РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ВШГУ РАНХиГС Высшая Школа Государственного Управления

ЦЕНТР ПОДГОТОВКИ РУКОВОДИТЕЛЕЙ И КОМАНД ЦИФРОВОЙ ТРАНСФОРМАЦИИ

ЭТИКА И «ЦИФРА»:

ОТ ПРОБЛЕМ К РЕШЕНИЯМ

Москва, 2021

УДК 17:001:008 (035.3)

ББК -5*65.2/4–65/9в6

Э90

Этика и «цифра»: от проблем к решениям / под ред. Е. Г. Потаповой,
Э90 М. С. Шклярук. — М.: РАНХиГС, 2021. — 184 с.

Во втором докладе серии «Этика и „цифра“» (первый вышел в 2020 году) рассматриваются этические проблемы, возникающие в связи с применением цифровых технологий в государственном секторе, и наиболее популярные подходы к их решению. Особое внимание авторы уделяют трем темам: сбору и обработке данных, приватности, этике в области искусственного интеллекта. Специально для доклада был создан фреймворк «Ответственная разработка цифровых решений», который можно использовать для оценки проектов на региональном и федеральном уровнях. Подчеркивается роль этики в повышении доверия граждан к цифровой трансформации госсектора и к государству в целом.

Издание будет полезно всем категориям госслужащих, специалистам, участвующим в разработке цифровых продуктов и услуг, а также читателям, интересующимся темой цифровой трансформации государства.

УДК 17:001:008 (035.3)
ББК -5*65.2/4–65/9в6

АВТОРЫ

Алферов Павел Александрович
профессор бизнес-практики Московской школы управления «Сколково», независимый эксперт по управлению проектами, управлению знаниями, цифровой трансформации

Архипов Алексей Владимирович
редактор направления исследований и аналитики Центра подготовки руководителей и команд цифровой трансформации ВШГУ РАНХиГС

Боровикова Кристина Игоревна
заместитель директора КПМГ в России и СНГ, соучредитель и член правления ассоциации Russian Privacy Professionals Association (RPPA)

Волкович Екатерина Константиновна
старший консультант КПМГ в России и СНГ

Гейн Яна Эдгаровна
дата-аналитик Центра подготовки руководителей и команд цифровой трансформации ВШГУ РАНХиГС

Готовцев Павел Михайлович
канд. техн. наук, руководитель российской рабочей группы IEEE по тематике «Этика и искусственный интеллект», заместитель начальника отдела биотехнологий и биоэнергетики НИЦ «Курчатовский институт»

Грязнова Юлия Борисовна
руководитель дирекции стратегии, аналитики и исследований АНО «Национальные приоритеты», член исполнительного совета Российской ассоциации по связям с общественностью (РАСО)

Гусев Александр Владимирович
канд. техн. наук, директор по развитию компании «К-Скай», член наблюдательного совета ассоциации разработчиков и пользователей ИИ для медицины «Национальная база медицинских знаний», член экспертного совета Минздрава России по вопросам использования ИКТ в системе здравоохранения

Данилин Иван Владимирович
канд. полит. наук, заведующий отделом науки и инноваций Национального исследовательского института мировой экономики и международных отношений имени Е. М. Примакова РАН

Димитров Илия Димитров
президент ГК Seldon, общественный омбудсмен по вопросам развития цифровой экономики, исполнительный директор НКО «Ассоциация электронных торговых площадок» (АЭТП)

Ефремов Алексей Александрович
канд. юрид. наук, вед. науч. сотр. Центра технологий государственного управления Института прикладных экономических исследований РАНХиГС

Земнухова Лилия Владимировна
канд. социол. наук, науч. сотр. Социологического института Федерального научно-исследовательского социологического центра РАН и Центра исследований науки и технологий ЕУСПб, член правления Санкт-Петербургской ассоциации социологов (СПАС)

Игнатьев Андрей Геннадьевич
руководитель направления аналитики Центра глобальной ИТ-кооперации, науч. сотр. — исследователь кафедры цифровой экономики и ИИ МГИМО МИД России, эксперт Технического комитета по стандартизации № 164 «Искусственный интеллект»

Кирин Александр Юрьевич
старший преподаватель бизнес-практики, исполнительный директор Центра бизнес-этики при поддержке компании РУСАЛ, академический директор и руководитель проектной работы в корпоративных программах Московской школы управления «Сколково»

Кириченко Ирина Вадимовна
канд. экон. наук, ст. науч. сотр. Национального исследовательского института мировой экономики и международных отношений им. Е. М. Примакова РАН

Киселева Ксения Львовна
канд. филол. наук, ст. науч. сотр. Института русского языка им. В. В. Виноградова РАН, главный редактор Центра подготовки руководителей и команд цифровой трансформации ВШГУ РАНХиГС

Комендантов Дмитрий Владимирович
член исполнительного совета Российской ассоциации по связям с общественностью (РАСО)

Коротких Сергей Сергеевич
руководитель направления «Консалтинг» АНО «Центр перспективных управленческих решений»

Коршунова Светлана Вячеславовна
аналитик Центра подготовки руководителей и команд цифровой трансформации ВШГУ РАНХиГС

Костюкова Коринна Сергеевна
мл. науч. сотр. Национального исследовательского института мировой экономики и международных отношений им. Е. М. Примакова РАН

Кохановская Елена Ивановна
директор по внешним коммуникациям и связям с общественностью ПАО МТС, член исполнительного совета Российской ассоциации по связям с общественностью (РАСО)

Крель Марианна Владимировна
эксперт Центра подготовки руководителей и команд цифровой трансформации ВШГУ РАНХиГС, executive coach

Мартинсон Роман Викторович
старший консультант КПМГ в России и СНГ

Мунтян Алексей Витальевич
соучредитель и член правления Russian Privacy Professionals Association (RPPA), член совета Торгово-промышленной палаты РФ по развитию антикоррупционного комплаенса и деловой этики

Незнамов Андрей Владимирович
канд. юрид. наук, управляющий директор Центра регулирования ИИ ПАО «Сбербанк» (центр компетенций «Искусственный интеллект»), основатель исследовательского центра «Робоправо», ст. науч. сотр. Института государства и права РАН

Орлова Алиса Анатольевна
редактор направления исследований и аналитики Центра подготовки руководителей и команд цифровой трансформации ВШГУ РАНХиГС

Полетаев Олег Викторович
первый вице-президент Российской ассоциации по связям с общественностью (РАСО), директор по развитию цифрового бизнеса группы «Интерфакс»

Потапова Екатерина Геомаровна
канд. филол. наук, руководитель направления исследований и аналитики Центра подготовки руководителей и команд цифровой трансформации ВШГУ РАНХиГС

Пьянченко Андрей Андреевич
заместитель директора — директор программ ФГАУ НИИ «Восход»

Романова Екатерина Владимировна
канд. экон. наук, ст. науч. сотр. Национального исследовательского института мировой экономики и международных отношений им. Е. М. Примакова РАН

Синюшин Константин Станиславович
управляющий партнер The Untitled Ventures

Теплякова Дарья Олеговна
редактор-переводчик направления исследований и аналитики Центра подготовки руководителей и команд цифровой трансформации ВШГУ РАНХиГС

Ткачева Ксения Андреевна
директор Центра подготовки руководителей и команд цифровой трансформации ВШГУ РАНХиГС

Трубинова Елена Сергеевна
заместитель начальника отдела по связям с общественностью Центра подготовки руководителей и команд цифровой трансформации ВШГУ РАНХиГС

Туманова Мария Витальевна
аналитик Центра подготовки руководителей и команд цифровой трансформации ВШГУ РАНХиГС

Федоров Максим Валериевич
канд. физ.-мат. наук, д-р хим. наук, вице-президент в области ИИ и математического моделирования Сколковского института науки и технологий, представитель РФ в специальной экспертной группе ЮНЕСКО по подготовке Рекомендации в области этики ИИ, член российских делегаций в специальном комитете по искусственному интеллекту Совета Европы и при ОЭСР

Фирсов Алексей Владимирович
председатель совета директоров Центра социального проектирования «Платформа», вице-президент Российской ассоциации по связям с общественностью (РАСО)

Шавлай Эллина Петровна
канд. экон. наук, науч. сотр. Национального исследовательского института мировой экономики и международных отношений им. Е. М. Примакова РАН

Шелюбская Наталья Владимировна
канд. экон. наук, ст. науч. сотр. Национального исследовательского института мировой экономики и международных отношений им. Е. М. Примакова РАН

Шепелева Ольга Сергеевна
руководитель проектного направления «Цифровое право» АНО «Центр перспективных управленческих решений», эксперт Центра подготовки руководителей и команд цифровой трансформации ВШГУ РАНХиГС

Шклярук Мария Сергеевна
академический директор Центра подготовки руководителей и команд цифровой трансформации ВШГУ РАНХиГС, генеральный директор АНО «Центр перспективных управленческих решений»

БЛАГОДАРНОСТИ

Центр подготовки РКЦТ выражает благодарность авторам первого доклада «Этика и „цифра“» (2020), поделившимся своими идеями при подготовке нового доклада:

Двинских Дарье Юрьевне, независимому эксперту;

Душкину Роману Викторовичу, директору по науке и технологиям Агентства Искусственного Интеллекта;

Разину Александру Владимировичу, заведующему кафедрой этики философского факультета МГУ им. М. В. Ломоносова;

Ройзензону Григорию Владимировичу, старшему научному сотруднику Института системного анализа ФИЦ ИУ РАН, члену российской Рабочей группы IEEE по тематике «Этика и искусственный интеллект»;

Талапиной Эльвире Владимировне, главному научному сотруднику Института государства и права РАН;

Тюрину Владиславу Владимировичу, директору проекта Дирекции цифровой трансформации РАНХиГС.

Центр благодарит за содействие в подготовке доклада и участие в тестировании фреймворка «Ответственная разработка цифровых решений» цифровые команды Татарстана, Новосибирской, Смоленской, Оренбургской областей и лично

Гисмятова Радика Расыховича, заместителя министра цифрового развития государственного управления, информационных технологий и связи Республики Татарстан;

Дюбанова Анатолия Васильевича, министра цифрового развития и связи Новосибирской области;

Кормер Юлию Григорьевну, заместителя руководителя аппарата администрации Смоленской области, начальника управления по работе с обращениями граждан;

Толпейкина Дениса Владимировича, министра цифрового развития и связи Оренбургской области.

Центр также выражает признательность за участие в подготовке доклада:

Ахмадиевой Анне Фиркатовне, советнику министра цифрового развития, связи и массовых коммуникаций Российской Федерации;

Карелову Сергею Владимировичу, председателю совета Лиги независимых экспертов в области информационных технологий;

Клочкову Дмитрию Александровичу, первому заместителю директора ФГАУ НИИ «Восход»;

Кравцову Александру Александровичу, старшему научному сотруднику ИМЭМО РАН;

Федулову Владиславу Викторовичу, заместителю министра экономического развития Российской Федерации;

Шадаеву Максуту Игоревичу, министру цифрового развития, связи и массовых коммуникаций Российской Федерации.

СОДЕРЖАНИЕ

1. ВВЕДЕНИЕ. ЗАЧЕМ ЭТИКА ГОССЛУЖАЩИМ?

— Искусство управлять умклайдетом, — сказал незнакомец, — это сложное и тонкое искусство. Вы ни в коем случае не должны огорчаться или упрекать себя. Курс управления умклайдетом занимает восемь семестров и требует основательного знания квантовой алхимии. Как программист вы, вероятно, без особого труда освоили бы умклайдет электронного уровня, так называемый УЭУ-17... Но квантовый умклайдет... гиперполя... трансгрессивные воплощения... обобщенный закон Ломоносова — Лавуазье... — Он виновато развел руками. — О чем разговор! — поспешно сказал я. — Я ведь и не претендую... Конечно же, я абсолютно не подготовлен.

А. и Б. Стругацкие. Понедельник начинается в субботу

Время чтения — 21 минута

Для реализации цифровой трансформации государства необходимо своевременно отвечать на этические вопросы, возникающие при использовании цифровых технологий. По мере того как цифровые технологии становятся основой госуправления, меняется роль госслужащих и государства в целом. В новых условиях служащие должны принимать решения под свою ответственность, в то время как раньше они могли строго следовать регламенту и опираться на многолетние исследования вопроса. В этой ситуации этика в области цифровых технологий критически влияет на степень доверия граждан к государству, а в перспективе — на его стабильность и благополучие.

В течение двух десятилетий человечество с оптимизмом смотрело в цифровое будущее; люди искренне верили, что технический прогресс сделает жизнь лучше. В последние годы этот оптимизм сошел на нет: ИТ-компании собирают персональные данные пользователей и передают сторонним организациям, социальные сети манипулируют пользовате-

лями, даже крупные игроки не способны защитить данные клиентов, а алгоритмы, используя непрозрачные метрики, повышают статус одних социальных групп и дискриминируют другие. По мере того как инновационные технологии становятся повседневностью в экономике, обороне, здравоохранении, в наших отношениях с государством и в частной жизни, рисков становится все больше.

«В эпоху больших данных и машинного обучения человеческая индивидуальность испытывает все большее давление», — отмечает профессор гарвардской Школы управления им. Джона Ф. Кеннеди Матиас Риссе[1]. Технологические прорывы последних десятилетий готовили почву для повсеместных масштабных изменений, а пандемия стала их катализатором: услуги и работа онлайн, дистанционная учеба и медицина, государственные цифровые услуги и т. д., вплоть до новой экономической модели — «бесконтактной экономики»[2]. Локдаун 2020 года смягчился год спустя, но остается значительным фактором влияния, как и принятые в этот период управленческие решения в области цифровизации.

С одной стороны, использование цифровых технологий во время пандемии принесло огромную пользу. Миллиард учеников и студентов закончили учебный год онлайн, тогда как еще десять лет назад такая ситуация привела бы к коллапсу образования. Медицинские организации собрали огромное количество данных для анализа и обучения систем искусственного интеллекта (ИИ), развития цифровой медицины[3] и медицины в целом. Экологи получили уникальную возможность оценить вклад транспорта и промышленности в загрязнение воздуха[4].

С другой стороны, непродуманные решения, пренебрежение последствиями потом ради выгоды сейчас наносили и продолжают наносить репутационный вред самой идее цифровизации. Так, неэтичная работа приложения «Социальный мониторинг» и системы цифровых пропусков сделала фразу «цифровой концлагерь» популярным способом обозначения Москвы (см. раздел 2.3). Государствам приходится не столько возвращаться в прошлую жизнь, сколько учиться жить в новой, где нужно быть готовым в любой момент отреагировать на новую волну пандемии или другие острые ситуации[5]. Этические вопросы, которым долгое время не уделяли внимание, оказались слабым местом ускорившейся цифровой

Авторы раздела:


С. В. Коршунова


Е. Г. Потапова


К. А. Ткачева


М. В. Туманова

[1] Pazzanese C. Trailblazing initiative marries ethics, tech // The Harvard Gazette. URL: https://news.harvard.edu/gazette/story/2020/10/experts-consider-the-ethical-implications-of-new-technology/

[2] Что такое Low Touch Economy? // Агентство FCProject. URL: https://fcproject.ru/timeline-low-touch-economy/

[3] Как технологии цифровой медицины помогают бороться с пандемией // РБК. URL: https://pro.rbc.ru/demo/5ea82ae49a79472d3879c7ea

[4] Росприроднадзор сообщил об улучшении качества воздуха в семи городах в период пандемии // ТАСС. URL: https://tass.ru/obschestvo/8495057

[5] COVID-19: Briefing materials. Global health and crisis response. June 1, 2020 // McKinsey & Company. URL: https://www.mckinsey.com/~/media/mckinsey/business%20functions/risk/our%20insights/covid%2019%20implications%20for%20business/covid%2019%20july%209/covid-19-facts-and-insights-july-6.pdf

трансформации (ЦТ). Технологии, применение которых в 2020–2021 годах вызвало возмущение, отторжение и социальные проблемы, зачастую внедряются бесконтрольно и без каких-либо ограничений. Так что настало время установить правила и принципы для принятия решений, которые влияют на жизнь, здоровье и экономическое положение миллионов людей.

«Вопросы этики, связанные с применением цифровых технологий государством и частными корпорациями, активно обсуждаются на мировом уровне. Для России этот вопрос тоже актуален, так как цифровые технологии дают тому, кто владеет данными пользователей, огромные возможности для проникновения в их частную жизнь. Этические вызовы требуют новой культуры работы с данными, повышения цифровой грамотности как госслужащих, так и граждан. Сегодня при разработке и внедрении сервисов решения принимаются скорее интуитивно, тогда как растущие объемы персональных данных требуют прикладного регулирования этой сферы».

Мария Шклярук, академический директор Центра подготовки РКЦТ

В нынешней ситуации особая ответственность легла на **государственных заказчиков цифровых сервисов**, что ярко проявилось в период пандемии. Во всем мире ситуативные решения по борьбе с пандемией принимались госслужащими, которым пришлось создавать и адаптировать сервисы в условиях хаоса и неопределенности[6], бороться не только с распространением болезни, но и с ее социально-экономическими последствиями. Они оказались на передовой, не имея готовой стратегии и тактики, поэтому вынуждены были импровизировать. В новых условиях госслужащие и работники бюджетных организаций обеспечивали:

- непрерывность предоставления государственных услуг с помощью новых цифровых инструментов и методов;
- быстрое внедрение инноваций и креативных решений;
- информирование населения о развитии пандемии;
- привлечение экспертов и распределение сотрудников;
- укрепление легитимности государственных институтов, повышение доверия населения к правительству[7].

В 2019 году социолог и философ Шошана Зубофф подробно описала[8] капитализм слежки, или надзорный капитализм (англ. surveillance capitalism), — явление, построенное на сборе больших массивов данных о пользователях. В любом обществе, которое переходит к капитализму слежки, происходит разделение на тех, кто наблюдает, и тех, за кем

[6] Kauzya J.-M., Niland E. UN/DESA Policy Brief #79: The role of public service and public servants during the COVID-19 pandemic // The United Nations. URL: https://www.un.org/development/desa/dpad/publication/un-desa-policy-brief-79-the-role-of-public-service-and-public-servants-during-the-covid-19-pandemic/

[7] Taddeo M. The Ethical Governance of the Digital During and After the COVID-19 // Pandemic National Library of Medicine. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7289936/

[8] Zuboff S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: Public Affairs, 2019.

наблюдают. В число последних попадают практически все граждане, чьи данные беспрепятственно собирают дата-корпорации и государство. Государство — одновременно и потребитель данных, которые необходимы для принятия решений на всех уровнях власти, и регулятор, обеспечивающий в том числе защиту данных граждан. Во время пандемии соединение этих двух ролей создает конфликт интересов. Что приоритетнее при отслеживании перемещений граждан: права и интересы людей (в первую очередь сохранение приватности) или безопасность государства и общества? Так выглядит этическая дилемма государства.

Директор АНО «Информационная культура» Иван Бегтин обращает внимание на то, что в пандемию Минцифры[9], которое раньше занималось прокладкой кабелей и компьютеризацией школ, взяло на себя новую роль — массово следить за гражданами. Его беспокоит, что «практика „социального мониторинга“ с легкостью переносится на контроль домашнего ареста, а идеи вроде приложения „Мигрант“ по контролю трудовых мигрантов так же легко транслируются на другие категории граждан: строителей особо важных объектов, людей, работающих под присягой, условно-досрочно освобожденных. <...> Появится ли самоограничение государства в этой сфере? Будут ли этические аспекты приватности реальным или имитационным предметом государственной и публичной политики?»[10]

По его словам, важными аспектами новой реальности стали снижение ограничений на доступ к личным данным («если ранее доступ к данным о передвижении человека требовал процедур оперативно-розыскной деятельности и сами данные собирались в инфраструктурных предприятиях, то сейчас данные доступны сразу в государственной системе и сотрудникам гражданских ведомств») и цифровая опека (переход к активной цифровой протекционистской политике, включая мобильные приложения и интернет вещей для защиты детей, пенсионеров и др.). Эти тенденции, безусловно, вызывают вопросы: «будут ли работать органы парламентского контроля, какова здесь роль регуляторов систем безопасности вроде ФСТЭК и защиты персональных данных вроде Роскомнадзора»[11].

Этические принципы нельзя назвать чем-то новым для российской госслужбы. Работа государственного или муниципального служащего в России регламентируется комплексом нормативных правовых актов (НПА), которые достаточно детально определяют, что может, а что не может делать госслужащий. Федеральный закон «О государственной гражданской службе Российской Федерации» от 27.07.2004 № 79-ФЗ содержит перечень

[9] Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации создано 15 мая 2018 года. До сентября 2020 года имело официальное сокращенное название «Минкомсвязь России», сейчас — «Минцифры России»; далее мы будем использовать это сокращение, независимо от даты описываемых событий.

[10] Бегтин И. Государственное регулирование экосистемы мобильных приложений // Ivan Begtin blog. URL: https://begtin.tech/govmobile/

[11] Бегтин И. Экосистема государственной и негосударственной слежки через мобильные устройства и интернет вещей // Ivan's Begtin Newsletter on digital, open and preserved government. URL: https://begtin.substack.com/p/9-

прав, обязанностей, ограничений, запретов и требований к служебному поведению госслужащего, в том числе правила общения госслужащего с отдельными людьми и общественностью, обязанность беспристрастного отношения ко всем гражданам, обязанность корректного и уважительного обращения к ним и т. п. Отдельные нормы деловой этики госслужащего утверждены рядом законов[12]. Кроме того, в органах власти, местного самоуправления, в госучреждениях существуют специальные кодексы этики, стимулом к созданию которых послужили рекомендации кабинета министров Совета Европы «О кодексах поведения для государственных служащих»[13]. В 2010 году был принят Типовой кодекс этики и служебного поведения государственных служащих РФ и муниципальных служащих[14]. На основе типового кодекса были разработаны региональные[15] и муниципальные кодексы[16], кодексы отдельных органов власти. Однако кодексов техноэтики для госслужбы в России пока не существует.

Все названные факторы свидетельствуют о том, что этикой ЦТ нельзя пренебрегать. Этика напрямую связана с доверием, а доверие — с успешностью страны в долгосрочной перспективе (см. об этом раздел 3). Пусть не сегодня, но в ближайшее десятилетие в условиях турбулентности и глобальных потрясений государству будет критически важно иметь выстроенные и основанные на доверии коммуникации с гражданами, понятные и этичные принципы принятия решений.

Компании, использующие этически неоднозначные решения при разработке продуктов, ставят под удар репутацию своего бренда[17]. Организаций, имеющих собственный этический подход, пока не так много, но именно их можно назвать наиболее технологически зрелыми. Доверие означает уже не просто хорошую репутацию и общественную поддержку, а возможность в перспективе остаться на рынке[18], и это актуально не только для компаний, но и для целых стран.

Доверие граждан государству тает, когда технологии используют неэтично, когда их применение вызывает страх и наносит вред гражданам[19]. «В постковидном мире государства, которые ценят доверие граждан,

[12] Федеральный закон от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» содержит требования к деловой переписке госслужащего с гражданами; федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» устанавливает требования к работе с персональными данными граждан, в том числе биометрическими; федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» обязывает госорганы обеспечивать доступ граждан к информации о своей деятельности и определяет ограничения на распространение информации.

[13] Рекомендация № R(2000)10. О кодексах поведения для государственных служащих // Электронный фонд правовых и нормативно-технических документов. URL: https://docs.cntd.ru/document/901802716

[14] Типовой кодекс этики и служебного поведения государственных и муниципальных служащих // Минтруд России. URL: https://mintrud.gov.ru/ministry/programms/anticorruption/9/3

[15] Кодекс этики и служебного поведения государственных гражданских служащих Республики Крым // Правительство Республики Крым. URL: https://rk.gov.ru/ru/structure/901

[16] Кодекс этики и служебного поведения муниципальных служащих муниципального образования «город „Екатеринбург“» // ГАРАНТ.ру. URL: http://base.garant.ru/35183741/d8e34e7b9274ff56b4ab44c1bd6398fb/

[17] Don’t Leave “Ethical Tech” Out of Your Digital Transformation Plan // Harvard Business Review. URL: https://hbr.org/sponsored/2020/04/dont-leave-ethical-tech-out-of-your-digital-transformation-plan

[18] Bannister C. Golden D. Ethical technology and trust // Deloitte. URL: https://www2.deloitte.com/us/en/insights/focus/tech-trends/2020/ethical-technology-and-brand-trust.html

[19] Warner S. Digital Trust will be Pivotal in the Post Covid-19 World // ETCIO. URL: https://cio.economictimes.indiatimes.com/news/strategy-and-management/digital-trust-will-be-pivotal-in-the-post-covid-19-world/76444619

будут работать над тем, чтобы восстановить его, — пишет Тереза Скасса, профессор юридического факультета Оттавского университета (Канада). — Они будут принимать законы о защите персональных данных… чтобы обеспечить соблюдение прав и реальное применение этих законов на практике. Они будут применять к технологии подходы, основанные на этике и правах человека… Государства будут уделять больше внимания этическому и правовому измерению технологий и укреплять доверие граждан, создавая нормы и обеспечивая соблюдение их прав»[20].

Этика технологий — это разговор о том, как взаимодействуют технологии и ценности, о решениях, которые мы принимаем в связи с появлением новых технологий, и о том, как они могут повлиять на общество. Это комплекс ценностей, определяющих подход организации к использованию технологий в целом, а также принципы, которыми руководствуются работники всех уровней при внедрении этих технологий в бизнес-стратегию и операционную деятельность. Этика технологий охватывает широкий спектр вопросов — от защиты приватности до предвзятости алгоритмов, от замены труда человека на труд робота до запрета на манипуляцию поведением человека[21].

Именно поэтому Центр подготовки РКЦТ продолжает исследование этических вопросов цифровизации, начатое в 2020 году двухтомной публикацией «Этика и „цифра“: этические проблемы цифровых технологий». Новый доклад посвящен уже не только проблемным зонам и дилеммам, но и подходам к решению этих проблем: технологическим, управленческим, регуляторным. Как и в предыдущей публикации, упор делается на решениях для государства и госслужащих. Отметим также, что заголовок серии — «Этика и „цифра“» — задает максимально широкую рамку для обсуждения самых разных этических вопросов, так или иначе возникающих при разработке цифровых решений и смежных с ними тем.

«Сейчас, когда из-за кризиса мы находимся на пороге следующей, более масштабной волны цифровой трансформации, для организаций как никогда важно обращать внимание на цифровую этику, — считают ведущие сотрудники крупнейшей мировой аудиторской компании PwC. — Цифровая этика должна стать неотъемлемой частью бизнеса. Сейчас организациям сложно внедрять цифровую этику, в основном из-за отсутствия этических норм, укрепляющих доверие общества к цифровой экономике, и нехватки компетентного персонала. В то же время, чтобы достичь поставленных целей цифровой трансформации и развиваться в темпе рынка, крайне важно, чтобы организации работали над цифровой этикой…»[22]

[20] Scassa T. The Post-pandemic Future of Trust in Digital Governance // Centre for International Governance Innovation. URL: https://www.cigionline.org/articles/post-pandemic-future-trust-digital-governance

[21] Bannister C., Sniderman B., Buckley N. Ethical tech: Making ethics a priority in today's digital organization // Deloitte Review. № 26. 2020. URL: https://www2.deloitte.com/content/dam/insights/us/articles/6289_ethical-tech/DI_DR26-Ethical-tech.pdf

[22] de Boer M., van de Merwe D. Digital ethics: main ingredient for successful digital transformation // PwC. URL: https://www.pwc.nl/en/topics/blogs/digital-ethics-necessary-for-successful-digital-transformation.html

Назовем **три ключевых момента**, определяющих значимость этики для цифровой трансформации государства. Во-первых, создание цифровых услуг и цифровизация госуправления в целом — это не просто переход в онлайн уже существующих форм, а **процесс, меняющий принципы взаимоотношений между государством и гражданином**. Изменения касаются всех областей жизни: создаются новые законы и НПА, новые формы общения (чат-боты вместо людей) и контроля (видеонаблюдение с распознаванием лиц), новые способы получения медицинской помощи и образования (удаленно). «Мы находимся в том месте в истории, где, наконец, пришло время изобрести законы, институциональные формы, которые позволят нам приблизиться к цифровому будущему, совместимому с демократией»[23], — пишет Шошана Зубофф. В одночасье происходит много быстрых и почти необратимых изменений, рождается новая реальность. Этот процесс не слишком предсказуем и слабо поддается управлению. При отсутствии этических норм и ограничений он может привести к самым неожиданным и неприятным последствиям для общества.

Второе ключевое изменение — **стремительный рост ответственности тех, кто создает и внедряет технические решения**. В прежней парадигме решения, связанные с «преступлением и наказанием», ограничениями для граждан и т. д., принимались на основании известных законов. Законы составляли юристы, имеющие представление об этических дилеммах, изучавшие эту сферу, знакомые с ее практическим применением. Был отлажен процесс принятия законов с регламентированным взаимодействием участников. Сейчас значимые решения принимают в том числе руководители среднего звена департамента информационных технологий (ИТ). У них может не быть времени, чтобы погружаться в этические нормы, и не всегда хватает компетенций, чтобы разобраться в философских, юридических или социологических аспектах этики, но при этом их власть и ответственность беспрецедентны (см. раздел 7). Нужно осознать тот факт, что сейчас практическое управление, особенно экстренное и кризисное, выполняется с помощью цифровых решений. Даже если эти решения временны, их последствия могут остаться с нами надолго. Именно эти решения и та логика, которая в них заложена, определяют жизнь людей.

Есть и третий, возможно, главный момент: кроме временных решений и экстренно создаваемых продуктов разрабатываются цифровые платформенные решения по масштабному управлению государством, вводятся новые **технологии с большим потенциалом, но не до конца проясненными этическими и социальными рисками** (например, скоринговые[24] модели на основе технологии ИИ). При этом остается множество нерешенных вопросов, начиная от предвзятости ИИ (AI bias[25])

[23] Skelton S. Surveillance capitalism in the age of Covid-19 // ComputerWeekly.com. URL: https://www.computerweekly.com/feature/Surveillance-capitalism-in-the-age-of-Covid-19

[24] Скоринг — это технология расчета оценки и присвоения рейтинга пользователю для выявления его ценности как клиента, например при выдаче банковского кредита, аренде квартиры, предоставлении социальной помощи, госуслуг, а также для выявления рисков, связанных с предоставлением услуги данному пользователю. Любые системы ранжирования или определения значимости человека — это скоринговые системы.

[25] Черняк Л. Сексизм и шовинизм искусственного интеллекта. Почему так сложно его побороть? // TAdviser. URL: https://www.tadviser.ru/index.php/Статья:AI_bias_(предвзятость_искусственного_интеллекта)

и заканчивая невозможностью отследить, что именно влияет на его выводы. С одной стороны, цифровые решения разрабатываются более масштабно и качественно, чем быстрые решения эпохи пандемии, с другой, это по-прежнему плод работы не столько юристов, философов и экспертов из общественных организаций, сколько чиновников, разработчиков, специалистов по данным и т. д. Ни одна из этих специальностей не предполагает глубокого погружения в тему этики. Эту ситуацию необходимо срочно менять. Подобные решения уже на нынешнем этапе развития технологий должны быть этичными, это позволит избежать серьезных социальных последствий (см. раздел 3). Хотя пандемия была на руку надзорным капиталистам, а усиление государственной слежки создает новые риски, Шошана Зубофф уверена, что еще ничего не решено и будущее в руках граждан: «Нам нужны новые общественные движения, новые формы общественной солидарности. Законодатели должны чувствовать, что мы будем настаивать на своем. <...> Перемены не случатся в одночасье, но сейчас то десятилетие, когда мы должны действовать»[26].

Названные ключевые проблемы не абстрактны. В конечном счете каждый госслужащий работает не для того, чтобы выполнять указания; его задача — улучшать качество жизни людей, их удовлетворенность госуслугами и в целом работой государства. И учитывать этику в принятии повседневных решений — значит предвидеть последствия, которые эти решения могут иметь для разных групп населения.

«Идеальных решений не бывает, но в каждом случае нужно четко понимать, кто выиграет и кто проиграет, уметь обосновать логику решения, иметь ответы на сложные вопросы. Если же власть не может объяснить эту логику, устраняется от ответственности, ссылается на приказы — значит, не она управляет цифровыми решениями, а цифровые решения управляют ею».

Ксения Ткачева,
директор Центра подготовки РКЦТ

Авторы доклада хотели бы, чтобы этика была не только модной темой для дискуссий, а этические кодексы систематически применялись бы при разработке технологий. Пока сложно оценить глубину и опасность этического разрыва, в том числе и потому, что нет общественного контроля за процессом разработки цифровых решений. Доклад отражает разные точки зрения на вопросы этики в принятии решений в госсекторе. Когда мы говорим об этике решений, нужен индивидуальный подход к каждому госслужащему: для кого-то важна репутация органа, региона, для кого-то — личная репутация, для кого-то — успешность решения или все названное вместе. Поэтому в этой книге каждый найдет аргументы, которые будут важны для него, и инструменты, которые он сможет использовать в работе.

[26] Skelton S. Surveillance capitalism in the age of Covid-19 // ComputerWeekly.com. URL: https://www.computerweekly.com/feature/Surveillance-capitalism-in-the-age-of-Covid-19

Как это сделать? Рецепт простой: в процессе принятия решения надо понимать, присутствует ли в нем этическая составляющая (она присутствует не всегда, но в большинстве случаев), не рассчитывать только на свою экспертность, а привлекать специалистов для консультаций. Не надо бояться выносить этические проблемы на обсуждение — о них надо постоянно думать, анализировать их, следить за мировой повесткой, смотреть, что делают коллеги.

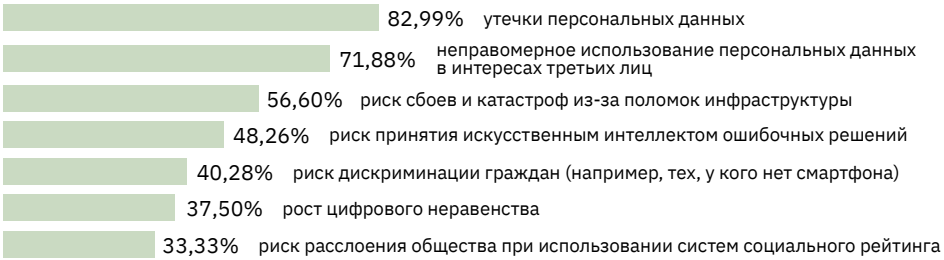
С самого начала работы Центра слушателей интересовала этика принятия решений, хотя еще не было четкого понимания места этики в работе государственных органов. Преподаватели Центра, читавшие лекции по этой теме с 2018 года, сумели показать, что этические вопросы требуют к себе особого внимания, что они должны быть фундаментом всей работы. Пандемия COVID-19 сделала этику принятия решений трендом, и этим надо воспользоваться — ведь пока тема недостаточно популярна, ее сложнее продвигать, амбассадорам этики труднее отстаивать свое мнение. Например, госслужащий после обучения в Центре проникся значимостью этического подхода, возвращается в свою команду и встречает скепсис: «Нам тут надо работать, показывать результаты, выполнять показатели, а он хочет этику обсуждать». В 2018 и 2019 годах этика была именно такой маргинальной темой. Сейчас ситуация коренным образом изменилась, об этике стали больше говорить и писать, хотя, к сожалению, реальных практических сдвигов в России пока не произошло. Необходимо, чтобы эта тема из сферы обсуждений перешла в сферу ежедневной рутинной работы.

Чтобы убедиться в актуальности заявленных тем не только для слушателей Центра, но и для более широкого круга госслужащих и руководителей ЦТ, авторы доклада обратились к потенциальным читателям. Результаты анонимного опроса специалистов, причастных к разработке или эксплуатации государственных цифровых сервисов или интересующихся этим направлением[27], представлены на рисунке 1. Главной этической проблемой при создании и использовании цифровых технологий респонденты считают неправильное обращение с персональными данными (ПДн). 83% опрошенных считают наиболее критичной утечку ПДн, также вызывают опасения риск передачи данных третьим лицам (72%) и сбои и поломки инфраструктуры (57%): цифровой мир респонденты воспринимают как во многом непрочный и ненадежный.

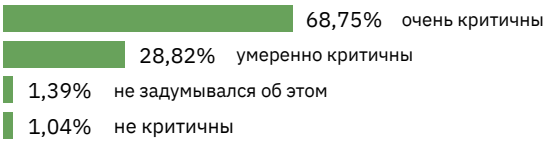
Отдельно предлагалось оценить, насколько критичен риск недостаточной защиты ПДн — и 98% опрошенных говорят о той или иной степени критичности этой проблемы. Если говорить о конкретных типах цифровых услуг, то наибольшее беспокойство вызывают сервисы реестрового типа, аккумулирующие все данные о гражданине («цифровой профиль»), использование биометрии и цифровая слежка. В целом респонденты

[27] Опрос проводился онлайн, были получены ответы от 288 респондентов (выгрузка 05.04.21). Основу выборки составили государственные и муниципальные служащие, руководители и специалисты. Каждый четвертый респондент был руководителем проекта цифровой трансформации, 23,6% являлись заказчиками и разработчиками цифровых продуктов и сервисов.

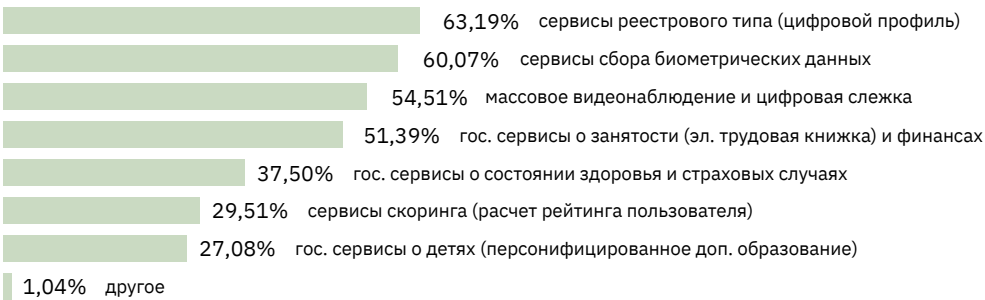
Какие отрицательные стороны вы видите в массовом внедрении цифровых технологий?



Как вы думаете, насколько критичны риски недостаточной защиты персональных данных при разработке цифровых сервисов?



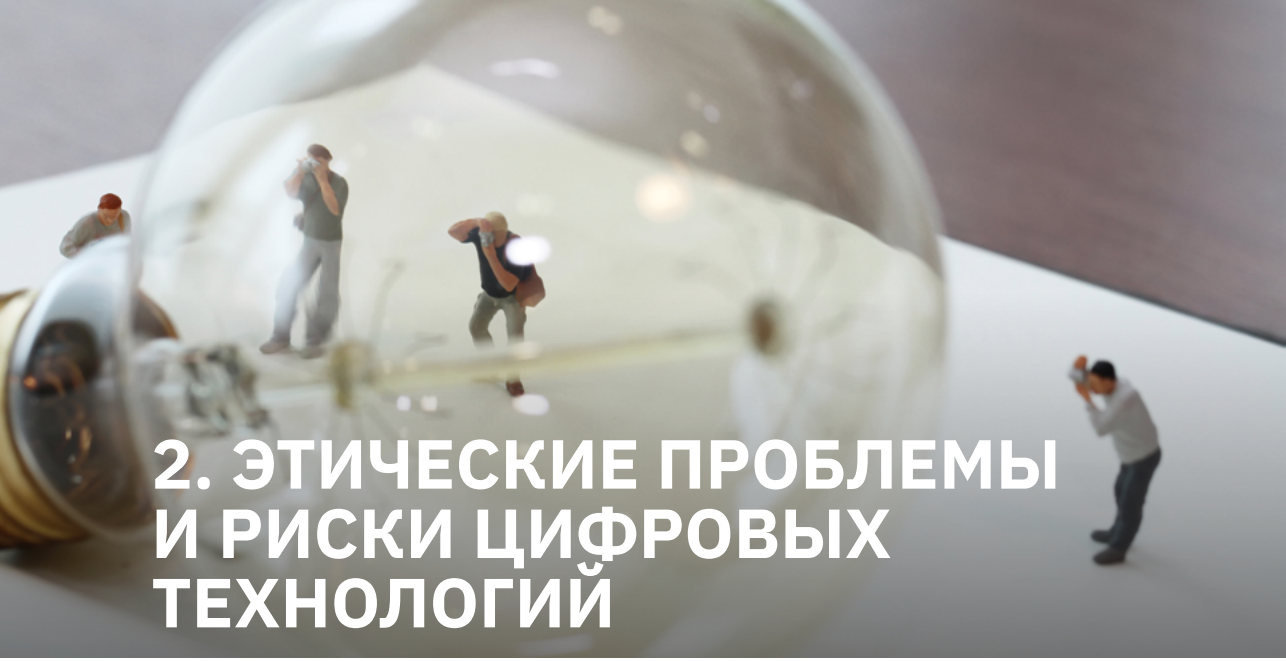
При использовании каких технологий выше риск утечек персональных данных или их нецелевого использования?



В каких сферах следует уделить больше внимания вопросам этики при внедрении цифровых технологий?

Рисунок 1. Результаты онлайн-опроса об этической стороне цифровых технологий

считают тему важной для себя; лишь 4% не интересуются темой и ничего о ней не знают. В публикациях о цифровой этике аудитории интересна прежде всего практическая составляющая: примеры этичных решений, оценка рисков при создании цифровых продуктов, способы сделать эти продукты более этичными, нормативное регулирование. Именно этим темам и посвящен доклад.



2. ЭТИЧЕСКИЕ ПРОБЛЕМЫ И РИСКИ ЦИФРОВЫХ ТЕХНОЛОГИЙ

— Главное, — сказал Форд, — перестань паниковать.
— А кто сказал, что я паникую? — огрызнулся Артур. —
Это пока просто шок. Вот подожди, я освоюсь,
осмотрюсь. Тогда и начну паниковать!

