о планетах Солнечной системы. То есть с разных, как говорится, мест тоже стараюсь привить вот эти вот моменты, связанные с обучением.* (Инф. 1)

Репертуар использования варьируется в зависимости от пространственного размещения «умной» колонки, и особенно хорошо это просматривается на примере тех информантов, которые либо регулярно переносят устройства из одной локации в другую, либо имеют несколько устройств, расположенных в разных комнатах. Подавляющее большинство пользователей располагают их в наиболее посещаемых местах своего дома — либо в гостиной, либо на кухне. В таком случае они становятся досуговыми центрами, объединяющими членов семьи за совместным времяпрепровождением. Однако если в гостиной гаджет отвечает преимущественно за реализацию «принципа удовольствия», то на кухне он может выполнять функции радио, таймера или интерактивной книги рецептов, то есть решать преимущественно утилитарные задачи. Существенно реже информанты заявляли о том, что устройства находятся во взрослой спальне или в комнате ребенка. В первом случае доминирующие мотивы использования — прослушивание музы-

DOI: 10.14515/monitoring.2023.3.2314

ки, просмотр фильмов, установка будильника; во втором — прослушивание музыки, чтение сказок, интерактивные игры.

Так как в основном мы слушаем музыку, то утром включаю, чтобы разбудить сына, ему нравится, когда его бужу песней, утренняя зарядка. Колонка находится на кухне, вечером сын может взять к себе послушать сказку перед сном. (Инф. 13)

Колонку на кухне используем в основном для прослушивания радио, музыки, поиска рецептов и т. д. В общей комнате вообще для разных целей — музыка, видео, сказки для ребенка, голосовые заметки и прочее. (Инф. 5)

Проникновение «умных» колонок, потенциально имеющих возможность вести запись окружающей обстановки, в пространство дома, ранее считавшееся приватным, представляет собой весьма любопытную ситуацию. Парадокс заключается в том, что информанты практически не рефлексируют по поводу проблем, связанных с безопасностью при использовании устройства, даже если они имеют высокий уровень образования, квалификации, или их деятельность связана с постоянным использованием новых информационных технологий.

Про угрозу конфиденциальности не задумывались. (Инф. 2)

Над этим вопросом не задумывалась, так как все наши вопросы не имеют никакой конфиденциальной информации. (Инф. 13)

Значительная часть пользователей, которым задавались вопросы о приватности, буквально были вынуждены «придумать» свои обоснования использования устройства при существующих потенциальных рисках утечки данных. Наиболее частный нарратив — «злой рок» всех устройств, подключенных к сети. По большому счету, это стоит интерпретировать как допустимый обмен «принципа безопасности» на «принцип удовольствия». Сопоставимые результаты получены в зарубежных исследованиях, посвященных изучению отношения собственников и иных категорий пользователей (*visitors*) к «умным» колонкам [Kowalczuk, 2018; Malkin et al., 2019; Meng, Keküllüoglu, Vaniea, 2021].

Те, кто приобретал устройство для своих детей, не считают, что тем самым помещают их в ситуацию информационных угроз и рисков, ссылаясь, главным образом, на отсутствие конфиденциальных данных в запросах ребенка.

Я считаю, что некая угроза конфиденциальности, конечно, есть при использовании любых технических устройств, в том числе и смартфонов. Но я не считаю это каким-то критичным: в современном мире нас везде окружают какие-либо устройства. Наверняка каждое из этих устройство кто-то куда-то записывает. Вопрос, будет ли это когда-то что-то использовано против тебя, но это такой… еще философский, скажем, вопрос. Может быть да, может быть нет. И когда-то, наверное, в далеком будущем. То есть я на эту тему сильно не переживаю. Да, я считаю, что куда-то что-то записывается, и не только с колонки, но не считаю, что как-то в массовом порядке там кто-то за кем-то сильно следит. (Инф. 8)

DOI: 10.14515/monitoring.2023.3.2314

Ну что здесь связано с безопасностью? Это <…>, как говорится, мой профиль <…>. Но это подвержено, в современное время, это подвержено любой современной технологии. <…> Но надежда на специалиста, да, который разрабатывал. (Инф. 1)

Тем не менее некоторая часть информантов заявляет о том, что их запросы рафинированы, не содержат ничего, кроме собственно музыкальных предпочтений или просьб осуществить определенные действия. Более того, редко кто из опрошенных сообщал, что использовал устройство для прослушивания новостей, в том числе, чтобы не быть скомпрометированными собственной историей поиска или кругом прослушиваемых тем. Подобные опасения не имеют рациональных оснований, критически не осмысливаются, однако косвенно проявляются в повседневных практиках взаимодействия с устройством.

Я ни о чем таком не спрашиваю, [ничего] *такого сверхъестественного, за что мне было бы а) стыдно и б) секретно. Соответственно, мои запросы музыкальные предпочтительно, которые никому не нужны.* (Инф. 6)

Я ничего такого не делаю, поэтому мне нечего скрывать, как бы… К тому же мы живем в таком мире, в котором конфиденциальности нет. (Инф. 17)

Прямое указание на то, что им известны проблемы с безопасностью при использовании «умных» колонок, дают лишь двое из двадцати информантов. Однако их точка зрения на проблему диаметрально противоположна: в первом случае упоминаются риски взлома, с которыми стоит мириться, например, сообщая меньшее количество конфиденциальной информации; во втором — говорится о возможности минимизации этих рисков при помощи программных инструментов. Подобная ситуация достаточно типична, и в целом дискурсы защиты персональных данных это подтверждают, когда локус контроля носит выраженный экстернальный («безопасность пользователей — дело рук разработчиков») или интернальный («безопасность пользователей — дело рук самих пользователей») характер.

В сети даже была информация о взломе колонок. <…> [Говорю ей] *просто запросы, ничего конфиденциального.* (Инф. 1)

Судя по изменению рекламных интеграций в зависимости от сказанного — вряд ли [остается в тайне то, что говорится «умной» колонке]. Но это всегда можно проверить и сделать ограничения в файрволле для данных, отправляемых колонкой. Все настраивается «вручную». (Инф. 15)

Действительно, если говорить о возможностях по защите своих данных, то один из способов, доступных пользователям, — глубокая настройка «умных» колонок, максимальная персонализация. Однако результаты интервью показывают, что редко кто из информантов готов погружаться в суть вопроса, особенно при рутинизации взаимодействий с устройством. Как правило, после покупки гаджета пользователи проходят три стадии: 1) бурное освоение устройства, оно осознает-

DOI: 10.14515/monitoring.2023.3.2314

ся как «магическая коробка», 2) определение базовых функций, происходит его «расколдовывание»; 3) повседневное использование, дополнительные настройки требуются только в критических ситуациях (перенастройка, зависание, поломка и т. д.). Показательно, что для освоения устройства может быть делегирован только один из членов семьи (в наших интервью это чаще всего супруг, на которого ложится ответственность по выбору и обслуживанию всей или практически всей техники в доме), обычно он же и является инициатором его приобретения.

> *Дети с мужем сразу разобрались в настройках. <…> Лично я — не занимаюсь* [индивидуальной настройкой «навыков»]. *Но муж и дети ее периодически настраивают.* (Инф. 11)

> *Умная колонка в моей семье — это интервент. Ее притащил муж. И поставил. Пришлось учиться с ней жить в одном доме.* (Инф. 17)

Проективный запрос на повышение безопасности «умных» колонок практически не декларируется — прямо на это указал лишь один из двадцати информантов. Большинство пользователей заявляют, что им хватает текущих функций (в том числе, только базовых), еще несколько человек предложили расширить возможности устройства за счет освоения преимуществ, которые есть у конкурентов или реализованы только в крупных городах (заказ такси, заказ продуктов и т. д.). Также высказываются общие соображения по улучшению искусственного интеллекта, его последующей гуманизации и даже определению гаджетом (sic!) запахов.

> *Маркетологи в итоге сделают так, что массам понравятся любые вносимые изменения. Я бы хотел, чтобы разработчики больше внимания уделяли обеспечению информационной безопасности. А так — все устраивает.* (Инф. 16)

Обсуждение

Полученные данные сопоставимы с результатами зарубежных коллег: проблема конфиденциальности артикулируется в публичном дискурсе, обсуждается пользователями «умных» колонок, но пока не является триггером для каких-либо масштабных изменений status quo. Впрочем, наблюдаются определенные межстрановые и региональные различия.