Д. Адамс. Автостопом по галактике

2.1 ОТНОШЕНИЕ К ДАННЫМ ГРАЖДАН

Время чтения — 22 минуты

Пожалуй, не осталось людей, которые не знают, что их данные собирают и используют городские системы видеонаблюдения, органы правопорядка, сотовые операторы, «Госуслуги», производители смартфонов, банки, кибермошенники и многие другие. Параллельно с ростом объемов собираемых данных растет не только количество полезных услуг и продуктов, но и количество утечек, случаев кибермошенничества и злоупотребления данными. Серьезные проблемы цифровых технологий касаются персональных данных[28] и больших данных[29].

[28] Персональные данные (ПДн) — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн) (см. ФЗ-152). В частности, это фамилия, имя и отчество человека, дата рождения, пол, место жительства.

[29] Большие данные (big data) — термин, который характеризует накопление и анализ информационных ресурсов, объем которых превышает возможности их хранения и анализа на основе созданных ранее аппаратных и программных средств (п. 31 доклада генерального секретаря ООН «Использование информационно-коммуникационных технологий для инклюзивного социально-экономического развития» / Комиссия ООН по науке и технике в целях развития // ООН. URL: https://undocs.org/ru/E/CN.16/2014/3). Обычно большие данные существуют в цифровой форме и не предполагают ручной обработки. Большие пользовательские данные — это большие данные, собранные о физических лицах в процессе использования ими различных сервисов; их источником являются в том числе частные устройства и интернет вещей. Часто содержат персональные данные.

2.1.1 НАРУШЕНИЕ НЕПРИКОСНОВЕННОСТИ ЧАСТНОЙ ЖИЗНИ

Возможность контролировать распространение информации о себе и своей частной жизни — неотъемлемый элемент приватности[30]. Чаще всего люди хотят, чтобы сведения об их личности и частной жизни оставались тайной. При этом аргумент «я не делаю ничего плохого и мне нечего скрывать»[31] уже не работает: мошенники, которые используют утекшие из государственных или коммерческих баз данные, не делают исключения для законопослушных граждан.

Проблемы возникают на всех этапах работы с данными. На этапе сбора информации имеют место: избыточность (данные собирают «с запасом», даже те, которые не требуются для достижения заявленной цели); излишняя инвазивность (вторжение в частную жизнь) и сбор данных без уведомления субъекта; обогащение (совмещение разных баз, в результате чего формируется более полный профиль пользователя с его личными предпочтениями, интересами, контактными и иными данными). На этапе хранения и обработки возможны нецелевое использование данных, утечки и кражи. Если данные утекли или были украдены, возникают разнообразные риски их противоправного использования (мошенничества, злоупотреблений и т. д.), причем такое использование может нанести особенно серьезный вред в случае обогащенных данных. Отдельно следует отметить непредсказуемость дальнейшего использования данных: субъект данных в момент сбора данных не знает, что с ними будет происходить в долгосрочной перспективе.

Во время пандемии неприкосновенность частной жизни и право на защиту личной информации были оттеснены главным требованием дня — избежать распространения инфекции, победить болезнь. На первый план вышло выявление тех, кто нарушает ограничения. Государства и ИТ-гиганты и раньше могли получать чувствительную информацию о гражданах, используя данные сотовых операторов, мобильных приложений, сетей Wi-Fi, геолокации, городских систем видеонаблюдения с распознаванием лиц и др. (мы писали о дата-корпорациях, бизнес которых построен на сборе данных пользователей и использовании их в коммерческих целях[32]). Те данные, которые ИТ-компании используют для получения прибыли, в 2020 году многие страны мира, стремясь ограничить распространение COVID-19, стали использовать для отслеживания перемещения людей и их контактов.

Авторы раздела:

С. В. Коршунова

Е. Г. Потапова

О. С. Шепелева

[30] Понятие приватности // Этика и «цифра»: этические проблемы цифровых технологий. В 2 т. М.: РАНХиГС, 2020. URL: http://ethics.cdto.center/5_1#5.1.1

[31] См. подробнее о вопросах восприятия приватности гражданами и госорганами в эссе профессора юридического факультета Университета Джорджа Вашингтона Дэниела Дж. Солова (Daniel J. Solove) 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. URL: https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?referer=https://etnowiki.ru/&httpsredir=1&article=1159&context=faculty_publications

[32] Капитализм слежки // Этика и «цифра»: этические проблемы цифровых технологий. В 2 т. М.: РАНХиГС, 2020. URL: https://ethics.cdto.center/5_2

Раньше законы и общественное сопротивление замедляли и ограничивали развитие систем слежки, построенных на сборе данных, но во время пандемии приоритеты сместились от защиты прав и свобод к обеспечению безопасности, ради которого допустимы временные ограничения для граждан (например, ограничение свободы передвижения). В некоторых странах мобильные приложения для трекинга заболевших были обязательными к установке. Существуют вполне обоснованные опасения, что временные ограничения останутся после окончания эпидемии и станут постоянными. В аэропортах до сих пор действуют меры безопасности и ограничения, введенные после терактов 2001 года, и никто не думает их отменять.

Жителям Катара грозил штраф в размере до 55 тыс. долл. или лишение свободы сроком до трех лет за отказ от установки правительственного приложения, разработанного для борьбы с пандемией[33].

В китайском Ханчжоу в мае 2020 года предложили на постоянной основе использовать приложение для отслеживания больных COVID-19 и после пандемии[34]. Это приложение должно было стать полноценным инструментом отслеживания многих показателей здоровья граждан. Похоже, эта идея не была воплощена в жизнь.

Эпидемиологи в США летом 2020 года заявляли, что защита ПДн затрудняет борьбу с пандемией, а значит, данные следует делать более доступными для государственных и медицинских организаций. Например, из-за требований законодательства сложно или невозможно делиться с другими регионами и тем более государствами такой информацией, которая помогла бы выявлять пути распространения болезни[35].

Технология распознавания лиц — часть новой системы «Большого брата», которая зарождается в разных странах мира[36]. Государству технология распознавания лиц интересна в первую очередь для обеспечения общественной и национальной безопасности и борьбы с преступностью, в том числе для противодействия терроризму. Сложность заключается в поддержании справедливого баланса общественных и частных интересов, обеспечения безопасности и защиты прав гражданина.

Проблема слежки проявляется на всех уровнях. При желании многие цифровые решения можно использовать для слежки за людьми.

[33] Sadek G. Qatar: Installing COVID-19 Tracing App on Mobile Phones and Wearing Face Masks among Recent Mandatory Anti-pandemic Measures Instituted by Authorities // Library of Congress. URL: https://www.loc.gov/law/foreign-news/article/qatar-installing-covid-19-tracing-app-on-mobile-phones-and-wearing-face-masks-among-recent-mandatory-anti-pandemic-measures-instituted-by-authorities/

[34] Davidson H. Chinese city plans to turn coronavirus app into permanent health tracker // The Guardian. URL: https://www.theguardian.com/world/2020/may/26/chinese-city-plans-to-turn-coronavirus-app-into-permanent-health-tracker

[35] Data secrecy is crippling attempts to slow COVID-19's spread in U.S., epidemiologists warn // Science. URL: https://www.sciencemag.org/news/2020/07/us-epidemiologists-say-data-secrecy-covid-19-cases-cripples-intervention-strategies

[36] Подробнее об этом см.: Государственная слежка — «Большой брат» // Этика и «цифра»: этические проблемы цифровых технологий. В 2 т. М.: РАНХиГС, 2020. URL: http://ethics.cdto.center/5_3

Компания Apple в 2021 году выпустила устройства-метки AirTags. Энтузиасты быстро доказали, что метки вполне можно использовать не только для поиска своих вещей, как предполагали разработчики, но и для слежки за людьми: достаточно незаметно подбросить метку в сумку или в карман объекта слежки. Разумеется, разработчики задумывались о безопасности использования девайса, поэтому устройство Apple уведомит владельца, если рядом с ним появилась чужая метка. Но вот владелец устройства на Android обнаружить такую метку в своих вещах не сможет. Таким же образом можно использовать GPS-метки, метки для собак и другие устройства, давно существующие на рынке.

Есть и позитивные тенденции. Общепринятое мнение об этичности систем распознавания лиц еще не сформировалась, но их активное использование во время пандемии подстегнуло общество к обсуждению этого вопроса. Общество получает все больше информации о проблеме нарушения приватности. В 2020 году появились заметные проекты, которые занимаются сбором и анализом сведений о цифровой слежке. В России проект Pandemic Big Brother[37] (организаций «Роскомсвобода» и Human Constanta) показывает на интерактивной карте статус ограничений, введенных во время пандемии, и примеры конкретных технологий, которые использует «Большой брат». В базе американского проекта «Атлас слежки» (Atlas of Surveillance[38]), который ведет НКО Electronic Frontier Foundation, собраны тысячи случаев слежки с помощью технологий, включая распознавание лиц на фото и видео, камеры на одежде, автоматическое распознавание номеров машин, локальные партнерства по созданию реестров видеокамер и других устройств слежки, использование дронов, симуляторов базовых станций и многое другое.

Международная организация «Европейские цифровые права» (EDRi) запустила кампанию против массового биометрического наблюдения «Верни свое лицо» (Reclaim Your Face[39]). Организаторы утверждают, что «распознавание лиц может и будет использоваться против каждого из нас правительствами и корпорациями», и призывают подписать петицию за принятие закона, запрещающего видеонаблюдение с распознаванием лиц. Активные участники кампании из восьми европейских стран (Германии, Франции, Италии, Нидерландов, Чехии, Словении, Сербии, Греции) отмечают свои победы в борьбе за приватность (см. также раздел 5.3.2):

- **итальянское агентство по защите данных (DPA) запретило использование системы распознавания лиц SARI, приобретенной итальянской полицией в 2017 году;**
- **голландское DPA направило всем отраслевым ассоциациям разъяснения, какие действия являются законными, а какие — незаконными при использовании технологий распознавания лиц и биометрического наблюдения;**

[37] Pandemic Big Brother. URL: https://pandemicbigbrother.online/ru/

[38] Atlas of surveillance. Documenting Police Tech in Our Communities with Open Source Research // Electronic Frontier Foundation. URL: https://atlasofsurveillance.org/

[39] Reclaim Your Face. URL: https://reclaimyourface.eu/

› **греческое DPA начало официальное расследование по фактам создания полицией централизованной биометрической базы данных и использования интеллектуальных устройств, позволяющих распознавать лица и отпечатки пальцев тех, кого полицейские останавливают на улице.**

Эта реакция свидетельствует о другой важной тенденции: в ряде стран стали запрещать или серьезно ограничивать применение технологий, если потенциальный вред превышает потенциальную пользу. Неэтичное использование данных и технологий становится достаточным поводом для отказа от их использования, хотя бы временного.

В разгар движения Black Lives Matter в США цифровые гиганты IBM, Microsoft и Amazon, которые не один год развивали системы распознавания лиц, отказались предоставить эту технологию для городских систем видеонаблюдения[40]. По словам главы компании IBM[41], пользователи систем, в которых задействован ИИ, должны нести общую ответственность за продукт. Компания Google сообщила, что намерена ввести функцию автоматического удаления истории геолокаций пользователей, а также информации об активности в интернете по истечении 18 месяцев[42].

Летом 2020 года в Бостоне был принят закон о запрете использования технологии распознавания лиц городскими службами (прежде всего полицией)[43]. Ранее аналогичные акты приняли Сан-Франциско и Окленд (штат Калифорния), Кембридж (штат Массачусетс).

В Портленде (США) с 1 января 2021 года закон запрещает использование технологий распознавания лиц частными компаниями[44]. Запрет распространяется на общественные места в границах города, в том числе на все типы предприятий, банки, отели, магазины. Гражданин, который сочтет, что в отношении него этот закон был нарушен, может взыскать с виновника компенсацию вреда в размере 1 тыс. долл. США за каждый день нарушения, а также гонорар адвоката.

Компаниям за пределами Портленда рекомендуется соблюдать ряд этических принципов при создании технологий распознавания лиц:

- **тестировать программу на точность и отсутствие предвзятости;**
- **разработать общедоступную политику конфиденциальности,**

[40] IBM CEO's Letter to Congress on Racial Justice Reform // IBM. URL: https://www.ibm.com/blogs/policy/facial-recognition-susset-racial-justice-reforms/; Dastin J., Vengattil M. Microsoft bans face-recognition sales to police as Big Tech reacts to protests // Reuters. URL: https://www.reuters.com/article/us-microsoft-facial-recognition/microsoft-bans-police-face-recognition-sales-as-big-tech-reacts-to-protests-idUSKBN23I2T6; Fitch A. Amazon Suspends Police Use of Its Facial-Recognition Technology // The Wall Street Journal. URL: https://www.wsj.com/articles/amazon-suspends-police-use-of-its-facial-recognition-technology-11591826559

[41] Dastin J., Vengattil M. Microsoft bans face-recognition sales to police as Big Tech reacts to protests // Reuters. URL: https://www.reuters.com/article/us-microsoft-facial-recognition/microsoft-bans-police-face-recognition-sales-as-big-tech-reacts-to-protests-idUSKBN23I2T6

[42] Kelion L. Google to auto-delete users' records by default // BBC News. URL: https://www.bbc.com/news/technology-53165566

[43] Ng A. Boston votes to ban government use of facial recognition // CNET. URL: https://www.cnet.com/news/boston-votes-to-ban-government-use-of-facial-recognition/

[44] Oberly D. J. Time to comply with the nation's newest biometric privacy law: Portland's private sector facial recognition ban // Biometric Update. URL: https://www.biometricupdate.com/202101/time-to-comply-with-the-nations-newest-biometric-privacy-law-portlands-private-sector-facial-recognition-ban

письменно уведомлять пользователей о сборе данных для создания шаблона лица и о целях создания таких шаблонов;
- **получать письменное разрешение от каждого лица, шаблон которого создается;**
- **предусматривать возможность отказа пользователя от сбора его биометрических данных;**
- **обеспечивать безопасность данных;**
- **строго соблюдать запрет на использование технологий в целях дискриминации.**

2.1.2 ПРОТИВОПРАВНОЕ ИСПОЛЬЗОВАНИЕ ДАННЫХ О ЛЮДЯХ

Утечка данных о клиентах какого-то сервиса или просто учтенных в какой-то информационной системе (ИС) — одна из самых распространенных угроз, связанных с цифровыми технологиями. В России любые данные граждан могут оказаться оказаться в сети или на «черном рынке», где продаются и базы ИС госорганов[45], и базы коммерческих организаций. В финансовой сфере России число утечек конфиденциальных данных в 2020 году выросло на 36,5%, в то время как в мире снизилось на 7,3%[46]. Особенно часто данные утекают (или их воруют) при использовании мессенджеров и при удаленной работе, когда привычные требования безопасности ослабевают.

Данные, размещенные на досках сервиса Trello сотен тысяч мелких и средних компаний, в 2021 году обнаружили в открытом доступе сотрудники компании Infosecurity[47]. На таких досках часто содержится конфиденциальная информация.

Технологии развиваются быстро, и нормативная база в части обеспечения информационной безопасности (ИБ) не всегда за ними успевает, поэтому даже полного соблюдения требований может быть недостаточно для обеспечения безопасности[48]. Утечки случаются во всех странах мира, от них никто не застрахован. Чаще всего причинами утечек становятся:

- ошибки в законодательстве;
- недостаточно продуманная работа регулирующих и контролирующих органов;
- ошибки разработчиков баз данных (например, неправильно настроенные серверы);

[45] Проблемы и коллизии: можно ли «механизмами лечить недуги человечества»? // Этика и «цифра»: этические проблемы цифровых технологий. В 2 т. М.: РАНХиГС, 2020. URL: http://ethics.cdto.center/5_1#link285

[46] Исследование утечек информации из финансовых организаций в 2020 году: аналитический отчет // InfoWatch. URL: https://www.infowatch.ru/analytics/reports/issledovanie-utechek-informatsii-iz-finansovykh-organizatsiy-v-2020

[47] Степанова Ю. Свои в досках // Коммерсантъ. URL: https://www.kommersant.ru/doc/4781538

[48] Лукацкий А. Моделирование нарушителей по методике ФСТЭК: теория и реальность // Бизнес без опасности. URL: https://lukatsky.blogspot.com/2021/04/blog-post_19.html

› действия недобросовестных сотрудников, которые копируют данные для последующей продажи.

В США хакеры скачали базу данных в 250 Гб у городской полиции Вашингтона (США) и требовали выкуп, угрожая в противном случае передать информацию криминальным группировкам[49]. В слитой базе данных были отчеты о расследованиях, досье на сотрудников и преступников и др. В Бразилии в январе 2021 года произошла крупнейшая утечка данных в стране. Из государственной информационной системы утекли конфиденциальные данные 223 млн налогоплательщиков, физических лиц и организаций[50]. Ранее на GitHub попала база личных данных 16 млн бразильцев с диагнозом COVID-19, включая президента Бразилии[51].

Если организация не выполняет требования ИБ, на нее может быть наложен штраф, но штрафы составляют десятки тысяч рублей, а средства информационной защиты стоят миллионы, да и услуги специалистов по ИБ тоже дороги. Поэтому организации порой проще заплатить штраф в случае утечки, чем задумываться об обеспечении безопасности.

Суды по поводу мелких утечек проходят очень часто. Как правило, наказание в виде условного или реального лишения свободы получают сотрудники правоохранительных органов, банков, мобильных операторов за небольшие суммы, однако существенные по сравнению с их зарплатой. Более крупные утечки наносят репутационный ущерб, но редко приводят к штрафам или другим наказаниям. Например, в 2020 году в Москве утекли данные из ИС для выдачи цифровых пропусков во время пандемии[52].

Даже если компания заплатила штраф государству, тем гражданам, чьи данные утекли, ущерб никак не компенсируется. Этот ущерб может выражаться в дискомфорте от спам-звонков, в попытках (иногда успешных) кибермошенничества, в занижении рейтинга в скоринговых системах (например, при выдаче кредитов).

Более серьезную угрозу создает злоупотребление данными. Несмотря на существующие во многих странах законы о защите ПДн, граждане чаще всего не могут распоряжаться своими данными — негласно закрепилась норма «данные принадлежат тому, кто их собрал». В результате распространено нецелевое использование данных граждан с целью извлечения коммерческой и иной выгоды; скрытое манипулирование с использованием личной информации о пользователях, полученной

[49] Cimpanu C. Ransomware gang threatens to expose police informants if ransom is not paid // The Record. URL: https://therecord.media/ransomware-gang-threatens-to-expose-police-informants-if-ransom-is-not-paid/

[50] Mari A. Brazil Tech Round-Up: Government Responds To Massive Data Leak, Totvs Results, Healthtech Growth // The Forbes. URL: https://www.forbes.com/sites/angelicamarideoliveira/2021/02/13/brazil-tech-round-up-government-responds-to-massive-data-leak-totvs-results-healthtech-growth/

[51] Cimpanu C. Personal data of 16 million Brazilian COVID-19 patients exposed online // ZDNet. URL: https://www.zdnet.com/article/personal-data-of-16-million-brazilian-covid-19-patients-exposed-online/

[52] Депутат Лысаков сообщил в СБ РФ о передаче силовиками данных о машинах в мэрию Москвы // Интерфакс. URL: https://www.interfax.ru/moscow/704877

благодаря анализу больших данных и обогащению данных; злоупотребление служебным положением для доступа к конфиденциальным данным (например, к базам правоохранительных органов).

Коллекторы из новосибирского агентства угрожали сначала женщине, которая не вернула вовремя долг микрофинансовой организации, а затем ее друзьям и работодателю. Разумеется, согласия на такое использование ПДн никто из пострадавших не давал. В суде выяснилось, что коллекторское агентство не впервые нарушает закон подобным образом, поэтому суд назначил повышенный штраф — 300 тыс. руб.[53]

Технологии позволяют **извлечь дополнительную информацию** о людях из самых разных источников. При этом отдельные наборы данных могут не содержать ПДн, таких как паспортные данные, ФИО, адрес, медицинские, биометрические (включая те, по поводу которых идут споры[54], признавать ли их персональными). Зато они могут содержать данные геолокации, контент соцсетей, данные о финансовых транзакциях, заказах в интернет-магазинах. Даже данные тепловых счетчиков, уличной системы камер видеонаблюдения и других технических систем могут быть использованы, чтобы узнать периоды пребывания человека дома, его маршруты в городе, бытовые привычки.

Метаданные, которые можно извлекать из открытых данных, создают отдельную проблему, особенно если это метаданные определенных категорий (студентов, детей). От компаний требуется обезличивание этих метаданных, которые извлекают (прежде всего из соцсетей) для таргетирования рекламы и маркетинговых исследований. Если при анализе метаданных выявляются данные, попадающие в категорию приватности, они должны удаляться автоматически. Однако проследить за выполнением этого условия чаще всего невозможно. В зависимости от того, к кому попадут эти данные, их могут использовать не только в мошеннических целях, но с целью таргетинга рекламы, чтобы повысить вероятность продажи услуги, товара, подписки и т. п.

Бывший азартный игрок в соответствии с законами о защите данных Великобритании запросил информацию о себе у букмекерской конторы, клиентом которой он являлся долгое время. Помимо 34 страниц полной финансовой истории и тысяч полей данных об устройствах, на которых он пользовался сервисом, он увидел подробную информацию о своих личностных характеристиках. Алгоритм букмекерской конторы посчитал его «ценным пользователем» и пытался вернуть его с помощью промописем после того, как клиент решил оставить хобби из-за крупных долгов.

[53] Малинина А. Суд оштрафовал коллекторов, угрожавших жительнице Кузбасса и ее работодателю // A42.ru. URL: https://gazeta.a42.ru/lenta/news/99137-sud-oshtrafoval-kollektorov-ugrozhavshikh-zhitelnitse-kuzbassa-i-ee

[54] См. комментарий правового портала «ГАРАНТ» о неоднозначной судебной практике признания данных биометрическими: Биометрические персональные данные и технологии идентификации: какие правовые проблемы могут возникнуть? // ГАРАНТ.ру. URL: http://www.garant.ru/news/1460152/

Сервисы отслеживания делают всех граждан, независимо от положения, уязвимыми перед киберпреступниками. Большинство современных систем слежения построено на стыке технологий, когда информация о геолокации смартфонов уточняется с помощью данных с камер видеонаблюдения, а система распознавания лиц и видеоаналитики помогает узнать, кто входит в окружение человека. Много информации дают также транзакции и данные транспортных систем. Проанализировав информацию из нескольких источников, можно с большой точностью отслеживать перемещения человека и его контакты, в том числе не имея на это законных оснований[55].

В 2021 году полиция в Москве использовала систему видеонаблюдения с распознаванием лиц для выявления участников несанкционированных акций[56]. К некоторым полицейские приходили домой, другие были задержаны на рабочем месте. Во многих случаях задержанным устно сообщали, что их опознали с помощью камер видеонаблюдения, или к материалам дела прикреплялись распечатанные фотографии.

Избыточный сбор данных о людях создает условия для злоупотреблений данными в будущем, порой через годы после их сбора. Распространенная практика подписания «согласия на обработку персональных данных» фактически не защищает данные, а иногда позволяет использовать их против подписавшего. В момент получения согласия на обработку данных не всегда возможно уведомить человека о том, какие его данные и как именно будут обрабатываться и использоваться в будущем, потому что способы и цели обработки могут появиться гораздо позднее.

Вместо общественного обсуждения выгод и рисков переиспользования ранее собранных данных практикуется сбор данных безусловно и «по умолчанию» надолго. Согласие на сбор и обработку ПДн давно превратилось в неудобную для пользователя формальность. Достаточно один раз нажать «Согласен», и собранные сегодня данные могут использоваться даже через 10–20 лет. При этом оператор данных может записать в текст соглашения практически любые требования, ведь никто не читает их, прежде чем поставить свою подпись.

Соглашаясь на обработку ПДн при оформлении цифрового пропуска, москвичи передавали следующие ПДн: «фамилия, имя, отчество; дата рождения; адрес; профессия; место работы, адрес организации, иная информация о трудовой деятельности; должность в организации; данные документа, удостоверяющего личность; гражданство; образование; номера телефонов; адрес электронной почты; технические данные, которые автоматически передаются устройством, с помощью которого используются

[55] Новый В. Найти коронавирус: как власти могут развернуть систему слежки за контактами больных COVID-19 // Forbes.ru. URL: https://www.forbes.ru/tehnologii/395903-nayti-koronavirus-kak-vlasti-mogut-razvernut-sistemu-slezhki-za-kontaktami-bolnyh

[56] Позычанюк В., Стогней А. «Нам пришел видеоматериал». Умные камеры подключили к распознаванию лиц протестующих // The Bell. URL: https://thebell.io/nam-prishel-videomaterial-umnye-kamery-podklyuchili-k-raspoznavaniyu-lits-protestuyushhih

информационные системы и (или) сайт оператора (в том числе технические характеристики устройства (идентификатор устройства), IP-адрес, файлы cookies, информация о браузере и др.)», и не на время пандемии, а сроком на 10 лет с правом на обработку третьими лицами[57].

Злоумышленники могут использовать ПДн и иные данные о частной жизни человека, чтобы похитить его имущество, обманом выманить деньги или спланировать нападение на него. Чем больше транзакций происходит онлайн, чем больше через Сеть передается чувствительных данных, тем выше активность мошенников. Рост онлайн-мошенничества идет параллельно со снижением физического насилия по всему миру[58]: украсть деньги с карты проще, чем грабить людей на улице. Поэтому при разработке цифровых проектов необходимо продумывать максимально возможную защиту.

Нарастающие объемы кибермошенничества с использованием ПДн, полученных не всегда прозрачно, оставляют граждан один на один с технологиями социального инжиниринга. В основном из-за утечек страдают сами пользователи, чьи данные утекли. Каждая такая история вызывает у них недоверие, а то и открытое презрение к тем организациям, которые гарантируют конфиденциальность и безопасность переданных им данных. Граждане могут повысить свой уровень цифровой грамотности и овладеть приемами «цифровой самообороны», но обеспечение безопасной среды, в которой бы эти навыки были бы не слишком востребованы, остается задачей государства.

В мошеннических целях могут использоваться и подделка копий документов, и банальная кража паролей. Однако наибольшие опасения сейчас вызывают системы идентификации и подтверждения юридически значимых действий, в которых используются биометрические данные. Такие системы создают ряд рисков[59] и для граждан (например, кража денег с банковского счета), и для государства (в случае махинаций с налоговыми вычетами или кражи денег со счетов госорганизаций).

«Важно, чтобы новые технологии не оказались в руках злоумышленников. Известно, что когда изобрели ацетиленовую горелку, то первым ее применением была не сварка труб и не предотвращение аварии, а ограбление банка: грабители с ее помощью разрезали сейф. Современные технологии, безусловно, прогрессивны и полезны, но если они окажутся не в тех руках, то будут представлять опасность. Здесь нужно быть аккуратным».

Григорий Ройзензон, член российской Рабочей группы IEEE по тематике «Этика и искусственный интеллект»

[57] Согласие на обработку персональных данных. URL: https://i.moscow/media/download/11878

[58] Пинкер С. Лучшее в нас. Почему насилия в мире стало меньше. М.: Альпина нон-фикшн, 2021; Кнорре А., Кудрявцев В. Великое снижение преступности // Ведомости. URL: https://www.vedomosti.ru/opinion/articles/2017/09/28/735650-velikoe-snizhenie

[59] Единая биометрическая система: что не так? // VC.ru. URL: https://vc.ru/u/613130-data-privacy-office/219107-edinaya-biometricheskaya-sistema-chto-ne-tak

Как способ защиты биометрическая идентификация надежна только в комбинации с другими средствами (персональными кодами, паролями и т. д.). Использование методов социального инжиниринга создает риск манипулирования и мошенничества, когда человек сам выдает свои данные (голос, видео, пароли, секретное слово, пин-коды и т. д.) мошенникам, тем самым сводя на нет все преимущества сложной системы защиты.

Мошенники, в течение двух лет обманывавшие систему биометрической идентификации личности, украли более 76 млн долл. у налоговой службы Китая[60]. С помощью дипфейк-сервиса они «оживляли» фотографии, загружали их в специально «прошитые» смартфоны и оформляли на несуществующих людей компании-пустышки, которые затем выдавали поддельные налоговые накладные. В Москве уже зафиксированы случаи мошенничества с использованием образцов голоса клиентов банков[61]. Мошенники звонили людям, задавали вопросы, чтобы получить ответы «Да» и «Нет», а затем использовали запись для оформления кредитов.

По-видимому, перечисленные проблемы с данными в ближайшие годы будут только усугубляться — по тем же причинам, что и ранее: избыточный сбор данных о человеке, формальное или недостаточное соблюдение требований информационной защиты государственных баз данных и ГИС, утечки чувствительных данных (ПДн, медицинских, данных о детях, о финансовых транзакциях и т. п.), цифровая слежка со стороны ИТ-гигантов и государств.

Авторы раздела:

Л. В. Земнухова

С. В. Коршунова

О. С. Шепелева

2.2 ЦИФРОВОЕ НЕРАВЕНСТВО И ЦИФРОВАЯ ДИСКРИМИНАЦИЯ

Время чтения — 11 минут

Проблемы цифрового неравенства возникают по разным причинам, в том числе из-за отсутствия необходимой инфраструктуры, из-за физических ограничений, низкого уровня цифровой грамотности граждан. Нарушение прав и дискриминация отдельных граждан и групп все чаще происходят из-за применения алгоритмов и ИИ, имеющих скрытые предубеждения, недостаточно продуманные (или вообще необъяснимые, как при работе с нейросетями — черными ящиками) механизмы принятия решений.

[60] Chinese government-run facial recognition system hacked by tax fraudsters: report // South China Morning Post. URL: https://www.scmp.com/tech/tech-trends/article/3127645/chinese-government-run-facial-recognition-system-hacked-tax

[61] В Москве мошенники оформляют кредиты с помощью биометрии // SecurityLab.ru. URL: https://www.securitylab.ru/news/518707.php; Мошенники стали использовать голоса клиентов банков для получения кредитов // Коммерсантъ. URL: https://www.kommersant.ru/doc/4770172

2.2.1 РАЗНЫЙ УРОВЕНЬ ДОСТУПА К ЦИФРОВЫМ ТЕХНОЛОГИЯМ

Риск ущемления прав может быть связан, например, с тем, что некоторые группы в обществе имеют ограниченный уровень доступа к технологиям или находятся в состоянии цифровой эксклюзии. Например, кто-то живет в местности, где нет современных средств связи, у кого-то не хватает денег, чтобы купить устройство, поддерживающее работу современных приложений, кто-то не имеет навыков, чтобы при помощи цифровых технологий безопасно и эффективно общаться, делать покупки, работать, учиться и пр. Для этих людей повсеместная цифровизация государственных и коммерческих сервисов означает либо полную утрату доступа к ним, либо существенное снижение их доступности[62], хотя такой эффект противоречит задачам перехода на «цифру»: открывать новые возможности, ускорять, упрощать и удешевлять процессы.

В Норвегии[63] некоторым семьям с детьми-школьниками во время пандемии приходилось искать места вне дома с устойчивым интернет-соединением, чтобы дети продолжали учиться. В России стал широко известен случай деревни Новопетровка Пермского края, где школьники из-за проблем с Сетью залезали на старую телевышку для отправки домашних заданий[64]. В отчете Digital Planet[65] описаны случаи, когда родители везли детей на парковку ближайшего супермаркета с бесплатным Wi-Fi, а в семьях, в которых устройств не хватало, возникал сложный выбор: использовать единственное устройство для работы родителя или для обучения школьника в одно и то же время. Необходимость учиться перед компьютером или гаджетом негативно влияет[66] на слух, зрение, способность к концентрации, повышает утомляемость и общий уровень стресса у студентов и школьников. Обучению мешают невозможность уединиться в комнатах в общежитиях даже во время экзамена, отсутствие у многих студентов отдельного пространства дома и другие бытовые причины.

Цифровая дискриминация из-за неравного доступа к технологиям проявляется, как правило, по отношению к уже социально неблагополучным людям, что радикально усиливает риски социальной сегрегации. Исследования показывают[67], что лица, страдающие от цифровой эксклюзии, не распределяются равномерно по всем социальным

[62] Подробнее см.: Дискриминация и цифровое неравенство // Этика и «цифра»: этические проблемы цифровых технологий. В 2 т. М.: РАНХиГС, 2020. URL: https://ethics.cdto.center/6_1

[63] Norway's statistics agency was also the first in the world to calculate the permanent damage inflicted by school closures: every week of classroom education denied to students, it found, stymies life chances and permanently lowers earnings potential. (Nelson F. Norway health chief: lockdown was not needed to tame Covid // The Spectator. URL: https://www.spectator.co.uk/article/norway-health-chief-lockdown-was-not-needed-to-tame-covid)

[64] Школьники забирались на телевышку, чтобы отправить «домашку». Власти Прикамья прокомментировали ситуацию // Properm.ru. URL: https://properm.ru/news/society/184080/

[65] Digital in the time of COVID. Trust in the Digital Economy and Its Evolution Across 90 Economies as the Planet Paused for a Pandemic // Digital Planet. URL: https://sites.tufts.edu/digitalplanet/files/2021/03/digital-intelligence-index.pdf

[66] Трудности цифровизации: коллективное письмо студентов НИУ ВШЭ руководству и сотрудникам университета // Гражданская инициатива. URL: http://netreforme.org/news/trudnosti-tsifrovizatsii-kollektivnoe-pismo-studentov-niu-vshe-rukovodstvu-i-sotrudnikam-universiteta/

[67] Digital Exclusion. A research report by the Low Incomes Tax Reform Group of The Chartered Institute of Taxation. April 2012. URL: https://www.litrg.org.uk/sites/default/files/digital_exclusion_-_litrg_report.pdf

стратам, а сконцентрированы в группах, которые и без того относятся к уязвимым и неблагополучным, — пожилых людей, людей с физическими ограничениями и серьезными заболеваниями, малоимущих, мигрантов, представителей этнических и языковых меньшинств.

Фактически цифровизация государственных и коммерческих сервисов приводит к дискриминации указанных групп, если не предпринимаются специальные меры для помощи им, например разработка дизайна сайтов для людей с физическими ограничениями, сохранение аналоговой формы получения услуги (возможности лично обратиться за услугой или позвонить в контактный центр, использовать бумажные документы вместо электронных, привлечь человека-посредника) и т. д.[68]

В Индии в 2021 году некоторые жители не могли записаться на вакцинацию, поскольку не имели смартфонов или не умели ими пользоваться[69]. Иногда они узнавали о том, что прием только по записи, уже отстояв большую очередь в центр вакцинации. Необходимо иметь хотя бы один смартфон в семье или у друзей, чтобы вакцинироваться. Такое решение отсекает от услуги часть людей, для которых цифровые технологии недоступны: граждан с самыми низкими доходами, мигрантов, неграмотных и престарелых граждан.

Аналоговый способ получения услуги должен быть сохранен даже для тех, у кого есть доступ к цифровым решениям. Хотя исключение из процесса человека искореняет коррупцию и (частично) предвзятость, **оно усложняет решение проблем в нестандартных и редких ситуациях**, при сбоях и отказах системы (в том числе таких банальных, как отключение электричества). Аналоговая альтернатива позволяет в этих ситуациях сохранить гражданам доступ к жизненно важным продуктам и услугам и решить проблемы тех, кто не вписывается в сценарии алгоритмов.

101-летний житель Великобритании подал заявление о желании остаться в стране после вступления в силу договора о Брексите. Как гражданин Италии, он, хоть и жил в Лондоне с 1966 года, обязан был подать заявление о желании остаться жить в Великобритании. Документы распознавались автоматически, программа считала последние две цифры года рождения — 1919 — и посчитала 101-летнего дедушку годовалым ребенком. Далее алгоритм потребовал предоставить согласие родителей «ребенка» на его дальнейшее пребывание в стране[70]. Только вмешательство сотрудников ведомства помогло разрешить проблему и верно оформить документы.

У тотального навязывания «цифры» и отказа от якобы никем не востребованных аналоговых вариантов есть обратная сторона — цифровой луддизм. Есть ли у граждан право на отказ от цифровых

[68] Социальные вызовы технологий // Этика и «цифра»: этические проблемы цифровых технологий. В 2 т. М.: РАНХиГС, 2020. URL: http://ethics.cdto.center/6_1

[69] Wajihudin M. Digital divide: Lack of smartphones deprives many of jabs // The Times of India. URL: http://timesofindia.indiatimes.com/articleshow/82622523.cms

[70] O'Carroll L., Giuffrida A. Home Office tells man, 101, his parents must confirm ID // The Guardian. URL: https://www.theguardian.com/uk-news/2020/feb/12/home-office-tells-man-101-his-parents-must-confirm-id

технологий вообще? Может ли человек вообще не использовать их и при этом получать все положенные ему услуги, пользоваться всеми своими правами и выполнять свои обязанности? Сейчас в этом вопросе тоже нет этического консенсуса.

2.2.2 ПРЕДВЗЯТОСТЬ АЛГОРИТМОВ И БЕЗУСЛОВНОЕ ДОВЕРИЕ МАШИНЕ

Интеллектуальные системы, лежащие в основе онлайн-сервисов, цифровых услуг и продуктов, работают с огромным количеством данных и чаще всего непрозрачны даже для специалистов. Системы ИИ учатся получать информацию из таких наборов данных, которые раньше не воспринимались как источники информации или вовсе не существовали (например, социальных сетей). Системы на основе нейросетей в принципе не имеют заранее введенного алгоритма с предсказуемыми результатами работы. Это создает принципиально высокую сложность объяснения решений, которые принимает ИИ-система. Человек при желании может изучить работу машины и починить ее, но не может сам проанализировать действия интеллектуальной системы даже на уровне приложения в смартфоне: это технически невозможно для человеческого мозга (см. также раздел 5).

Тем временем распространенная и ранее презумпция безошибочности компьютера стремительно подменяет собой презумпцию невиновности человека. При этом государственные органы и службы иногда склонны доверять компьютеру, интеллектуальной системе, системе принятия решений в сложных ситуациях, будто бы она, в отличие от человека, непременно объективна и не может ошибаться. Системы обучаются на исторических данных (не свободных от предубеждений, искажений, неполноты и других недостатков), а алгоритмы создаются человеком, поэтому могут содержать различные ошибки.

В Великобритании недавно завершился один из крупнейших юридических скандалов, связанный с работой алгоритмов[71]. В 2000–2014 годах более 700 сотрудников почтовой службы получили наказания, включая тюремное заключение, за нарушения, которые они не совершали. Как доказали юристы, проблема была в ошибках компьютерной системы. Из-за этих ошибок возникали недостачи, порой размером в несколько тысяч фунтов. Несколько сотрудников даже закладывали свои дома, чтобы погасить недостачу из собственных средств. С тех пор некоторые из несправедливо обвиненных сотрудников уже умерли, другие разорились или получили ущерб для здоровья, семейных отношений, финансового состояния.

Бремя доказывания ошибок незаметно переложили на самих граждан. Поспешные решения и действия хоть и остаются формально в рамках

[71] Peachey K. Post Office scandal: What the Horizon saga is all about // BBC News. URL: https://www.bbc.com/news/business-56718036; Siddique H., Quinn B. Court clears 39 post office operators convicted due to 'corrupt data' // The Guardian. URL: https://www.theguardian.com/uk-news/2021/apr/23/court-clears-39-post-office-staff-convicted-due-to-corrupt-data

закона, зачастую неэтичны по смыслу, а человек оказывается самой незащищенной стороной в многостороннем взаимодействии госорганов, коммерческих организаций и граждан.

2.2.3 УХУДШЕНИЕ УСЛОВИЙ ТРУДА ИЗ-ЗА АЛГОРИТМОВ

Алгоритмы все активнее используются для контроля и оценки работников, причем не только удаленных. Проблема заключается в том, что алгоритмы могут приводить к **дискриминации и ухудшению условий труда**, косвенно причинять ущерб здоровью сотрудников — все дело в принципах, на основе которых сформирован алгоритм. Самое неприят-ное начинается, когда данные систем контроля становятся основой для управленческих решений: не люди, а алгоритмы подгоняют сотрудников и снижают заработную плату, если те работают слишком медленно, или, например, прослушивают работников кол-центра, добиваясь максимальной загрузки. Алгоритмы, управляющие людьми, усиливают напряжение, делают работу более изнурительной и опасной[72], приводят к выгоранию и увольнению сотрудников.

Журналистское расследование[73] современной практики расчета смен и контроля качества работы показывает, что работники супермаркетов в США из-за алгоритмов буквально превращаются в полуроботов. Становится очевидно, что работу потеряют не сотрудники касс и залов, а их начальство: управлять массовыми работниками сферы ритейла будут алгоритмы. Алгоритм рассчитывает сложные и непредсказуемые смены работы, из-за чего сотрудники не могут совмещать эту работу с работой в другом месте, родители малолетних детей не могут заранее пригласить няню на время работы, становится невозможно планировать свой досуг, из-за постоянной непредсказуемости повышается уровень стресса и т. п.

ПО для отслеживания активности пользователя в соцсетях, программах и приложениях применяется давно. В последние годы для контроля эффективности сотрудников[74] руководители все чаще используют средства удаленного мониторинга, которые анализируют содержание коммуникаций, файлов и действий сотрудника, движения его глаз, давление тела на сиденье кресла (как доказательство нахождения на рабочем месте). Тотальный мониторинг трафика устройств, на которых работает сотрудник, включая переписку, сложно назвать обоснованным и допустимым. Такие программы контроля при удаленной работе потенциально нарушают право на частную жизнь, поскольку сложно или невозможно разграничить личное, домашнее и рабочее пространство. Часто эти программы необходимо устанавливать на личный или даже семейный компьютер. Это влечет за собой многочисленные этические риски, от уязвимости ПДн

[72] Dzieza J. How hard will the robots make us work? // The Verge. URL: https://www.theverge.com/2020/2/27/21155254/automation-robots-unemployment-jobs-vs-human-google-amazon

[73] Schulte B. Why Today's Shopping Sucks // The Washington Post. URL: https://washingtonmonthly.com/magazine/january-february-march-2020/why-todays-shopping-sucks/

[74] Friedman Z. How COVID-19 Will Change The Future Of Work // The Forbes. URL: https://www.forbes.com/sites/zackfriedman/2020/05/06/covid-19-future-of-work-coronavirus/#1d0f03ea73b2

сотрудников до массового скоринга. Дата-сеты, собранные компаниями в период пандемии, могут быть в дальнейшем применены для других целей, например для определения производительности каждого специалиста и замены его автоматизированной системой.