Пользователи «умных» колонок из стран Западной Европы и США уделяют значительное внимание проблемам конфиденциальности и защиты своих персональных данных. Их беспокойство растет с расширением рынка гаджетов и развитием их функционала. Устройства получают биометрические данные — голоса, причем не только самих пользователей и членов их семей, но и гостей, курьеров, иных лиц, которые общаются с пользователями на территории их домохозяйств. Поэтому «умные» колонки воспринимаются либо как «шпионы», которые подслушивают, собирают данные, в том числе избыточные, либо как уязвимые устройства, которые, аккумулируя данные о частной жизни пользователей, могут быть взломаны третьими лицами [Mols, Wang, Pridmore, 2021: 3]. При этом в ряде случаев отношение пользователей «умных» колонок к возможным вариантам применения их личных данных выглядит парадоксальным. Так, по результатам качест-

DOI: 10.14515/monitoring.2023.3.2314

венного исследования, проведенного в Германии в 2019—2020 гг., выяснилось, что людей больше волнует использование их данных для персонализированной рекламы, чем, например, злоупотребление данными об их здоровье [Schroeder, Haug, Gewald, 2022].

Китайские пользователи, несмотря на то что коллективистская и корпоративная культура не способствует формированию настороженного отношения к конфиденциальности и неприкосновенности частной жизни, в последнее время также начинают проявлять беспокойство по поводу судьбы данных, собранных «умными» колонками [Liu et al., 2022: 2].

Российские пользователи выглядят менее обеспокоенными вопросами конфиденциальности, однако по косвенным признакам можно засвидетельствовать рост интереса к проблеме защиты приватной информации. Так, часть наших сограждан, которая не артикулирует заботу о конфиденциальности, обосновывает это тем, что им нечего скрывать, все их запросы «умной» колонке носят бытовой или досуговый характер. Однако все же отмечают, что предпочитают получать новостную информацию из иных источников. Это может свидетельствовать о настороженном, хотя и неотрефлексированном отношении к колонке. Наиболее сознательное отношение к вопросам конфиденциальности и приватности демонстрируют пользователи «умных» колонок — профессионалы из IT-сферы, поскольку они в большей степени погружены в тематическое дискурсивное пространство.

Определенные различия в отношении к проблеме конфиденциальности обусловлены спецификой функционала «умных» колонок. Например, в России еще не набрал большой популярности так называемый «голосовой шопинг» [Bawack, Wamba, Carillo, 2021] (*voice shopping*) — оформление покупки на интернет-платформе с использованием голосовых устройств, основанных на искусственном интеллекте. Однако американские потребители, активно прибегающие к данной услуге, уже столкнулись с проблемой: «умные» колонки предоставляют возможность использовать сервисы «голосового шопинга», созданные не производителями колонок, а третьими лицами. Когда пользователь устройства осуществляет покупку, он озвучивает свои персональные данные, в том числе, банковские реквизиты. Эти данные фактически получает колонка, и они могут быть использованы не только производителем голосового помощника, но и сторонней компанией [там же: 3].

Такого рода вопросы активно обсуждаются пользователями гаджетов, поскольку потеря банковских данных — реальная угроза, в отличие от рисков, связанных с передачей третьим лицам иных сведений (история запросов, семейный статус, «голосовые отпечатки» и т. п.). Можно предположить, что расширение функционала «умных» колонок, доступных российским пользователям, несколько изменит ситуацию, в которой предпочтение отдается удобству, а не конфиденциальности. Однако это только предположение, поскольку конфиденциальность «проигрывает» утилитарным потребностям и в иных сферах. Так, жители городов привыкли к повсеместному наличию камер видеонаблюдения, размещаемых в целях обеспечения безопасности личности и общественного порядка.

Может быть полезным обращение к китайскому опыту поиска баланса между конфиденциальностью и удобством пользователей «умных» колонок. В этих целях

DOI: 10.14515/monitoring.2023.3.2314

в КНР принят комплекс законов и кодексов этики, гарантирующих защиту персональных данных пользователей (особенно таких значимых, как биометрические, банковские данные и местоположение) и возлагающих ответственность за утечку на производителей гаджетов [Liu et al., 2022]. Принятие такого рода норм в российском законодательстве, на наш взгляд, не следует откладывать только потому, что проблема конфиденциальности пока еще не рефлексируется пользователями «умных» колонок. Действие на опережение с учетом зарубежного опыта позволит избежать ряда конфликтных ситуаций, связанных с утечкой персональных данных тех, кто активно пользуется голосовыми помощниками.

На данный момент становится очевидным, что позиция производителей гаджетов, согласно которой покупатели вынуждены принимать любые условия работы с «умными» колонками, если хотят использовать полноту функционала и получать качественные услуги, не отвечает концепции прав человека, в том числе на защиту личной информации и неприкосновенность частной жизни. При этом производители «умных» колонок часто пренебрегают защитой персональных данных пользователей, чтобы снизить стоимость устройств и не потерять свою часть рынка [Solera-Cotanilla et al., 2022]. Впрочем, представляются проигрышными и стратегии, ориентированные на ограничение функционала колонок. Так, запрет записи пользовательских запросов и разговоров существенно осложнит обучение искусственного интеллекта голосовых помощников, поскольку без больших данных невозможно из обычной колонки получить «умную» колонку.

В этой связи необходим поиск оптимального соотношения интересов пользователей, производителей гаджетов и государства, вопросов конфиденциальности и роста качества предоставляемых услуг. Требуется разработка и внедрение новых моделей информированного согласия, совершенствование законодательства и проведение дальнейших исследований, направленных на выявление отношения пользователей «умных» колонок к проблеме конфиденциальности.

Выводы

Проникновение «умных» колонок с голосовыми помощниками в дома пользователей — общемировой тренд, постепенно охватывающий нашу страну. Первые модели подобных устройств в России пережили рестайлинг, нашли свою целевую аудиторию. Пока она малочисленна, но поскольку существует осознанная потребность в инновациях, вероятно, будет расти.

Пока во взаимодействиях пользователей и «умных» устройств наблюдается процесс одомашнивания последних. Они встраиваются в структуры повседневности, отношение к ним рутинизируется, происходит их своеобразное расколдовывание. Колонка, хоть и неосознанно, занимает срединное место между человеком и домашней утварью: она уже не вещь, но еще и не человек.

Взаимодействуя с гаджетом, пользователи ежедневно передают ему ту или иную информацию о себе, начиная с названия любимой футбольной команды и заканчивая номером своей пластиковой карты. С учетом роста запросов на использование «умных» колонок (например, заказ такси, голосовой шоппинг и т. д.) количество фиксируемых данных будет только увеличиваться. Вопрос о последующем использовании этих данных остается открытым, поскольку несмотря на по-

DOI: 10.14515/monitoring.2023.3.2314

стоянное совершенствование законодательства в ответ на новые вызовы, технологии развиваются быстрее, в том числе — фишингового характера.

В будущих исследованиях, посвященных вопросам защиты персональных данных, необходимо учитывать не только тенденции развития рынка «умных» устройств, но и специфику их пользователей. Наиболее явный интерес к ним наблюдается среди зумеров, которые не осваивали *smart world*, а уже были рождены в нем. Так, по результатам недавнего общероссийского исследования компании Ipsos, каждый шестой молодой человек от 16 до 25 лет использует голосовые помощники дома (16 %), а каждый третий декларирует готовность использования гаджетов в будущем (32 %)[7]. Это существенно выше средних значений по стране. По всей видимости, зумеры не боятся потерять приватность и готовы пожертвовать ею ради возможности использовать новые технологии со всем возможным функционалом. Безопасность безнадежно проигрывает удовольствию, а конфиденциальность — удобству.

Впрочем, «шпионский» потенциал «умных» колонок не вызывает беспокойства у существенной части их пользователей по всему миру. Тревогу испытывают лишь отдельные владельцы, но, как правило, они не пытаются решить проблемы безопасности посредством «вербальной гигиены» (фильтрация запросов, индивидуализация настроек «умной» колонки и пр.). Гораздо более распространена практика возложения ответственности по защите своих персональных данных на государство или крупные корпорации. Безусловно, в ряде стран Европы, США и Китае интенсифицируются публичные дискуссии по проблеме, меняется законодательство, предпринимаются меры по технической защите пользовательской информации. Нашей стране, по всей видимости, только предстоит пройти этот путь, и будет лучше, если мы будем учиться на чужих ошибках и не изобретать велосипед.