2.2.4 ЗАВИСИМОСТЬ ОТ ПЛАТФОРМ И ВЛАСТЬ ИТ-ГИГАНТОВ

Предвзятыми могут быть не только алгоритмы, но и люди, принимающие решения о доступе к конкретным цифровым возможностям. С ростом влияния ИТ-гигантов и в результате монополизации рынка увеличивается риск деплатформинга — отказа в предоставлении услуг на платформе фактически в нарушение существующих правил использования сервиса. Главная опасность деплатформинга — лишение доступа к сервисам и ключевым компонентам ИТ-архитектуры не отдельных людей, а целых групп, сообществ, объединенных по признаку политических взглядов, ценностей, национальности, отношения к определенным событиям и т. п.

Пожалуй, самый громкий случай деплатформинга — это блокировка аккаунта бывшего президента США Дональда Трампа в Twitter. Аналогичным образом сервис Spotify в 2021 году заблокировал ряд старых эпизодов подкаста известного ведущего Джо Рогана без объяснения причин, но, скорее всего, из-за несовпадения взглядов основателей платформы и гостей заблокированных эпизодов[75].

2.3 ЭТИЧЕСКИЕ РИСКИ «ЦИФРЫ» ДЛЯ ГОСУДАРСТВА

Авторы раздела:

С. В. Коршунова

Е. Г. Потапова

О. С. Шепелева

Время чтения — 11 минут

Использование цифровых технологий создает риски для национальной безопасности и цифрового суверенитета, в частности риск зависимости от иностранных технологий и оборудования. Самым серьезным риском для государства авторы доклада считают потерю доверия граждан и как следствие — дискредитацию будущих усилий и достижений государства в сфере цифровых технологий.

2.3.1 РЕПУТАЦИОННЫЕ РИСКИ

В идеальной картине мира государство — представитель граждан, который защищает их интересы, права и свободы, обеспечивает

[75] Resnikoff P. Spotify Has Removed 40 Joe Rogan Episodes To Date — Here's the Full List // Digital Music News. URL: https://www.digitalmusicnews.com/2021/03/30/spotify-joe-rogan-episodes-removed/

охрану жизни и здоровья, поддержку слабых, руководствуется ценностями и т. п. Как уже было сказано в разделе 1, доверие собственных граждан — залог успешного существования такого государства. Использование цифровых технологий для ограничений и слежки, внедрение цифровых решений «на всякий случай» наносит вред, влечет финансовые потери, порождает страхи. Рост недоверия к государству может означать в будущем усиление сопротивления цифровым решениям (подробнее о доверии см. раздел 3). К потере доверия приводит ряд причин, в том числе:

- утечки данных граждан из ГИС;
- невозможность гарантировать защиту данных граждан в ИС из-за недостаточного уровня ИБ;
- необоснованное длительное хранение данных после достижения цели их сбора;
- применение технологий для несправедливых, с точки зрения граждан, действий (например, автоматическое выписывание штрафов);
- внедрение цифровых услуг, при оказании которых возможны ошибки и сбои, с одновременным удалением аналоговых вариантов.

2 июля 2020 года в официальном аккаунте ситуационно-кризисного центра МИД РФ 13 часов висело мошенническое сообщение о продаже базы данных российских граждан, которые находятся за пределами страны и получают выплаты от России[76].

С 2021 года в России трудовую книжку оформляют в электронном виде; те, у кого она уже есть, могут выбирать, вести ее далее в электронном формате или в бумажном. Информационная кампания в поддержку инициативы началась в 2019 году. В начале 2021 года компания HeadHunter выяснила[77], что четверти из опрошенных даже не предлагали переход на электронные трудовые книжки. 54% тех, кому предложили, отказались. Основная причина отказа (55%) — непонимание, как будет работать электронная трудовая книжка.

Московская система «Безопасный город» — одна из крупнейших в мире, в ней около 200 тыс. видеокамер[78]. В начале 2020 года в Москве запустили онлайн-систему распознавания лиц на основе данных с этих видеокамер. Во время пандемии технологии распознавания лиц стали использовать не только для поимки преступников и поиска потерявшихся людей, но и для отслеживания нарушителей карантина. Российский КоАП допускает автоматическую фиксацию правонарушений, однако до сих пор это были в основном нарушения правил дорожного движения и парковки.

[76] В официальном твиттер-аккаунте МИД предложили купить базу данных российских туристов // Медиазона. URL: https://zona.media/news/2020/07/02/mid

[77] Полный провал. Россияне отказались переходить на электронные трудовые книжки // Hi-Tech Mail.ru. URL: https://hi-tech.mail.ru/news/52747-polnyy-proval-rossiyane-otkazalis-perehodit-na-elektronnye-trudovye-knizhki/; Электронные трудовые книжки: результаты опроса соискателей // Служба исследований HH.ru. URL: https://hhcdn.ru/file/17003416.pdf

[78] Bischoff P. Surveillance camera statistics: which cities have the most CCTV cameras? // Comparitech. URL: https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/

Удаление данных, которые больше не нужны, — пример этичного обращения с данными. Отношение государства и бизнеса к удалению данных в период пандемии вообще очень показательно.

В 2020 году департамент здравоохранения Австралии выпустил акт о биобезопасности[79], защищающий права граждан на приватность в период пандемии и после нее, началась работа над законом о защите ПДн[80], собранных через мобильные приложения. Были приняты нормативные документы[81] об удалении всех данных по окончании пандемии.

Правительство Израиля разрешило спецслужбам использовать данные сотовых операторов для отслеживания контактов заболевших COVID-19, но на определенное время. Впоследствии надзорная группа в Кнессете заблокировала[82] инициативу правительства об использовании этих данных в дальнейшем, поскольку риски перевешивают возможные выгоды.

В апреле 2020 года жители Московской области столкнулись с рядом проблем: было сложно оформить пропуск по единому номеру 0250, отмечалась нестабильная работа приложения «Госуслуги СТОП Коронавирус», не приходили QR-коды. Минкомсвязи РФ совместно с руководством Московской области устранило проблемы, выявленные пользователями, а конце июня 2020 года глава Минцифры РФ сообщил[83], что все ПДн пользователей сервиса удалены.

В апреле 2020 года в Татарстане ввели цифровые пропуска, тогда же власти пообещали удалить все данные по окончании ограничительных мер. 12 мая 2020 года пропуска были отменены, созданный для их выдачи сайт закрыли[84], а 15 мая в присутствии специальной комиссии были удалены ПДн, собранные для выдачи цифровых пропусков[85].

В целом законодательные органы власти и нормативно-правовое регулирование цифровой экономики не успевают за развитием рынка. В неконтролируемой «серой» зоне создаются благоприятные условия для неэтичных, но формально законных (не запрещенных законом) действий, которые впоследствии могут иметь серьезные последствия для граждан и вызывают у них недовольство. Отсутствие системной работы с этическими рисками приводит к недостаточно продуманным цифровым

[79] Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements — Public Health Contact Information) Determination 2020 // Federal register legislation. URL: https://www.legislation.gov.au/Details/F2020L00480

[80] COVIDSafe legislation // Australian Government. URL: https://www.ag.gov.au/RightsAndProtections/Privacy/Pages/COVIDSafelegislation.aspx

[81] COVIDSafe app // Australian Government. URL: https://www.health.gov.au/resources/apps-and-tools/covidsafe-app#after-the-pandemic

[82] Coronavirus: Israel halts police phone tracking over privacy concerns // BBC News. URL: https://www.bbc.com/news/technology-52395886

[83] Полякова В., Скобелев В. Минкомсвязь сообщила об удалении личных данных для цифровых пропусков // РБК. URL: https://www.rbc.ru/society/30/06/2020/5efb38b89a794729e9c58169

[84] Цифровые пропуска: итоговые цифры // Министерство цифрового развития государственного управления, информационных технологий и связи Республики Татарстан. URL: https://digital.tatarstan.ru/rus/index.htm/news/1745760.htm

[85] В Татарстане уничтожили базу данных цифровых пропусков при участии спецкомиссии // Министерство цифрового развития государственного управления, информационных технологий и связи Республики Татарстан. URL: https://digital.tatarstan.ru/rus/index.htm/news/1749226.htm

решениям, в которых делается акцент на будущие положительные эффекты и недостаточно учитываются потенциальные негативные эффекты.

Приложение «Социальный мониторинг», разработанное ДИТ Москвы весной 2020 года для контроля передвижения москвичей с подтвержденным COVID-19, неоднократно называли инструментом создания «цифрового ГУЛАГа». Параллельно с «Социальным мониторингом» действовала система цифровых пропусков, которая работала с перебоями, временами была недоступна для оформления пропусков, в ней не были предусмотрены многие причины для получения пропуска.

Беспечная цифровизация, отсутствие системной работы по предупреждению этических проблем проявляются в противоречивых действиях разных госорганов, например при выборе места размещения ПДн. Госорганы активно используют мобильные приложения (не только для слежки), в результате чего растет влиятельность владельцев экосистем мобильных приложений: Google, Apple, Facebook, Huawei и др.

При изучении[86] 44 российских мобильных приложений, разработанных госорганами для оказания госуслуг, выяснилось, что большинство приложений содержит трекеры компаний Facebook и Google, 88% содержат хотя бы один трекер, который собирает данные и осуществляет их трансграничную передачу третьим лицам. При этом отсутствуют рекомендации и требования к передаче данных приложениями, разработанными за счет бюджетных средств[87].

2.3.2 УГРОЗЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Ярким примером того, как данные, этика и безопасность переплетаются в сложный клубок рисков для личности и для государства, служат утечки данных, собираемых через инфраструктуру «умного» города. Даже отдельные «умные» носимые устройства могут навредить своим владельцам и целым странам из-за непредумышленного раскрытия информации. Но основное звено потерь — люди. Они подписывают бумажные документы и общаются в мессенджерах, работают в засекреченном здании и используют режим геолокации на смартфоне. Технологии социального инжиниринга и обогащения данных позволяют получить много информации и без доступа к сейфу с документами. Недоразумения или беспечность сотрудников приводят к тому, что публичными становятся значимые данные, включая те, которые могут представлять государственную тайну[88].

[86] Бегтин И., Буров В., Орлова К. Приватность государственных мобильных приложений в России // АНО «Информационная культура», 2021. URL: https://privacygosmobapps.infoculture.ru/

[87] Там же.

[88] Риски оборота данных в России // Этика и «цифра»: этические проблемы цифровых технологий. В 2 т. М.: РАНХиГС, 2020. URL: http://ethics.cdto.center/2_1/#2.1.3

Центр спецназначения по обеспечению безопасности движения МВД России минимум три года собирал секретные данные о передвижении президента, премьера, руководства Совбеза, ФСБ и других высокопоставленных лиц в чатах WhatsApp[89] (принадлежит Facebook). По информации ряда источников вся связь с водителями Управления делами президента РФ осуществлялась через WhatsApp, зачастую со служебных и личных компьютеров. Технически не только компания — владелец мессенджера, но и другие посторонние лица могли в онлайн-режиме отслеживать передвижения первых лиц России: для этого достаточно было получить несанкционированный доступ хотя бы к одному из компьютеров, где был бы открыт такой чат. Были скомпрометированы не только маршруты передвижения, но и позывные объектов госохраны, номера их машин, фамилии сопровождающих.

В целом аналоговые технологии (бумажный документооборот) устойчивее к утечкам информации, чем электронные: проще обеспечить физический контроль и обнаружить нарушение мер ИБ, компрометацию документов, информации и т. д. Гораздо проще скопировать 1 Тб цифровых данных на флеш-карту, чем незаметно украсть 100 кг секретных документов.

Интегральный подход к обеспечению безопасности предполагает полный отказ от использования цифровых сервисов: только кнопочные телефоны, для коммуникаций с коллегами — защищенные линии видеоконференц-связи (ВКС) и радиостанции. Однако невозможно представить себе работу современного госоргана в условиях таких ограничений. В современном цифровом мире цифровой и аналоговый подходы неизбежно совмещаются.

В начале 2020 года российский «белый хакер» рассказал, как он нашел доступ к тысячам камерам наружного наблюдения РЖД, а затем помог компании закрыть уязвимость[90].

Хакерская атака на американскую компанию Colonial Pipeline привела к перебоям в поставке нефтепродуктов на восточном побережье США, вызвала рост цен на бензин, в связи с чем в 19 штатах было объявлен режим ЧС. Хакеры заявили, что не имеют политических требований, а только хотят заработать. Это крупнейшая в истории кибератака на энергетическую инфраструктуру[91].

В мае 2020 года хакерская атака на ИТ-системы нарушила работу службы здравоохранения и соцзащиты Ирландии: пришлось отменить или перенести записи на прием (кроме неотложных случаев), начались перебои в работе клиник, некоторые процедуры проводились без привычной помощи компьютеров. Как только Национальный центр кибербезопасности

[89] Дергачев В., Горяшко С., Зотова Н. В спецбатальоне МВД пожаловались на сбор данных о кортежах Путина через WhatsApp // BBC News. Русская служба. URL: https://www.bbc.com/russian/news-55496368

[90] Самый беззащитный — уже не Сапсан. Все оказалось куда хуже... // Хабр. URL: https://habr.com/ru/post/536750/; РЖД прокомментировала ситуацию с проникновением во внутреннюю сеть компании после публикации статьи на Хабре // Хабр. URL: https://habr.com/ru/news/t/537172/

[91] Наумов А., Черненко Е., Мордюшенко О. Бесполезные ископаемые // Коммерсантъ. URL: https://www.kommersant.ru/doc/4802807; Drivers start scrambling for gas as pipeline shutdown continues // CBS News. URL: https://www.cbsnews.com/amp/news/gas-prices-colonial-pipeline-ransomware-attack

(National Cyber Security Centre) обнаружил атаку, был приведен в действие план антикризисных мер. В частности, многие компьютеры и системы были просто выключены. Госорган отказался платить выкуп[92].

Помимо утечки данных и хакерских атак, опасность для государства представляет отсутствие цифрового суверенитета. Растущая зависимость от импорта электроники не позволит ни одной стране мира в ближайшем будущем иметь цифровой суверенитет. К примеру, российские компании могут создать алгоритмы, но техника, на которой они используются, будет произведена в Китае или США.

«Россия должна не просто наращивать технологическую, интеллектуальную мощь, но и стремиться к цифровому суверенитету, чтобы сохранять право на свое мнение по многим вопросам и возможность вести конструктивный диалог. Многие страны сегодня находятся в худшем положении не только по сравнению с Китаем и США, но и по сравнению с Россией. Экспорт цифрового суверенитета в технологически менее развитые страны — одна из возможных точек роста для России».

Илия Димитров, омбудсмен
по вопросам развития цифровой экономики

Другая опасность — копирование передового опыта других стран без учета локальных особенностей или вместо создания собственных уникальных продуктов. Само по себе использование чужого опыта целесообразно, но, чтобы быть лидером рынка, необходимо задавать тренды, а не только следовать им. При этом быть лидерами очень затратно: эксперты отмечают[93], что например российский аналог YouTube должен иметь мощнейшую инфраструктуру, для него придется построить серверные фермы стоимостью в несколько миллиардов долларов.

Национальная служба здравоохранения Великобритании (NHS) в апреле 2021 года попыталась обновить приложение-трекер заболевших COVID-19, включив в него возможность отслеживания местоположения пользователей. Изначально это приложение совместно разработали Google и Apple, и оно принципиально не собирало данные о геолокации пользователей. Обновление фактически нарушало условия использования приложения и было заблокировано на обеих площадках. Тем самым крупнейшие ИТ-экосистемы показали, что могут устанавливать свои правила игры и принуждать к их соблюдению даже таких пользователей, как госорганы европейских стран[94].

---

[92] Cyber attack 'most significant on Irish state' // BBC News. URL: https://www.bbc.com/news/world-europe-57111615

[93] «Теперь мы голые и беззащитные»: краткая история цифровой колонизации. Игорь Ашманов // ДеньТВ. URL: https://www.youtube.com/watch?v=4kEhtfFzKto

[94] Kelion L. NHS Covid-19 app update blocked for breaking Apple and Google's rules // BBC News. URL: https://www.bbc.com/news/technology-56713017

ВЫВОДЫ. КАК СНИЗИТЬ РИСКИ

В 2020–2021 годах в мире на первый план вышли проблемы техноэтики, связанные с использованием ПДн, слежкой, кибермошенничеством и неравным доступом к технологиям. Принципиально новых этических проблем не возникло, но обострились существовавшие ранее[95]. По-видимому, они и будут самыми актуальными в ближайшие несколько лет.

В то время как данных, используемых для контроля, собирается очень много, у государственных органов все еще недостаточно данных о гражданах и инфраструктуре, которые необходимы для оказания помощи. Они пригодились бы для стабильного обеспечения высокого уровня медицинской помощи там, где она более всего необходима, равного доступа к образовательным услугам онлайн, социальной поддержки малообеспеченных и безработных граждан и т. п.

Опыт внедрения цифровых продуктов и услуг показывает, что продуманные этичные решения сводят риски к минимуму, а непроработанные и поспешные могут быть опасны. Цифровизация разного рода сервисов может приводить к дискриминации отдельных уязвимых групп, если не предпринимаются специальные меры для снижения этого риска. Некорректная работа госорганов с цифровыми технологиями (прежде всего обработка данных граждан) может создать проблемы на стыке этики и самых широких вопросов безопасности: государства, граждан, общества в целом.

Описанные в этом разделе проблемы требуют своевременного решения на всех уровнях — регулирования, правоприменения, создания инфраструктуры, внедрения культуры работы с данными и т. д.[96] В первую очередь следует обращать внимание на следующие факторы.

- Объем собираемых данных. Известны ли заранее цели сбора данных? Можно ли собирать меньше?
- Возможные негативные последствия. У кого не будет доступа к сервису или продукту? Какие утечки данных возможны? Как злоумышленники могут использовать цифровой продукт или сервис?
- Сохранение аналоговых вариантов. Какие варианты предусмотрены для пользователей без доступа к интернету или не имеющих цифровых устройств? Предусмотрен ли вариант действий на случай непредвиденной ситуации или ошибки системы?
- Коммуникация с пользователями. Чем могут быть недовольны пользователи? Кто отвечает за коммуникацию с пользователями?

Подробнее алгоритм оценки этичности цифровых решений описан в разделе 6.2.

[95] Подробнее об этих рисках см.: Этика и «цифра»: Этические проблемы цифровых технологий. В 2 т. М.: РАНХиГС, 2020. URL: http://ethics.cdto.center/

[96] Государство и граждане // Этика и «цифра»: этические проблемы цифровых технологий. В 2 т. М.: РАНХиГС, 2020. URL: http://ethics.cdto.center/2_2/#2.2.2

3. СОЦИАЛЬНЫЕ АСПЕКТЫ ЦИФРОВЫХ РЕШЕНИЙ

— Корабли не в счет, — резко заявил Харлан, — нас с вами должны интересовать вот эти штучки.

А «штучками» были люди. Рядом с громадами кораблей они действительно казались карликами, точно так же, как сама Земля и все людские дела кажутся ничтожными из космической дали.

А. Азимов. Конец Вечности

3.1 ПРИЧИНЫ НЕДОВЕРИЯ К ЦИФРОВЫМ ТЕХНОЛОГИЯМ

Время чтения — 13 минут

Сейчас уровень политического доверия невысок во всем мире. В России недоверие к государству имеет давние исторические корни. Доверие — комплексный принцип: если цифровой сервис неудобен для граждан, они распространят свое недовольство на государственные цифровые инициативы в целом. Пандемия COVID-19 обострила ситуацию: сейчас все более реальным становится риск обвала доверия к цифровым решениям государства.

3.1.1 ГРАЖДАНЕ НЕ ДОВЕРЯЮТ ГОСУДАРСТВАМ

Доверие — один из ключевых этических принципов, важный критерий общественного благополучия. Говоря об уровне доверия в стране, обычно имеют в виду доверие не только межличностное, но и институциональное

(к организациям), международное (к другим странам) и политическое (населения к государству).

Доверие оказывает серьезное влияние на экономику[97], оно необходимо для совершения любой коммерческой сделки и экономического обмена в целом, многие исследования свидетельствуют о связи уровня доверия с уровнем доходов населения. Расчеты с использованием данных Всемирного исследования ценностей населения (World Values Survey, WVS) и Всемирного банка за 1998–2017 годы показали: рост уровня доверия на 10 пунктов коррелирует с увеличением среднедушевого ВВП на 21%[98]. Чем выше уровень доверия, тем больше инвестируют в экономику страны, а экономический рост, в свою очередь, способствует росту доверия.

«Развитие цифровых технологий требует укрепления доверительных отношений с гражданами и бизнесом. Над развитием таких отношений государству предстоит еще долго работать, поскольку в нашей стране преобладает скептическое восприятие цифровой трансформации, в особенности в сфере образования и здравоохранения. От нашей клиентоориентированности напрямую зависит успех цифровизации и экономики в целом».

Владислав Федулов, заместитель министра экономического развития РФ

Доверие — «критический фактор достижения стратегических целей социально-экономического и политического развития государства»[99], при этом доверие и готовность добровольно сотрудничать с государством не могут возникнуть фрагментарно («одному ведомству доверяю, другому — нет»). Чаще всего доверие теряется целиком. В этом смысле каждый госслужащий отвечает за всех остальных. Если какая-то организация скомпрометировала себя во взаимодействии с гражданами, то эффект негативного восприятия или недоверия коснется как минимум всех связанных с этой организацией госслужащих, а то и государства в целом. Если ИС или сервис, который проектируется госорганами, не принимает в расчет удобство граждан, то у граждан возникает недоверие к государству и системе.

Авторы раздела:


Ю. Б. Грязнова


Д. В. Комендантов


М. В. Крель


О. В. Полетаев


Е. С. Трубинова


А. В. Фирсов

[97] Бахтигараева А. И., Ставинская А. А. Сможет ли доверие стать фактором роста экономики? Динамика уровня доверия у российской молодежи // Вопросы экономики. 2020. № 7. С. 92–107. URL: https://doi.org/10.32609/0042-8736-2020-7-92-107

[98] Авдеева Д. Доверие и недоверие в России // Финам. URL: https://www.finam.ru/analysis/forecasts/doverie-i-nedoverie-v-rossii-20181015-111223/

[99] Доверие как критический фактор достижения стратегических целей социально-экономического и политического развития государства: материалы научно-методического семинара Аналитического управления в рамках подготовки заседания Научно-экспертного совета при Председателе Совета Федерации / Совет Федерации Федерального Собрания Российской Федерации. М., 2020. URL: council.gov.ru/media/files/ZuyffAndc55HCTkMIVsA5A1r22tq2ZQx.pdf

«В Конституции РФ Президент определен как гарант прав и свобод гражданина. Госслужащие обязаны ему помогать и выполнять свои функции по защите этих прав. Если каждый на своем месте будет честно исполнять свои обязанности, соблюдая этические нормы, тогда и доверие к государству будет высоким. Государство, во-первых, является обладателем самого большого количества сведений о гражданах, объектах и т. д., а во-вторых, предоставляет разного рода выгоды гражданам, причем не только в денежном эквиваленте. Поэтому если госслужащим нет доверия, то о каком социально-экономическом развитии можно говорить? Государственное развитие, социальное развитие без доверия к государству практически невозможно».

Радик Гисмятов, заместитель РЦТ Республики Татарстан

Кроме того, как отмечает экономист, декан экономического факультета МГУ Александр Аузан, «в соответствии с данными международных сопоставлений доверие граждан к властям в значительной степени зависит не от качества госуслуг, а от доверия к полиции, а оно у нас низкое»[100].

Сейчас уровень доверия граждан к органам власти невысок во всем мире. Аналитики Edelman Trust Barometer (см. рисунки[101] 2 и 3) считают,

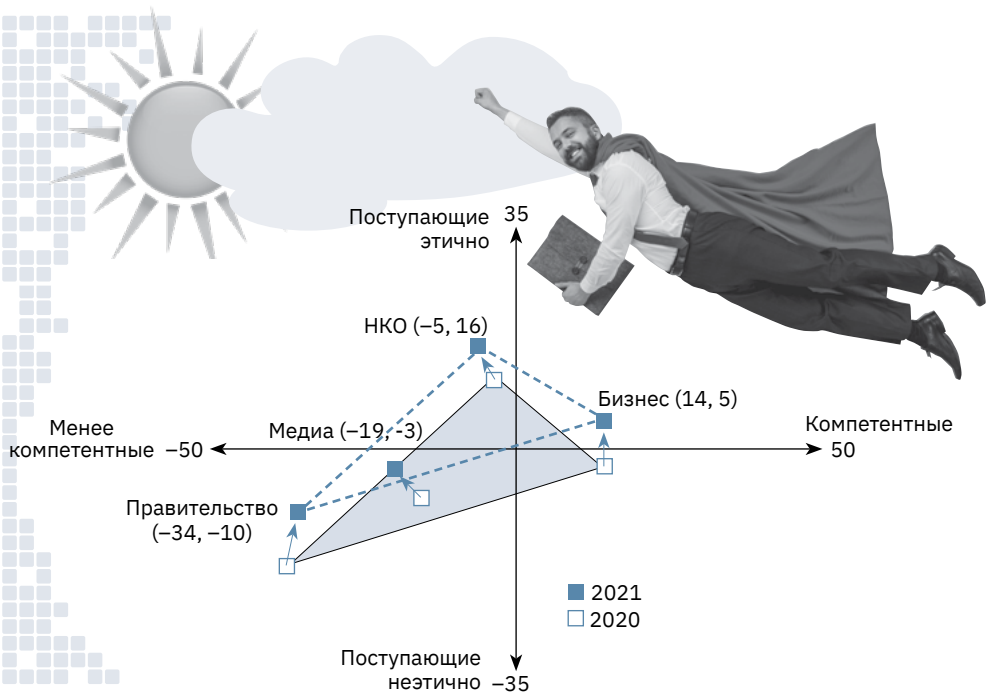


Рисунок 2. Сравнительный уровень доверия в мире к правительствам, медиа, НКО, бизнесу (данные из России и Китая не учитывались)

[100] Хейфец В. Александр Аузан: «Недоверие — такая же опасная ловушка, как коррупция» // Плюс Один. URL: https://plus-one.ru/society/aleksandr-auzan-nedoverie-takaya-zhe-opasnaya-lovushka-kak-korrupciya-

[101] Рисунки выполнены на основе данных отчета Edelman Trust Barometer 2021. URL: https://www.edelman.com/sites/g/files/aatuss191/files/2021-03/2021%20Edelman%20Trust%20Barometer.pdf

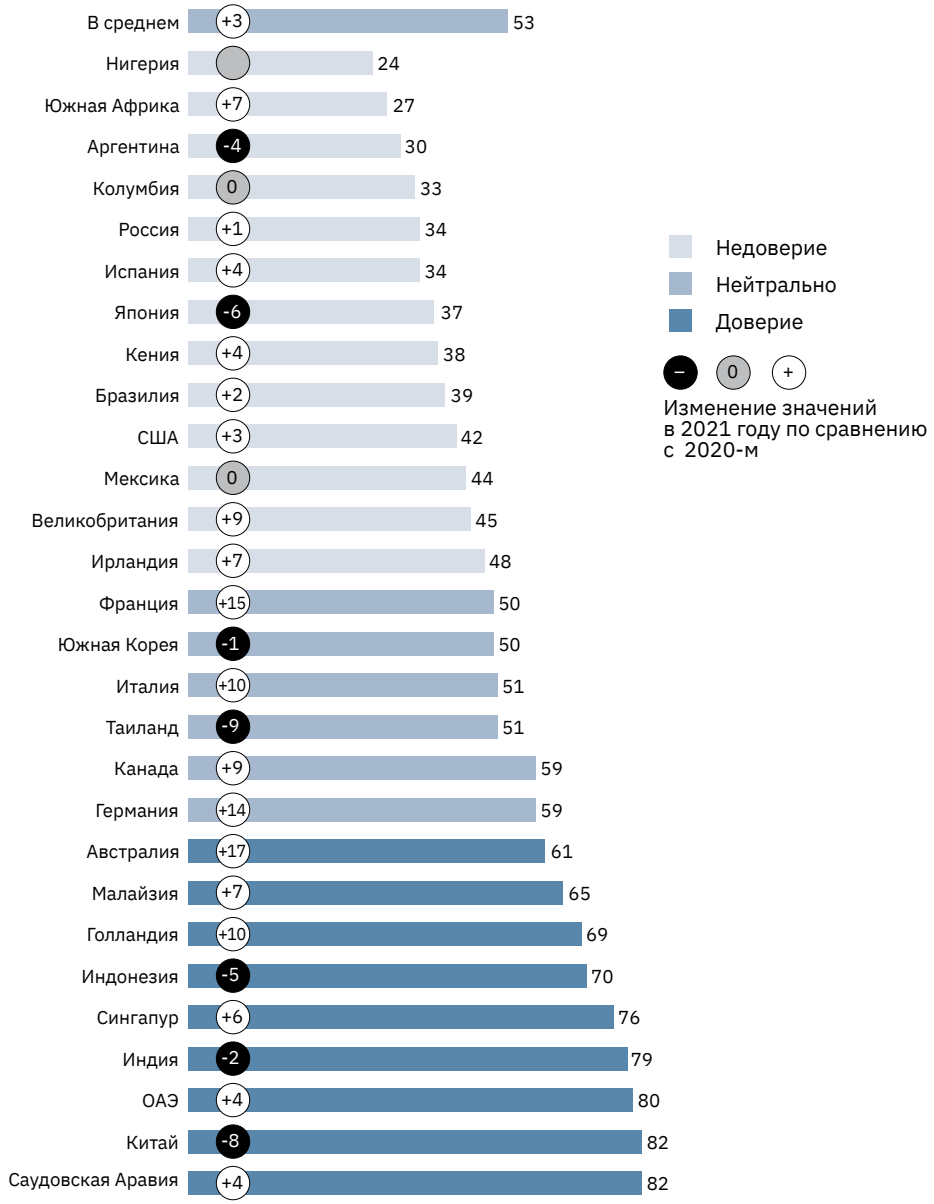


Рисунок 3. Уровень доверия к правительству в странах мира. Россия входит в пятерку стран с самым низким уровнем политического доверия

что пандемия, экономический кризис и политическая нестабильность привели к всплеску дезинформации и повсеместному снижению доверия к социальным институтам и политическим лидерам. Правительства сейчас воспринимаются в мире как институт, чаще всего поступающий неэтично и некомпетентно, в отличие от бизнеса. Впрочем, в мае 2020 года наблюдался резкий рост доверия к государству: общество полагалось на

него в борьбе с пандемией и восстановлении экономического равновесия. Однако государство не выдержало экзамен, и «пузырь доверия» лопнул[102].

В России недоверие к государству имеет ряд исторических причин, среди которых:

- отсутствие культуры доверия в целом — и межличностного, и институционального[103];
- страх оказаться жертвой произвола властей[104];
- непрозрачность государственных расходов, несформированность традиции отчитываться перед обществом.

Пандемия обострила проблему доверия общества к государственным инициативам, которые нередко реализовывались без учета воли граждан. «Причинами снижения доверия к СМИ и властям стали противоречивость официальной информации и рассогласованность действий чиновников, подозрения в сокрытии информации, дефицит проявления эмпатии и двусторонних коммуникаций, чувство несправедливости и разочарование, вызванное нарушенными обещаниями», — считают исследователи[105]; доверие к государственным институтам и вера в помощь государства снизились у 61% россиян.

Неприятие, в частности, вызвали московские решения: лишение пожилых граждан права на свободное перемещение (и блокировка проездных документов), требование к москвичам с подтвержденным COVID-19 устанавливать приложение для контроля передвижения. В целом по стране кризисным с точки зрения доверия граждан к государству стал переход на онлайн-обучение[106].

«Большинство родителей не просто драматично восприняли переход к дистанционному обучению во время карантина — они перенесли затем это отношение и на цифровизацию в целом. По данным наших опросов, 95% родителей не хотят даже частичного перехода на дистанционное образование. Влияние этого фактора мы будем ощущать еще долго».

Юлия Грязнова, руководитель дирекции стратегии, аналитики и исследований АНО «Национальные приоритеты»

[102] См.: Edelman Trust Barometer 2021. URL: https://www.edelman.com/trust/2021-trust-barometer

[103] В исследованиях Edelman Trust Barometer 2020 и 2021 года Россия занимала последнее место по общему уровню доверия (см.: 2020 Edelman Trust Barometer // Edelman. URL: https://www.edelman.com/trust/2020-trust-barometer) и находилась в конце рейтинга в большинстве разделов. А по данным опроса, проведенного Институтом социального анализа и прогнозирования РАНХиГС, почти 50% респондентов на вопрос, много ли есть людей, которым они доверяют, ответили, что их мало или нет совсем. См.: Кругом враги: почему россияне не верят даже родне // Газета.ру. URL: https://www.gazeta.ru/comments/2019/08/09_e_12568099.shtml

[104] Этот страх, вместе со страхом перед возможностью возврата массовых репрессий, входит в пятерку тревог, испытываемых абсолютным большинством россиян, согласно исследованию «Левада-Центра», проведенному в марте 2021 года. См.: Гудков Л. Характер и структура массовой тревожности в России // Левада-Центр («Левада-Центр» внесен в реестр НКО-иноагентов по решению Минюста РФ). URL: https://www.levada.ru/2021/04/21/harakter-i-struktura-massovoj-trevozhnosti-v-rossii/

[105] Макушева М. О., Нестик Т. А. Социально-психологические предпосылки и эффекты доверия социальным институтам в условиях пандемии // Мониторинг общественного мнения: экономические и социальные перемены. 2020. № 6. С. 427–447. URL: https://doi.org/10.14515/monitoring.2020.6.1770

[106] В новый учебный год — со старым форматом образования? // ВЦИОМ. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/v-novyj-uchebnyj-god-so-starym-formatom-obrazovaniya

3.1.2 ТЕХНООПТИМИЗМ В ТЕОРИИ, НО НЕ НА ПРАКТИКЕ

Почти половина опрошенных россиян относят себя к технооптимистам[107], и это самый высокий показатель в Европе. Они признают выгоды от цифровизации, такие как онлайн-госуслуги, быстрые соцвыплаты, дешевые такси и бесплатные приложения на смартфоне. По данным другого исследования, «85% взрослого населения (18–75 лет) доверяет цифровым сервисам государства, созданным на порталах госуслуг, МФЦ, ФНС России, ГИБДД»[108]. При этом доверие к частным цифровым сервисам выше, чем к правительству: 59% и 49% соответственно[109].

При том что в целом уровень одобрения цифровых технологий высок[110], опыт пандемии пошатнул доверие граждан к переводу социальной сферы в цифровую форму; они увидели риски в массированном сборе и не всегда правомерном использовании их ПДн. Кроме того, стало очевидно, что общество пока не овладело в достаточной степени новыми технологиями. Низкая цифровая грамотность мешает гражданам пользоваться преимуществами цифровизации: продвинутым уровнем цифровых компетенций обладает лишь около 27% россиян[111]. Хотя «Госуслуги» и Mos.ru популярны, большинство посетителей пользуются единичными услугами (оформить паспорт, проверить платежи ЖКХ). К цифровому паспорту и цифровым водительским правам граждане пока не готовы: электронный паспорт хотел бы оформить каждый пятый россиянин, среди молодежи — каждый третий; водительские права в электронном виде предпочла бы иметь лишь четверть россиян[112]. Не способствуют доверию постоянные утечки данных и возможность при желании свободно купить любые «слитые» базы данных (см. также об этом раздел 2).

«Недоверие граждан связано с отсутствием мощных систем защиты данных во многих организациях. Люди боятся взлома и поэтому не хотят заводить электронные трудовые книжки, водительские удостоверения, паспорта, не говоря уже о медицинских услугах, оказываемых с помощью искусственного интеллекта. Акцент в укреплении доверия граждан к цифровизации необходимо сделать на защите данных и на прозрачности. Мы стремимся к тому, чтобы гражданин был уверен: государство аккуратно обращается с переданными ему персональными данными».

Владислав Федулов, заместитель министра экономического развития РФ

[107] Исследование: Больше половины россиян с оптимизмом воспринимают роботизацию, искусственный интеллект и дронов-курьеров // РВК. URL: https://www.rvc.ru/press-service/news/company/149919/

[108] Исследование: порядка 85% взрослого населения доверяет цифровым госсервисам // ТАСС. URL: https://tass.ru/ekonomika/11121571

[109] Хейфец В. Александр Аузан: «Недоверие — такая же опасная ловушка, как коррупция» // Плюс Один. URL: https://plus-one.ru/society/aleksandr-auzan-nedoverie-takaya-zhe-opasnaya-lovushka-kak-korrupciya-

[110] Скрынникова А. Большинство россиян допустили сбор персональных данных для борьбы с COVID. Как изменилось их отношение к чипированию и дистанционному обучению из-за пандемии // РБК. URL: https://www.rbc.ru/technology_and_media/19/10/2020/5f89aa049a7947cb06832e79

[111] Вынужденная цифровизация: исследование цифровой грамотности россиян в 2021 году // Аналитический центр НАФИ. URL: https://nafi.ru/analytics/vynuzhdennaya-tsifrovizatsiya-issledovanie-tsifrovoy-gramotnosti-rossiyan-v-2021-godu/

[112] Электронный паспорт: за и против // ВЦИОМ. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/elektronnyj-pasport-za-i-protiv

Граждан беспокоит сохранность данных о кредитах, страховках, семейном положении, месте работы. Особенно остро стоит вопрос о медицинских данных. В ходе пандемии произошел откат и в отношении к телемедицинским сервисам (подробнее см. раздел 3.3). При росте количества пользователей телемедицины уровень скепсиса сохранился: к ней скептически относятся и те, кто уже попробовал эти сервисы[113].

«Многие, даже молодые и „продвинутые“, не пользуются банковскими онлайн-системами, опасаясь мошенничества[114]. Можно утешать себя графиками роста, на эту экспоненту и рассчитаны все прогнозы и планы наших госцифровизаторов. Но проблема доверия только увеличивается. В небольших банках нередки случаи взлома: у них нет таких денег, как у Сбербанка, чтобы сделать мощные системы, к тому же их нужно постоянно развивать, потому что и мошенники не дремлют. Без решения вопроса защиты данных доверие может рухнуть, что вызовет глобальный кризис».

Павел Готовцев, руководитель российской Рабочей группы IEEE по тематике «Этика и искусственный интеллект»

3.1.3 ОТСУТСТВИЕ ОБЩЕСТВЕННОЙ ДИСКУССИИ

Практика широкого обсуждения этических проблем, создаваемых технологиями, пока не распространена в России. Недостаточно сформирован язык и стиль таких коммуникаций; запрос на подобную дискуссию слабо выражен не только у госслужащих, но и в бизнес-сообществе, и у граждан. При принятии решений граждане так или иначе обращаются к своим ценностям — и в этой точке возникает напряжение. Цифровые продукты априори воспринимаются с подозрением; оно усиливается в среде, не предполагающей разъяснений прав и свобод человека. Коммуникация с гражданами в стремительно цифровизирующейся реальности не может ограничиваться декларациями («сдайте биометрию — получите цифровой паспорт»). Если представители власти не разъясняют, каким образом гражданам будут гарантированы права и свободы при появлении цифровых решений, отторжение будет усиливаться.

У государства есть разные каналы обратной связи: механизмы подачи жалоб, общественные советы, социологические опросы. Инцидент-менеджмент, к примеру, предполагает постоянный мониторинг конструктивной критики власти в соцсетях — им занимается система Центров управления регионами, созданная АНО «Диалог», а также развиваемая Минэкономразвития РФ система мониторинга качества госуслуг ИАС МКГУ «Ваш контроль». Проблема состоит в том, что **результаты этой обратной связи не всегда учитываются в полной мере**. Нужна воля руководителей или госслужащих, их желание

[113] Можно ли доверять телемедицине? Мнение россиян // Анкетолог. URL: https://iom.anketolog.ru/2020/05/27/telemedicina-2020. См. также опрос РВК 2019 года, в котором 40% респондентов признавались, что будут чувствовать себя спокойно при пользовании телемедицинскими услугами: Исследование: Больше половины россиян с оптимизмом воспринимают роботизацию, искусственный интеллект и дронов-курьеров // РВК. URL: https://www.rvc.ru/press-service/news/company/149919/

[114] Молодежь отказывается от смартфонов. Что происходит // Hi-tech. URL: https://hi-tech.mail.ru/news/54069-novaya-moda-pochemu-molodye-lyudi-vse-chasche-otkazyvayutsya-ot-smartfonov/

эффективно использовать эти инструменты. Другая проблема состоит в том, что сфера продуктивного взаимодействия государства с обществом в основном сводится к вопросам местного значения (дороги, поликлиники, ЖКХ), а дизайн решений более высокого уровня, например в масштабе министерства, отвечающего за развитие капитальной инфраструктуры, социальную политику, экологию, в эту сферу пока не входит.

ЦТ предполагает, что пользователи цифровых продуктов заинтересованы в изменениях и должны от них выиграть. Но в органах власти РФ всех уровней пока почти нет команд, которые отвечали бы за **клиентский сервис** и клиентский опыт[115], то есть за то, чтобы результат трансформации удовлетворил граждан. Один из положительных примеров — разработка суперсервисов (новой итерации цифровых услуг, предоставляемых государством проактивно). В ходе подготовки к запуску первого пакета суперсервисов Минцифры создала о них специальную страницу на сайте «Госуслуги», самом посещаемом государственном ресурсе страны со стомиллионной аудиторией, и предложила гражданам принять участие в обсуждении рабочих гипотез.

«Допустим, руководитель регионального департамента образования ставит задачу коллеге из департамента информационных технологий: „Мне нужна новая соцсеть, в которой мы зарегистрируем всех школьников, чтобы они там общались на темы учебы и здорового образа жизни“. И в ответ слышит: „Есть, к 1 сентября исполним“. И начинают исполнять. Где в схеме согласования итогового образа цифрового продукта представители бизнес-сообщества, которые, обладая экспертностью и готовыми цифровыми решениями, помогут государству избежать ненужных ошибок? Где учителя, родители, школьники, которым предстоит пользоваться новым сервисом? Когда решение появляется на свет, часто выясняется, что оно абсолютно „сырое“ и неудобное для пользователей, но они становятся заложниками обстоятельств. Еще одна сложность связана с доработкой не вполне удачных решений. Чтобы запустить цикл доработки, кому-то из госзаказчиков нужно взять на себя ответственность за неудачный запуск, что может вызвать нежелательное мнение об уровне компетентности лиц, утвердивших ТЗ и принявших по ним работы».

Олег Полетаев, директор по развитию цифрового бизнеса группы «Интерфакс»

В этой связи можно говорить о высоком потенциале государственно-частного партнерства в разработке цифровых решений для госуправления (см. также раздел 3.3.2), тем более в особо чувствительной социальной сфере, предполагающей консультации с бизнес-экспертами и диалог с будущими пользователями.

[115] Отчасти этот опыт изучается на площадках соцсетей, которые сегодня «для многих ведомств являются в большей степени не практикой вовлечения в обсуждение решений, а особым интерактивным способом взаимодействия, современным каналом осуществления маркетинговых коммуникаций и отработки „писем граждан“». См.: Открытость государства в России — 2020 / под ред. П. Демидова. URL: https://ach.gov.ru/upload/pdf/Otkrytost-2020.pdf

3.2 ОТНОШЕНИЕ К НОВЫМ ИТ-ТЕХНОЛОГИЯМ НА ПРИМЕРЕ ЗДРАВООХРАНЕНИЯ

Авторы раздела:

А. В. Архипов

А. В. Гусев

А. А. Орлова

Время чтения — 12 минут

Цифровые решения и ИИ в здравоохранении перестают быть вспомогательными ИТ-системами; с точки зрения безопасности и эффективности они все больше напоминают лекарства или медицинское оборудование. Но если фармацевтические корпорации проводят исследования и публикуют их результаты, их деятельность регулируется стандартами, а сами они находятся под жестким надзором, применительно к системам ИИ подобные практики только начинают складываться.

3.2.1 ПРОБЛЕМА ДОВЕРИЯ В МЕДИЦИНЕ

Медицина — яркий пример того, как доверие к технологиям влияет на сами технологии и, напротив, как использование технологий влияет на уровень доверия к отрасли в целом. Цифровые технологии становятся основным инструментом повышения эффективности практического здравоохранения: они позволяют сократить число врачебных ошибок и разгрузить врачей от рутинной обработки больших данных, а также создают возможности для масштабных исследований.

«Проблема доверия в медицине при использовании цифровых продуктов на базе искусственного интеллекта существует из-за того, что сложно учесть индивидуальные особенности каждого пациента. С помощью экспериментальных правовых режимов мы в том числе разрабатываем механизмы работы телемедицины, которые направлены на достижение самого высокого уровня точности анализа данных и результатов, которые выдает система».

Владислав Федулов, заместитель министра экономического развития РФ

Скорость развития в медицине таких технологий, как ИИ и прогнозная аналитика, напрямую зависит от доступности качественных больших данных, получение которых невозможно без доверия пациентов. При создании новых медицинских сервисов этические[116] вопросы требуют

[116] Под этикой в данном случае имеется в виду необходимость оценивать не только намерения и обязанности игроков, связанных с ИИ в системе здравоохранения (врачей, разработчиков, лиц, разрабатывающих политику), но и эффект, который их действия произведут на получателей услуг (конкретных людей, группы людей или целые поколения), на их ожидания, запросы, потребности и права. Morley J., Floridi L. NHS AI Lab: why we need to be ethically mindful about AI for healthcare // SSRN. 2019. URL: https://poseidon01.ssrn.com/delivery.php

детальной проработки. Если при создании сервиса «Электронная медкнижка», который позволяет выявлять (и не допускать к работе) людей, имеющих недостоверные или фальсифицированные данные о прохождении медосмотров, вмешательство в частную жизнь кажется обоснованным, то идея ведения единого реестра людей с психическими расстройствами, которая активно обсуждалась в России в 2016 году, не получила общественной поддержки[117].

Проблема доверия в медицине возникает и при использовании цифровых продуктов на базе ИИ, которые все сильнее влияют на постановку диагноза, принятие врачами решений и даже на выполнение лечебных манипуляций. Алгоритмы, которые используются для диагностики заболеваний, часто обучены на дата-сетах, где недостаточно представлены данные некоторых категорий пациентов.

Метаанализ 207 клинических исследований, которые проводились с 2001 по 2018 год, показал систематическую нехватку информации о кардиологических пациентах — женщинах и темнокожих пациентах. С жалобами на боль в груди обращается одинаковое количество мужчин и женщин, но мужчин направляют к кардиологу в 2–5 раз чаще[118].

Доказать, что медицинская технология достойна доверия, — задача ее разработчика[119]. Один из сильных аргументов — наличие государственного разрешения на использование технологии. Чтобы его получить, производитель цифровых продуктов должен создать у себя систему менеджмента качества, пройти сложные процедуры независимых технических и клинических испытаний, а затем и экспертизу.

В последние годы в России стал активно обсуждаться[120] ряд этических проблем, связанных с цифровым здравоохранением, особенно в том, что касается использования систем на основе ИИ[121] (см. таблицу 1). В частности, введены критерии отнесения программного обеспечения к программным медицинским изделиям (ПМИ). В соответствии с методическими рекомендациями Международного форума регуляторов медицинских изделий (International Medical Device Regulators Forum, IMDRF)[122] определены классы потенциального риска применения ПМИ, в том числе созданных с использованием ИИ.

[117] Никитина О. Перепись отклонения // Коммерсантъ. URL: https://www.kommersant.ru/doc/3163442

[118] Tat E., Bhatt D., Rabbat M. Addressing bias: artificial intelligence in cardiovascular medicine // The Lancet. URL: https://www.thelancet.com/journals/landig/article/PIIS2589-7500(20)30249-1/fulltext

[119] Показателен проведенный в конце 2019 года опрос об отношении пациентов к цифровизации здравоохранения: 75% опрошенных вообще никогда не пользовались телемедицинскими сервисами (хотя опрашивали именно хронических больных, для которых такие сервисы чрезвычайно важны). См.: Результаты опроса пациентов об их отношении к цифровизации здравоохранения // EverCare. URL: https://evercare.ru/news/rezultaty-oprosa-pacientov-ob-ikh-otnoshenii-k-cifrovizacii-zdravookhraneniya

[120] Белоусов Д., Хохлов А. Этические аспекты применения программного обеспечения с технологией искусственного интеллекта // Качественная клиническая практика. 2021. № 1. С. 70–84.

[121] См.: ИИ и машинное обучение в медицине. Ч. 3. Проблемы использования «умных» технологий в медицине // Хабр. URL: https://habr.com/ru/company/cloud4y/blog/507800/

[122] IMDRF documents // IMDRF. URL: http://www.imdrf.org/documents/documents.asp

Таблица 1. Технические и этические проблемы использования систем ИИ в медицине

Тип проблемы	Суть проблемы	Описание
Техническая	Недостаточная точность распознавания, ошибки	Системы ИИ самообучаются на основе предоставленных наборов данных и в отличие от алгоритмов, программируемых человеком, не могут гарантировать неизменную точность результатов анализа. У системы ИИ всегда есть некая вероятность вывода правильного ответа. Чем сложнее задача, тем меньше вероятность. Обеспечение высокой точности анализа данных является ключевой технической задачей современного ИИ.
	Проблема черного ящика	Отсутствие прозрачности при принятии решений с помощью ИИ.
Этическая	Ответственность за ошибочные решения, принятые медицинским работником на основе рекомендаций ИИ	При применении систем ИИ есть риск причинения вреда здоровью пациента из-за ошибки в программном обеспечении, например если оно не заметит симптомы заболевания или неправильно интерпретирует медицинские данные. Кто должен отвечать за последствия: врачи или разработчики?
	Предвзятость результатов	Системы ИИ обучаются на данных, в которых могут отсутствовать примеры редких заболеваний, определенные группы пациентов, другая важная информация. Поэтому обученные на таких данных модели будут работать с ошибками в реальной клинической практике, что может приводить к дискриминации или предвзятости. Например, система ИИ может хорошо выявлять распространенные заболевания, но не распознавать орфанные болезни, потому что в предоставленном для обучения наборе просто не оказалось таких пациентов.
	Врачи с недоверием относятся к ИИ	Данных о пользе цифровых продуктов пока недостаточно, а получить эти данные невозможно без массового применения новых технологий.
	Возможный конфликт интересов стейкхолдеров	Каждый участник системы здравоохранения — от органов власти до поставщиков лекарств, медицинского оборудования и представителей страховых организаций — заботится о своих интересах. Кто будет защищать интересы пациента при внедрении технологий ИИ?
	Обеспечение конфиденциальности ПДн и соблюдения законодательства	Обезличивание данных не гарантирует их анонимности. Обмен данными между базами данных для анализа с помощью алгоритмов ИИ — проблема с точки зрения действующего законодательства.

3.2.2 БИОМЕДИЦИНСКИЕ ДАННЫЕ

Создание цифровых продуктов невозможно без данных. Биомедицинские данные имеют особый статус и специальные режимы использования. Сегодня не всегда можно превратить медицинскую информацию в данные, пригодные для дальнейшей работы. Медицинская информация

и данные сейчас разрозненны, содержатся в изолированных хранилищах и несовместимых системах и форматах (многое существует только на бумаге или на пленке) и почти всегда защищены законом[123].

Для научных исследований и создания медицинских цифровых продуктов необходимы качественные наборы данных, получение которых в России сейчас затруднено[124]. В процессе лечения собирается как медицинская информация (история болезни, результаты анализов и исследований, рентгеновские снимки и т. п.), так и некоторые ПДн пациента (ФИО, дата рождения, пол, возраст, регион). Сейчас в России не определены условия, на которых можно было бы предоставлять обезличенные данные пациентов разработчикам систем ИИ или научным организациям.

«Если изображение анонимизировать (лишить идентификаторов), его использование не угрожает пациенту, даже если оно попадет в открытый доступ. Но тут есть другая проблема: если изображения хранятся отдельно от другой информации о пациенте, невозможно решение некоторых задач, потому что отсутствует важная часть клинической информации».

Александр Гусев, член Экспертного совета Минздрава РФ по вопросам использования ИКТ в системе здравоохранения

При обращении к врачу пациент подписывает согласие на использование его данных в конкретном медицинском учреждении и только для оказания медицинской помощи. Научные исследования и разработка систем ИИ не входят в список целей обработки ПДн, предусмотренных законом и текстом согласия. Это означает, что в стране накапливается огромное количество ценнейшей медицинской информации, но использовать ее для развития ИИ-рынка пока сложно. Единого федерального банка обезличенных медицинских данных, пригодного для создания ИИ, нет, как нет возможности проводить научные исследования и разработки в этой сфере на том же уровне, что и в США, Китае, Великобритании.

Этот вопрос имеет два аспекта. С одной стороны, от его решения зависит, как скоро появятся российские цифровые продукты в медицинской сфере, — потребность в них велика, и есть вероятность, что, если время будет упущено, нишу займут импортные производители. С другой стороны, пациенты совершенно оправданно опасаются за безопасность своих данных, и их права должны быть в полной мере соблюдены (см. рисунок 4).

Сейчас Россия существенно отстает от стран-лидеров как по количеству научных публикаций, так и по числу разработок и исследований в сфере

[123] Подробнее о биомедицинских данных в цифровой медицине см.: Биомедицинские данные и большие данные в цифровой медицине // Этика и «цифра»: этические проблемы цифровых технологий. В 2 т. М.: РАНХиГС, 2020. URL: https://ethics.cdto.center/7_2#7.2.1

[124] Проблема качества данных имеет еще одну этическую составляющую: при сложившейся в России практике нельзя исключить возможности манипуляций со статистикой и административного давления на врачей при постановке диагнозов. См.: Гусев А. Управление здравоохранением давно пора модернизировать // Комплексные медицинские информационные системы. URL: https://kmis.ru/blog/meditsinskaia-statistika-nuzhdaetsia-v-razvitii

Рисунок 4. Проблема использования данных в медицине

ИИ для медицины. Те немногочисленные примеры сбора и подготовки обезличенных медицинских данных, которые есть в нашей стране, не удовлетворяют спрос разработчиков и ученых, содержат относительно небольшое количество записей в наборе, обычно несколько тысяч пациентов. В Европе и в Китае выходят публикации[125] с масштабными, часто миллионными выборками, потому что там разработчик может получить доступ к качественным обезличенным данным через этический комитет, через соглашение о партнерстве с научно-исследовательской организацией или через готовые национальные базы данных.

Необходимо внести точечные изменения в законодательство, чтобы сохранить ценность данных для ИИ, но при этом страховать риски пациентов — особенно учитывая, что по планам Минздрава к 2024 году не менее 50% учреждений здравоохранения должны будут использовать изделия и сервисы с ИИ[126]. Предполагается также, что доступ к медкартам россиян могут получить в том числе и частные компании[127].

3.2.3 ОТВЕТСТВЕННОСТЬ ВРАЧА

В России сейчас вся ответственность за принятие решений лежит на враче. Вся его деятельность строго регламентирована; например, врач

[125] Tarroni G., Bai W., Oktay O., Schuh A., Suzuki H., Glocker B. Large-scale Quality Control of Cardiac Imaging in Population Studies: Application to UK Biobank // Scientific Reports. Vol. 10. № 2408 (2020). URL: https://www.nature.com/articles/s41598-020-58212-2

[126] Манукиян Е. На приеме у робота // Российская Газета Digital. URL: https://rg.ru/2020/11/23/iskusstvennyj-intellekt-budet-pomogat-vracham-v-poliklinikah.html

[127] Королев Н. Добрый доктор AIболит. Власти хотят открыть медкарты граждан искусственному интеллекту // Коммерсантъ. URL: https://www.kommersant.ru/doc/4730016

в государственной клинике не может потратить на прием пациента больше отведенного времени и при этом должен успеть оформить все документы[128]. Предположим, врач использует цифровой продукт, созданный с применением ИИ. Кто будет отвечать в этом случае за врачебную ошибку, врач или разработчик? Как понять, допущена ошибка из-за неправильного применения или из-за ошибки в алгоритме? (Подробнее об ответственности разработчиков см. раздел 7.)

«Рост прозрачности ведет к изменениям в системе контроля. Сейчас у каждого пациента появляется цифровой профиль; электронные медицинские карты впервые сделали первичную медицинскую документацию доступной и прозрачной, в том числе и для пациента. Это может привести к усилению контроля со стороны пациентов, которые будут стремиться воздействовать на врача, в том числе через обращение в страховые компании. Существует такое явление, как пациентский экстремизм[129], растет и количество уголовных дел против медиков[130], а с распространением электронных медкарт таких дел может стать больше».

Александр Гусев, член Экспертного совета Минздрава РФ по вопросам использования ИКТ в системе здравоохранения

Все это влияет на представление о границах ответственности врача и оправданности медицинского риска. Сейчас врачи боятся применять технологии ИИ по двум причинам. Во-первых, потому что не имеют доказательств того, что цифровой продукт полезен и безопасен, а во-вторых, боятся, что ИИ негативно оценит результаты их работы. Искусственному интеллекту невозможно объяснить, что врач устал и что времени, отведенного на прием пациента, для подробного осмотра недостаточно, но то, что протокол осмотра в историях болезни создан с помощью копипаста, ИИ в состоянии отследить.

Инструменты, созданные с помощью ИИ, становятся все точнее. Они будут указывать на несовершенства системы, на возможные должностные нарушения, фальсификации, отписки, ошибки диагностики[131], нарушение протоколов лечения. Чем точнее инструмент, тем быстрее он вскрывает проблему. Но является ли это благом? Это этический вопрос, и он требует общественной дискуссии.

[128] Невинная И. Минздрав установил новые нормы времени приема больных в поликлинике // Российская Газета. URL: https://rg.ru/2020/10/30/minzdrav-ustanovil-novye-normy-vremeni-priema-bolnyh-v-poliklinike.html

[129] В России растет пациентский экстремизм — врачи ходят по лезвию ножа // MedRussia. URL: https://medrussia.org/30464-v-rossii-rastyot-pacientskiy-yekstremi/

[130] Калашников И. Процесс с анамнезом: «Медвестник» подсчитал количество «врачебных» дел в судах // Медвестник. URL: https://medvestnik.ru/content/articles/Process-s-anamnezom-Medvestnik-podschital-kolichestvo-vrachebnyh-del-v-sudah.html

[131] Житель Уфы рассказал в соцсети, что обнаружил в своей медицинской карте запись о беременности и направление к гинекологу. Руководством больницы было проведено служебное расследование, установившее, что при оформлении документов пациента произошла техническая ошибка. См.: Медики объяснили, почему у мужчины в Уфе «диагностировали» беременность // РИА Новости. URL: https://ria.ru/20201021/diagnoz-1580790347.html

Авторы раздела:

Ю. Б. Грязнова

Д. В. Комендантов

Е. И. Кохановская

М. В. Крель

О. В. Полетаев

Е. С. Трубинова

А. В. Фирсов

3.3 ИНСТРУМЕНТЫ ПОВЫШЕНИЯ ДОВЕРИЯ

Время чтения — 20 минут

Укрепление доверия к государственным цифровым сервисам — одна из ключевых задач любой стратегии цифровой трансформации. Для этого государственным органам необходимо изучать клиентский опыт, поддерживать общественную дискуссию, использовать механизмы внешнего и внутреннего аудита, обеспечивать реальную защиту данных, задействовать инструменты корректировки и отзыва данных в любом сервисе.

3.3.1 СОВЕРШЕНСТВОВАНИЕ ЗАКОНОВ И САМОАУДИТ ВЛАСТИ

Работу над доверием в обществе государству предстоит начинать с себя. Для этого необходимо разработать и принять понятные для всех и достаточно жесткие законы, защищающие данные граждан, а затем добиться неотвратимости наказания за преступления в цифровой сфере. Эти два фактора создают базовый уровень доверия к цифровым сервисам и цифровым решениям. Если граждане увидят справедливые судебные решения, убедятся, что при утере или краже данных для нарушителей наступают указанные в законе последствия, что в этой области нет двойных стандартов, уровень доверия постепенно будет расти.

Помимо работы над законодательством и правоприменением эффективны разные формы самоаудита, в том числе и самые простые. Если на сайте организации указан телефон, необходимо убедиться, что граждане могут по нему дозвониться и, например, записаться на прием к губернатору[132]. Цена недоступности услуг бывает довольно высока: от задержки выплат, необходимых для существования семьи, до депортации, если иностранный гражданин не смог вовремя встать на учет. Если госслужащий участвует в цифровизации в своем ведомстве, он может, опираясь на известные ему ситуации, предлагать адекватные решения для оптимизации процессов.

Повышение доверия к «цифре» происходит и благодаря совершенствованию регулирования. Сейчас во всех странах меняется регулирование в связи с появлением новых технологий. В России для этого принят ряд НПА, касающихся ИИ (см. раздел 5). Принятый в 2020 году закон «Об экспериментальных правовых режимах

[132] Врио губернатора Белгородской области не смог записаться к себе на прием // РИА Новости. URL: https://ria.ru/20210301/gubernator-1599516650.html

в сфере цифровых инноваций» (о т. н. «регуляторных песочницах») дает бизнесу возможность тестировать инновационные технологии (ИИ, распределенный реестр, нейротехнологии, квантовые вычисления) для различных отраслей экономики на основе законодательных изъятий.

«Одним из принципов программ экспериментальных правовых режимов (ЭПР) является их прозрачность. Компания, участвующая в ЭПР, должна информировать потребителей, что те получают товар или услугу в рамках эксперимента. Государство сейчас расширяет правовую базу для ЭПР. Так, принятый в мае 2021 года законопроект позволяет создавать такие режимы в сферах, где барьеры для инновационной деятельности закреплены в подзаконных актах Правительства или федеральных ведомств. Благодаря ЭПР вырабатывается и тестируется новое регулирование, и, если результат успешен, механизм в дальнейшем будет использоваться по всей стране».

Владислав Федулов, заместитель министра экономического развития РФ

Поскольку развитие законодательной базы отстает от развития технологий, большое значение приобретает техническое регулирование, которое можно разрабатывать как на уровне стран, так и на уровне организаций. Оно выражается прежде всего в создании стандартов: международных, государственных, отраслевых (см. раздел 5.3). Существенную роль могут сыграть и методические рекомендации, исходящие из авторитетного источника (аналоги этического кодекса, который выпустил Сбер[133]).

«Право — регулятор жесткий и медленный, консервативный. Что бы ни говорили о скором создании адаптивного, машиночитаемого права, само право будет этому сопротивляться. Этика объективно идет впереди права, и уже на основе этических правил, этических алгоритмов поведения людей, коллективов и даже государств будет формироваться право».

Алексей Ефремов, ведущий научный сотрудник Центра технологий государственного управления ИПЭИ РАНХиГС

3.3.2 ВЗАИМОДЕЙСТВИЕ С БИЗНЕСОМ И ОБЩЕСТВЕННЫМИ ОРГАНИЗАЦИЯМИ

Если подходить к ЦТ как к средству, а не как к цели, то необходима независимая внешняя экспертиза цифровых решений, общественная рефлексия в виде системы экспертных органов, которые могут до принятия решения проводить общественную дискуссию и представлять все за и против. Это может быть, к примеру, этический комитет с правом вето, в состав которого входят специалисты и граждане, чье мнение имеет вес в обществе. В роли таких институтов отчасти могли бы выступать общественные советы при министерствах.

[133] Кодекс корпоративной этики Сбербанка // Сбербанк. URL: https://www.sberbank.com/ru/about/ethics

«Каждый законопроект, каждое управленческое решение в рамках цифровизации, направленные на улучшение условий ведения бизнеса и жизни граждан, обсуждаются с самими предпринимателями и гражданами. Именно в результате обсуждения с бизнесом Минэкономразвития выявило законодательные барьеры в таких областях, как ИИ, медицина, телекоммуникации, беспилотный транспорт, связь, обработка персональных данных».

Владислав Федулов, заместитель министра экономического развития РФ

Если стейкхолдеры ведомств, будь то пациенты или ИТ-компании, вовлечены в разработку, обсуждение, проектирование, то они с куда большей готовностью потом участвуют в реализации проектов. Драйверами диалога могли бы стать НКО: через них можно развивать цифровые компетенции граждан, поощрять их к использованию новых сервисов.

«У нас догоняющая позиция: кажется, что мир ушел дальше, мы отстаем, надо срочно догнать. Вопросы цифровизации включили в КПЭ министерствам, чиновникам, то есть поставили их перед фактом. „Если вы хотите быть эффективными и, соответственно, оставаться на своих позициях — цифровизируйтесь“. Средство стало целью».

Алексей Фирсов, председатель совета директоров Центра социального проектирования «Платформа»

Передача функций государственной цифровизации (кроме защиты критической инфраструктуры) в модель государственно-частного партнерства (ГЧП) позволит проводить настоящие, а не имитационные клиентские исследования, перенести внимание на конечных пользователей. Позитивным кейсом можно считать портал «Госуслуги», который делает не государство напрямую, а ПАО «Ростелеком» (бизнес-структура с опытом налаживания службы поддержки и итерационных доработок системы). Госзаказчик (Минцифры и Минэкономразвития) осуществляет мониторинг качества оказания государственных услуг.

«Можно рассматривать удовлетворенность пользователей как одну из целей в каждом крупном проекте ЦТ; например, добиваться удовлетворенности пациентов в первичном звене медицины. Государство ставит такую задачу — бизнес идет и ищет решение: тестирует гипотезы, проводит фокус-группы, проводит оценку минимально работоспособного продукта и продукта, который будет обеспечивать положительный пользовательский опыт (и за который пациенты будут благодарны). Да, это более сложный цикл, но в нем нет ничего невозможного, если смотреть на него в логике ГЧП».

Олег Полетаев, директор по развитию цифрового бизнеса группы «Интерфакс»

3.3.3 КОММУНИКАЦИЯ С ГРАЖДАНАМИ И КЛИЕНТОЦЕНТРИЧНОСТЬ

В России пока нет таких институтов, которые могли бы достаточно точно выявлять предпочтения населения[134], поэтому для повышения доверия к государственным решениям важно общаться с гражданами, изучать их запросы, опыт, поведение, эмоции, восприятие инноваций и на основе этих данных строить востребованные и клиентоцентричные цифровые сервисы. Опишем подробнее некоторые важные шаги, которые в этом помогут.

1. Тестировать инновационные технологии. При выработке решений важно прислушиваться к мнению экспертного сообщества, внимательно изучать международный опыт и поэтапно внедрять нововведения на основе результатов пилотных проектов.

> **«В бизнесе, когда клиент дает негативную обратную связь, пилотный проект либо сворачивается, либо кардинально модернизируется. А наше госуправление в силу своей модели обречено на то, чтобы 99,9% проектов признавались успешными — по критерию соответствия формальным ТЗ, независимо от того, удовлетворены ли граждане, ради которых решение было воплощено в жизнь. В сущности, нет пространства для экспериментов и „права на ошибку“. Если ты допустил ошибку, значит, может возникнуть вопрос об эффективности расходования бюджетных средств. И тогда вышестоящим руководителям нужно наказать „виновных“, а контролирующим органам — начать проверку. У всех свои КПЭ».**
>
> **Олег Полетаев, директор по развитию цифрового бизнеса группы «Интерфакс»**

2. Развивать проактивные госуслуги. Проактивность рассматривается как важный принцип предоставления госуслуг[135] и входит в стратегию портала «Госуслуги», в частности в концепцию развития суперсервисов[136]. Концепция ЦТ социальной сферы[137] предполагает, что к 2025 году все меры социальной поддержки будут предоставляться в электронном виде без заявлений и подтверждающих документов. Уже сейчас в беззаявительном порядке выдается, например, материнский капитал. Концепция суперсервисов — наиболее перспективная модель, которую можно распространять на другие типы отношений человека и государства, на муниципальные и региональные услуги.

---

[134] Об этом говорит директор Московской школы экономики МГУ, академик РАН Андрей Некипелов, см.: Доверие как критический фактор достижения стратегических целей социально-экономического и политического развития государства: материалы научно-методического семинара Аналитического управления в рамках подготовки заседания Научно-экспертного совета при Председателе Совета Федерации / Совет Федерации Федерального Собрания Российской Федерации. М., 2020. URL: council.gov.ru/media/files/ZuyffAndc55HCTkMIVsA5A1r22tq2ZQx.pdf

[135] Новый принцип предоставления госуслуг — электронный вид, проактивность и экстерриториальность // Минэкономразвития РФ. URL: https://www.economy.gov.ru/material/news/novyy_princip_predostavleniya_gosuslug_elektronnyy_vid_proaktivnost_i_eksterritorialnost.html

[136] Суперсервисы: госуслуги без бумажных документов и визитов в госорганы // Госуслуги. URL: https://www.gosuslugi.ru/superservices

[137] Михаил Мишустин утвердил Концепцию цифровой трансформации социальной сферы // Правительство России. URL: http://government.ru/news/41634/

«Если мы говорим о клиентоцентричности в „цифре“, возможно, хорошей государственной идеологией была бы гражданоцентричность. Все сервисы государственной системы в такой идеологии строятся вокруг потребностей граждан и с максимальным удобством для них. При этом граждане должны быть уверены, что цифровая прозрачность не будет использована против них самих. Может быть, у нас появится citizen journey map, двигаясь по которой, гражданин получает от государства услуги в разных жизненных ситуациях. Начало на „Госуслугах“ уже положено»[138].

Марианна Крель, эксперт Центра подготовки РКЦТ

3. Изучать пользовательский опыт, сделать его качество базовым критерием при разработке цифровых сервисов. Существенно поднять уровень доверия к цифровым разработкам госсектора могло бы более широкое применение практик, принятых в бизнесе: тестирования прототипов, А/Б-тестирования, customer journey тестов, фокус-групп. Привязка КПЭ руководителя к удовлетворенности граждан качеством услуг и анализ обратной связи показали себя как действенный механизм улучшения работы с гражданами.

Система ИАС МКГУ «Ваш контроль» признана одной из крупнейших в мире онлайн-платформ для обратной связи с населением[139]. Ежемесячно через эту систему граждане оценивают 2–2,5 млн оказанных им государственных и муниципальных услуг с привязкой к конкретной точке. Обратная связь от граждан позволяет составить представление о деятельности руководителей территориальных органов власти и центров оказания услуг «Мои документы» и совершенствовать их работу. Однако в системе пока оцениваются не все услуги, что существенно ограничивает ее применение.

Ценная обратная связь была получена после того, как 11 мая 2020 года президент России Владимир Путин сообщил о выплате с 1 июня единовременного пособия семьям с детьми в возрасте с 3 до 16 лет.

Заявление можно было подать на портале «Госуслуги», однако первоначальная форма оказалась неудобной и нуждалась в доработке. Для изучения пользовательского опыта 30 мая 2020 года был запущен информационный проект «Госуслуги: для родителей» на портале и в социальных сетях. Редакция публиковала ответы на вопросы о выплатах, разъяснения законов и нюансов подачи заявлений, инструкции для родителей, вебинары с экспертами, обзоры мер поддержки семей. В июле и декабре выплата единовременных пособий была организована в беззаявительном порядке и без повторного внесения данных.

---

[138] «Жизненные ситуации» — новый раздел портала Госуслуг // Госуслуги. URL: https://www.gosuslugi.ru/help/news/zhiznennye_situacii_novyy_razdel_portala_gosuslug

[139] Проект Минэкономразвития «Ваш контроль» стал чемпионом премии WSIS Prizes 2020 // Минэкономразвития РФ. URL: https://economy.gov.ru/material/news/proekt_minekonomrazvitiya_vash_kontrol_stal_chempionom_premii_wsis_prizes_2020.html

4. Изучать эмоции пользователей и реагировать на них. Важно учитывать чувства человека и его эмоциональное состояние при контакте с сервисами, получаемыми от государства. Недостаточно знать, что услуга оказана и у пользователя была возможность ее оценить. Организация может не задумываться, через какую «боль» услуга была оказана на самом деле, а эти вопросы играют важнейшую роль в пользовательском опыте и, соответственно, в оценке работы организации. Примером того, как государство, совмещая быстрые цифровые решения и эффективное межведомственное взаимодействие, может реагировать на состояние граждан в сложной ситуации, служит организация возвращения россиян на родину в апреле — июне 2020 года[140].

После того как 27 марта 2020 года авиасообщение России с другими странами было приостановлено из-за пандемии[141], десятки тысяч российских граждан, находившихся за рубежом в качестве туристов и студентов, на лечении и в деловых поездках, попали в сложную ситуацию. Минцифры России начало собирать информацию о тех, кто желал вернуться на родину и претендовал на материальную помощь, с помощью формы «Регистрация прибывающих в РФ»[142] на ЕПГУ. При составлении списков пассажиров для вывозного рейса для оперативности было решено использовать Telegram. «Мы формировали списки, — вспоминает глава Минцифры Максут Шадаев, — рейс планировался на следующий день, и мы создали Telegram-канал для услуги, в котором объявили: все, кто готов лететь, присылайте в канал номер заявления на „Госуслугах“». Каналы в Telegram оказались понятной и прозрачной формой коммуникации с туристами и практически единственным средством связи для напуганных и раздраженных людей. Максут Шадаев лично координировал помощь россиянам на острове Пхукет, присутствуя в чате на правах администратора. Администраторы канала взаимодействовали с консулом, с авиакомпанией и с самим пассажиром.

Если сервис позволяет гражданам быстро решить свою проблему, получить ответ на вопрос, если правила его работы прозрачны и понятны пользователю, такой сервис будет улучшать репутацию государственных цифровых решений и вызывать положительные эмоции.

Удобным сервисом, который позволяет гражданину управлять своими персональными данными, стал новый раздел личного кабинета на Едином портале госуслуг www.gosuslugi.ru. В этом разделе пользователь может увидеть все организации или электронные сервисы, которым он давал согласие на обработку своих ПДн, и перечень всех ПДн, которые обрабатывает каждая организация. Одним нажатием кнопки «Отозвать разрешение» пользователь может запретить конкретной организации обрабатывать свои ПДн.

[140] Здесь и далее в описании кейса использованы материалы и интервью министра цифрового развития, связи и массовых коммуникаций М. И. Шадаева и советника министра А. Ф. Ахмадиевой, предоставленные для книги «Общество и пандемия: опыт и уроки борьбы с COVID-19 в России». М., 2020.

[141] Россия прекратит авиасообщение с другими странами // ТАСС. URL: https://tass.ru/ekonomika/8080827

[142] Регистрация прибывающих в Российскую Федерацию // Госуслуги. URL: https://www.gosuslugi.ru/394604/1

5. Вводить новые формы коммуникации с гражданами. В обществе сложился высокий уровень недоверия к ура-мобилизационным инициативам. Граждане больше не реагируют на директивные сообщения о необходимости менять бумажный паспорт на цифровой или проходить вакцинацию. Назрела необходимость перехода от трансляционной модели к полноценному диалогу и новым моделям взаимодействия. Такие модели предполагают, в частности, что вместо директивной подачи информации (например, единственного телевизионного сюжета на заданную тему) следует проводить семплинг (тестирование образцов), работать с добровольцами, мотивировать граждан пробовать и делиться впечатлениями[143]. Активной стороной коммуникации может выступать общество или конкретные целевые сообщества.

Выстраивая комплексную коммуникацию с гражданами по сложным этическим вопросам, власти Оренбургской области решили уделять особое внимание разъяснительным материалам. «В период пандемии население стало пользоваться дистанционными цифровыми решениями, и сразу обострился ряд проблем, — рассказывает Денис Толпейкин, министр цифрового развития и связи Оренбургской области. — Мы поняли, что людей надо заранее готовить к цифровизации, всю нашу работу по внедрению цифровых решений надо переводить на понятный язык и объяснять людям, что и зачем мы делаем. У нас появилось онлайн-сообщество, где мы размещаем информацию о цифровых проектах, чтобы получить обратную связь и почувствовать отношение людей к этому проекту».

6. Сохранять доступ к «аналоговым» сервисам для граждан, которые не захотят пользоваться цифровыми решениями; предусмотреть возможность бумажного пути получения госуслуг, а также личного участия в деловых, семейных, правовых процессах (подробно об этом см. раздел 2.2.1). Не должно быть дискриминации тех, кто выбирает аналоговые инструменты: они должны быть не менее комфортными, чем цифровые. Альтернативные пути нужны в том числе для того, чтобы снизить зависимость от конкретной технологии, которая может оказаться уязвимой.

В феврале 2021 года почти половина ветряных электростанций в штате Техас прекратила работу из-за обмерзания турбин[144]. Без отопления и света осталось до пяти миллионов человек, массовый сбой в электроснабжении продолжался почти неделю[145]. К энергетическому кризису привели аномальные погодные условия, не учтенные при строительстве ветряков.

[143] Попыткой отойти от трансляционной коммуникативной модели может быть кампания в СМИ и соцсетях по теме доверия к ИИ и план создания национального онлайн-портала по ИИ. См.: Власти планируют повышать доверие россиян к ИИ через СМИ и соцсети // ТАСС. URL: https://tass.ru/nacionalnye-proekty/9299615

[144] Детинич Г. В Техасе энергетический кризис: ледяной шторм остановил ветряные турбины // 3DNews. URL: https://3dnews.ru/1032754/v-tehase-energeticheskiy-krizis-ledyanoy-shtorm-ostanovil-vetryanie-turbini

[145] Идеальный шторм или провал альтернативной энергетики? Три причины энергетического кризиса в США // The Bell. URL: https://thebell.io/idealnyj-shtorm-ili-proval-alternativnoj-energetiki-tri-prichiny-energeticheskogo-krizisa-v-ssha

7. Использовать риск-ориентированный подход и инструменты кризисных коммуникаций. Риск-ориентированный подход — бизнес-практика, которая предполагает оценку новых инициатив с точки зрения конфликтов со стейкхолдерами (внутренними и внешними, коммерческими и некоммерческими), с государством. Этот подход может с успехом использоваться и в госсекторе. Речь об исследованиях, тестах, анализе потенциальных реакций как на идею цифрового решения, так и на процесс и результат разработки. Необходимо также предусмотреть верификацию для последующих фаз жизненного цикла цифрового решения.

«В время пандемии неожиданной была не только скорость внедрения цифровых решений, но и степень неготовности общества отвечать на эти вызовы. Все конспирологические страхи про чипирование и так далее возникают от недостатка информации, от отсутствия грамотной, открытой и моделируемой государством дискуссии, в том числе по этическим вопросам внедрения и применения „цифры“ в разных сферах жизни».

Алексей Ефремов, ведущий научный сотрудник Центра технологий государственного управления ИПЭИ РАНХиГС

Уже на этапе проектирования цифрового сервиса должны использоваться механизмы обратной связи: фокус-группы, изучение пользовательского опыта похожих сервисов, международной практики внедрения аналогичных решений и взаимодействия с обществом и стейкхолдерами, открытый диалог с экспертным сообществом для выявления критичных недостатков сервисов на этапе разработки и доработки.

«Для работы с репутационными рисками, возможными при реализации цифровых решений с неоднозначным этическим контекстом, в бизнесе существует практика включения таких рисков в общекорпоративную карту управления рисками. Такая карта требует регулярной переоценки и актуализации и позволяет руководству и органам управления компании иметь структурированное понимание существующих рисков и учитывать их при принятии управленческих решений в момент запланированного и срочного запуска цифровых сервисов».

Елена Кохановская, директор по внешним коммуникациям и связям с общественностью ПАО МТС

В так называемую **карту рисков** необходимо включить все категории известных, предсказуемых форс-мажорных обстоятельств, которые могут вызвать негативную реакцию у пользователей цифрового сервиса, экспертного сообщества, вышестоящих органов государственной власти, конкурирующих организаций и подрядчиков.

В любой кризисной ситуации время — самый ценный ресурс, поэтому для оперативного реагирования заранее разрабатывается регламент действий с перечнем возможных кризисных ситуаций по категориям «запланированные», «предсказуемые» и «непредсказуемые». Регламент включает не менее 15–20 потенциальных кризисов и вероятных сценариев развития ситуации. Этот документ позволяет управлять повесткой в информационном поле на всех этапах работы цифровых сервисов.

Чтобы выявить риски, необходимо провести ретроспективный анализ кризисных ситуаций, связанных с аналогичными цифровыми сервисами, за последние 3–5 лет на уровне региона, страны, изучить международную практику. Также помогут регулярный сбор и анализ обратной связи от пользователей существующих цифровых сервисов, фокус-группы, глубинные интервью с пользователями и экспертами.

Важно определить основные группы целевых аудиторий, с которыми необходимо поддерживать диалог в кризисной ситуации, и составить список официальных источников информирования граждан (пресс-служба, сайт, аккаунты в соцсетях) и список официальных спикеров, которые закреплены за каждой группой. У организации должны быть заранее подготовлены ответы на «неудобные» вопросы.

Негативную реакцию вызвал инцидент в декабре 2020 года, когда в свободный доступ попали более 360 файлов с ПДн 300 тыс. москвичей, переболевших коронавирусом. Сотрудники ДИТ Москвы допустили передачу файлов в Telegram-каналах третьим лицам. При этом ДИТ Москвы ограничился стандартным заявлением о начале проверки и сослался на «человеческий фактор»[146]. Результаты проверки так и не были представлены общественности, что подрывает доверие к позиции государства в отношении ПДн и ставит под сомнение компетентность сотрудников ИТ-подразделения органа власти.

ВЫВОДЫ. КАК ИЗМЕНИТЬ ВОСПРИЯТИЕ ЦИФРОВЫХ ИНИЦИАТИВ ГОСУДАРСТВА

Известно, что доверие сокращает транзакционные издержки, а прозрачность и диалог необходимы в любой сфере жизни. Россия, как и многие государства, переживает сейчас кризис доверия — как межличностного, так и политического. Доверие к цифровым сервисам, которые разрабатывает государство, тоже под угрозой. Первый и главный рецепт — **клиентоцентричность.** Применительно к государственным решениям она состоит в том, чтобы поставить гражданина во главу угла, строить всю государственную работу вокруг его потребностей. Это фундамент создания доверия в цифровую эпоху.

[146] Мэрия Москвы назвала причиной утечки данных переболевших COVID-19 человеческий фактор // Коммерсантъ. URL: https://www.kommersant.ru/doc/4605338

«Можно ли создать универсальную этическую систему ответов, которая помогла бы в разработке цифровых продуктов? Нет, это невозможно: таких этических систем много, и каждая из них имеет собственную логику. При этом хочется, чтобы идея этичной разработки, этичного взаимодействия, этичного отношения к гражданам была на повестке дня. Каждый раз, когда мы говорим про технологии, про цифровизацию, мы говорим про этику тоже: какой тип ценностей, какую базовую логику в отношениях мы хотим укоренить. Если мы принимаем, например, что нам подходит кантианская система, где человек — это самоценность, то главным будет все то, что происходит вокруг человека как пользователя технологии, и мы начинаем отталкиваться от этой идеи. Но тогда нужно все отношения, не только технологические, выстраивать вокруг этой логики. Это значит, что все, от интерфейса госуслуг или дизайна беспилотного автомобиля до распределения денег для социальных групп или на военные нужды, — все это должно меняться».

Лилия Земнухова, научный сотрудник
Центра исследований науки и технологий ЕУСПб

Помимо человекоцентричности в широком смысле выход из сложившейся ситуации разумно искать еще в нескольких направлениях.