Список литературы (References)

Корбут А. М. Одомашнивание искусственного интеллекта: умные колонки и трансформация повседневной жизни // Мониторинг общественного мнения: экономические и социальные перемены. 2021. № 1. С. 193—216. https://doi.org/10.14515/monitoring.2021.1.1808.
Korbut A. M. (2021) Domestication of Artificial Intelligence: Smart Speakers and Transformation of Everyday Life. Monitoring *of Public Opinion: Economic and Social Changes*. No. 1. P. 193—216. https://doi.org/10.14515/monitoring.2021.1.1808. (In Russ.)

Ушкин С. Г., Коваль Е.А, Яськин А. Н. Жить с Алисой: как голосовые помощники трансформируют практики коммуникации? // Журнал исследований социальной политики. 2022. Т. 20. № 3. С. 361—376. https://doi.org/10.17323/727-0634-2022-20-3-361-376.
Ushkin S.G, Koval E. A., Yaskin A. N. (2022) Living with Alice: How Do Voice Assistants Transform Communication Practices? *The Journal of Social Policy Studies*. Vol. 20. No. 3. P. 361—376. https://doi.org/10.17323/727-0634-2022-20-3-361-376.

[7] Trend Vision 2022. Куда дальше? URL: https://www.ipsos.com/sites/default/files/ct/publication/documents/2022-09/TrendVision2022-Ipsos-RUS.pdf (дата обращения: 22.06.2023).

DOI: 10.14515/monitoring.2023.3.2314

Чередеева А. А., Савинская О. Б. Гендерное (не)равенство в детском саду: материнские нарративы о скрытом учебном плане и девичей идентичности // Журнал исследований социальной политики. 2018. Т. 16. № 3. С. 441—456. https://doi.org/10.17323/727-0634-2018-16-3-441-456.
Cheredeeva A. A., Savinskaya O. B. (2018) Gender (In)equality in the Kindergarten: Mother's Narratives on Hidden Curriculum and Girl's Identity. *The Journal of Social Policy Studies*. Vol. 16. No. 3. P. 441—456. https://doi.org/10.17323/727-0634-2018-16-3-441-456. (In Russ.)

Barbosa N. M., Zhang Z., Wang Y. (2020). Do Privacy and Security Matter to Everyone? Quantifying and Clustering User-Centric Considerations about Smart Home Device Adoption. In: *Proceedings of 16th Symposium on Usable Privacy and Security, USENIX Association (2020)*. USENIX Association. P. 417—435. https://natabarbosa.com/soups_smart_home.pdf (дата обращения: 23.06.2023).

Bawack R. E., Wamba S. F., Carillo K. D.A. (2021) Exploring the Role of Personality, Trust, and Privacy in Customer Experience Performance during Voice Shopping: Evidence from SEM and Fuzzy Set Qualitative Comparative Analysis. *International Journal of Information Management*. Vol. 58. https://doi.org/10.1016/j.ijinfomgt.2021.102309.

Cannizzaro S., Procter R., Ma S., Maple C. (2020) Trust in the Smart Home: Findings from a Nationally Representative Survey in the UK. *PLoS ONE*. Vol. 15. No. 5. P. e0231615:1—e0231615:30. https://doi.org/10.1371/journal.pone.0231615.

Chalhoub G., Flechais I. (2020) "Alexa, Are You Spying on Me?": Exploring the Effect of User Experience on the Security and Privacy of Smart Speaker Users. In: Moallem A. (ed.) *HCI for Cybersecurity, Privacy and Trust*. *HCII 2020. Lecture Notes in Computer Science. Vol. 12210.* Cham: Springer. P. 305—325. https://doi.org/10.1007/978-3-030-50309-3_21.

Gerber N., Gerber P., Volkamer M. (2018) Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior. *Computers & Security*. Vol. 77. No 1. P. 226—261. https://doi.org/10.1016/j.cose.2018.04.002.

Jayatilleke A., Thelijjagoda S., Pathirana P. (2019) Security Awareness among Smart Speaker Users. *2019 National Information Technology Conference (NITC)*. Colombo: IEEE. P. 1—6. https://doi.org/10.1109/NITC48475.2019.9114497.

Hamblin K. (2020) Technology and Social Care in a Digital World: Challenges and Opportunities in the UK. *Journal of Enabling Technologies*. Vol. 14. No. 2. P. 115—125. https://doi.org/10.1108/JET-11-2019-0052.

Huang Y., Obada-Obieh B., Beznosov K. K. (2020) Amazon vs. My Brother: How Users of Shared Smart Speakers Perceive and Cope with Privacy Risks. In: Nichols J. (ed.) *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, ACM (2020)*. New York, NY: Association for Computing Machinery. P. 1—13. https://doi.org/10.1145/3313831.3376529.

DOI: 10.14515/monitoring.2023.3.2314

Kowalczuk P. (2018) Consumer Acceptance of Smart Speakers: A Mixed Methods Approach. *Journal of Research in Interactive Marketing*. Vol. 12. No. 4. P. 418—431. https://doi.org/10.1108/JRIM-01-2018-0022.

Lau J., Zimmerman B., Schaub F. (2018) Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-Seeking Behaviors with Smart Speakers. In: Karahalios K., Monroy-Hernandez A., Lampinen A., Fitzpatrick G. (eds.) *Proceedings of the ACM on Human-Computer Interaction*. Vol. 2. No. CSCW. New York, NY: Association for Computing Machinery. P. 1—31. https://doi.org/10.1145/3274371.

Liu Y., Huang L., Yan W., Wang X., Zhang R. (2022) Privacy in AI and the IoT: The Privacy Concerns of Smart Speaker Users and the Personal Information Protection Law in China. *Telecommunications Policy*. Vol. 46. Issue 7. https://doi.org/10.1016/j.telpol.2022.102334.

Lutz C., Newlands G. (2021) Privacy and Smart Speakers: A Multi-Dimensional Approach. *The Information Society.* Vol. 37. No. 3. P. 147—162. https://doi.org/10.1080/01972243.2021.1897914.

Maccario G., Naldi M. (2022) Alexa, Is My Data Safe? The (Ir)relevance of Privacy in Smart Speakers Reviews. *International Journal of Human–Computer Interaction*. Vol. 39. No. 6. P. 1244—1256. https://doi.org/10.1080/10447318.2022.2058780.

Malkin N., Deatrick J., Tong A., Wijesekera P., Egelman S., Wagner D. (2019) Privacy Attitudes of Smart Speaker Users. *PoPETs*. No. 4. P. 250—271. https://doi.org/10.2478/popets-2019-0068.

Marky K., Voit A., Stöver A., Kunze K., Schröder S., Mühlhäuser M. (2020) “I Don’t Know How to Protect Myself”: Understanding Privacy Perceptions Resulting from the Presence of Bystanders in Smart Environments. In: Nichols J. (ed.) *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society*. New York, NY: Association for Computing Machinery. P. 1—11. https://doi.org/10.1145/3419249.3420164.

Meng N., Keküllüoglu D., Vaniea K. (2021) Owning and Sharing: Privacy Perceptions of Smart Speaker Uses. In: Nichols J. (ed.) *Proceedings of the ACM on Human-Computer Interaction*. Vol. 5. New York, NY: Association for Computing Machinery. P. 1—29.

Mhaidli A., Venkatesh M. K., Zou Y., Schaub F. (2020) Listen Only When Spoken To: Interpersonal Communication Cues as Smart Speaker Privacy Controls. In: *PoPETs*. No. 2. P. 251—270. https://doi.org/10.2478/popets-2020-0026.

Mols A., Wang Y., Pridmore J. H. (2021) Household Intelligent Personal Assistants in the Netherlands: Exploring Privacy Concerns Around Surveillance, Security, and Platforms. *Convergence: The International Journal of Research into New Media Technologies*. Vol. 28. No. 6. P. 1841—1860. https://doi.org/10.1177/13548565211042234.