- Доверие граждан во многом зависит от того, насколько аккуратно государство обращается с переданными ему ПДн. Гражданин должен быть уверен, что его **данные защищены** и что любой мошенник, который их украл, будет найден и наказан.
- Создание или сохранение **аналоговых альтернатив** цифровым сервисам повышают надежность их работы и укрепляют доверие граждан.
- Избежать многих рисков можно за счет **прозрачности** процессов подготовки и разработки новых цифровых решений. Откровенный и конструктивный **диалог** с экспертами и потенциальными пользователями на этапе разработки страхует от критики и репутационных рисков на этапах запуска и эксплуатации.
- Любое цифровое изменение в госсекторе носит **публичный характер**, потому что оно изначально адресовано неопределенному кругу пользователей, и с этим неопределенным кругом пользователей нужно работать. Государственные организации занимаются разработкой систем, с которыми будет взаимодействовать большое количество граждан с низким уровнем цифровой грамотности и желанием как можно меньше контактировать с государством. В этом смысле любая массовая система, запроектированная без учета описанных выше принципов, будет подрывать усилия государства в области цифровизации. Ложка дегтя в виде одного-двух непродуманных решений может испортить в глазах граждан всю бочку меда продвигаемых государством полезных цифровых технологий.

4. ПРИВАТНОСТЬ И ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

Один из двоих незнакомцев, высокий, с сединой на висках, достал из ящика стола каучуковый колокольчик и беззвучно зазвонил. «Что за адские предосторожности!» — подумал я.

С. Лем. Звездные приключения Ийона Тихого

4.1 СПОСОБЫ ОБЕСПЕЧЕНИЯ ПРИВАТНОСТИ

Время чтения — 12 минут

Существенная часть важнейших требований к разработке и функционированию цифровых решений связана с обеспечением приватности, а именно надлежащих обработки[147], конфиденциальности[148] и безопасности ПДн. Необходимость обеспечения приватности потребовала мультидисциплинарного подхода к защите ПДн при их обработке в ИС[149]. Воплощением этого подхода стала концепция PbDD: Privacy by Design и Privacy by Default.

[147] Обработка персональных данных — любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (п. 3 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»).

[148] Обязанность не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законом (ст. 7 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»).

[149] Информационная система персональных данных — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (п. 10 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»).

4.1.1 КОНЦЕПЦИЯ PBDD: PRIVACY BY DESIGN И PRIVACY BY DEFAULT

Автор раздела:

А. В. Мунтян

Термин «приватность» — калька с английского privacy, которое, в свою очередь, появилось в конце XIX века как отражение желания уединиться и защитить личное пространство в ответ на развитие технологий, в частности фотографии[150]. Под приватностью в самом общем смысле понимают неприкосновенность частной и личной жизни. Выделяют несколько видов приватности: телесную, пространственную, информационную и коммуникационную, и все они актуальны в цифровом мире.

Концепция Privacy by Design (проектируемой приватности[151]) и Privacy by Default (приватности по умолчанию) применительно к ИС и ПДн была разработана в 1990-х годах Энн Кавукян, которая на тот момент занимала пост уполномоченного по вопросам информации и приватности в канадской провинции Онтарио. В 2009 году она опубликовала программный документ «Privacy by Design: 7 основополагающих принципов»[152]. Эти принципы приведены ниже.

1. Проактивность, а не реактивность. Превентивные меры для предотвращения вреда, а не реагирование на нанесенный вред и устранение последствий.
2. Защита приватности как настройка по умолчанию.
3. Приватность как часть устройства информационных систем. Интеграция инструментов защиты приватности в продукт при его проектировании.
4. Сочетание интересов приватности с бизнес-интересами. Стратегия, при которой в выигрыше остаются все участники (win-win).
5. Сквозная безопасность: защита информации на протяжении всего жизненного цикла продукта, от начала и до конца ее обработки.
6. Открытость документации и прозрачность (транспарентность) обработки данных.
7. Уважение к интересам пользователя и клиентоцентричность как основа архитектуры информационных систем и бизнес-процессов.

Концепция Privacy by Design обеспечивает непрерывное и безопасное управление жизненным циклом ПДн начиная с фазы проектирования процессов и (или) систем и до завершения обработки данных.

---

[150] Блог компании «Дата Прайваси Офис». URL: https://data-privacy-office.com/chto-takoe-privatnost/ Подробнее см.: Приватность человека и защита его персональных данных // Этика и «цифра»: этические проблемы цифровых технологий. В 2 т. М.: РАНХиГС, 2020. URL: https://ethics.cdto.center/5_1

[151] Термин Privacy by Design имеет и другие переводы: спроектированная приватность, приватность по замыслу, стратегически встроенная приватность; часто встречается и его использование в русских текстах без перевода. Вместо «приватности» в составе этого термина иногда используется слово «конфиденциальность». Далее мы будем употреблять в основном английские термины.

[152] Cavoukian A. Privacy by Design: The 7 Foundational Principles. URL: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

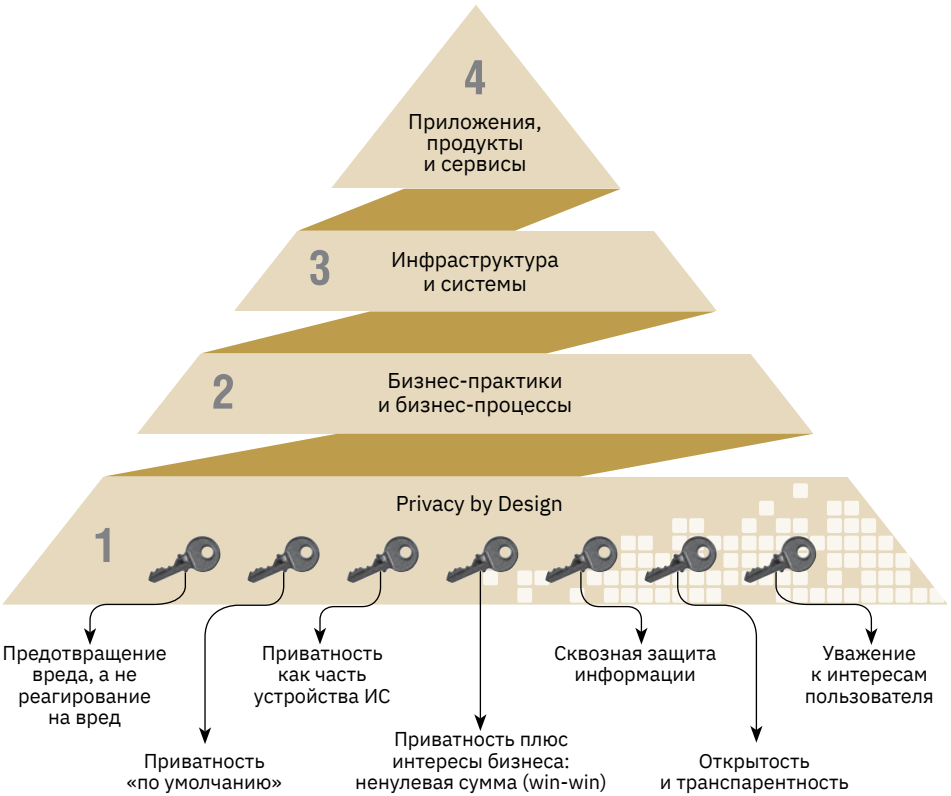


Рисунок 5. Privacy by Design как основа культуры защиты ПДн в организации

Защита данных на протяжении всего жизненного цикла (Full Lifecycle Protection) гарантирует, что все ПДн надлежащим образом обрабатываются и защищаются, а затем надежно и своевременно уничтожаются. При этом проектируемая приватность может и должна быть реализована без ущерба для функциональности бизнеса или систем. Эти принципы управления данными, а также философию и методологию, на которых они основаны, можно применять к технологиям, элементам операционной деятельности, физической архитектуре, сетевой инфраструктуре и целым информационным экосистемам. Роль этой концепции в общих механизмах защиты ПДн[153] показана на рисунке 5.

Privacy by Default, в свою очередь, означает, что принципы приватности должны учитываться оператором ПДн[154] в любом процессе или системе. Пользователь (субъект данных) не должен предпринимать никаких

[153] Agencia Española de Protección de Datos: Guía de Privacidad desde el Diseño. URL: https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf

[154] Оператор — государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными (п. 2 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»).

специальных действий для защиты своих прав и свобод при обработке ПДн, не должен нести бремя их защиты при использовании каких-либо услуг или продуктов. Приватность по умолчанию означает, что право на неприкосновенность частной жизни будет защищаться автоматически в качестве настройки по умолчанию.

«Инструменты защиты приватности должны быть интегрированы в сетевые системы и технологии по умолчанию на начальном этапе разработки. Защита приватности должна стать одним из приоритетов, входить в число целей проекта, бизнес-процессов и стратегического планирования. Принципы защиты приватности должны быть включены в каждый стандарт, протокол и процесс, с которым мы сталкиваемся в повседневной жизни»[155].

Энн Кавукян, автор концепции Privacy by Design

Концепция PbDD получила международное признание в 2010 году на 32-й Международной конференции уполномоченных органов защиты ПДн и конфиденциальности, где была принята Резолюция о проектируемой приватности[156]. Позднее, в середине 2010-х годов, принципы PbDD, сформулированные Кавукян, были использованы европейскими законодателями при разработке Общего регламента защиты персональных данных (GDPR, см. о нем раздел 4.3.1), в который была включена соответствующая норма. В 2019 году был принят международный стандарт ISO/IEC 27701 «Менеджмент персональных данных»[157], который является расширением двух более ранних стандартов: ISO/IEC 27001 «Система обеспечения информационной безопасности» и ISO/IEC 27002 «Методы и средства обеспечения безопасности».

4.1.2 PRIVACY BY DESIGN

Концепция Privacy by Design предполагает, что операторы ПДн будут продумывать механизмы обеспечения приватности еще на этапе планирования процедур обработки ПДн в бизнес-процессах и ИС. Эта концепция должна быть внедрена в процессы жизненного цикла разработки системы (System/Software Development Life Cycle, SDLC), в управление изменениями и в проектное управление.

Согласно философии Privacy by Design лучший способ снизить риски, связанные с приватностью, — это не создавать их. Чем меньше данных оператор ПДн собирает и обрабатывает, тем меньше риск нарушения прав и свобод субъектов данных, а также нанесения ущерба самому оператору.

[155] Cavoukian A. Privacy by Design: The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices. URL: https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf

[156] Resolution on Privacy by Design. 32nd International Conference of Data Protection and Privacy Commissioners. Jerusalem (Israel) 27–29/10/2010. URL: https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf

[157] ISO/IEC 27701 — Менеджмент персональной информации // BSI. URL: https://www.bsigroup.com/ru-RU/isoiec-27701/

Рисунок 6. Принципиальная схема применения стратегий Privacy by Design

На начальных этапах работы помогают стратегии проектируемой приватности (Privacy Design Strategies)[158]. Стратегии служат мостом между принципами обработки ПДн, закрепленными законодательно, и их реализацией в конкретных приложениях, устройствах или системах. Специалисты чаще всего выделяют восемь стратегий Privacy by Design[159], которые условно делятся на две категории. На рисунке 6 показано, как применять эти стратегии при обработке данных[160].

1. **Стратегии, ориентированные на данные**, имеют скорее технический характер и фокусируются на обработке ПДн с учетом требований приватности: минимизация, сокрытие, разделение, объединение.

2. **Стратегии, ориентированные на процессы**, имеют организационный характер и ориентированы на определение процессов, обеспечивающих ответственное управление ПДн: информирование, контроль, принуждение, демонстрация.

[158] Hoepman J.-H. Privacy Design Strategies. Oct 2012. URL: https://www.cs.ru.nl/~jhh/publications/pdp.pdf

[159] Hoepman J.-H. Privacy Design Strategies (The Little Blue Book). Mar 2019. URL: https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf; Colesky M., Hoepman J.-H., Hillen C. A Critical Analysis of Privacy Design Strategies. May 2016. URL: https://www.researchgate.net/publication/305870977_A_Critical_Analysis_of_Privacy_Design_Strategies

[160] Источник рисунка: Agencia Española de Protección de Datos: Guía de Privacidad desde el Diseño. URL: https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf

Стратегии проектируемой приватности проявляются в том числе как элементы пользовательского интерфейса, названные паттернами приватности (Privacy Patterns)[161]. Такие паттерны используются на стадии проектирования процессов или систем и могут применяться для решения общих проблем приватности. Privacy Patterns — это способ превращения Privacy by Design в практические советы для разработки ПО. Для многократного использования в проектировании согласно канонам PbDD (и для стандартизации самого процесса такого проектирования) создаются каталоги релевантных паттернов приватности[162].

4.1.3 PRIVACY BY DEFAULT

Суть Privacy by Default состоит в минимизации процессов обработки ПДн. Чем меньше объем данных, чем меньше способов используется при их обработке, чем короче сроки и меньше круг вовлеченных лиц, тем безопасней обработка для субъектов данных и самого оператора. Минимизация позволяет вывести часть бизнес-процессов из-под действия законодательства о ПДн и тем самым сэкономить силы и средства операторов. Кроме того, концепция Privacy by Default требует подотчетности (accountability): оператор должен знать, в каких процессах и ИС обрабатываются данные, в каком объеме, с какой целью и как долго.

При реализации Privacy by Default применяются три стратегии, непосредственно связанные со стратегиями минимизации и контроля в Privacy by Design.

1. Оптимизация направлена на анализ обработки ПДн с точки зрения приватности, что означает принятие мер в целях минимизации объема собираемых данных, способов и длительности их обработки, а также степени их доступности.

2. Конфигурирование (возможность настройки параметров обработки ПДн с помощью функций, доступных пользователю в приложениях, устройствах или системах) передает разумную часть этих параметров под контроль пользователя.

3. Ограничение гарантирует, что обработка данных осуществляется с максимальным соблюдением приватности, поэтому настройки параметров должны быть по умолчанию установлены таким образом, чтобы способствовать ограничению обработки данных.

4.1.4 ИНЖЕНЕРИЯ ПРИВАТНОСТИ

После вступления в силу в 2018 году регламента GDPR (см. раздел 4.3.1) растет внимание к концепции PbDD со стороны коммерческих и государственных структур разных стран. Спрос на имплементацию PbDD в процессы и системы активизировал развитие такой прикладной дисциплины, как инженерия приватности (Privacy Engineering).

[161] Hoepman J.-H. Privacy Design Strategies. Oct 2012. URL: https://www.cs.ru.nl/~jhh/publications/pdp.pdf

[162] С примером такого публичного каталога можно ознакомиться на сайте https://privacypatterns.org/patterns/

Под инженерией приватности понимают совокупность технологий приватности и представлений о дизайне продукта, разработке ПО, кибербезопасности, взаимодействии человека и компьютера, а также деловых и юридических аспектов обеспечения приватности.

Активная фаза работ по инженерии приватности началась в 2014 году, когда были опубликованы книги Privacy Engineer's Manifesto[163] и Privacy Engineering[164] (последнюю написал инженер компании Nokia Йэн Оливер). Во внутреннем отчете Национального института стандартов и технологий США (NIST) «Введение в инженерию приватности и управление рисками»[165], опубликованном в январе 2017 года, показано, что приватность служит важным техническим и стратегическим фактором укрепления доверия и репутации. Отмечается отсутствие строгого определения Privacy Engineering и предлагается рассматривать инженерию приватности как специальную дисциплину системного проектирования, задача которой — избежать при обработке ПДн неприемлемых для людей последствий. В документе также показано, что информационная безопасность и приватность — это не одно и то же (см. рисунок 7).

Рисунок 7. Соотношение между безопасностью и приватностью

[163] Dennedy M. F., Fox J., Finneran Th. R. The Privacy Engineer's Manifesto. Getting from Policy to Code to QA to Value. Springer Nature, 2014. URL: https://library.oapen.org/handle/20.500.12657/28156

[164] Oliver I. Privacy Engineering: A Dataflow and Ontological Approach. CreateSpace Independent Publishing Platform, 2015.

[165] An Introduction to Privacy Engineering and Risk Management in Federal Systems. National Institute of Standards and Technology Internal Report 8062. URL: https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf

4.2 DATA PROTECTION OFFICER: РОЛЬ, ФУНКЦИИ И КОМПЕТЕНЦИИ

Время чтения — 14 минут

Автор раздела:

А. В. Мунтян

Ответственные за организацию обработки ПДн (Data Protection Officers, DPO) в России уже выделились в отдельную группу со своей повесткой и своими интересами, самостоятельный DPO появился у многих крупных и даже средних коммерческих организаций. Отечественный субинститут DPO находится на этапе перехода от обслуживающей роли при нанимателе к позиции посредника между различными подразделениями, имеющими отношение к обработке ПДн.

4.2.1 РОЛЬ И ФУНКЦИИ DPO

Хотя сам субинститут лиц, ответственных за организацию обработки ПДн, был включен в российское законодательство еще в 2011 году, ему довольно долго не уделяли должного внимания субъекты данных, надзорные органы, консультанты и даже сами операторы ПДн. Ситуация начала меняться в связи со вступлением в силу Федерального закона от 21.07.2014 № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях»[166] и появлением у операторов обязанности «локализовывать» базы с ПДн граждан РФ при их сборе. Это породило спрос на квалифицированных DPO, которые на регулярной основе помогали бы нанимателям разбираться с запутанными требованиями законодательства и хитросплетениями потоков ПДн. Второй импульс возник в 2018 году и был связан с регламентом GDPR, в котором роли и функциям DPO уделено особое внимание. Хотя положения GDPR могут быть прямо применены лишь к относительно небольшому количеству российских организаций, европейский опыт сохраняет релевантность для нашей страны.

Тем не менее до сих пор в России роль DPO традиционно сводится к выполнению ряда обслуживающих функций по отношению к основной деятельности организации-нанимателя. Такое понимание этой роли во многом проистекает из ч. 4 ст. 22.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (ФЗ-152)[167]. Лица, ответственные за организацию обработки ПДн в российских организациях, обязаны выполнять функции, показанные на рисунке 8.

[166] Согласно ст. 2 закона операторы обязаны при получении ПДн от субъектов — граждан РФ обеспечивать запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение ПДн с использованием баз данных, расположенных (локализованных) на территории РФ.

[167] Федеральный закон № 152-ФЗ «О персональных данных» // КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/

Важно отметить, что вышеупомянутой ст. 22.1 установлено требование о получении DPO указаний непосредственно от исполнительного органа организации, являющейся оператором, и о подотчетности DPO данному органу. Кроме того, оператор обязан предоставлять DPO основные сведения о детальности организации по обработке ПДн[168].

Задачи DPO в странах Европейской экономической зоны (ЕЭЗ) базово определены в статье 39 GDPR. Если же обратиться к существующей правоприменительной и судебной практике ЕЭЗ, то можно выделить функции и задачи, описанные на рисунке 9.

Следует отметить непривычную для российских организаций роль DPO как своеобразного советника для своего нанимателя-оператора («контролера» в терминах GDPR). Главными функциями DPO являются 1) информирование руководства организации о выявленных несоответствиях в области обработки и защиты ПДн и 2) предоставление нанимателю активных рекомендаций по выполнению требований GDPR и по устранению выявленных несоответствий. При этом DPO не несет ответственности за определение приоритетов и выполнение действий, направленных на сохранение конфиденциальности и соблюдение GDPR. Эта ответственность ложится на контролера данных или процессора[169].

Рисунок 8. Основные функции DPO согласно российскому законодательству

[168] Состав таких сведений приведен в ст. 22 ФЗ-152.

[169] Это физическое или юридическое лицо, государственный орган, учреждение или другой орган, который обрабатывает ПДн от имени по поручению контролера (см. ст. 4 (8) GDPR).

Рисунок 9. Функции и задачи DPO в Европейской экономической зоне

4.2.2 КОМПЕТЕНЦИИ DPO И ИХ РАЗВИТИЕ

DPO как лицам, ответственным за организацию обработки ПДн и их защиту, необходимо постоянно повышать свой профессиональный уровень, чтобы эффективно выполнять должностные обязанности в организации, так как нормы права и технологические аспекты постоянно меняются. В ЕС уже существует несколько систем сертификации DPO, созданных в рамках правового поля GDPR. Надзорные органы стран — членов ЕС[170] публикуют рекомендации, помогающие интерпретировать требования GDPR. Одним из таких органов является Национальная комиссия по информационным технологиям и гражданским свободам Франции (Commission Nationale de l'Informatique et des Libertés, CNIL). В частности, CNIL в 2018 году опубликовала[171] руководство по сертификации действующих на территории Франции (или франкоязычных) DPO. В руководстве приводятся требования к кандидатам и условия рассмотрения заявлений кандидатов, а также перечислены 17 квалификационных критериев (компетенций), которым необходимо соответствовать для получения статуса сертифицированного DPO от органов сертификации, аккредитованных CNIL.

[170] Сайты надзорных органов государств — членов ЕС на сайте European Data Protection Board. URL: https://edpb.europa.eu/about-edpb/board/members_en

[171] Certification des compétences du DPO: la CNIL adopte deux référentiels // CNIL. URL: https://www.cnil.fr/fr/certification-des-competences-du-dpo-la-cnil-adopte-deux-referentiels

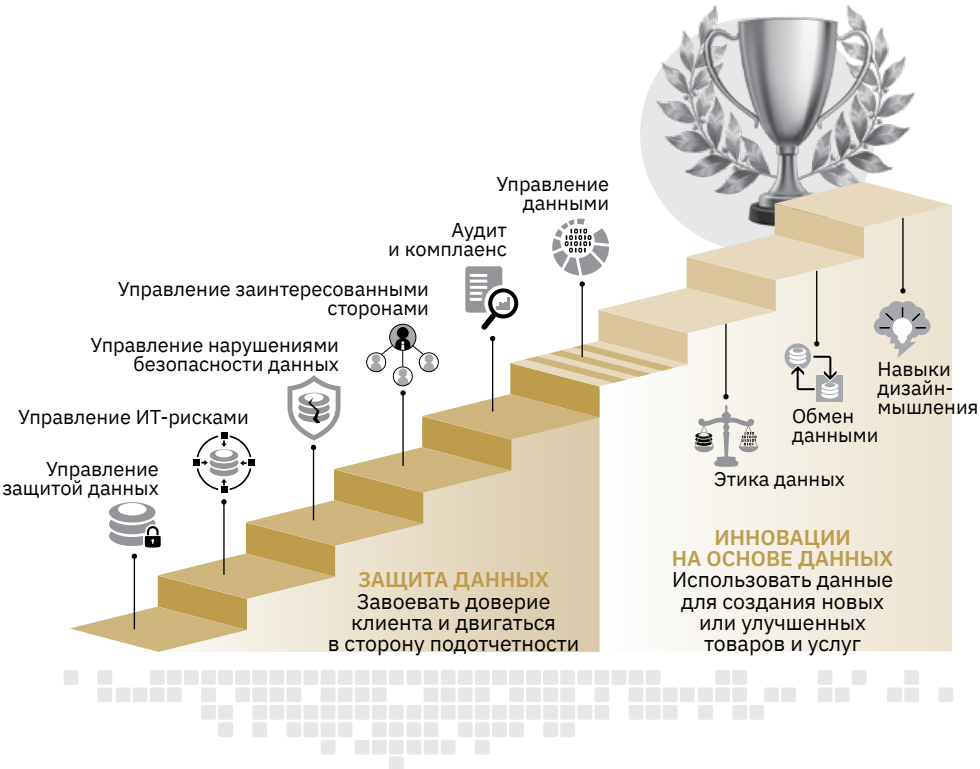


Рисунок 10. Описание компетенций и дорожной карты развития DPO

Одно из самых наглядных и всеобъемлющих описаний[172] компетенций DPO и дорожной карты их развития подготовлено Комиссией по защите персональных данных Сингапура (Personal Data Protection Commission, PDPC). Это описание[173] схематично представлено на рисунке 10.

Каждая из ступеней развития компетенций DPO может быть кратко охарактеризована следующим образом.

1. Управление защитой данных — разработка и внедрение политик и процедур управления защитой ПДн организации в соответствии с применимым законодательством и лучшими практиками.

2. Управление ИТ-рисками — эффективное прогнозирование и оценка существующих и потенциальных ИТ-рисков, которые влияют на работу и (или) прибыльность организации, а также на разработку и внедрение общеорганизационных стратегий и процессов, для снижения рисков, связанных с обработкой ПДн.

3. Управление нарушениями безопасности данных — выявление инцидентов в сфере кибербезопасности и утечек данных, определение

[172] DPO Competency Framework and Training Roadmap // Personal Data Protection Commission Singapore. URL: https://www.pdpc.gov.sg/dp-competency

[173] DP Roadmap // Personal Data Protection Commission Singapore. URL: https://www.pdpc.gov.sg/-/media/Images/PDPC/DP-Roadmap-v2.png?h=auto&max-width=100%&la=en

фактических обстоятельств и последствий нарушений, принятие мер для устранения или уменьшения масштаба последствий инцидентов и утечек, эффективные коммуникации по поводу нарушений с заинтересованными лицами.

4. Управление заинтересованными сторонами — управление ожиданиями и потребностями сторон (стейкхолдеров), заинтересованных в состоянии защищенности ПДн, с учетом требований и целей организации в целом.

5. Аудит и комплаенс — организация эффективного внешнего и внутреннего мониторинга и контроля (в том числе путем реализации процедур информирования о нарушениях и проведения служебных расследований) за соблюдением применимых норм в области ПДн.

6. Управление данными — разработка и внедрение в деятельность организации принципов и правил надлежащей обработки ПДн на различных этапах их жизненного цикла, а также предоставление активных рекомендаций в отношении обработки данных и устранения утечек данных в различных сложных, неоднозначных или многогранных контекстах.

7. Этика данных — применение этических принципов[174] при формировании процессов обработки ПДн в контексте деятельности организации.

8. Обмен данными — умение адекватно определять ценность ПДн для достижения конкурентного преимущества и (или) целей организации.

9. Навыки дизайн-мышления — руководство методологическими и процессными аспектами дизайн-мышления[175] для решения конкретных задач организации и управление заинтересованными сторонами на этапах определения проблемы, исследования, формирования идеи и ее осуществления.

4.2.3 КОНФЛИКТ ИНТЕРЕСОВ DPO И ЕГО РАБОТОДАТЕЛЯ

Назначая DPO, организация показывает, что управляет всеми процессами и рисками, связанными с обработкой ПДн. В преамбуле GDPR постулируется самостоятельный статус DPO: будучи сотрудником организации или нанятым извне работником, он должен исполнять свои обязанности независимо от воли нанимателя. Для этого DPO не должен быть подчинен какой-либо функции в организации или быть элементом ее управленческого контура, но должен быть наделен необходимыми полномочиями со стороны организации. DPO в ситуации конфликта интересов не сможет качественно выполнять свои функции и задачи. Этот вопрос особенно актуален для России, где эта роль еще не очень распространена и пока не наработана практика разрешения подобных конфликтов.

Рассмотрим несколько моделей конфликта интересов, которые встречаются в организациях довольно часто.

[174] См., например, отчет «Этика данных: проявление морали в технологиях» Всемирной федерации рекламодателей (World Federation of Advertisers, WFA). URL: https://wfanet.org/leadership/data-ethics

[175] См., например, книгу Герберта Саймона «Науки об искусственном» (The Sciences of the Artificial). URL: https://monoskop.org/images/9/9c/Simon_Herbert_A_The_Sciences_of_the_Artificial_3rd_ed.pdf

1. Модель «DPO-босс». Роль DPO выполняет один из руководителей организации, который сталкивается с конкурирующими интересами при принятии решений. Как DPO он должен защищать права и законные интересы субъектов ПДн. Как топ-менеджер (уровня финансового или ИТ-директора) он оценивает «стоимость» своих решений для организации, и на практике интересы компании оказываются для него приоритетны.

2. Модель «DPO-сам-себе-контролер». Роль DPO выполняет сотрудник, принимающий решения в важной области ИТ-инфраструктуры (ИТ-менеджер, системный администратор, ответственный за ведение ИС, в которой обрабатываются ПДн, и др.). DPO вынужден сам контролировать свою работу. Это создает предпосылки для внутреннего конфликта интересов: в большинстве ситуаций для такого сотрудника приоритетны текущие задачи и риски в его основной области.

3. Модель «DPO-мастер-на-все-руки». Роль DPO поручена сотруднику, который выполняет рекомендации, написанные им же. В качестве DPO сотрудник выявляет риски в сфере защиты данных и разрабатывает рекомендации по снижению этих рисков. В роли внутреннего консультанта он разрабатывает локальные документы (согласия, политики, положения и даже техническую документацию) и контролирует их внедрение в организации. В результате конфликта интересов сотрудник упрощает себе задачу — разрабатывает план действий с минимальными затратами времени и сил.

Институт DPO в России развит пока недостаточно, и конфликт интересов начинается уже на этапе выбора DPO. Многие организации не задумываются, кого назначить DPO, или не имеют возможности выбрать сотрудника так, чтобы избежать конфликта интересов. В ст. 22.1 ФЗ-152 «Лица, ответственные за организацию обработки персональных данных в организации» статус DPO описан очень общо. Среди других сотрудников его выделяет ответственность за организацию обработки ПДн, но при этом он получает указания непосредственно от исполнительного органа организации — оператора ПДн и подотчетен ему (в ЕС, в отличие от России, DPO ни от кого не получает указаний в отношении своих обязанностей; но и там возник дефицит квалифицированных специалистов на роль DPO).

Как предотвратить конфликт интересов или хотя бы попробовать им управлять? Есть стандартные отраслевые подходы.

- Определить критерии конфликта интересов и составить внутренний документ о том, какие специалисты могут играть роль DPO, с учетом разъяснений регуляторов и прецедентов.
- Использовать внутренние процедуры по предотвращению и урегулированию конфликта интересов. Очевидный инструмент — подписание будущим DPO декларации об отсутствии конфликта интересов и обязательство уведомлять нанимателя о возникновении конфликта интересов и совместно устранять его в соответствии с существующими процедурами.

› Применять нормы GDPR о конфликте интересов. Согласно ч. 3 ст. 38 компания должна гарантировать, что DPO не получает иных указаний относительно выполнения своих задач, то есть никто не может сказать DPO, каким образом ему проводить оценку. Там же в ч. 2 указано, что DPO не может быть отстранен либо оштрафован нанимателем за выполнение своих задач, а значит, наниматель не может прямо или косвенно воздействовать на DPO таким образом. В ч. 6 указано, что DPO может выполнять иные задачи и обязанности, если они не влекут за собой конфликт интересов. Эта оговорка сделана для компаний с небольшим штатом сотрудников.

Регулирование конфликта интересов DPO — непростая, но решаемая задача. Для ее решения необходимо следовать лучшим практикам, накопленным в сфере комплаенса[176]. Особенность DPO в том, что конфликт интересов связан не только с экономической стороной, с безопасностью организации, но и с публичным интересом — защитой прав субъектов ПДн. Важнейшим инструментом этой защиты является автономность и независимость DPO. Мы уже видим зарождение в нашей стране профессиональной общности DPO, которые придерживаются единых ценностей и принципов работы. В ближайшие годы DPO, скорее всего, станут лицами, принимающими решения и определяющими политику своих нанимателей в сфере обработки ПДн.

4.3 ЕВРОПЕЙСКИЙ ПОДХОД К ЗАЩИТЕ ДАННЫХ В КОНТЕКСТЕ ПАНДЕМИИ

Время чтения — 8 минут

Автор раздела:

Я. Э. Гейн

Пандемия COVID-19 и вызванное ею ускорение цифрового развития привлекли внимание граждан и властей к защите данных. Разработка стандартов и правил обращения с персональными данными необходима для того, чтобы избежать вторжения в частную жизнь граждан, не допустить нецелевого использования данных и их утечек. Европейское регулирование, основанное на регламенте GDPR, в период пандемии показало себя как взвешенный подход к работе с ПДн.

4.3.1 КОНВЕНЦИЯ 108+ И РЕГЛАМЕНТ GDPR

В 1981 году Совет Европы выпустил Конвенцию о защите физических лиц при автоматизированной обработке персональных данных, известную как Конвенция 108 — «первый обязывающий международный инструмент,

[176] Одно из значений слова compliance в английском языке — соблюдение. Применительно к бизнесу этот термин означает регулирование внешней и внутренней деятельности компании в соответствии с требованиями законодательных, этических и социальных норм. См. портал АО «Национальная Юридическая Сеть». URL: https://legal-network.ru/o_komplaens_prostyimi_slovami/45

защищающий физических лиц от злоупотреблений, которые могут иметь место при сборе и обработке данных, и ставящий задачу регулирования трансграничного потока персональных данных»[177]. Документ разъясняет функции и обязанности участников цифровой среды, уделяет особое внимание защите человеческого достоинства и личной автономии при обработке ПДн[178]. Конвенция запрещает обработку чувствительной информации: о расовой принадлежности, здоровье, политических и религиозных взглядах, — если национальное право не обеспечивает надлежащих гарантий защиты этой информации. Также Конвенция дает физическим лицам право знать о факте сбора данных и о содержании собранных данных и в случае необходимости гарантирует возможность внести в них исправления.

Поправки 2018 года[179] ввели более строгие ограничения для сбора данных, расширили понятие чувствительных данных (включив в них генетическую, биометрическую и этническую информацию), обязали организации информировать об утечках данных. Обновленная Конвенция 108+ предполагала более прозрачную обработку данных и в целом расширила права субъекта данных за счет повышения ответственности операторов ПДн[180]. К 2021 году Конвенцию 108+ подписали 55 стран; международный характер делает ее открытой для дальнейшего развития[181].

В России Конвенция вступила в силу в 2013 году[182], а в октябре 2018 года постоянный представитель России при Совете Европы подписал протокол[183] СДСЕ № 223 об изменениях в Конвенцию. В примечании к договору отмечено, что Россия допускает возможность ограничивать права субъектов данных в случае, если это необходимо для обеспечения государственной безопасности и общественного правопорядка[184].

Наиболее значимый из европейских документов — Общий регламент защиты персональных данных (General Data Protection Regulation, GDPR)[185]. Регламент должен обеспечивать баланс между правами субъектов данных

[177] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. No. 108. 1981. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

[178] Terwangne C. Council of Europe convention 108+: A modernised international treaty for the protection of personal data // Computer Law & Security Review. 2020. URL: https://doi.org/10.1016/j.clsr.2020.105497

[179] Modernisation of the Data Protection “Convention 108” // Council of Europe. URL: https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet

[180] Terwangne C. Council of Europe convention 108+: A modernised international treaty for the protection of personal data // Computer Law & Security Review. 2020. URL: https://doi.org/10.1016/j.clsr.2020.105497

[181] Mantelero A. The future of data protection: Gold standard vs. global standard // Computer Law & Security Review. 2020. URL: https://doi.org/10.1016/j.clsr.2020.105500

[182] Chart of signatures and ratifications of Treaty 108 // Council of Europe. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=cN6J4BCa

[183] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data // Council of Europe. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures

[184] Reservations and Declarations for Treaty No. 108 — Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data // Council of Europe. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/declarations

[185] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) // EUR-Lex. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj Русский перевод: URL: https://gdpr-text.com/ru/

и государственными и коммерческими интересами при использовании ПДн: «Право на защиту персональных данных не является абсолютным; оно должно рассматриваться исходя из его функций в обществе и должно быть уравновешено другими основными правами в соответствии с принципом пропорциональности».

Конференция ООН по торговле и развитию (ЮНКТАД) высоко оценила GDPR, заявив, что он «в настоящее время является примером наиболее комплексного подхода к защите данных»[186] и тем самым может претендовать на роль эталона защиты ПДн.

4.3.2 ЗАЩИТА ДАННЫХ В УСЛОВИЯХ ПАНДЕМИИ

При том что регламент GDPR довольно гибок, во время пандемии европейские страны не рассматривали возможность использования данных о местоположении и передвижении пользователей для ограничения контактов. Подобные приложения реализовали Китай[187] и Израиль[188], чем вызвали подозрения в передаче данных правоохранительным органам[189]. Основными аргументами против таких приложений были вмешательство в частную жизнь и посягательство на свободы, а также вероятность организации системы массового наблюдения, которая позволяла бы правительствам продолжать сбор конфиденциальной информации сверх необходимости, в том числе после завершения чрезвычайной ситуации (ЧС)[190].

Во время пандемии большинство стран — участниц Евросоюза запустили национальные сервисы (мобильные приложения) **для оповещения пользователей в случае контактов с носителями вируса**[191]. Приложения устанавливаются добровольно, применяют технологию Bluetooth и не отслеживают местонахождение и передвижение пользователей.

В апреле 2020 года Еврокомиссия выпустила Рекомендацию 2020/518[192] о наборе технологий и данных для борьбы с кризисом COVID-19. Следует, в частности, **предотвращать деанонимизацию и идентификацию** лиц посредством соответствующего уровня защиты данных, провести оценку рисков повторной идентификации при сопоставлении анонимизированных данных с другими данными; гарантировать немедленное и необратимое

[186] Доклад о цифровой экономике 2019 // ЮНКТАД. URL: https://unctad.org/system/files/official-document/der2019_overview_ru.pdf

[187] Mozur P., Zhong R., Krolik A. In coronavirus fight, China gives citizens a color code, with red flags // New York Times. 2020. URL: https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html

[188] Amit M., Kimhi H., Bader T. et al. Mass-surveillance technologies to fight coronavirus spread: the case of Israel // Nature Medicine. 26. 1167–1169 (2020). URL: https://doi.org/10.1038/s41591-020-0927-z

[189] Ram N., Gray D. Mass surveillance in the age of COVID-19 // Journal of Law and the Biosciences. V. 7. I. 1. 2020. URL: https://doi.org/10.1093/jlb/lsaa023

[190] Ventrella E. Privacy in emergency circumstances: data protection and the COVID-19 pandemic // ERA Forum 21. 379–393 (2020). URL: https://doi.org/10.1007/s12027-020-00629-3

[191] Mobile contact tracing apps in EU Member States // European Commission. URL: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/mobile-contact-tracing-apps-eu-member-states_en

[192] Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data // EUR-Lex. URL: https://eur-lex.europa.eu/eli/reco/2020/518/oj

удаление всех случайно собранных и обработанных данных, позволяющих идентифицировать пользователей, ограничить обработку данных целями, указанными выше, и исключить передачу данных третьим лицам.

Европейский совет по защите данных (European Data Protection Board, EDPB) признал[193], что даже в условиях ЧС должна быть обеспечена защита личных данных, а **любые принимаемые меры должны соответствовать общим принципам права**. Закон позволяет ограничить права граждан, если эти ограничения соразмерны и действуют только в условиях ЧС.

EDPB подчеркнул, что широкомасштабный мониторинг контактов между физическими лицами является «серьезным вторжением в частную жизнь людей»[194]. Поэтому **установка приложений должна быть добровольной**, а те, кто их не использует, не должны испытывать неудобства.

Директива 2002/58/ЕС[195] разъясняет, что данные о местоположении могут законно обрабатываться только после того, как были обезличены (анонимизированы)[196]. Обезличивание данных не допускает возможности обратного действия, то есть деанонимизации. Тем самым агрегированные статистические данные об использовании приложений для отслеживания контактов, не позволяющие идентифицировать конкретных физических лиц, не считаются личными данными и не подпадают под действие GDPR. Это верно и для агрегированных статистических данных о здоровье.

В большинстве случаев сервисы работают децентрализованно без агрегации данных в единую базу. При использовании централизованных решений данные хранят на защищенных серверах национального органа здравоохранения. Схема работы[197] сервиса представлена на рисунке 11.

Мобильные приложения, запущенные для борьбы с пандемией, обрабатывают не только данные о контактах пользователей; они также используют **данные тестирования на COVID-19**, которые пользователи самостоятельно загружают в приложение. Последние относятся к данным о здоровье, которые Еврокомиссия классифицирует как чувствительную информацию; их использование требует соблюдения особых условий[198]. Согласно ст. 9 GDPR обработка данных о здоровье возможна только при

[193] Statement on the processing of personal data in the context of the COVID-19 outbreak // European Data Protection Board. 2020. URL: https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-processing-personal-data-context-covid-19-outbreak_en

[194] Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak // European Data Protection Board. 2020, April 21. URL: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

[195] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) // EUR-Lex. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0058

[196] What is personal data? // European Commission. 2021. URL: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

[197] Digital Warfare Against COVID-19: Global Use of Contact-Tracing Apps // Asia Pacific Journal of Public Health. URL: https://pubmed.ncbi.nlm.nih.gov/33715449/

[198] What personal data is considered sensitive? // European Commission. URL: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en

Рисунок 11. Схема централизованной и децентрализованной моделей цифрового отслеживания контактов

согласии субъекта данных на их обработку для одной или нескольких обозначенных целей.

Основные принципы работы мобильных приложений для отслеживания контактов в странах — участницах ЕС (Рекомендация 2020/518) выглядят следующим образом.

- Добровольность установки и использования приложения; отсутствие негативных последствий для тех, кто отказался от его использования.
- Минимизация используемых данных: собираются только те данные, которые необходимы для работы сервиса, и не более того.
- Приложения должны использовать данные о дистанции между пользователями, полученные с помощью технологии Bluetooth (приложение не запрашивает и не использует данные о местоположении, не отслеживает передвижения людей).
- Данные должны быть защищены с помощью современных методов, включая шифрование.
- Данные не должны храниться дольше необходимого.
- Приложения должны быть централизованно деактивированы, как только пандемия закончится.

Регламент GDPR прошел первое серьезное испытание, продемонстрировав, как можно поддерживать баланс между сохранением конфиденциальности и общественными интересами в чрезвычайных обстоятельствах.

4.4 ОЦЕНКА ВОЗДЕЙСТВИЯ ОБРАБОТКИ ДАННЫХ (DPIA)

Авторы раздела:

К. И. Боровикова

Е. К. Волкович

Р. В. Мартинсон

Время чтения — 6 минут

Оценка воздействия обработки ПДн на права и свободы субъекта данных (англ. Data Protection Impact Assessment, DPIA) входит в число требований регламента GDPR. Такая оценка позволяет понять, создает ли обработка риски для субъектов ПДн. В случаях, когда тип обработки ПДн создает риски, оператор ПДн должен их оценить до начала процесса и в случае изменения процесса[199].

Оценка воздействия обработки данных DPIA позволяет понять, создает ли обработка данных риски для субъектов ПДн, и необходима в случаях, когда имеет место:

- систематическая и глубокая оценка личностных качеств физических лиц, основанная на автоматизированной обработке ПДн (в том числе профилировании), причем эта оценка используется для принятия решений, имеющих юридические последствия для физического лица или существенно влияющих на него;
- обработка в большом объеме специальных категорий ПДн, упомянутых в ст. 9 (1) GDPR, или обработка ПДн, относящихся к сведениям о судимости и совершенных преступлениях (указанных в ст. 10 GDPR);
- мониторинг общедоступных мест в большом объеме.