O’Maonaigh C., Saxena D. (2021) Investigating Personalisation-Privacy Paradox Among Young Irish Consumers: A Case of Smart Speakers. In: *Proceedings of the 1st Virtual*

DOI: 10.14515/monitoring.2023.3.2314

Conference on Implications of Information and Digital Technologies for Development, 2021. arXiv:2108.09945. URL: https://doi.org/10.48550/arXiv.2108.09945.

Pattnaik N., Li S., Nurse J. R.C. (2023) Perspectives of Non-Expert Users on Cyber Security and Privacy: An Analysis of Online Discussions on Twitter. *Computers & Security*. Vol. 125. Art. 103008. https://doi.org/10.1016/j.cose.2022.103008.

Poushneh A. (2021) Humanizing Voice Assistant: The Impact of Voice Assistant Personality on Consumers' Attitudes and Behaviors. *Journal of Retailing and Consumer Services*. Vol. 58. Art. 102283. https://doi.org/10.1016/j.jretconser.2020.102283.

Schroeder T., Haug M., Gewald H. (2022) Data Privacy Concerns Using mHealth Apps and Smart Speakers: Comparative Interview Study Among Mature Adults. *JMIR Formative Research*. Vol. 6. No. 6. Art. e28025. https://doi.org/10.2196/28025.

Solera-Cotanilla S., Vega-Barbas M., Pérez J., López G., Matanza J., Álvarez-Campana M. (2022) Security and Privacy Analysis of Youth-Oriented Connected Devices. *Sensors*. Vol. 22. No. 11. https://doi.org/10.3390/s22113967.

DOI: 10.14515/monitoring.2023.3.2314

Приложение

Список информантов

Инф. 1 — мужчина, 40 лет, женат, 2 детей, руководитель подразделения, кандидат наук (личное интервью);

Инф. 2 — женщина, 37 лет, замужем, 1 ребенок, маркетолог, кандидат наук (личное интервью);

Инф. 3 — женщина, 27 лет, замужем, детей нет, экономист, высшее образование (телефонное интервью);

Инф. 4 — женщина, 31 год, замужем, детей нет, специалист, высшее образование (телефонное интервью);

Инф. 5 — мужчина, 32 года, женат, 1 ребенок, продавец-консультант, высшее образование (телефонное интервью);

Инф. 6 — женщина, 36 лет, замужем, 2 детей, руководитель подразделения, кандидат наук (личное интервью);

Инф. 7 — мужчина, 50 лет, женат, детей нет, заведующий складом, высшее образование (личное интервью);

Инф. 8 — женщина, 32 года, замужем, 2 детей, муниципальный служащий, высшее образование (голосовые сообщения в социальной сети «ВКонтакте»);

Инф. 9 — женщина, 31 год, замужем, 2 детей, инженер по нормированию труда, высшее образование (личное интервью);

Инф. 10 — мужчина, 35 лет, женат, 1 ребенок, полицейский, высшее образование (телефонное интервью);

Инф. 11 — женщина, 38 лет, замужем, 3 детей, технический специалист, высшее образование (телефонное интервью);

Инф. 12 — женщина, 35 лет, замужем, 3 детей, руководитель подразделения, высшее образование (личное интервью);

Инф. 13 — женщина, 35 лет, разведена, 1 ребенок, специалист, высшее образование (личное интервью);

Инф. 14 — женщина, 32 года, замужем, 2 детей, заместитель директора, высшее образование (личное интервью);

Инф. 15 — мужчина, 21 год, холост, детей нет, бармен, среднее профессиональное образование (личное интервью);

Инф. 16 — мужчина, 22 года, холост, детей нет, оператор колл-центра, среднее профессиональное образование (телефонное интервью);

Инф. 17 — женщина, 31 год, замужем, 2 детей, учитель, кандидат наук (личное интервью);

Инф. 18 — женщина, 40 лет, замужем, 2 детей, руководитель подразделения, высшее образование (личное интервью);

Инф. 19 — мужчина, 24 года, холост, детей нет, технический специалист, среднее специальное образование (текстовое интервью в социальной сети «ВКонтакте»);

Инф. 20 — женщина, 24 года, замужем, детей нет, специалист, высшее образование (текстовое интервью в социальной сети «ВКонтакте»).