В соответствии с разъяснениями[200] рабочей группы WP29[201] и рекомендациями по проведению DPIA[202] оценка необходима, если в процессе обработки ПДн имеет место:

- скоринг;
- профилирование и прогнозирование;
- автоматизированное принятие решений с юридическим или аналогичным значимым эффектом;
- систематический мониторинг;
- обработка чувствительной информации;

[199] В разделе приведена общая характеристика методики оценки рисков. Для получения полной информации о методике см.: Практическое руководство по соответствию требованиям GDPR. Опыт работы КПМГ с требованиями GDPR // KPMG. URL: https://assets.kpmg/content/dam/kpmg/ru/pdf/2021/05/ru-ru-gdpr-guide.pdf

[200] Разъяснения WP29 по DPIA см.: Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01) // European Commission. URL: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

[201] Article 29 Data Protection Working Party (WP29) — рабочая группа, созданная во исполнение ст. 29 Директивы 95/46/ЕЭЗ. Этот консультативный орган состоял из представителей регуляторов: Европейского союза по защите данных, Европейского наблюдателя по вопросам защиты данных (European Data Protection Supervisor, EDPS) и Еврокомиссии. 25 мая 2018 года рабочая группа WP29 была заменена на Европейский совет по защите данных.

[202] List of processing operations requiring data protection impact assessment (DPIA) pursuant to Art. 35, paragraph 4 of Regulation (EU) 2016/679 // Republic of Bulgaria. Commission for Personal Data Protection. URL: https://www.cpdp.bg/en/index.php?p=element&aid=1186

- широкомасштабная обработка ПДн;
- сопоставление или объединение баз данных;
- обработка данных об уязвимых субъектах ПДн (например, детях, сотрудниках, инвалидах, пациентах);
- инновационное использование или применение новых технологических или организационных решений.

Согласно рекомендациям упомянутого выше надзорного органа CNIL[203] и разъяснениям WP29, для оценки воздействия обработки данных на права и свободы субъектов ПДн следует определить контекст обработки ПДн, необходимость и соразмерность операций обработки ПДн; оценить риски для субъекта, связанные с обработкой ПДн; разработать рекомендации по митигированию выявленных рисков (то есть смягчению последствий в случае их реализации).

Предлагаемые надзорными органами подходы к оценке рисков позволяют провести качественную, но не количественную оценку рисков, а качественная оценка может быть субъективной и неточной. При оценке рисков также рассматривается возможность несанкционированного изменения ПДн, незаконного доступа к ПДн, уничтожения ПДн, то есть проводится **анализ возможных последствий в случае нарушения конфиденциальности, целостности и доступности ПДн.** Оценивается вероятность реализации угроз, связанных с уязвимостью средств обработки данных, оценивается возможный ущерб для субъектов ПДн (финансовый, моральный или ущерб репутации).

Анализ реестра нарушений и штрафов, связанных с обработкой и защитой ПДн[204], позволяет оценить вероятность реализации риска и рассчитать вероятную величину ущерба. Методология количественной оценки рисков нарушения требований GDPR, разработанная консалтинговой компанией KPMG, состоит из следующих этапов.

1. Вычисление вероятности реализации риска.
2. Вычисление ущерба для компании от реализации риска.
3. Вычисление статистического значения риска.
4. Построение графиков распределения, расчет отклонения, определение значения статистических величин.
5. Экспертная оценка уровня подготовленности организации на основании интервью и разработанных документов (см. таблицу 2).
6. На основании полученных оценок рисков и их соотношения вырабатывается шкала критериев, позволяющих определить уровень риска. Риск с наименьшей оценкой является низким, риск с наибольшей оценкой — высоким.

[203] Методические рекомендации CNIL по оценке воздействия на конфиденциальность данных см.: Privacy Impact Assessment (PIA) // CNIL. URL: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf

[204] Компания КПМГ, в которой работают авторы раздела, ведет такой реестр. КПМГ — международная сеть фирм, предоставляющих аудиторские, налоговые и консультационные услуги.

Таблица 2. Уровень соответствия организации требованиям GDPR

Меры и принципы	Насколько они приняты/выполняются		
Организационные и технические меры защиты	Приняты	Частично приняты	Не приняты
Принципы обработки ПДн	Выполняются	Частично выполняются	Не выполняются
Меры для реализации прав субъектов ПДн	Приняты	Частично приняты	Не приняты
Уровень соответствия требованиям GDPR	Высокий	Средний	Низкий

В зависимости от полученных результатов организация может принять решение о внедрении соответствующих мер защиты, например ввести дополнительные функции в системах обработки ПДн, использовать соглашения о защите ПДн с операторами, установить дополнительные средства защиты, шифровать данные. Также можно изменить сам процесс обработки ПДн, отказаться от сбора определенных категорий ПДн (например, специальных категорий) или ограничить географический охват обработки ПДн, не обрабатывать ПДн физических лиц, находящихся на территории стран — участниц Европейской экономической зоны (ЕЭЗ).

С точки зрения российского законодательства операторы ПДн обязаны в соответствии с ч. 1 ст. 18.1 ФЗ-152 принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных законом и принятыми в соответствии с ним НПА. Организация самостоятельно определяет состав и перечень мер, необходимых и достаточных для выполнения ФЗ-152. К таким мерам могут, в частности, относиться оценка вреда, который может быть причинен субъектам ПДн в случае нарушения ФЗ-152, соотношение указанного вреда и принимаемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ-152. Определение угроз безопасности ПДн, актуальных для ИС, производится с учетом оценки возможного вреда. В ФЗ-152 отсутствуют требования к методам и способам оценки вреда субъектам ПДн, однако в государственных и муниципальных учреждениях обязательна к использованию «Методика оценки угроз безопасности информации», утвержденная ФСТЭК России 5 февраля 2021 года[205].

Описанная выше методика широко используется в европейских организациях, в том числе в госсекторе. В России госорганизации могут применять эту методику по своему усмотрению в качестве дополнительной — для расчета рисков, приоритизации угроз и повышения уровня приватности в организации.

[205] Методика оценки угроз безопасности информации // ФСТЭК России. 05.02.2021. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021-g

ВЫВОДЫ. КАК ЗАЩИТИТЬ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

В концепции PbDD (Privacy by Default и Privacy by Design) описаны принципы управления персональными данными. Хранить и обрабатывать ПДн будет проще, быстрее и безопаснее, если собирать минимум необходимых данных и ограничивать доступ к ним (Privacy by Default), заранее продумывать процедуры обработки и учитывать их на этапе проектирования (Privacy by Design). Соблюдать концепцию PbDD для оператора данных означает защищать данные пользователей и их право на неприкосновенность частной жизни (приватность) в качестве настройки по умолчанию.

Концепция PbDD легла в основу GDPR и в значительно меньшей степени — ФЗ-152. И хотя в настоящее время российское законодательство прямо не требует соблюдать принципы концепции PbDD, их уже применяют в коммерческих организациях для снижения вероятности возникновения проблем с ПДн в будущем, предотвращения рисков и в целом в качестве конкурентного преимущества. Поэтому институт DPO (в России — «лицо, ответственное за обработку персональных данных») развивается последние годы в коммерческом секторе. Многие из рекомендаций по работе DPO, описанные в регламенте GDPR, не противоречат ФЗ-152, и их можно уже сейчас применять в России.

«Российское государство не очень-то заинтересовано в сохранении приватности граждан. Я думаю, оно довольно легко поддастся на лоббирующее давление частных компаний и легализует коммерческий оборот данных. У нас присутствует тенденция к коммерциализации, и, скорее всего, в нынешних экономических условиях она будет только усиливаться».

Эльвира Талапина, главный научный сотрудник Института государства и права РАН

Для государственных органов внимательное отношение к ПДн и защите права на приватность служит инструментом укрепления репутации и повышения доверия граждан. Использование лучших практик в сфере защиты приватности, комплаенса, оценки рисков, накопленного опыта разрешения конфликтов в работе DPO позволяет избежать многих потенциальных проблем и при этом повысить уровень защиты ПДн в организации.

5. ДОВЕРЕННЫЙ ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: КОНЦЕПЦИЯ И ДОКУМЕНТЫ

— Любая новая техника требует в начальной стадии жертв. Мольтерис сконструировал одноместный времяходик безо всяких предохранительных устройств. Он поступил точь-в-точь как тот средневековый мужик, который, нацепив крылья, влез на колокольню и тут же разбился.

С. Лем. Звездные приключения Ийона Тихого

5.1 РАЗВИТИЕ ИИ В КОНТЕКСТЕ ЭТИКИ

Время чтения — 17 минут

Из всех рассматриваемых в докладе тем этика искусственного интеллекта — наиболее обсуждаемая в СМИ и вызывающая наибольшие споры. Причины этого лежат как в области социальных представлений об ИИ как о чем-то совершенно особенном и уникальном, так и в объективных отличиях этики ИИ от прочих дисциплин.

5.1.1 ДВА АСПЕКТА ЭТИКИ В ОБЛАСТИ ИИ

Принципиально важно, что «система ИИ способна самостоятельно принимать решения, касающиеся человека, и анализировать данные в таких объемах и с такой скоростью, как человек делать не в состоянии (следовательно, человек не может физически проверить верность решений)»[206]. Тем самым одной из основных проблем, связанных с интеллектуальной автономной

[206] Об этом авторы раздела подробно писали в предыдущем докладе: Зачем искусственному интеллекту этика? // Этика и «цифра»: этические проблемы цифровых технологий. В 2 т. М.: РАНХиГС, 2020. URL: https://ethics.cdto.center/3_1

системой (ИАС)[207], является определение того, насколько решения, принятые системой в рамках ее автономности, соответствуют этическим нормам. Не менее значим и второй аспект этики в области ИИ — риски и социальные последствия внедрения ИАС (например, риск безработицы при замене тех или иных профессий ИС, риски дискриминации и предубежденности алгоритмов и т. д.). Два разных аспекта этики в области ИИ представлены на рисунке 12. Отметим также, что, хотя мы и говорим об этике в области ИИ как об отдельной сфере, ее ни в коем случае нельзя рассматривать обособленно от вопросов техноэтики и этики науки, уже десятилетиями обсуждаемых в научном и практическом ключе, и от широкого спектра проблем, связанных с взаимодействием людей между собой, с обществом и государством в связи с использованием ИИ.

Первый аспект (принятие решений) состоит в том, что отдельные виды систем ИИ, созданные разработчиками, могут обладать значительным уровнем автономности, самосовершенствоваться, реструктурироваться, улучшать свои параметры и пр. Создавая ИАС, которая принимает критически важные для человека решения, мы хотим получить гарантии, что эти решения этичны, а для этого должны привнести этичность в саму технологию ИИ. Сложность состоит в том, что моральный выбор — это выбор, который определяется не четкими нормами закона, а правилами, принципами, личными взглядами и всем тем, что описывается категориями «хорошо» или «плохо». Более того, набор этих принципов сильно зависит как

ИИ – искусственный интеллект
ИАС – интеллектуальная автоматизированная система

Рисунок 12. Основные аспекты этики ИАС

[207] С точки зрения теории и методологии наиболее корректным является термин «интеллектуальная автономная система», однако в связи с широким распространением терминов «ИИ» и «система ИИ» в докладе встречаются все три варианта.

Авторы раздела:


П. М. Готовцев


А. В. Незнамов


А. Г. Игнатьев


Е. Г. Потапова


М. В. Федоров

от исторического периода, так и от конкретного социума. Соответственно, его сложно формализовать и заложить в ИИ, он требует обсуждения с обществом, специалистами в области гуманитарных наук (философами, социологами, историками, антропологами), представителями религиозных конфессий.

Второй аспект (внедрение) подразумевает анализ и предотвращение этических коллизий, возникающих в процессе применения ИИ. К таким коллизиям относятся нарушение приватности, возможная дискриминация, социальное расслоение, проблемы трудоустройства и т. д. Отдельно стоит тема профессиональной этики разработчиков систем ИИ; она также требует рассмотрения, уже создаются этические кодексы и рекомендации для разработчиков.

Для полноты картины приведем три разноплановых определения этики ИИ из различных источников.

Этика в области ИИ — это область прикладной этики, в которой изучаются этические вопросы, связанные с разработкой, внедрением и использованием искусственного интеллекта. Основная задача этики ИИ — определить, как ИИ может развиваться и какие проблемы, касающиеся благополучия человека (в том числе качества жизни, автономии и свободы, необходимой для существования демократического общества), могут возникнуть в связи с его развитием[208]. (Группа экспертов высокого уровня по ИИ Еврокомиссии)

Этика в области ИИ — это организационная конструкция (корпоративные ценности, политики, этические кодексы и руководства), которая разграничивает «правильное» и «неправильное» в отношении использования ИИ[209]. (Deloitte)

Этика в области ИИ — это комплекс ценностей, принципов и методов, основанных на общепринятых критериях добра и зла, который определяет моральное поведение при разработке и использовании технологий ИИ[210]. (Институт Тьюринга)

Ряд тем, важных для понимания этики ИИ, был рассмотрен в докладе «Этика и „цифра“: этические проблемы цифровых технологий» (включая риски неэтичного применения ИИ, вопросы создания машинной этики, регулирование ИИ); в этом разделе речь пойдет в основном об изменениях в этой области, которые произошли с момента выхода первого доклада, а также о нескольких концепциях в области этики ИИ, которые не обсуждались нами ранее.

---

[208] Ethics guidelines for trustworthy AI // European Commission. URL: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

[209] AI ethics: A business imperative for boards and C-suites // Deloitte. URL: https://www2.deloitte.com/us/en/pages/regulatory/articles/ai-ethics-responsible-ai-governance.html

[210] Leslie D. Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector // The Alan Turing Institute. URL: https://www.turing.ac.uk/sites/default/files/2019-06/understanding_artificial_intelligence_ethics_and_safety.pdf

«Сегодня в некоторых проектах документов по развитию ИИ делается попытка создать и формализовать некую новую „цифровую этику“ для человека и машины; при этом этику в области ИИ рассматривают как вновь возникшее и обособленное явление цивилизационного развития, отбрасывая не только многовековой философский дискурс, идущий от Сократа, Платона и Аристотеля, но и важнейшие исследовательские наработки в технонауке и философии техники. Не всегда учитываются и современные нормы и положения, уже разработанные в информационной этике, в компьютерной этике, в этических кодексах для инноваторов, в стандартах социально ответственного поведения».

Андрей Игнатьев, руководитель направления аналитики Центра глобальной ИТ-кооперации

Другой важной проблемой является научно выверенное и обоснованное понимание места и роли этики в общем процессе развития и регулирования технологии. При формировании инструментов регулирования не должен уходить на второй план традиционный инженерно-технический подход, основанный в том числе на инструментальной оценке рисков, обеспечении безопасности, методиках измерения и тестирования. Поэтому краткий обзор документов, представленный в разделе 5.3, содержит не только регуляторные документы и кодексы, но и технические стандарты.

За последние два года в общественном сознании произошел перелом: в России о цифровой этике заговорили в высоких кабинетах, она всерьез заинтересовала университеты и компании. Идет работа над несколькими важными проектами, и есть шанс, что в скором времени мы увидим интересные научные публикации в этой области.

В России действует сообщество экспертов в области этики ИИ, которое объединяет представителей науки, бизнеса, образования. Эта область развивается и в научном плане, и в плане стандартизации (см. раздел 5.3), и в поле общественных дискуссий. Российские специалисты активно включились в эту работу и в мировой науке, и в нормативном регулировании (обсуждаются российские стандарты, стандарты ISO и IEEE выпускаются с российским участием и т. д.). На нескольких крупных конференциях[211] с участием разработчиков, исследователей, представителей бизнеса обсуждалась этика ИИ; известные лица, в том числе президент России, говорили об этом в своих выступлениях[212].

Из новых трендов следует отметить сегментацию исследований: появляются работы, посвященные этике применения ИИ **в узких областях**,

[211] Вот некоторые из конференций, состоявшиеся в 2020 и 2021 годах: Национальный Конгресс по когнитивным исследованиям, искусственному интеллекту и нейроинформатике (РАН), URL: https://caics.ru; «Этико-правовые проблемы цифровой трансформации: от конфликта к гармонии» (НИУ ВШЭ), URL: https://digitallaw.hse.ru/announcements/408477372.html; Skolkovo AI 2020, URL: https://ai.sk.ru/#program; AI 2021 — reality and possibilities (МГИМО), URL: https://mgimo.ru/about/news/main/ai-2021-reality-and-possibilities/

[212] Президент России В. В. Путин принимал участие в международных конференциях AI Journey Сбербанка, которые состоялись в 2019 и 2020 годах. См.: Конференция по искусственному интеллекту // Президент России. URL: http://www.kremlin.ru/events/president/transcripts/62003 (2019 год) и http://www.kremlin.ru/events/president/news/64545 (2020 год)

в первую очередь в области медицины (см. об этом раздел 3.2). Самый яркий пример — это ответственное использование результатов ИИ-обработки так называемых brain data (данных ЭЭГ, фМРТ и т. п.). Если считать чувствительными, к примеру, данные о перемещениях человека, то максимально чувствительными будут данные, полученные от медицинских и немедицинских нейротехнологических устройств[213].

Другие очевидные тренды — это интеллектуальные программы для смартфонов и прочих **смарт-устройств**; **автономные машины** и все связанные с ними этические вопросы; доставка дронами; «умный» город и системы слежения за городом. Активно развивается **анализ метаданных**, особенно собираемых с носимых устройств и «умных» домов.

Во многих проектах, предложенных на финском конкурсе устойчивого развития городов Helsinki Energy Challenge[214], ключевым элементом была интеллектуальная система управления расходом тепла и электроэнергии. ИИ стал важнейшим элементом управления тепловыми сетями, позволив исключить ископаемое топливо из систем теплоснабжения и электроснабжения. Без интеллектуальных систем управления сегодня было бы сложно добиться максимума эффективности от подобных технологий. За счет тонкого и максимально точного регулирования, реализуемого с помощью ИИ, такие системы становятся окупаемыми и начинают конкурировать с ископаемым топливом.

Возникает новый аспект приватности[215] — все, что относится к жилищу: по датчикам контроля температуры и освещения можно узнать, как часто жилец бывает дома, что он там делает и т. д. Эта область приватности относится к описанному выше (см. раздел 2.1.2) анализу метаданных, когда максимальное количество данных о человеке — активность в соцсетях, данные датчиков, видеокамер и т. д. — собирают, совмещают и получают полную картину его жизни, деятельности, эмоций и контактов.

5.1.2 ПОЛИТИКА РОССИИ В СФЕРЕ ИИ

В августе 2020 года президиум правительственной комиссии по цифровому развитию под руководством вице-премьера Д. Н. Чернышенко утвердил федеральный проект «Искусственный интеллект» национальной программы «Цифровая экономика Российской Федерации». Основаниями для разработки проекта послужили Концепция регулирования технологий ИИ и робототехники до 2024 года[216] и Национальная стратегия развития

[213] Kellmeyer P. Big Brain Data: On the Responsible Use of Brain Data from Clinical and Consumer-Directed Neurotechnological Devices // Neuroethics. 2021. Vol. 14. P. 83–98. URL: https://link.springer.com/article/10.1007/s12152-018-9371-x

[214] Helsinki Energy Challenge. URL: https://energychallenge.hel.fi/; Helsinki announces energy challenge winners // Smart Cities World. URL: https://www.smartcitiesworld.net/news/news/helsinki-announces-energy-challenge-winners-6194

[215] Понятие приватности // Этика и «цифра»: этические проблемы цифровых технологий. В 2 т. М.: РАНХиГС, 2020. URL: https://ethics.cdto.center/5_1

[216] Распоряжение Правительства РФ от 19.08.2020 № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» // КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_360681/

искусственного интеллекта на период до 2030 года[217]. Задачи, поставленные Национальной стратегией, вошли в федеральный проект[218]:

1) поддержка научных исследований;

2) создание комплексной системы правового регулирования, разработки и развития программного обеспечения;

3) повышение доступности и качества данных;

4) увеличение доступности аппаратного обеспечения;

5) рост обеспеченности квалифицированными кадрами;

6) повышение уровня информированности населения.

Проект состоит из нескольких блоков, за которые отвечают разные министерства: Минэкономразвития курирует мероприятия по развитию экосистемы ИИ, Минкомсвязи — мероприятия по внедрению ИИ и формированию наборов данных, Минпромторг реализует разработку отечественных аппаратных комплексов и микросхем[219]. В конце 2020 года вице-премьер Д. Н. Чернышенко дал поручение Минцифре создать реестр готовых решений в сфере ИИ для внедрения в федеральных ведомствах, а всем ФОИВ — сформировать дата-сеты для ИИ. Минэнерго, Минпромторг, Минкультуры, Минобрнауки, Росреестр, Россельхознадзор, ФНС уже представили проекты по внедрению ИИ-решений в своих ведомствах и формированию отраслевых дата-сетов. В перечень решений на основе ИИ, которые будут внедряться в 2023–2024 годах[220], входят в том числе:

1) Минздрав — технологии анализа рентгеновских снимков и КТ-изображений для выявления новообразований и признаков COVID-19;

2) МВД — технологии идентификации лиц, анализа биоматериала, выявления взаимосвязей между событиями;

3) МЧС — технологии анализа спутниковых снимков для выявления ЧС, создание голосовых помощников;

4) Росреестр — технологии анализа изображений для классификации объектов капитального строительства.

Разработки в области создания доверенных систем и этичного ИИ относятся к первой из шести задач — поддержке научных исследований. Также в федеральном проекте вопросы этики ИИ отражены в ряде мероприятий. В частности, планируется широкая дискуссия по ключевым вопросам этики применения ИИ в формате ежегодного форума «Этика применения ИИ» (первый форум должен состояться в 2021 году). Идея в том, чтобы дать возможность высказаться всем желающим: этика в области ИИ пока не сформирована, и формировать ее должно общество в целом. Федеральный

[217] Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» // ГАРАНТ.ру. URL: https://www.garant.ru/products/ipo/prime/doc/72738946/

[218] Утверждена Указом Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации». URL: https://www.garant.ru/products/ipo/prime/doc/72738946/

[219] Национальная стратегия развития искусственного интеллекта // TAdviser. URL: https://www.tadviser.ru/index.php/Статья:Национальная_стратегия_развития_искусственного_интеллекта

[220] Реестр готовых решений в сфере искусственного интеллекта для федеральных ведомств // TAdviser. URL: https://www.tadviser.ru/index.php/Продукт:Реестр_готовых_решений_в_сфере_искусственного_интеллекта_для_федеральных_ведомств

проект предполагает развитие международного сотрудничества, в том числе в части определения правовых этических норм (Россия активно участвует в этом процессе, см. раздел 5.3.2.) Еще один ключевой документ — Концепция регулирования технологий ИИ и робототехники до 2024 года[221], которая, в частности, закрепила приоритет базовых этических норм при разработке технологий ИИ[222]:

- регуляторное воздействие, основанное на риск-ориентированном междисциплинарном подходе и предусматривающее принятие ограничительных норм в случае, если применение технологий ИИ и робототехники (РТ) несет объективно высокий риск причинения вреда участникам общественных отношений, правам человека и интересам общества и государства;
- расширение применения инструментов урегулирования и саморегулирования, формирование кодексов (сводов) этических правил разработки, внедрения и применения технологий ИИ и РТ;
- человекоориентированный подход, предусматривающий в качестве конечной цели развития технологий ИИ и РТ обеспечение защиты гарантированных российским и международным законодательством прав и свобод человека и повышение качества жизни граждан;
- оценка воздействия технологий и систем ИИ и РТ на все сферы жизни человека, общества и государства, основанная на научно выверенных исследованиях с подключением широкого круга ученых;
- обеспечение баланса интересов разработчиков, потребителей и иных лиц в сфере ИИ и РТ, а также определение границ их ответственности за возможные негативные последствия использования технологий;
- оценка при разработке НПА и иных документов в сфере ИИ и РТ социально-экономических последствий и рисков в условиях постоянного развития технологий, учет как положительного, так и отрицательного международного опыта регулирования.

Развитие технологий должно основываться на базовых этических нормах и предусматривать:

- приоритет благополучия и безопасности человека, защиты его основополагающих прав и свобод;
- запрет на причинение вреда человеку по инициативе систем ИИ и РТ;
- подконтрольность человеку (в той мере, в которой это возможно с учетом требуемой степени автономности систем ИИ и РТ);
- проектируемое соответствие закону, в том числе требованиям безопасности (применение систем ИИ не должно с ведома разработчика приводить к нарушению правовых норм);
- недопущение противоправной манипуляции поведением человека.

[221] Распоряжение Правительства РФ от 19.08.2020 № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» // КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_360681/

[222] Развитие искусственного интеллекта // Минэкономразвития РФ. URL: https://www.economy.gov.ru/material/departments/d01/razvitie_iskusstvennogo_intellekta/

У концепции есть только два аналога: «Белая книга об искусственном интеллекте: европейский подход к совершенству и доверию»[223] и указ президента США, подписанный в декабре 2020 года, об этических границах использования ИИ в американском госуправлении[224]. В августе 2020 года правительство России объявило о начале создания рабочих документов по реализации концепции; назначенные руководители цифровой трансформации (РЦТ) приступили к разработке планов и мероприятий[225].

Среди основных отечественных документов следует также упомянуть ряд стандартов. В 2019 году в России создан Технический комитет по стандартизации № 164 «Искусственный интеллект» (ТК 164)[226]. В его состав входит подкомитет «Искусственный интеллект в здравоохранении», разрабатывающий национальные и международные стандарты, которые распространяются на требования к разработке, проведению испытаний, а также применению и эксплуатации медицинского программного обеспечения (ПО), работающего на основе ИИ (подробнее о «цифре» в медицине см. раздел 3.2).

В 2019 году принят национальный стандарт «Информационные технологии. Большие данные. Обзор и словарь»[227]. Также утверждена Перспективная программа стандартизации по приоритетному направлению «Искусственный интеллект» на период 2021–2024 годов. К числу перспективных стандартов относится рассмотренный выше ГОСТ Р 59276-2020 «Системы искусственного интеллекта. Способы обеспечения доверия. Общие положения».

«Европа настроена на жесткое регулирование даже в тех вопросах, где нет очевидного консенсуса. Российский путь пока выглядит более адекватным. Анализируя деятельность международных органов (ЮНЕСКО, Совета Европы, ОЭСР, ОБСЕ) и международного агентства по стандартизации, я понимаю, что в России пока удивительным образом складывается очень здравое восприятие ситуации и регулятором, и бизнесом».

Андрей Незнамов, управляющий директор Центра регулирования ИИ ПАО «Сбербанк»

Государству и обществу равно нужны и этические кодексы, и стандарты, гайдлайны, практические руководства. Важно понимать разницу между ними и уметь использовать разные инструменты во благо. Так, кодекс этики ИИ — это высокоуровневый и короткий документ, который должен

[223] White paper on Artificial Intelligence — A European approach to excellence and trust // European Commission. URL: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

[224] Executive Order 13960 of December 3, 2020. Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government // Federal Register. URL: https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government

[225] Дмитрий Чернышенко принял участие в стратегической сессии по искусственному интеллекту для руководителей цифровой трансформации // Правительство России. URL: http://government.ru/news/40262/

[226] Технический комитет по стандартизации № 164 «Искусственный интеллект». URL: https://www.tc164.ru/

[227] ГОСТ Р ИСО/МЭК 20546-2019 «Информационные технологии. Большие данные. Обзор и словарь». М.: Стандартинформ, 2020. URL: https://api.bigdata-msu.ru/media/uploads/2020/05/06/1-025-20-20546-2019-end.pdf

задавать опорные точки, а технические стандарты должны быть, наоборот, подробными: они позволяют настолько детально описать ситуацию, насколько это нужно в данный конкретный момент для данной конкретной технологии.

В России первой этической инициативой крупного бизнеса стал кодекс этики ИИ Сбера. В нем описаны принципы этики в области ИИ: контролируемость и управляемость систем ИИ, прозрачность и предсказуемость функционирования, стабильность и надежность систем ИИ, ответственное применение ИИ, непредвзятый ИИ)[228].

Одна из задач федерального проекта «Искусственный интеллект» касается регулирования этических вопросов. В последний год в России экспертным сообществом и представителями бизнеса ведется разработка универсального Кодекса этики в области ИИ. Сам кодекс (или его проект) пока не опубликован, но представление о его содержании можно получить из общественных обсуждений, в частности на секции «Новые технологии. Искусственный интеллект и этика» Российского форума по управлению интернетом (RIGF 2021)[229]. Исследователи и инженеры из России активно участвуют в больших международных проектах, связанных с этикой ИАС и инициированных ЮНЕСКО, Еврокомиссией, крупнейшими международными организациями по стандартизации (ISO, IEEE), о чем будет подробнее сказано далее.

Авторы раздела:

П. М. Готовцев

Е. Г. Потапова

М. В. Федоров

5.2 КОНЦЕПЦИЯ ДОВЕРЕННОГО ИИ

Время чтения — 23 минуты

Доверенный искусственный интеллект — одна из ведущих концепций в области этичного ИИ. Термин «доверенный» используется в ряде международных и российских документов. Доверенный ИИ отвечает таким критериям, как прозрачность, безопасность, робастность, техническая устойчивость и другие.

5.2.1 ОПРЕДЕЛЕНИЕ И ОСОБЕННОСТИ

Понятие доверенного (англ. trustworthy, буквально ‘заслуживающий доверия, достойный доверия’) искусственного интеллекта зафиксировано в «Руководстве по этике для надежного ИИ» Группы экспертов высокого уровня по искусственному интеллекту Еврокомиссии (Ethics guidelines for trustworthy AI, 2019)[230].

[228] Принципы этики искусственного интеллекта Сбера // Сбербанк. URL: https://www.sberbank.com/ru/sustainability/principles-of-artificial-intelligence-ethics

[229] Видеозапись секции см.: URL: https://rigf.ru/press/?p=video&vid=pdTQahZV5TQ

[230] Ethics guidelines for trustworthy AI // European Commission. URL: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

Согласно этому документу, доверенный ИИ должен обладать следующими базовыми характеристиками:

- **законный** — соответствующий применимому законодательству;
- **этичный** — соответствующий этическим принципам и ценностям;
- **робастный** — надежный с технической точки зрения и разработанный с учетом актуального социального контекста.

В России понятие доверенного ИИ с марта 2021 года отражено в стандарте ГОСТ Р 59276-2020 «Системы искусственного интеллекта. Способы обеспечения доверия. Общие положения»[231].

Доверие к системам искусственного интеллекта является важнейшим условием, определяющим возможность применения этих систем при решении ответственных задач обработки данных. Примерами таких задач являются поддержка принятия врачебных решений, беспилотное управление транспортными средствами и некоторые другие, ошибки при решении которых могут привести к тяжким последствиям, связанным с угрозой жизни и здоровью людей, серьезным экономическим и экологическим ущербом.

Доверие к системе искусственного интеллекта — уверенность потребителя и, при необходимости, организаций, ответственных за регулирование вопросов создания и применения систем искусственного интеллекта, и иных заинтересованных сторон, в том, что система способна выполнять возложенные на нее задачи с требуемым качеством.

Доверенная система искусственного интеллекта — система искусственного интеллекта, в отношении которой потребитель и, при необходимости, организации, ответственные за регулирование вопросов создания и применения систем искусственного интеллекта, проявляют доверие.

Доверенный ИИ — это важная, интересная, многогранная тема. Разработчикам предстоит создать технологии, которым можно доверять в техническом плане (они надежны, устойчивы, безопасны) и психологически. Также к области доверенного ИИ относятся вопросы, связанные с риском внедрения технологий: сама по себе технология может быть безопасной, надежной и устойчивой, но ее внедрение порождает, например, экологические риски, риски безработицы и т. д.

Любое регулирование ИИ должно принимать в расчет особенности ИАС, отличающие их от других программ и показанные на рисунке 13. Кто отвечает за принятые решения, когда речь идет об ИИ? Нормативная база по ИАС предполагает, что отвечает либо оператор системы, либо разработчик, если ошибка не зависит от обслуживания, а была заложена изначально. Есть и противоположное мнение, согласно которому ответственность несет сама ИАС, но большинство экспертов, а также международные

[231] ГОСТ Р 59276-2020 «Системы искусственного интеллекта. Способы обеспечения доверия. Общие положения» // Электронный фонд правовых и нормативно-технических документов. URL: https://docs.cntd.ru/document/1200177291

Рисунок 13. Отличия систем ИИ от большинства систем с фиксированным алгоритмом функционирования

организации, занимающиеся стандартизацией и регулированием ИИ, настаивают на обязательной ответственности человека.

5.2.2 КОМПОНЕНТЫ ДОВЕРЕННОГО ИИ

Основные компоненты доверенного ИИ представлены на рисунке 14: это проверяемость, управляемость, стабильность, отказоустойчивость, безопасность и робастность. Перечисленные и некоторые другие компоненты будут подробно рассмотрены ниже.

1. Проверяемость (прозрачность, объяснимость) ИИ. Проверяемость подразумевает, что ИАС не является черным ящиком. Основная дискуссия идет в области использования результатов обученных нейросетей. У разработчиков нет четкого понимания, почему нейросеть, обученная на той или иной выборке, принимает то или иное решение. Известно, что в системе, основанной на дереве решений, ошибки следует искать за пределами дерева решений; в случае нейросетей определить пространство ошибок на текущем уровне развития науки и технологий невозможно. Во многих отраслях, особенно с максимально высоким риском (аэрокосмическая, атомная и т. д.), нейросети не применяют для критически важных систем. Например, по одной из версий катастрофы Boeing 737 Max произошли из-за излишнего доверия к нейросетям в конструкции этих самолетов.

Две авиакатастрофы Boeing 737 Max — в Индонезии и Эфиопии — произошли с перерывом всего в пять месяцев и унесли 346 жизней. Причиной катастроф специалисты назвали недостатки ПО системы автоматизированного пилотирования MCAS, которые могли привести к тому, что самолет вскоре после взлета вошел в штопор[232].

Объяснимость и прозрачность ИИ подразумевает среди прочего четкое и внятное объяснение для пользователя, с каким типом интерфейса он общается в данный момент: с человеком, с человеком, которому ассистирует ИИ, или только с ИИ.

2. Управляемость. Интеллектуальные системы должны быть управляемы человеком. Он должен иметь возможность применять весь спектр воздействий, от выключения или включения системы до управления в ручном режиме. Принципы работы системы и принципы ее управления должны быть понятны — это часть человекоцентричного подхода.

Рисунок 14. Компоненты доверенного ИИ

[232] Boeing 737 Max, чьи катастрофы унесли 346 жизней, получил разрешение на полеты в США // BBC News. Русская служба. URL: https://www.bbc.com/russian/news-54990444

Согласно одной из гипотез, нейросети в принципе работают как черный ящик; это их неотъемлемое свойство, не требующее исправления. Сторонники этой гипотезы проводят аналогию с людьми: мы тоже черные ящики друг для друга, но мы при этом сосуществуем, принимаем решения и т. д., значит, люди и ИАС могут общаться таким же способом, как и люди между собой.
На это можно возразить, что, во-первых, люди не такие уж черные ящики, мы неплохо понимаем друг друга. Второй момент — люди прошли через горнило биологической и социальной эволюции, и в каждом из нас огромное количество механизмов коррекции ошибок, от репарации ДНК каждую миллисекунду до нейропластичности, культурных и прочих аспектов. Другое дело — системы, написанные никому не известными программистами (известно, что хороший программист делает одну ошибку на 200 строк кода). Если мы делегируем важные решения устройствам, в которых заведомо будут ошибки, люди перестанут им доверять, потому что люди не доверяют черному ящику.
И третий момент: технологии продолжают развиваться, исследователи решат проблему черного ящика или найдут другие решения, поэтому смиряться с непрозрачностью алгоритмов нельзя.

3. Стабильность, безопасность, отказоустойчивость. Для технической устойчивости важны надежность инфраструктуры (в первую очередь доступность интернета), которая требует постоянной поддержки, и наличие альтернативных аналоговых путей. Должен быть аналоговый путь решения всех вопросов, связанных с функционированием гражданина, а остальные пути должны не заменять его, а давать более простую альтернативу.

Математическая теория катастроф утверждает, что динамическая система устойчива в том случае, если она способна игнорировать малые изменения[233]. Если же изменения нарастают и приводят к качественному скачку (катастрофе), система теряет устойчивость и ее развитие становится труднопредсказуемым. Выделяют несколько признаков неустойчивости системы[234], в том числе несимметричность, когда один из вариантов развития системы получает преимущество. Чем больше разнообразие внутри системы, тем ниже вероятность катастроф[235]. Сложная экосистема современных цифровых технологий также подчиняется этому правилу.

Если принцип разнообразия нарушен и доминирует какая-то одна альтернатива, даже небольшое событие способно существенно изменить состояние системы и вызвать катастрофу. Известны случаи пожаров и затоплений, которые приводили к приостановке производства только одного компонента в экосистеме, но это влияло на всю цепочку поставок, на стоимость и доступность конечной продукции.

---

[233] Бекман И. Н. Катастрофы: учебное пособие. URL: https://beckuniver.ucoz.ru/Katastrofy/Lec1.pdf
[234] Меньше чем за месяц DRAM-память подорожала на 42% // DailyComm. URL: http://www.dailycomm.ru/m/24337/
[235] Воронков Н. А. Стабильность и устойчивость экосистем // Основы общей экологии. М.: Агар, 1999. URL: http://www.bibliotekar.ru/ecologia-6/55.htm

В 2013 году сильный пожар на заводе в китайском городе Уси[236], где производили 10% мирового объема чипов DRAM (модулей памяти, широко используемых в компьютерах, смартфонах и т. д.), привел к дефициту чипов и их удорожанию[237].

В марте 2021 года сошлось несколько факторов, повлиявших на всю автоиндустрию. Пожар на заводе Renesas в Японии привел к временной остановке производства полупроводников для автомобилей, в результате чего пострадал японский автопром, а также полтора десятка европейских автомобильных концернов, таких как BMW, Maybach, Mercedes-Benz, Volkswagen, Skoda, Audi, Lamborghini и т. д.[238]

Из-за локдауна в период пандемии COVID-19 резко возросли продажи бытовой электроники, ноутбуков и смартфонов, для которых используются те же микросхемы. Производители микросхем сделали выбор в пользу домашних гаджетов, а крупнейшим автопроизводителям приходится останавливать конвейеры[239]. Volkswagen и Renault прогнозируют падение производства на 100 тыс. автомобилей в год в каждой компании[240] и рост цен летом 2021 года, а новая модель Peugeot 308 вместо виртуальной приборной панели получит обычную аналоговую[241].

4. Робастность, то есть устойчивость к внешним воздействиям. Под такими воздействиями имеются в виду ситуации, когда, например, в выборку из миллиона фото, на которой работает алгоритм распознавания лиц, добавили еще одну фотографию. Если алгоритм «ломается», перестает правильно распознавать лица, это говорит об отсутствии робастности. Она необходима и в случае, когда алгоритм перезапускают на новом устройстве: он должен продолжать корректно работать.

5. Защита персональных данных. Разработчик должен позаботиться о том, чтобы ПДн нельзя было вынуть из системы (для этого иногда имеет смысл, например, их уничтожить или зашифровать) и чтобы были учтены все случаи непрямого получения ПДн (путем деперсонификации данных и т. д.). (Подробнее об этом см. раздел 4.1.)

6. Право отказаться от использования ИИ. С этической точки зрения не следует принуждать людей к использованию цифровых платформ, даже если кому-то такой выбор кажется безусловным благом. По ряду причин — физических, финансовых, религиозных — человек должен иметь право не использовать систему и тем не менее оставаться работоспособным членом общества. Кроме технических и социальных причин важен исторический взгляд на современный уровень развития человечества.

[236] Гавриченков И. Пожар не прошел бесследно: цены на память скакнули вверх // 3DNews. URL: https://3dnews.ru/760538/

[237] Меньше чем за месяц DRAM-память подорожала на 42% // DailyComm. URL: http://www.dailycomm.ru/m/24337/

[238] Хасанов Т. На Россию не хватит чипов: иномарки подорожают из-за пожара в Японии // Газета.Ru. URL: https://www.gazeta.ru/business/2021/03/31/13542014.shtml

[239] Jaguar Land Rover приостановит производство на двух британских заводах из-за нехватки чипов // Коммерсантъ. URL: https://www.kommersant.ru/doc/4783434

[240] Глобальный автопром ждет длительный дефицит чипов // Интерфакс. URL: https://www.interfax.ru/world/753996

[241] Искендеров Б. Volvo намерен сэкономить сотни млн долларов благодаря вторичной переработке // CarsWeek. URL: https://carsweek.ru/news/News_in_the_world/1227116/

«Почему мы думаем, что наши разработки — это предел мечтаний? В истории были прецеденты, когда в рамках идеологии и достигнутого технического прогресса люди делали совершенно неэтичные вещи и верили, что поступают правильно. А кто гарантирует, что то, что мы сейчас делаем, нашим потомкам не покажется так же дико, как сейчас нам кажутся устои нацистской Германии? Именно поэтому всегда должен быть простор для маневра, и для этого необходимо оставить аналоговый путь».

Максим Федоров, вице-президент в области ИИ и математического моделирования Сколковского института науки и технологий

7. Равный доступ. В государстве не должно быть преференций для доступа к ИАС у отдельных категорий граждан, выделенных по социальному, экономическому, политическому признаку. К системе должны иметь доступ абсолютно все. Обязательно должны учитываться права инвалидов и других категорий граждан с ограниченными возможностями здоровья: для них должны разрабатываться специальные интерфейсы, например версии сайтов для слабовидящих или интерфейсы с сурдопереводом.

8. Преодоление дискриминации. В ИИ-системах может быть (непреднамеренно) встроена дискриминация людей по расовым, этническим, социологическим и прочим признакам; надо стремиться тому, чтобы подобных перекосов не было.

Муниципалитеты Амстердама (Нидерланды) и Хельсинки (Финляндия) ведут открытый онлайн-реестр алгоритмов ИИ, которые применяются в этих городах[242]. Любой житель может узнать, где и как используется искусственный интеллект. В реестрах описаны в том числе:

1) сканирование и распознавание номеров автомобилей, чтобы выявить нарушителей правил парковки Амстердама;

2) выявление случаев незаконной сдачи жилья в аренду в Амстердаме (алгоритм анализирует случаи нарушений правил аренды за последние пять лет и вычисляет вероятность повторных нарушений в текущем периоде по указанному адресу);

3) медицинский чат-бот, который отвечает на медицинские вопросы и консультирует по поводу работы учреждений здравоохранения Хельсинки.

Каждая технология описана в реестре по разделам: дата-сет (способ сбора и хранения данных), обработка данных (описание модели), защита от дискриминации, контроль со стороны человека, управление рисками.

5.2.3 ЧЕЛОВЕКОЦЕНТРИЧНЫЙ ПОДХОД К ИИ

Значительную часть перечисленных выше компонентов доверенного ИИ можно считать реализацией человекоцентричного подхода к его разработке и внедрению. Три группы принципов (прозрачность,

[242] What is the Algorithm Register? // City of Amsterdam Algorithm Register. URL: https://algoritmeregister.amsterdam.nl/en/ai-register/; What is AI Register? // City of Helsinki AI Register. URL: https://ai.hel.fi/en/ai-register/

Рисунок 15. Основные принципы ИИ, принятые в ведущих международных организациях

надежность, человекоцентричность), на которых строится современный ИИ, показаны на рисунке 15.

Человекоцентричный подход к развитию ИИ означает, что человек имеет право на любом этапе разработки, внедрения или применения ИИ отменять или запрещать любые действия или решения, принимаемые ИИ, и государство должно обеспечить своим гражданам возможность воспользоваться таким правом. Также следует закрепить в соответствующих документах **баланс между развитием технологий и защитой общечеловеческих ценностей** и вообще человечности (к ней относятся конфиденциальность, эмоции, спонтанность, интуиция, духовность и т. д.). Однако в комплексном виде этого не происходит; как правило, из этого комплекса «выдергиваются» отдельные права, на которые ИИ обязан не посягать, например гендерная проблематика, хотя с технической точки зрения ИИ не имеет половой принадлежности и сама постановка вопроса лишена смысла[243].

Человекоцентричность имеет и другое измерение, а именно требует ответа на вопрос, **насколько ориентированным на человека (пользователя) является то или иное техническое решение**. В человекоцентричной системе пользователь в каждый конкретный момент времени точно

[243] Федоров М., Цветков Ю. Этические вопросы технологий искусственного интеллекта — как избежать судьбы Вавилонской башни // D-Russia. URL: https://d-russia.ru/jeticheskie-voprosy-tehnologij-iskusstvennogo-intellekta-kak-izbezhat-sudby-vavilonskoj-bashni.html

понимает, что он взаимодействует не с человеком, а с роботом. Это правило должно соблюдаться как в отношении простейших алгоритмов (например, чат-ботов на сайте организации), так и применительно к сложнейшим устройствам, например антропоморфным роботам.

Ситуация, когда пользователь не может отличить робота от живого человека, критична с точки зрения этики, а сейчас для ее возникновения есть немало предпосылок. Так, некоторые пожилые люди или люди с невысоким уровнем цифровой грамотности воспринимают робота как живого человека и пытаются общаться с ним как с человеком: «Девушка, ну вы уж мне, пожалуйста, то-то и то-то». Невозможность установить полноценную коммуникацию будет фрустрировать такого пользователя, не только создавая негативный клиентский опыт, но и препятствуя получению услуги. Если речь идет о госуслугах или банковских услугах, такая ситуация становится причиной дискриминации целых групп граждан.

Сотрудники Университета Палермо (Италия) научили робота Пеппера «думать вслух», чтобы алгоритм принятия им решений был прозрачен и понятен для пользователя[244]. Озвучивание роботом своих действий также помогло исследователям понять, как связаны между собой решения и поступки робота. Кроме того, эта опция может быть особенно полезна в случаях, когда роботы и люди взаимодействуют друг с другом.

Помимо дискриминации, взаимодействие с роботом влечет за собой обширный блок проблем, связанных с психологическими аспектами коммуникации человека и ИИ. Отметим лишь некоторые из них, несущие наибольшие этические риски.

В профессиональном жаргоне маркетологов есть понятие «липкая технология» — что-то, что привлекает внимание, удерживает человека, заставляет пользоваться сервисом или продуктом снова и снова. ИАС добавляют новые измерения в пространство липких технологий, позволяя, например, сделать человека эмоционально зависимым от чат-бота и создавая тем самым простор для манипуляций. Идентификация собеседника как робота обязательно должна быть закреплена в законодательстве и на уровне технических решений.

Еще одна ситуация из этого ряда — когда от пользователя требуются неудобные для него форматы взаимодействия с ИИ.

[244] Grover N. Study explores inner life of AI with robot that 'thinks' out loud // The Guardian. URL: https://www.theguardian.com/technology/2021/apr/21/study-inner-life-ai-robot-thinks-out-loud

Голосовой помощник Николай единого контактного центра при правительстве Тульской области[245] требует специальных формулировок и разговора по особым правилам, описанным на сайте тульского цифрового министерства. В частности, при общении с ботом Николаем следует:

- **называть населенный пункт одним словом (не указывая тип населенного пункта, район, область, адрес или номер подразделения);**
- **отвечать односложно на все вопросы типа «Вы будете подавать документы на услугу или получать готовые?»;**
- **в ответ на вопрос «Пожалуйста, уточните услугу, на которую будете подавать документы» называть только наименование услуги, например СНИЛС, пособие на ребенка, субсидия по ЖКХ, паспорт и т. п. Ответ «подать документы» приведет к некорректной записи, поэтому следует исключить это словосочетание при указании услуги;**
- **называть свою фамилию одним словом, слитно, избегая произношения по слогам, так как это может затруднить распознавание.**

Очевидно, что взаимодействовать с таким помощником и, следовательно, получить услугу пользователю будет весьма затруднительно.

Говоря об антропоморфных роботах, нельзя не упомянуть теорию «зловещей долины» (см. рисунок 16). Выводы исследователей подтверждают сказанное выше: пользователь должен совершенно четко понимать, что имеет дело с роботом, а не с человеком.

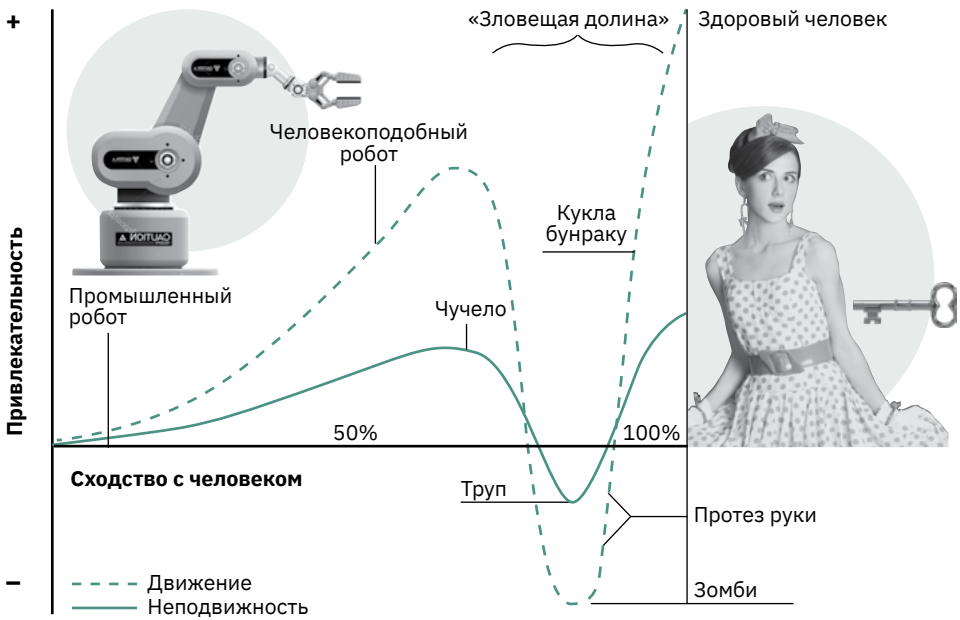


Рисунок 16. Эффект «зловещей долины»

[245] Голосовой помощник: запись на прием в отделение МФЦ // Министерство по информатизации, связи и вопросам открытого управления Тульской области. URL: https://it.tularegion.ru/press_center/news/golosovoy-pomoshchnik-zapis-na-priem-v-otdelenie-mfts/

Рисунок 17. Роботы Алекс и Даша, сотрудники московского МФЦ, — примеры устройств, которые попадают в «зловещую долину» Мори

ГИПОТЕЗА «ЗЛОВЕЩЕЙ ДОЛИНЫ»

Гипотезу об эффекте «зловещей долины» (uncanny valley) впервые сформулировал японский ученый-робототехник Масахиро Мори. Согласно гипотезе, робот или другой неживой объект, который выглядит и действует почти как человек, но не полностью идентичен ему, вызывает у наблюдателя отвращение и страх. Мори представил свою гипотезу в виде графика (см. рисунок 16), расположив на нем антропоморфные существа. После плавного подъема по шкале привлекательности для человека на графике виден резкий провал («долина»), в который попадают такие объекты, как зомби, трупы, а также человекоподобные андроиды. По мнению Мори, похожая на человека машина перестает восприниматься как техника. Антропоморфный робот начинает казаться нездоровым или мертвым человеком, ожившим трупом, вызывая у наблюдателя страх смерти (см. рисунок 17).

В связи с феноменом «зловещей долины» нельзя не упомянуть работы одного из самых знаменитых робототехников современности Хироси Исигуро. В его лаборатории при Университете Осаки[246] создаются роботы-андроиды и ведутся исследования проблемы «зловещей долины»[247]. Поэтому, в частности, самые современные роботы имеют иногда немного карикатурный или «мультяшный» вид: это помогает не попасть в «зловещую долину» и повышает доверие к технологиям.

5.2.4 ВЕРИФИКАЦИЯ ЭТИЧЕСКИХ ХАРАКТЕРИСТИК ИИ

Еще одним важным свойством доверенного ИИ считается возможность верификации его этических характеристик, а для этого необходимы международные этические стандарты. Когда компании выпускают свои кодексы, это только декларация о намерениях, которая должна быть со

[246] Intelligent Robotics Laboratory, Osaka University. URL: https://eng.irl.sys.es.osaka-u.ac.jp/

[247] Добрюха Е. Мечтают ли андроиды об электролюдях // Кот Шрёдингера. URL: https://kot.sh/statya/391/mechtayut-li-androidy-ob-elektrolyudyah

временем воплощена в прикладных технологических и управленческих решениях и, среди прочего, в верификации на соответствие тем или иным стандартам. Сейчас валидация, точнее верификация по этическим стандартам всех ИАС, — это один из главных вопросов развития ИИ.

Кто пишет стандарты? Каждый разработчик должен будет проверить свой продукт на соответствие требованиям, которые указаны в стандартах. Причем проверять продукты корпорации нужно будет не по кодексам этой корпорации, а по государственным стандартам. Для этого государство создает исполнительный орган, который отвечает за проверку.

Как будут проходить проверки? Самое важное и одновременно самое сложное — это объяснить разработчику, как именно созданный им ИИ будут проверять на соответствие стандартам. Технологии и процедуры верификации также должны быть зафиксированы в стандартах в том или ином виде. Пока неясно, как можно, например, валидировать на этичность интеллектуальную систему, которая извлекает метаданные. Вариативность тех данных, с которыми работают программы, колоссальна. По сути, практически каждый человек генерирует какие-то свои данные с собственной структурой, и система может в каждом случае извлекать разные данные. Вопросы проверки здесь пока открыты.

> **«При разработке концепции доверенного ИИ важно помнить, что ничего мистического и принципиально нового в технологии ИИ нет: это „старые добрые“ информационно-коммуникационные технологии, только с учетом выделенных в отдельный стек технологий машинного обучения, сбора и обработки данных и т. д. Поэтому можно и нужно применять все методы (отладки, разработки и так далее), которые существовали раньше; а новое придумывать на базе старого, руководствуясь принципом „созидая, не разрушай“».**
>
> **Максим Федоров, вице-президент в области ИИ и математического моделирования Сколковского института науки и технологий**

Право не раскрывать данные. Предположим, в компании «Око» разработали систему, которая имеет дело с данными в соцсетях, извлекает из них информацию и помогает пользователю соцсетей. Компания использует собственные разработки в области алгоритмизации, которые защищены патентом. Она не хочет раскрывать эти данные проверяющей организации и имеет на это законное право. Для проверяющих работа алгоритмов должна быть черным ящиком, потому что это ноу-хау и нет никаких гарантий, что чиновник, который проводит проверку, завтра не уволится и не устроится на работу к конкурентам «Ока». Разработчики и владельцы продуктов заинтересованы в том, чтобы неопределенность закончилась и появились методы валидации. Эти методы начнет использовать государство, но бизнес при этом будет знать, что это за методы и как они работают, и понимать, с чем он имеет дело. Это сделает ситуацию более удобной для всех.

Авторы раздела:

П. М. Готовцев

А. А. Ефремов

А. Г. Игнатьев

А. В. Незнамов

Д. О. Теплякова

М. В. Федоров

5.3 ДОВЕРЕННЫЙ ИИ В РЕГУЛИРОВАНИИ И СТАНДАРТАХ

Время чтения — 22 минуты

Доверенность систем ИИ обеспечивается строгим выполнением законов, требований нормативно-технического регулирования, профессиональных руководств, инструкций и других утвержденных правил; обеспечением безопасности работы на техническом и инженерном уровне; этически корректным поведением человека на всех этапах создания и эксплуатации этих систем. Ниже представлен краткий обзор некоторых важнейших документов и инициатив в этих областях.

5.3.1 КЛЮЧЕВЫЕ ИГРОКИ И ДОКУМЕНТЫ

На международном уровне действует больше тысячи документов, затрагивающих вопросы этики ИИ. Совет Европы и ЮНЕСКО проявили огромный интерес к теме. Не остались в стороне от этой работы Всемирная организация интеллектуальной собственности, ОЭСР, ISO, G20, а Европейский союз активно формирует нормативное регулирование в сфере ИИ для своих государств-членов.

Совет Европы может принимать обязательные для России нормативные документы — конвенции. Россия — участник и один из ключевых спонсоров Совета Европы. В Совете Европы в 2019 году был создан Специальный комитет по регулированию ИИ (CAHAI). На сегодняшний день это ключевая мировая площадка, где разрабатываются подходы к будущему регулированию ИИ, в том числе рассматривается вопрос о создании специальной конвенции (которая станет обязательной для России в случае ратификации). Представитель России избран председателем рабочей группы Спецкомитета по межгосударственным консультациям; эксперты от России входят в другие рабочие группы. В декабре 2020 года Спецкомитет опубликовал предварительное исследование[248], на которое будет опираться конвенция.

Кроме того, Советом Европы уже приняты важные рекомендательные документы по вопросам ИИ:

1) Европейская этическая хартия Совета Европы по использованию ИИ в судебных системах (12.2018)[249];

[248] AD HOC COMMITTEE ON ARTIFICIAL INTELLIGENCE (CAHAI). Feasibility study // Council of Europe. URL: https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da

[249] Европейская этическая хартия об использовании искусственного интеллекта в судебных системах и окружающих их реалиях. Страсбург, 2018. URL: https://rm.coe.int/ru-ethical-charter-en-version-17-12-2018-mdl-06092019-2-/16809860f4

2) Руководство о защите данных при использовании ИИ (01.2019)[250];

3) Декларация комитета министров о манипулятивных возможностях алгоритмов (02.2019)[251];

4) Рекомендации комиссара Совета Европы по правам человека — 10 шагов для защиты прав человека при использовании ИИ (05.2019)[252];

5) Рекомендация комитета министров о влиянии алгоритмов на права человека (04.2020)[253].

ЮНЕСКО принимает нормативные документы — конвенции, которые обязательны для России как члена ЮНЕСКО. В 2020 году разработан первый глобальный акт по этике ИИ в формате **Рекомендации по этике ИИ**[254]. Формирование российской позиции осуществлялось через комитет по ИИ Комиссии по делам ЮНЕСКО МИД РФ. Окончательная версия документа будет подготовлена для возможного принятия на 41-й сессии Генеральной конференции ЮНЕСКО в конце 2021 года.

Организация Объединенных Наций (ООН) тоже действует в сфере ИИ: прошла серия обсуждений и докладов по теме влияния технологий ИИ на регулирование в сфере интеллектуальной собственности, группа ООН по устойчивому развитию разработала методический документ[255] о роли приватности, этики и защиты данных в достижении целей развития.

Организация экономического сотрудничества и развития (ОЭСР) служит платформой для проведения многосторонних переговоров по экономическим проблемам; Россия не является участником ОЭСР, но взаимодействует с ней. ОЭСР подготовила «Рекомендацию ОЭСР по ИИ»[256] и доклад «Привет, мир! Использование ИИ в государственном секторе»[257]. Запущена платформа OECD AI Policy Observatory, которая предоставляет данные и проводит междисциплинарный анализ в области ИИ. Эта платформа — самый масштабный и системный информационно-аналитический ресурс[258] среди других подобных площадок (например, Human-Centered AI[259] или AI Watch[260]).

---

[250] Guidelines on artificial intelligence and data protection. Strasbourg, 2019. URL: https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8

[251] Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes // Council of Europe. URL: https://search.coe.int/cm/pages/result_details.aspx?ObjectId=090000168092dd4b

[252] Unboxing Artificial Intelligence: 10 steps to protect Human Rights. Commissioner for Human Rights Recommendations. URL: https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64

[253] Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems // Council of Europe. URL: https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154

[254] Итоговый документ. Первый проект рекомендации об этических аспектах искусственного интеллекта // UNESDOC. Цифровая библиотека. URL: https://unesdoc.unesco.org/ark:/48223/pf0000373434_rus

[255] Data Privacy, Ethics and Protection Guidance Note on Big Data for Achievement of the 2030 Agenda. URL: https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf

[256] Recommendation of the Council on Artificial Intelligence // OECD. URL: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

[257] Hello, World! Artificial Intelligence and its Use in the Public Sector // OECD. URL: https://www.oecd.org/gov/innovative-government/working-paper-hello-world-artificial-intelligence-and-its-use-in-the-public-sector.htm

[258] Система международного мониторинга в области развития искусственного интеллекта: вклад ОЭСР // D-Russia.ru. URL: https://d-russia.ru/sistema-mezhdunarodnogo-monitoringa-v-oblasti-razvitija-iskusstvennogo-intellekta-vklad-ojesr.html

[259] Human-Centered AI // Stanford University. URL: https://hai.stanford.edu/ai-index-2019

[260] AI Watch // European Commission. URL: https://knowledge4policy.ec.europa.eu/ai-watch_en

Большая двадцатка (G20) известна как неформальный форум для обсуждения вопросов глобальной экономики; Россия является членом G20. В рамках G20 подготовлены Принципы «Группы двадцати» в области развития ИИ[261] и Заявление лидеров G20 в Осаке[262].

Европейский союз обладает собственной правосубъектностью и издает обязательные для государств-членов акты, в том числе по вопросам ИИ. Из последних — «Скоординированный план по ИИ»[263], коммюнике «Укрепление доверия к человекоориентированному ИИ»[264], план создания регуляторных норм и требований «Белая книга об ИИ: европейский подход к совершенству и доверию»[265].

Разработано примерно три десятка корпоративных кодексов в сфере ИИ, в первую очередь в крупных мировых компаниях: «Принципы ИИ Microsoft»[266], «Руководящие принципы ИИ» в SAP[267], «Повседневная этика для ИИ»[268] у IBM, «Ответственный ИИ — прозрачность, предубежденность и ответственность в эпоху доверенного ИИ» в Siemens[269], «ИИ в Google»[270].

5.3.2 ЭТИЧНЫЙ ИИ В ПРОЕКТЕ ЕВРОКОМИССИИ

В начале 2021 года Еврокомиссия предложила первый в своем роде проект общеевропейского законодательства, который регулирует риски, связанные с применением ИИ[271]. По мнению зампреда Еврокомиссии Маргрете Вестагер, которая отвечает за политику в области конкуренции и за кластер «Европа, готовая к цифровой эпохе», Европейский союз, продвигая такие стандарты, может «проложить путь к этичным технологиям во всем мире»[272]. Предложения Еврокомиссии направлены на гармонизацию регулирования в сфере ИИ и охватывают все области за исключением военных технологий. Согласно проекту, правила должны применяться ко всем поставщикам систем с ИИ, включая расположенных в третьих странах, если результат их работы будет использован в ЕС. Однако

[261] G20 Ministerial Statement on Trade and Digital Economy. URL: https://www.meti.go.jp/press/2019/06/20190610010/20190610010-1.pdf

[262] G20 Osaka Leaders' Declaration // Ministry of Foreign Affairs of Japan. URL: https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/documents/final_g20_osaka_leaders_declaration.html

[263] Coordinated Plan on Artificial Intelligence 2021 Review // European Commission. URL: https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review

[264] Communication: Building Trust in Human Centric Artificial Intelligence // European Commission. URL: https://digital-strategy.ec.europa.eu/en/library/communication-building-trust-human-centric-artificial-intelligence

[265] White paper on Artificial Intelligence. A European approach to excellence and trust // European Commission. URL: https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

[266] Microsoft AI principles // Microsoft. URL: https://www.microsoft.com/en-gb/ai/responsible-ai

[267] SAP's Guiding Principles for Artificial Intelligence // SAP. URL: https://news.sap.com/2018/09/sap-guiding-principles-for-artificial-intelligence/

[268] Everyday Ethics for Artificial Intelligence / IBM. https://www.ibm.com/watson/assets/duo/pdf/everydayethics.pdf

[269] Responsible AI — Transparency, Bias, and Responsibility in the Age of Trustworthy Artificial Intelligence // Siemens. URL: https://ingenuity.siemens.com/2020/11/responsible-ai-transparency-bias-and-responsibility-in-the-age-of-trustworthy-artificial-intelligence/

[270] Artificial Intelligence at Google: Our Principles // Google. URL: https://ai.google/principles/

[271] Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) // European Commission. URL: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-approach-artificial-intelligence

[272] Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence // European Commission. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682

регулирование не распространяется на органы государственной власти и международные организации в третьих странах, если они используют системы с ИИ в рамках международных соглашений.

Маргрете Вестагер считает[273], что в проекте используется соразмерный и основанный на оценке риска подход: чем выше риск применения конкретной системы ИИ, тем строже правила. Всего было выделено четыре уровня рисков.

- **Неприемлемый риск.** К этой категории относятся ИИ-системы, которые могут представлять угрозу для прав граждан и их безопасности, например разработки, позволяющие манипулировать поведением пользователей. Подобные системы будут запрещены.
- **Высокий риск.** К таким системам относятся решения в области критической инфраструктуры (например, транспорта), медицины (в частности, роботизированная хирургия), образования, права и др. Отнесенные к этой категории разработки должны соответствовать строгим критериям безопасности (иметь четкую систему оценки рисков, контроль со стороны людей и др.).
- **Умеренный риск.** Пользователи таких ИИ-систем должны четко понимать, что взаимодействуют с машиной (например, чат-ботом), а не человеком.
- **Минимальный риск.** В эту категорию попадает большинство ИИ-систем: интеллектуальные спам-фильтры, видеоигры с поддержкой ИИ и так далее.

В основном законопроект направлен на регулирование систем с высоким риском. Внимание общественности привлекают в первую очередь те практики в сфере ИИ, которые будут запрещены в случае принятия нового законодательства. К таким случаям относятся:

- системы, манипулирующие поведением, что может причинить физический или психологический ущерб;
- системы, которые используют слабые места определенной группы лиц (возраст, физические или умственные особенности), чтобы существенно исказить поведение, и в результате могут причинить физический или психологический ущерб;
- оценка или классификация органами госуправления (или по их поручению) благонадежности физических лиц в течение определенного периода времени на основе их социального поведения, известных или прогнозируемых личных или личностных характеристик, если оценка приводит к неблагоприятному отношению к определенным физическим лицам или их группам в социальных контекстах, не связанных с условиями, в которых данные были первоначально созданы или собраны, либо к такому отношению, которое неоправданно или несоразмерно их социальному поведению;

[273] Speech by Executive Vice-President Vestager at the press conference on fostering a European approach to Artificial Intelligence // European Commission. URL: https://ec.europa.eu/commission/presscorner/detail/en/speech_21_1866

› использование правоохранительными органами удаленных систем биометрической идентификации в режиме реального времени в общедоступных местах, кроме случаев, когда это критически необходимо, например для целенаправленного поиска потенциальных жертв преступлений, в том числе пропавших без вести детей.

Проект «основан на ценностях и основных правах ЕС и направлен на то, чтобы уверить пользователей в безопасности решений на основе ИИ, а также побудить компании развивать такие решения»[274]. Однако критики полагают, что некоторые запреты сформулированы слишком расплывчато и не способны в достаточной мере защитить права граждан[275]. Например, запрет на системы социального рейтинга (если они ведут к дискриминации) распространяется только на органы госуправления. Это не мешает частным компаниям развивать свои системы, а госорганам — использовать их результаты. В запрете указана биометрическая идентификация «в режиме реального времени», что можно истолковать как разрешение использовать ПО для распознавания лиц по уже отснятым изображениям; в этом случае европейская полиция может использовать сервисы типа Clearview AI[276], которые получили распространение в США. Примечательно, что сама по себе «биометрическая идентификация и категоризация физических лиц» не запрещена, но внесена в список систем с высоким риском, внедрение и развитие которых должны контролироваться. На них будет распространяться набор из пяти обязательств[277].

1. Поставщики систем с ИИ обязаны использовать качественные данные, чтобы результаты не были предвзятыми или дискриминирующими.

2. Они должны предоставлять подробную документацию о том, как работают их системы ИИ, чтобы власти могли оценить их соответствие стандартам.

3. Поставщики должны делиться информацией с пользователями, чтобы помочь им понять и правильно использовать системы с ИИ.

4. Они должны обеспечить соответствующий уровень человеческого надзора как при разработке, так и при внедрении ИИ.

5. Они должны соблюдать самые высокие стандарты кибербезопасности.

ЕС стремится стать лидером в разработке безопасного, надежного и человекоориентированного искусственного интеллекта. Поэтому, несмотря на недочеты, этот проект можно считать первым шагом ЕС на пути к созданию подхода, отличного от моделей Китая и США.

[274] Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) // European Commission. URL: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-approach-artificial-intelligence

[275] Vincent J. EU outlines wide-ranging AI regulation, but leaves the door open for police surveillance // The Verge. URL: https://www.theverge.com/2021/4/21/22393785/eu-ai-regulation-proposal-social-credit-ban-biometric-surveillance-exceptions

[276] Mac R., Haskins C., McDonald L. Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA // BuzzFeed News. URL: https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement

[277] Speech by Executive Vice-President Vestager at the press conference on fostering a European approach to Artificial Intelligence // European Commission. URL: https://ec.europa.eu/commission/presscorner/detail/en/speech_21_1866

5.3.3 ОЦЕНКА ВОЗДЕЙСТВИЯ И ЕЕ ОТРАЖЕНИЕ В СТАНДАРТЕ IEEE

Научно-технологический процесс в XX веке и бурное внедрение технологий во все сферы жизни сделали актуальным появление нового института в области государственного управления и правового регулирования — технологической оценки. Этот институт во многом пересекается с иными оценочными процедурами в сфере государственного управления и права, в том числе с оценкой регулирующего воздействия (ОРВ). После принятия ООН в 2011 году Руководящих принципов предпринимательской деятельности в аспекте прав человека[278] и их развития в 2016 году в Рекомендации комитета министров Совета Европы о правах человека и бизнесе[279] возросло значение оценки того воздействия, которое внедрение технологий оказывает на права человека.

Практически все существующие оценочные процедуры подразумевают либо широкую экспертную дискуссию, либо публичные консультации для неограниченного круга лиц, что делает их достаточно эффективным инструментом выработки оптимальных управленческих и регуляторных решений на основе баланса позиций всех заинтересованных сторон. Принятый в России спустя 10 лет после внедрения ОРВ федеральный закон от 31.07.2020 № 247-ФЗ «Об обязательных требованиях в Российской Федерации» наконец-то создал для ОРВ законодательную основу[280], что в перспективе позволит развивать эту процедуру при введении любых обязательных требований к применению цифровых технологий.

2020 год стал драйвером развития института оценки. 8 апреля 2020 года комитет министров принял рекомендацию государствам — членам Совета Европы, в которой обсуждается влияние алгоритмических систем на права человека[281]. Документ предлагает этим государствам пересмотреть в соответствии с рекомендацией свою законодательную базу, политику и практику в отношении закупки, проектирования, разработки и развертывания алгоритмических систем и регулярно оценивать эффективность принимаемых мер с участием всех заинтересованных сторон. Также рекомендовано с помощью законодательных, регулирующих и надзорных структур сделать так, чтобы развертывание алгоритмических систем, в разработке которых участвовали субъекты частного сектора, соответствовало законодательству и отвечало обязательствам стран по соблюдению прав человека (обязательствам, зафиксированным в Руководящих принципах предпринимательской деятельности в аспекте прав человека ООН, региональных и международных стандартах).

[278] Руководящие принципы предпринимательской деятельности в аспекте прав человека ООН. URL: https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_RU.pdf

[279] Recommendation CM/Rec(2016)3 to member States on human rights and business. URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c1ad4

[280] Голодникова А. Е., Ефремов А. А., Цыганков Д. Б. Под знаком «регуляторной гильотины»: как разорвать замкнутый круг дерегулирования и ре-регулирования? // Закон. 2021. № 2. С. 105–117.

[281] Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems. URL: https://rm.coe.int/09000016809e1154

Как мы уже писали ранее[282], именно Руководящие принципы ООН заложили основу для внедрения оценки воздействия на права человека.

Названный выше проект «Рекомендация по этическим аспектам ИИ»[283] ЮНЕСКО требует (п. 58), чтобы органы власти и управления проводили самостоятельную оценку имеющихся и предлагаемых к внедрению систем ИИ, в том числе для определения целесообразности применения этих систем. Государствам следует создать механизмы, которые обеспечат соблюдение прав человека, мониторинг и надзор в том, что касается социально-экономических последствий применения ИИ-систем. Также рекомендуется создать и другие механизмы управления, в том числе:

- независимые органы по вопросам защиты данных;
- структуры надзора на уровне секторов;
- государственные органы надзора в сфере закупки ИИ-систем для чувствительных с точки зрения прав человека сфер использования, таких как система уголовного правосудия и независимого судопроизводства, правоохранительная деятельность, социальное обеспечение, занятость, здравоохранение.

17 марта 2021 года комитет министров Совета Европы принял Декларацию о рисках принятия решений с помощью компьютерных программ и алгоритмов искусственного интеллекта в области социального обеспечения[284]. В ней комитет министров обращает внимание на ответственность и подотчетность субъектов ИИ, проектирующих, развертывающих или оценивающих системы ИИ в случаях, когда не соблюдаются правовые нормы или причинен ущерб.

В России внедрение указанной оценки пока предусматривается только на уровне документов стратегического планирования. Упомянутая выше Концепция развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года устанавливает, что достижение цели и задач регулирования отношений, складывающихся в связи с разработкой и применением систем ИИ и робототехники, должно осуществляться с учетом принципов, перечисленных выше (см. раздел 5.1.2). Отметим в Концепции обязательность обоснованной оценки возникающих при применении ИИ и робототехники рисков причинения вреда жизни и здоровью человека, угроз безопасности государства и принятие мер, направленных на минимизацию таких рисков и угроз.

Актуальным примером документа, посвященного оценке воздействия систем ИИ, является новый стандарт IEEE — Института инженеров электротехники и электроники (Institute of Electrical and Electronics

[282] Этика и «цифра»: этические проблемы цифровых технологий. В 2 т. М.: РАНХиГС, 2020. Т. 1. С. 82–83.

[283] Outcome document: first draft of the Recommendation on the Ethics of Artificial Intelligence. URL: https://unesdoc.unesco.org/ark:/48223/pf0000373434

[284] Declaration by the Committee of Ministers on the risks of computer-assisted or artificial-intelligence-enabled decision making in the field of the social safety net. Adopted by the Committee of Ministers on 17 March 2021 at the 1399th meeting of the Ministers' Deputies. URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680a1cb98

Engineers)[285]. Этот институт разрабатывает стандарты для электронных и электротехнических устройств, в том числе и для сферы применения ИИ. Стандартизация в области ИИ и данных ведется в институте силами множества ученых со всего мира. Так, в разработке основного установочного документа Ethically Aligned Design приняли участие 700 экспертов: программисты и специалисты по ИИ, философы, культурологи, психологи, нейроученые и другие специалисты. Свой вклад вносит и российская Рабочая группа IEEE по тематике «Этика и искусственный интеллект».

В разработке сейчас находится более 10 стандартов IEEE, так или иначе связанных с этическими вопросами создания и использования ИАС[286]. В 2021 году принят стандарт IEEE 7010 «Рекомендованная практика оценки воздействия автономных систем и систем искусственного интеллекта на благополучие человека»[287], который содержит набор метрик для оценки такого воздействия (Well-being Impact Assessment, WIA).

WIA — это инструмент, позволяющий тем, кто создает ИАС, учитывать фактор благополучия человека на всех этапах жизненного цикла системы и на всех уровнях — индивидуальном, популяционном и социетальном (то есть на уровне, где общество рассматривается как единое целое). Стандарт 7010 предназначен для дизайнеров, разработчиков, инженеров, программистов и других специалистов, создающих такие системы и работающих с ними.

Стандарт помогает:

- определить понятие «благополучие человека» в отношении ИАС;
- определить способы измерения влияния ИАС на благополучие человека с момента проектирования до окончания жизненного цикла системы;
- управлять развитием ИАС;
- определить болевые точки;
- подготовить стратегии минимизации рисков;
- оценить эффективность системы;
- выявить целевых и нецелевых пользователей, а также намеренные и ненамеренные способы применения и факты влияния ИАС на благополучие человека.

В основе WIA как инструмента оценки лежит итеративный подход, который обеспечивает непрерывное получение информации о влиянии системы на благополучие человека в ходе ее применения, а значит, и непрерывный цикл совершенствования системы.

[285] Некоммерческая профессиональная ассоциация, содействующая технологическим инновациям во всех областях, связанных с применением электричества. В ней состоят около 500 тысяч студентов и профессионалов из более чем 160 стран мира. URL: https://www.ieee.org/

[286] Стандарты на этичный искусственный интеллект // Этика и «цифра»: Этические проблемы цифровых технологий. В 2 т. М.: РАНХиГС, 2020. URL: https://ethics.cdto.center/3_5

[287] IEEE Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems on Human Well-Being // IEEE. URL: https://ieeexplore.ieee.org/document/9084219

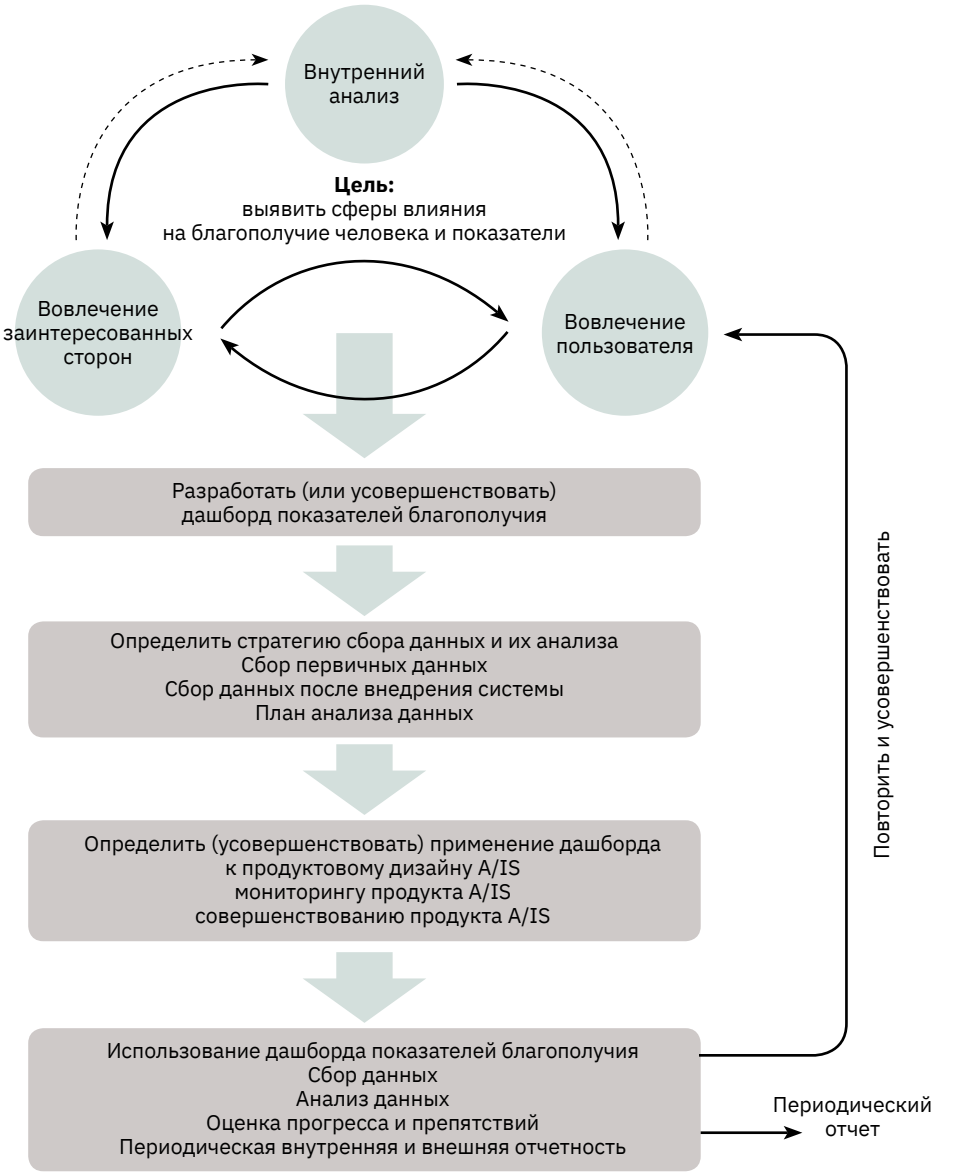


Рисунок 18. Методика оценки воздействия ИАС на благополучие человека (Well-being Impact Assessment, WIA)

Процесс состоит из нескольких этапов (activities), которые включают в себя конкретные задачи (tasks). Каждый этап завершается чек-листом с закрытыми вопросами («да/нет»). Ядро WIA представляет собой дашборд показателей, распределенных по 13 группам, которые охватывают все сферы благополучия человека. Весь процесс WIA, таким образом, можно представить в виде цикличной схемы (рисунок 18).

5.3.4 СТАНДАРТЫ ISO

Международная организация по стандартизации (International Organization for Standardization, ISO, ИСО) играет ключевую роль в развитии международной стандартизации. В деятельность этой независимой организации вовлечены национальные органы 165 стран. Национальные органы состоят из экспертов, которые делятся лучшими практиками и разрабатывают основанные на консенсусе стандарты.

Международные стандарты способствуют внедрению инноваций и преодолению глобальных трудностей. Кроме того, стандарты помогают решать вопросы, связанные с оценкой различных технологий или систем, и преодолевать технические барьеры при коммерциализации систем. Стандарты ИСО являются добровольными; они не включают договорные, юридические или законодательные требования, не заменяют собой национальные законы — последние всегда имеют приоритет.

Вопросами ИИ в ИСО занимается Подкомитет 42 (SC 42), который был создан в 2017 году и структурно входит в Объединенный технический комитет 1 «Информационные технологии» (JTC 1). Сейчас этот комитет разрабатывает более 3 тыс. стандартов, из которых 504 направлены на достижение целей в области устойчивого развития[288]. Подкомитет 42 «Искусственный интеллект» имеет семь опубликованных стандартов и 22 стандарта в стадии разработки. Из уже опубликованных пять относятся к большим данным и ИИ, один — к вопросам робастности нейронных сетей, один посвящен доверию. В течение года подкомитет 42 завершит работу над стандартом «Концепции и терминология в области искусственного интеллекта» (ISO/IEC DIS 22989 Information technology — Artificial intelligence — Artificial intelligence concepts and terminology), публикация документа намечена на весну 2022 года. Стандарты, имеющие отношение к этике, рассматриваются в рабочей группе подкомитета, которая занимается вопросами доверия к ИИ (WG3). Среди проектов WG3 выделим три наиболее значимых для понимания этических аспектов развития ИИ.

«Искусственный интеллект. Этические и социальные проблемы. Общие положения» (ISO/IEC AWI TR 24368 Information technology — Artificial intelligence — Overview of ethical and societal concerns).

В проекте будет расширена терминология в области ИИ применительно к этическим аспектам и проанализирована взаимосвязь вопросов этики с общими задачами и проблемами развития технологий. Документ будет содержать перечисление международных документов, которые имеют отношение к этике ИИ, в том числе в области обеспечения прав человека и социальной ответственности вовлеченных лиц. Будут проанализированы принципы развития технологий на основе ИИ, представлены способы построения социально приемлемых систем ИИ в контексте вопросов этики.

[288] Повестка дня в области устойчивого развития на период до 2030 года, где указаны 17 целей устойчивого развития, была единогласно принята на саммите ООН в сентябре 2015 года. URL: https://www.un.org/sustainabledevelopment/ru/about/development-agenda/

«Смещения[289] в системах искусственного интеллекта и системах поддержки принятия решений с использованием искусственного интеллекта» (ISO/IEC DTR 24027 Information technology — Artificial Intelligence (AI) — Bias in AI systems and AI aided decision making)[290].

Будут описаны методы измерения и оценки степени смещений с целью их устранения и снижения факторов уязвимости систем на разных этапах. Будут представлены источники и общая классификация видов смещений, описаны возможности их положительного, нейтрального или отрицательного влияния на принимаемые решения. Подготовка стандарта должна завершиться в 2021 году.

«Искусственный интеллект. Доверенность в искусственном интеллекте. Общие положения» (ISO/IEC TR 24028:2020 Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence) — проект стандарта, опубликованный в мае 2020 года.

Его цель — анализ факторов, которые могут влиять на доверенность систем ИИ. В документе кратко рассматриваются существующие подходы, которые могут поддерживать или повышать доверие к техническим системам. Перечислены, в частности, возможности установления доверия к системам ИИ через прозрачность, объяснимость, контролируемость. Разобраны отдельные инженерные аспекты, типичные угрозы и риски для систем ИИ, методы и практики смягчения негативных последствий на разных этапах жизненного цикла систем. Приведены общие способы достижения доверенности и оценки доступности, устойчивости, надежности, точности, безопасности и конфиденциальности систем ИИ.

ВЫВОДЫ. ПЯТЬ ТЕЗИСОВ ОБ ЭТИЧНОМ ИИ

1. Этика ИИ как дисциплина — это область прикладной этики и направление философии, которые изучают этические вопросы, связанные с разработкой, внедрением и использованием ИИ; этика ИИ как практика — это поведение человека и взаимодействие людей между собой в контексте вопросов использования ИИ на всех этапах жизненного цикла.

2. Доверие к системам ИИ — важнейшее условие их применения при решении ответственных задач обработки данных. Основные компоненты доверенного ИИ — проверяемость (объяснимость), управляемость, стабильность, отказоустойчивость, безопасность и робастность.

3. Значительную часть компонентов доверенного ИИ можно считать реализацией человекоцентричного подхода к его разработке и внедрению; это относится и к трем группам принципов (прозрачность, надежность, человекоцентричность), на которых строится современный ИИ.

[289] Как правило (в том числе и в настоящем докладе), в качестве перевода англ. bias используются слова «предвзятость, предубежденность, необъективность».

[290] Три новых проекта международных стандартов в сфере ИИ разработают с участием российских экспертов // РВК. URL: https://www.rvc.ru/press-service/media-review/rvk/135639/

«Прежде чем идти в этичность ИИ, надо предотвратить преступность и не допускать утечку данных. Если это требование из формальности не превратится в действительно жесткое регулирование с серьезнейшей ответственностью в случае утечки, то говорить об этике в цифровых системах нет смысла. Мы можем принять хоть все стандарты всех организаций, которые хоть что-то делают на эту тему, но если данные будут вот так легко утекать, то какой смысл во всем этом?»

Павел Готовцев, координатор российской Рабочей группы IEEE по тематике «Этика и искусственный интеллект»

4. Объяснимость и прозрачность ИИ подразумевает среди прочего, что пользователю понятно объяснили, с каким типом интерфейса он общается в данный момент: с человеком, с человеком, которому ассистирует ИИ, или только с ИИ. В частности, этот аспект актуален для массовых государственных сервисов, в которых используются чат-боты и голосовые помощники (например, для записи к врачу).

5. Этические принципы создания и применения ИИ в России затрагиваются в таких документах, как Национальная стратегия развития искусственного интеллекта на период до 2030 года[291], федеральный проект «Искусственный интеллект» национальной программы «Цифровая экономика Российской Федерации», Концепция регулирования технологий ИИ и робототехники до 2024 года[292]. Ведется работа над российским универсальным кодексом ИИ. На международном уровне ключевые игроки в области этики ИИ — это Совет Европы, ООН (в первую очередь ЮНЕСКО), ОЭСР, ISO, IEEE, Европейский союз.

«У нас создан Национальный комитет по этике искусственного интеллекта при Комиссии РФ по делам ЮНЕСКО, но это только первый шаг. Наши органы госуправления должны занимать более активную позицию по участию России в разработке международных этических стандартов. Многие представители академической среды по разным причинам перешли в бизнес и в госорганы, но оставили за собой позиции в вузах или академических институтах. Пока именно они наиболее активны в обсуждении вопросов этики ИИ. Задача в том, чтобы российский бизнес тоже занял внятную консолидированную позицию. Пока заметную активность в этом направлении проявляет только Сбер, хотелось бы услышать мнения других компаний. Если сейчас выработать согласованную позицию, которая будет устраивать большинство сторон в большинстве вопросов, это будет комфортно для всех».

Максим Федоров, вице-президент в области ИИ и математического моделирования Сколковского института науки и технологий

[291] Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» // ГАРАНТ.ру. URL: https://www.garant.ru/products/ipo/prime/doc/72738946/

[292] Распоряжение Правительства РФ от 19.08.2020 № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» // КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_360681/

6. ЭТИКА ПРИНЯТИЯ РЕШЕНИЙ

Не требуйте гарантий. И не ждите спасения от чего-то одного — от человека, или машины, или библиотеки. Сами создавайте то, что может спасти мир, — и если утонете по дороге, так хоть будете знать, что плыли к берегу.

Р. Брэдбери. 451 градус по Фаренгейту

6.1 ЦЕННОСТНЫЙ ПОДХОД К ЦИФРОВЫМ РЕШЕНИЯМ

Время чтения — 13 минут

При всех ограничениях у государственного или муниципального служащего всегда остается определенная свобода в выборе решения поставленной перед ним задачи. Какими ценностями должен руководствоваться служащий, создавая и развивая цифровые сервисы и инструменты или устанавливая правила использования цифровых технологий? Как госслужащему включить анализ этических вопросов в свою повседневную работу? Какие инструменты могут ему помочь?

6.1.1 ПОЧЕМУ ЭТО ВАЖНО?

Начнем с характеристики тех функций, при выполнении которых важно уделить внимание вопросам этики. Государственные и муниципальные органы и их должностные лица выполняют две группы функций. Первая связана с регулированием, с установлением правил деятельности разных

организаций и отдельных людей. В число этих правил входят и те, что касаются применения цифровых технологий, производства, продажи, приобретения и использования цифровых продуктов, товаров и услуг.

Вторая группа — это все прочие функции, начиная от оказания различных государственных услуг и заканчивая совершенствованием внутренних управленческих процессов. Сейчас цифровые технологии активно внедряются как инструмент, помогающий оптимизировать внутренние процессы в государственных органах и подведомственных им учреждениях, сделать более удобными и доступными госуслуги, повысить эффективность контрольно-надзорной деятельности и т. п. Это внедрение происходит в том числе в ходе ЦТ федеральных и региональных органов власти.

Порядок выполнения государственным или муниципальным служащим своих функций, сфера его компетенций детально регламентированы. Есть правовые требования, определяющие порядок оказания государственных и муниципальных услуг и выполнения других функций. Кроме того, есть требования руководства, стратегические решения, которым надо следовать, и ранее принятые проекты, которые должны быть реализованы.

Однако при всех ограничениях у государственного или муниципального служащего всегда остается определенная свобода в выборе решения поставленной перед ним задачи. Например, при создании новых правил игры для бизнеса и граждан можно выбрать разные модели регулирования, использовать разные юридико-технические приемы. В случае создания цифровых инструментов возникает вопрос выбора концепции, дизайна цифрового сервиса и конкретных технических решений, включая способы сбора, обработки и хранения данных, работу алгоритмов и т. д.

Когда речь идет о цифровых технологиях, четкого руководства к действию может и не быть. Сейчас нормативное регулирование не всегда успевает за развитием технологий. Поэтому руководители и сотрудники государственных органов и учреждений вполне могут оказаться в ситуации, когда им предстоит внедрять цифровые инструменты, не имея четкой регламентации их использования.

«Одна из главных задач цифровизации — заставить госслужащих увидеть клиента. В цифровую эпоху очень важно поменять образ мыслей, задуматься о том, какую ценность я даю своими действиями, какую ценность я даю цифровыми решениями».

Мария Шклярук, академический директор Центра подготовки РКЦТ

Авторы раздела:

П. А. Алферов

А. Ю. Кирин

О. С. Шепелева

Выбор, сделанный при создании новых правил или новых цифровых инструментов, может иметь значение для большого числа людей и организаций. Цена ошибки высока. Недальновидные решения могут не только испортить карьеру отдельным сотрудникам, но и негативно повлиять на репутацию государственных органов. Поэтому важно, чтобы выбор не делался вслепую.

6.1.2 МЕСТО ЦЕННОСТЕЙ В ПРИНЯТИИ РЕШЕНИЙ

Эксперты в сфере управления предлагают различные подходы к тому, как делать выбор и принимать решения. Но все они единодушны в том, что следует осознанно подойти к процессу и, в частности, оценить позитивные стороны и риски каждого из вариантов, в том числе риски этического характера (подробнее об этических рисках см. раздел 2). На первый взгляд они могут показаться малозначительными, особенно на фоне вызовов, связанных с финансированием или соблюдением требований законодательства. Однако их игнорирование может создать серьезные проблемы в дальнейшем. Как было отмечено в предыдущих разделах, этика использования цифровых технологий приобретает все большее значение в сфере управления бизнесом и в госуправлении, причем как в контексте формирования стратегии, так и в повседневной работе.

Международная компания Deloitte пришла к выводу, что внимание к этическим аспектам использования технологий связано со степенью цифровой зрелости компаний: интерес к вопросам этики чаще проявляют те, кто активнее использует прорывные технологии и дальше продвинулся в цифровизации[293].

В госсекторе появляются этические фреймворки использования цифро-вых технологий и инструменты, которые помогают выявлять этические риски. К таким инструментам относятся, в частности, программный документ Института Алана Тьюринга «Руководство по ответственной разработке и внедрению систем на основе ИИ в государственном секторе»[294] и «Фреймворк по этике данных» правительства Великобритании[295].

Этические требования, включая этику использования цифровых технологий, вытекают из ценностей. Этичные решения и действия конкретного служащего согласуются с ценностями общества или организации, а неэтичные — противоречат им. Поэтому самый простой способ выявить и оценить этические риски того или иного решения — проанализировать ценности, которые оно затрагивает.

[293] Bannister C., Sniderman B., Buckley N. Ethical tech: Making ethics a priority in today's digital organization // // Deloitte Review. 2020. Iss. 26. URL: https://www2.deloitte.com/content/dam/insights/us/articles/6289_ethical-tech/DI_DR26-Ethical-tech.pdf

[294] Leslie D. Understanding artificial intelligence ethics and safety. A guide for the responsible design and implementation of AI systems in the public sector // Alan Turing Institute. URL: https://www.turing.ac.uk/sites/default/files/2019-06/understanding_artificial_intelligence_ethics_and_safety.pdf

[295] Data Ethics Framework // UK Government. URL: https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework-2020

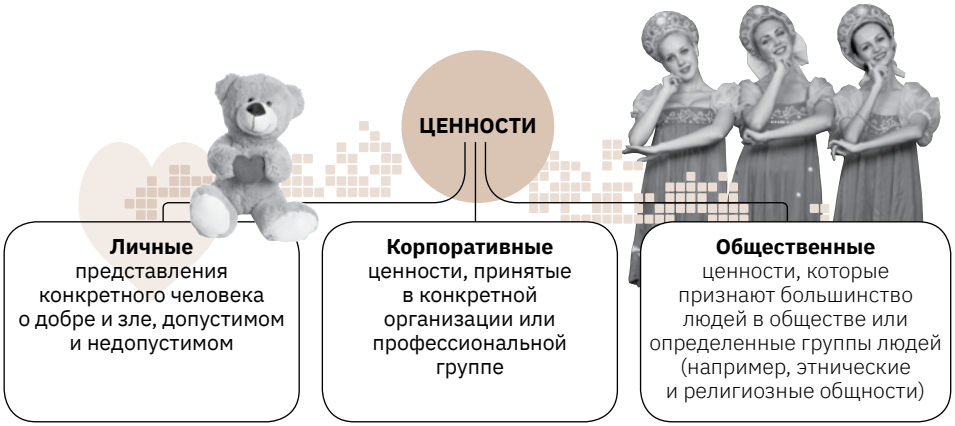


Рисунок 19. Группы ценностей

Принимая решения, люди исходят из разных ценностей: личных, корпоративных, общественных (см. рисунок 19). Поскольку решения, принимаемые государственными и муниципальными служащими, влияют на жизнь множества людей, они не могут основываться только на личных или корпоративных ценностях; значительно важнее ценности, признаваемые в обществе. Их игнорирование может вызвать общественный протест или привести к саботажу принятых органами власти решений.

«Те, кто, внедряя цифровые технологии, заботятся исключительно о показателях эффективности своей работы, идут на изменение практики отношений между людьми и создание другого типа культуры. В нем не к кому апеллировать, там нет правды. Алгоритм рейтингования или оценки высказываний сам будет решать, кого банить в Facebook, кому не давать кредит и кого не принимать на работу. Когда это делается без объяснения причин, а на решение нельзя пожаловаться, то это другое мироустройство».

Сергей Карелов, председатель совета Лиги независимых экспертов в области информационных технологий

6.1.3 КАК ПРИНЯТЬ ЭТИЧНОЕ РЕШЕНИЕ

Какими ценностями должны руководствоваться служащие, развивая цифровые сервисы или формулируя правила использования цифровых технологий? Ответить на этот вопрос помогают исследования Организации экономического сотрудничества и развития (ОЭСР). В них отмечается корреляция между высоким уровнем доверия (между людьми и людей к институтам) и экономическим ростом, повышением благосостояния, поддержкой проводимых государством реформ. Уровень доверия зависит в том числе от поведения должностных лиц, действий государственных и муниципальных органов[296].

[296] См.: Algan Y. Trust and social capital in For Good Measure // Advancing Research on Well-being Metrics Beyond GDP. Paris: OECD, 2018. URL: https://www.oecd-ilibrary.org/sites/9789264307278-12-en/index.html?itemId=/content/component/9789264307278-12-en

Рисунок 20. Открытость, справедливость и добросовестность — три источника доверия

Такого мнения придерживаются многие эксперты: по словам декана экономического факультета МГУ Александра Аузана, «недоверие — такая же институциональная ловушка, как коррупция, низкий уровень конкуренции и административные барьеры»[297].

Ключевые драйверы доверия к государственным и муниципальным органам и структурам — это их компетентность и те ценности, которым они следуют. Чтобы вызвать доверие, действия и решения властей должны быть основаны на ценностях[298], показанных на рисунке 20.

Что это означает применительно к использованию цифровых технологий в государственном и муниципальном секторах? Если мы говорим об **открытости**, то важно проконтролировать следующие аспекты. Во-первых, при разработке решения надо собирать, анализировать и учитывать опыт предполагаемых пользователей, а после того как цифровой инструмент был выпущен в эксплуатацию — поддерживать каналы обратной связи. Во-вторых, до пользователей надо доводить в понятной им форме информацию о работе сервиса. Это не только удобные инструкции, но и сведения о значимых технических характеристиках. Например, если сервис использует пользовательские данные, важно объяснить, как они хранятся и передаются, кто имеет к ним доступ, как они обрабатываются и уничтожаются. В некоторых случаях открытость может потребовать публикации кода. Недостаточная открытость — источник разнообразных рисков: например, сервис не отвечает потребностям целевой аудитории или люди не хотят его использовать, опасаясь за сохранность своих данных.

[297] Александр Аузан: «Недоверие — такая же опасная ловушка, как коррупция» // Плюс Один. URL: https://plus-one.ru/society/aleksandr-auzan-nedoverie-takaya-zhe-opasnaya-lovushka-kak-korrupciya-

[298] Trust and Public Policy: How Better Governance Can Help Rebuild Public Trust // OECD. URL: http://dx.doi.org/10.1787/9789264268920-en

«Важно внимательно отслеживать законность запроса и обработки данных. Вот вы знаете, какими вашими персональными данными на этой неделе пользовались государство и коммерческие структуры? Допустим, у вас есть кредит, который вы успешно погасили. А вы свои персональные данные отозвали у банка? Нет. Государственные и коммерческие услуги должны оказываться по принципу „Я, ФИО, пришел в банк получать услугу, и, когда моя услуга оказана, система мне автоматом подсказывает, что услуга оказана, и задает вопрос о том, нужно ли отозвать мои данные". Нужно, чтобы у гражданина был единый прозрачный инструмент отзыва. К сожалению, сейчас мы не владеем а) пониманием того, кто какие данные в каких целях использует, и б) инструментами, чтобы быстро и просто прекратить использование этих данных».

Радик Гисмятов, заместитель РЦТ Республики Татарстан

Справедливость — более сложная концепция. Дизайн цифрового решения должен быть **инклюзивным** и учитывать особенности разных групп пользователей[299]. Адресаты услуг часто не отличаются высокой цифровой грамотностью и менее оптимистичны в отношении цифровых технологий, чем разработчики сервисов и должностные лица, которые их курируют. Кроме того, создание новых сервисов не должно усиливать цифровой разрыв[300] (подробнее об этом см. раздел 2.2).

«Нужно продумывать, как организовать равный доступ к системе и исключить дискриминацию. Обязательно должны учитываться права граждан с ограниченными возможностями. Многие интерфейсы разработаны для людей с хорошим зрением и моторикой, но надо двигаться дальше: например, мы в Сколково разрабатываем интерфейсы с сурдопереводом для глухонемых».

Максим Федоров, вице-президент в области ИИ и математического моделирования Сколковского института науки и технологий

Порядок работы цифрового сервиса или иного инструмента **не должен создавать избыточных рисков** и чрезмерных обременений для граждан или бизнеса. Иногда можно оценить риски и обременения в денежном выражении и сопоставить их с получаемыми выгодами. Другой способ — провести оценку путем сопоставления ценностей, которые планируется поддержать за счет нового цифрового механизма, и тех, что могут оказаться урезаны и ущемлены.

Если инструмент предполагает принятие индивидуальных решений (о предоставлении льгот, наложении санкций и пр.), он должен отвечать требованиям **процессуальной справедливости**. Технические решения и данные, которые используются при принятии решений, не должны

[299] Доступность цифровых технологий и услуг для граждан // Этика и «цифра»: этические проблемы цифровых технологий. В 2 т. М.: РАНХиГС, 2020. URL: https://ethics.cdto.ranepa.ru/6_2

[300] Там же.

допускать дискриминации или предвзятости в отношении отдельных категорий людей. Дизайн цифровых процедур должен быть понятен и удобен: граждане, которые сталкиваются с этими процедурами, не должны чувствовать беспомощность. В дизайн процедуры, опирающейся на цифровые технологии, должна быть заложена возможность изучения аргументов и доказательств, предоставленных человеком, в отношении которого принимается решение.

Важно, чтобы люди были **уверены в справедливости цифровых решений**. Это еще одна причина, по которой важно вовлекать представителей целевой аудитории и других заинтересованных лиц в процесс разработки таких решений, а также в понятной и доступной форме информировать о том, как работает тот или иной цифровой сервис.

Понятие **добросовестности** предполагает **надежность решения**, его **высокое качество**, достаточные степени защиты и т. д. Последствия взаимодействия с цифровым инструментом или сервисом должны быть **предсказуемы**. Если для оказания услуги собирают данные пользователей, они не должны затем использоваться для других целей. Например, информация о месте проживания, переданная государственным органам для оформления цифровых пропусков в период пандемии, не должна использоваться для наказания тех, кто живет не по месту регистрации или сдает квартиру, не декларируя это.

Цифровые технологии разнообразны и могут быть использованы государством для решения разных задач. Невозможно предложить детальный и одновременно универсальный, применимый ко всем цифровым проектам набор требований, вытекающих из принципа справедливости. Однако можно опираться на накопленный опыт использования конкретных технологий, на знания о рисках, которые проявили себя на практике.

6.2 ФРЕЙМВОРК «ОТВЕТСТВЕННАЯ РАЗРАБОТКА ЦИФРОВЫХ РЕШЕНИЙ»

Время чтения — 12 минут

Авторы доклада проанализировали ряд популярных фреймворков принятия решений и управления данными, после чего, опираясь на собственный опыт управления данными и этическими рисками, используя корпоративные стандарты в сфере бизнеса, а также адаптировав зарубежные инструменты к российским реалиям, предложили свой вариант такого фреймворка.

Помимо традиционных механизмов ответственности, обеспечивающих добросовестность работы госучреждений, при создании цифровых решений полезно использовать инструменты (фреймворки и чек-листы),

которые помогают выявлять и оценивать риски, связанные с дизайном и параметрами работы конкретного цифрового сервиса, и находить способы справляться с ними[301]. Фреймворки и чек-листы помогают сделать процесс принятия решений более осознанным, лучше структурировать его.

Предлагаемый нами фреймворк «Ответственная разработка цифровых решений» — это инструмент, который поможет команде выявить этические болевые точки на ранних стадиях работы над проектом. Вопросы из категории «В ходе проекта» можно воспринимать как ориентиры на будущее: на стадии подготовки проекта команда должна подумать над созданием инструментов, которые помогут ответить на эти вопросы.

При разработке фреймворка использовались три основных источника:

- Data Ethics Decision Aid (DEDA)[302] — список вопросов для обсуждения в команде при разработке цифрового проекта, составленный Утрехтским университетом;
- Data Ethics Canvas[303] — графический инструмент этичной работы с данными, разработанный Открытым институтом данных;
- Data Ethics Framework[304] — фреймворк Правительства Великобритании по этичной работе с данными и разработке цифровых решений.

На момент публикации доклада фреймворк был протестирован в нескольких пилотных регионах. Давая обратную связь после заполнения опросника, РЦТ отметили, что такой фреймворк был бы полезен для их работы и они готовы рекомендовать его коллегам.

Эту версию фреймворка можно рассматривать как **план воркшопа**: все участники проекта собираются вместе и последовательно отвечают на вопросы. Закрытые вопросы (с ответом «да/нет») желательно сопровождать краткими комментариями. Ответы на открытые вопросы обсуждаются в команде и фиксируются прямо в опроснике. Желательно при обсуждении ответов понимать, где и как именно они могут быть зафиксированы в документах проекта: ответы известны и зафиксированы, ответы известны, но нигде не зафиксированы, ответы найдены во время обсуждения и будут зафиксированы в документации и т. д.

Авторы раздела:


П. А. Алферов


А. Ю. Кирин


С. В. Коршунова


Е. Г. Потапова


Д. О. Теплякова


О. С. Шепелева

[301] Bannister C., Sniderman B., Buckley N. Ethical tech: Making ethics a priority in today's digital organization. Deloitte Development LLC, 2020. URL: https://www2.deloitte.com/content/dam/insights/us/articles/6289_ethical-tech/DI_DR26-Ethical-tech.pdf

[302] Data Ethics Decision Aid (DEDA) // Utrecht Data School. URL: https://dataschool.nl/en/deda/

[303] What is the Data Ethics Canvas? // Open Data Institute. URL: https://theodi.org/article/data-ethics-canvas/

[304] Data Ethics Framework // UK Government. URL: https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework-2020

ОТВЕТСТВЕННАЯ РАЗРАБОТКА ЦИФРОВЫХ РЕШЕНИЙ

На сайте доклада предлагается вариант фреймворка в форме теста для быстрого прохождения (с вариантами ответа). Его можно использовать как анкету для самопроверки, а также в качестве дополнения к документации проекта или при планировании информационной кампании.

1 ОБЩАЯ ИНФОРМАЦИЯ О ЦИФРОВОМ РЕШЕНИИ

1.1. Название решения, дата и место разработки
1.2. Участники проекта

2 ЦЕЛИ

До старта проекта

2.1. Какую пользу принесет цифровое решение тем, кто будет им пользоваться?
2.2. Какую пользу принесет цифровое решение обществу в целом?
2.3. Есть ли группы граждан, которым цифровое решение может навредить?
2.4. Что можно с этим сделать?

В ходе проекта

2.5. Не изменились ли потребности пользователей?
2.6. По-прежнему ли цифровое решение приносит пользу обществу?
2.7. Не произошли ли события, которые могли повлиять на изначальные цели разработки цифрового решения?
2.7.1. (Если да) Как вы можете адаптировать решение к новым условиям?
2.8. Можно ли измерить пользу, которую принесет цифровое решение?
2.9. Есть ли группы граждан, которые не получат от цифрового решения никакой пользы?
2.9.1. (Если да) Что можно с этим сделать?

3 ТЕХНОЛОГИИ РЕАЛИЗАЦИИ ПРОЕКТА

3.1. Какие технические решения будут использоваться в ходе проекта?
3.2. Насколько функционирование проекта будет зависеть от специфики таких решений?
3.3. Почему выбрали именно эти решения?
3.4. Какие варианты рассматривались?
3.5. Были ли у этих решений в прошлом инциденты, связанные с утечками данных или иными нарушениями в области приватности?
3.6. Какие этапы развертывания технологий предусмотрены?
3.7. Будет ли возможность использования (встраивания) сертифицированных ФСТЭК/ФСБ средств защиты информации и/или проведения аттестации решений/проекта по требованиям ФСТЭК/ФСБ?

4 КОМАНДА

4.1. Есть ли в команде четкое распределение полномочий и сфер ответственности?
4.2. Есть ли в команде DPO (Data Protection Officer)[305]?
4.3. Есть ли четкое распределение ролей среди сотрудников, работающих с данными?
4.4. Обладают ли сотрудники уровнем компетенций, необходимым для выполнения своих обязанностей?
4.5. Есть ли в команде человек, ответственный за хранение данных?
4.6. Какие курсы и тренинги, в том числе по хранению данных, нужны членам команды?

5 ЗАИНТЕРЕСОВАННЫЕ СТОРОНЫ

5.1. Перечислите основные заинтересованные стороны проекта.
5.2. Кому этот проект будет полезен?
5.3. Как заинтересованные стороны вовлечены в процесс создания цифрового решения?
5.4. Как учитывается клиентский опыт при разработке цифрового решения?
5.5. Есть ли группы граждан, чьи возможности может ограничить цифровое решение?
5.6. Какие группы граждан будут непосредственно вовлечены в работу цифрового решения?
5.7. Кого проект может затронуть в будущем?
5.8. Понимают ли заинтересованные стороны цель проекта и ход его реализации?

6 КОММУНИКАЦИИ

6.1. Можете ли вы объяснить гражданам, какую пользу принесет цифровое решение?
6.2. Можете ли вы объяснить, в чем суть вашего цифрового решения и как будет проходить его разработка?
6.3. Можете ли вы объяснить, почему вы использовали те или иные данные?
6.4. Можете ли вы объяснить неспециалисту, как работают модели и алгоритмы?
6.5. Проверяли ли вы, насколько выбранные вами каналы коммуникации соответствуют привычным для целевых групп способам получения информации?
6.6. Есть ли каналы обратной связи для пользователей?
6.7. Могут ли пользователи отправить запрос на изменение своих данных или отозвать их?
6.8. Могут ли пользователи подать жалобу?
6.9. Разработаны ли стратегии коммуникации[306] на случай кризисной ситуации?

[305] Подробнее о роли DPO см. раздел 4.2.
[306] Подробнее о коммуникации с пользователями см. раздел 3.3.3.

7 ОБЩЕСТВЕННЫЕ ЦЕННОСТИ

7.1. Приведет ли разработка цифрового решения к ограничению законных прав и интересов каких-то людей и организаций?
7.2. Приведет ли разработка цифрового решения к возникновению дополнительных обязанностей для каких-то людей и организаций?
7.3. Как проект способствует:
— расширению возможностей человека?
— инклюзии слабо представленных слоев населения?
— уменьшению экономического, социального, гендерного, этнического неравенства?
7.4. Повлияет ли цифровое решение на окружающую среду?
7.4.1. (Если да) Как можно уменьшить это влияние?

8 ДОСТУПНОСТЬ И ИНКЛЮЗИВНОСТЬ

7.5. Какова вероятность того, что решение усиливает цифровое неравенство?
7.6. Если вы используете в работе ИИ, оценивались ли данные на предвзятость[307]?
7.7. Что вы сделали, чтобы избежать предвзятости?

8.1. Следуете ли вы стандарту WCAG 2.0 при разработке интерфейсов и при верстке?
8.2. Есть ли аналоговая замена цифровому решению?
8.3. Если вы используете языковые модели для коммуникации с пользователем (например, чат-боты):
— Предупреждаете ли вы пользователя, что с ним говорит не человек?
— Переадресовывается ли вопрос специалисту-человеку, если чат-бот не может решить проблему?
— Кто несет ответственность за решения, принятые ИИ?

9 ДАННЫЕ

Объем данных

9.1. Можно ли достичь целей проекта, используя меньший объем данных?
9.2. Можно ли достичь целей проекта, используя псевдонимизированные или анонимизированные данные?

Контроль доступа

9.3. Используете ли вы данные, с помощью которых можно идентифицировать человека (персональные данные)?
9.3.1. (Если да) Как контролируется доступ к данным?
9.4. У кого из членов команды есть доступ к данным?
9.5. Собираетесь ли вы передавать данные в другие организации? В какие? На каких условиях?
9.6. Есть ли у вас обязательство публиковать данные в открытом доступе?
9.7. Проводилось ли тестирование устойчивости системы к взлому?
9.8. Какие положительные и отрицательные последствия могут быть у публикации всего корпуса данных или его части?

Анонимизация данных

9.9. Проверяли ли вы процессы сбора, хранения и обработки данных на соответствие методическим рекомендациям Роскомнадзора?
9.10. Если в проекте используются анонимизированные данные, ответьте на следующие вопросы.
— Можете ли вы продемонстрировать, что данные были анонимизированы в максимально возможной степени?
— Можно ли соотнести данные с другими дата-сетами, которые сделают возможной идентификацию субъекта данных?
— Какие меры вы приняли, чтобы этого не допустить?
9.11. У кого из команды есть доступ к ключу шифрования, с помощью которого можно соотнести псевдонимизированные данные с их субъектами?

[307] Подробнее о предвзятости алгоритмов см.: Этика и «цифра»: этические проблемы цифровых технологий. В 2 т. М.: РАНХиГС, 2020. URL: https://ethics.cdto.center/

10

РИСКИ

10.1. К каким негативным последствиям может привести внедрение цифрового решения?
10.2. Перевешивают ли эти негативные последствия те риски, которые возникнут, если проект не будет реализован?
10.3. Может ли цифровое решение усугубить социальное, гендерное или этническое неравенство?
  10.3.1. (Если да) Есть ли механизмы, которые помогут вам избежать увеличения неравенства?
10.4. Может ли цифровое решение вызвать возмущение граждан?
10.5. Можно ли с помощью данных, которые вы используете, узнать что-то о частной жизни граждан?
10.6. Есть ли риск, что проект приведет к дискриминации определенных людей или группы людей?
10.7. Все ли группы граждан, которых касается проект, в равной степени представлены в корпусе данных?
10.8. Можете ли вы представить ситуацию, в которой результаты вашего проекта будут использоваться незаконно?
10.9. Что самое плохое может произойти в результате использования (в том числе противоправного) вашего цифрового решения (скандал на местном/региональном/российском/международном уровне)?

Классификация рисков

10.10. Есть ли классификация рисков?
10.11. Сведены ли они в отдельный документ (реестр/карту рисков)?
10.12. Определена ли категория критических рисков?

Стратегии и инструменты управления рисками

10.13. Есть ли стратегия управления рисками?
10.14. Можете ли вы рассказать, какие инструменты управления рисками вы используете?
10.15. Есть ли план мероприятий по снижению рисков?
10.16. Есть ли сотрудник, ответственный за управление рисками?

11

СОБЛЮДЕНИЕ ЗАКОНОДАТЕЛЬСТВА

11.1. Обсуждали ли вы цифровое решение с юристами вашей организации?
11.2. Обсуждали ли вы цифровое решение с отделом информационной безопасности?
11.3. Какие законы и нормативные акты применимы к вашему проекту?
11.4. Проверили ли вы решение на соответствие:
  — Федеральному закону от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
  — Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных»?
11.5. Придерживаетесь ли вы стандартов Ethically Aligned Design (IEEE) и ISO/IEC JTC 1/SC 42 Artificial Intelligence[308]?

[308] Подробнее о стандартах см. раздел 5.3.

6.3 ПРИМЕР ИСПОЛЬЗОВАНИЯ ФРЕЙМВОРКА

Время чтения — 22 минуты

Авторы раздела:

П. А. Алферов

А. Ю. Кирин

Е. Г. Потапова

Д. О. Теплякова

О. С. Шепелева

Чтобы понять, как фреймворк можно использовать на практике, предлагаем изучить вымышленный кейс разработки цифрового решения, который авторы придумали специально для этого доклада. Этот проект очень похож на те, которые действительно разрабатывают руководители и команды цифровой трансформации в России. Кейс максимально приближен к реальности, поэтому в нем есть зоны роста — области, которые могут вызвать этические проблемы. Авторы доклада проанализировали ответы вымышленной проектной команды и предложили возможные пути работы над болевыми точками.

Команда из мэрии города Энска планирует разработать приложение для маломобильных граждан с хроническими и излечимыми заболеваниями опорно-двигательного аппарата «Опора в пути». Работа над приложением планируется в июне — сентябре 2021 года. Команда проекта (включая разработчиков и специалистов по ИБ) организовала воркшоп по выявлению и оценке рисков, связанных с реализацией проекта. Воркшоп прошел 14 апреля 2021 года. В качестве плана воркшопа команда использовала опросник «Ответственная разработка цифровых решений».

Приложение будет включать несколько сервисов:

- запись на прием к специалистам в городские поликлиники;
- поиск кафе, ресторанов, кинотеатров, библиотек и музеев, оборудованных для маломобильных граждан;
- индивидуальное информирование граждан об их заболевании в соответствии с их состоянием здоровья и диагнозом (на основе заполненной анкеты в приложении);
- информирование о новых инициативах и средствах помощи от НКО.

Опросник заполнялся в электронном виде одним из участников команды прямо во время воркшопа. Там, где это необходимо, ответы на закрытые вопросы (с вариантами «да/нет») сопровождаются краткими пояснениями, зафиксированными письменно в ходе воркшопа. Ответы на открытые вопросы резюмируют устные ответы участников команды. Если какой-то вопрос не актуален для проекта, это отмечалось во фреймворке.

БЛОК 1. ОБЩАЯ ИНФОРМАЦИЯ О ЦИФРОВОМ РЕШЕНИИ

1.1. Название решения, дата и место разработки

Приложение «Опора в пути», цикл разработки: июнь — сентябрь 2021 года, г. Энск.

1.2. Участники проекта

Инициатива — мэрия г. Энска; партнеры — министерство здравоохранения Энской области, министерство социальной защиты населения Энской области, АНО «Энский центр гражданских инициатив и социального партнерства», Энское региональное общественное движение инвалидов «Доступная среда для всех».

БЛОК 2. ЦЕЛИ

До старта проекта

2.1. Какую пользу принесет цифровое решение тем, кто будет им пользоваться?

Маломобильные люди получат больше возможностей: смогут посещать больше мест в городе (кафе, кинотеатры, библиотеки и т. д.), получать сопровождение в органах социальной поддержки, получать актуальную информацию о предназначенных для них сервисах, предоставляемых НКО и коммерческими организациями (реабилитация, образование, спорт, досуг и т. д.).

2.2. Какую пользу принесет цифровое решение обществу в целом?

Приложение сделает городскую среду более доступной, то есть удобной не только для тех, кто маломобилен постоянно, но и для тех, кто маломобилен временно (человек со сломанной ногой, человек с коляской).

2.3. Есть ли группы граждан, которым цифровое решение может принести вред?

Нет.

2.4. Что можно с этим сделать?

Неактуально.

В ходе проекта

2.5. Не изменились ли потребности пользователей?

2.6. По-прежнему ли проект приносит пользу обществу?

2.7. Не произошли ли события, которые могли повлиять на изначальные цели разработки цифрового решения?

2.7.1. (Если да) Как можно адаптировать решение к новым условиям?

Неактуально, однако в ходе обсуждения стало понятно, что необходимы инструменты, которые помогут адаптировать решение к изменениям ситуации. На этом этапе таких инструментов нет.

2.8. Можно ли измерить пользу, которую принесет цифровое решение?

Да. Можно измерить количество пользователей, собирать пользовательский опыт (в том числе через само приложение), отслеживать количество сервисов внутри приложения (участников, которые предоставляют услуги); если мы сотрудничаем с НКО, которые представляют целевую социальную группу, они тоже могут дать отзывы и решения.

2.9. Есть ли группы граждан, которые не получат от цифрового решения никакой пользы?

Да. Например, люди старшего возраста, которые не умеют пользоваться мобильными устройствами, или люди с низким уровнем дохода, которые не могут позволить себе такие устройства.

2.9.1. (Если да) Что можно с этим сделать?

Для людей, которые не умеют пользоваться мобильными устройствами, и для тех, у кого их нет, — находить решения, чтобы люди получали такие устройства (например, субсидирование, организация акций типа «Подари смартфон»).

БЛОК 3. ТЕХНОЛОГИИ РЕАЛИЗАЦИИ ПРОЕКТА

3.1. Какие технические решения будут использоваться в ходе проекта?

Мы создаем приложение для iOS и Android с функцией геолокации и чат-ботом.

3.2. Насколько функционирование проекта будет зависеть от специфики таких решений?

Можно сказать, что функционирование проекта полностью зависит от специфики технологических решений.

3.3. Почему выбрали именно эти решения?

Мы выбираем приложение, а не сайт, потому что важно, чтобы люди пользовались этим в процессе перемещения по городу; для этого же и нужна служба геолокации; чат-бот поможет решить простые вопросы и предоставить персонализированные рекомендации.

3.4. Какие варианты рассматривались?

Другие варианты не рассматривались.

3.5. Были ли у этих решений в прошлом инциденты, связанные с утечками данных или иными нарушениями в области приватности?

Да.

3.6. Какие этапы развертывания технологий предусмотрены?

Стандартные этапы разработки приложения и регулярные обновления после релиза.

3.7. Будет ли возможность использования (встраивания) сертифицированных ФСТЭК/ФСБ средств защиты информации и/или проведения аттестации решений/проекта по требованиям ФСТЭК/ФСБ?

Нет.

БЛОК 4. КОМАНДА

4.1. Есть ли в команде четкое распределение полномочий и сфер ответственности?

Да.

4.2. Есть ли в команде DPO (Data Protection Officer)?

Нет. В нашей организации нет такой должности.

4.3. Есть ли четкое распределение ролей среди сотрудников, работающих с данными?

Нет.

4.4. Обладают ли сотрудники уровнем компетенций, необходимым для выполнения своих обязанностей?

Да.

4.5. Есть ли в команде человек, ответственный за хранение данных?

Нет.

4.6. Какие курсы и тренинги, в том числе по хранению данных, нужны членам команды?

Мы не думали об этом.

БЛОК 5. ЗАИНТЕРЕСОВАННЫЕ СТОРОНЫ

5.1. Перечислите основные заинтересованные стороны проекта.

Мэрия г. Энска, люди с заболеваниями опорно-двигательного аппарата, люди, осуществляющие уход за ними, частные компании-партнеры, НКО.

5.2. Кому этот проект будет полезен?

Людям с заболеваниями опорно-двигательного аппарата, людям, осуществляющим уход за ними, частным компаниям-партнерам, НКО.

5.3. Есть ли группы граждан, чьи возможности может ограничить цифровое решение?

Нет.

5.4. Какие группы граждан будут непосредственно вовлечены в работу цифрового сервиса?

Сотрудники НКО и сотрудники коммерческих структур, предоставляющих услуги для людей с заболеваниями опорно-двигательного аппарата, служба соцзащиты, медицинские организации.

5.5. Кого проект может затронуть в будущем?

Возможно, людей с нарушениями опорно-двигательного аппарата, которые живут в интернатах или других организациях.

5.6. Понимают ли заинтересованные стороны цель проекта и ход его реализации?

Да. Мы уже провели консультации с партнерскими НКО, сетью кафе и руководством двух крупных городских ТРЦ. Кроме того, мы планируем кампанию по информированию целевой аудитории.

БЛОК 6. КОММУНИКАЦИИ

6.1. Можете ли вы объяснить гражданам, какую пользу принесет цифровое решение?

Да. Мы планируем информационную кампанию для целевой аудитории, а также информационное сотрудничество с НКО.

6.2. Можете ли вы объяснить, в чем суть вашего цифрового решения и как будет проходить его разработка?

Да.

6.3. Можете ли вы объяснить, почему вы использовали те или иные данные?

Да. В приложении будут оповещения, которые объясняют пользователям, почему мы собираем данные.

6.4. Можете ли вы объяснить неспециалисту, как работают модели и алгоритмы?

Нет. Пока что мы не готовы это сделать.

6.5. Проверяли ли вы, насколько выбранные вами каналы коммуникации соответствуют привычным для целевых групп способам информации?

Да, с распространением информации нам помогают партнерские НКО. Например, одним из каналов коммуникации будет реклама в холлах в поликлиниках.

6.6. Есть ли каналы обратной связи для пользователей?

Да, обратную связь можно давать прямо в чат-боте. Кроме того, есть система оценок (рейтинга) каждого сервиса.

6.7. Могут ли пользователи отправить запрос на изменение своих данных или отозвать их?

Нет. Пока у нас нет такого механизма, мы не подумали об этом.

6.8. Могут ли пользователи подать жалобу?

Да. Внутри приложения можно оставить жалобу на сервис или услугу, которую мы предлагаем.

6.9. Разработаны ли стратегии коммуникации на случай кризисной ситуации?

Сейчас четко видим две группы реальных рисков. Первая — плохая координация между сервисом и ведомством или учреждением, которое предоставляет услуги. Например, система записи к врачам в каких-то поликлиниках не будет достаточно связана с приложением, и человека, который записался к врачу через приложение, не примут в поликлинике в выбранное при записи время. Вторая — недобросовестность со стороны коммерческих партнеров. Например, в киноцентре номинально будет туалет для людей на колясках, но на практике он не будет работать или не будет достаточно приспособлен для них. Наша основная стратегия — своевременно реагировать на жалобы и исключать из приложения недобросовестных партнеров.

БЛОК 7. ОБЩЕСТВЕННЫЕ ЦЕННОСТИ

7.1. Приведет ли разработка цифрового решения к ограничению законных прав и интересов каких-то людей и организаций?

Нет.

7.2. Приведет ли разработка цифрового решения к возникновению дополнительных обязанностей для каких-то людей и организаций?

Нет.

7.3. Как проект способствует:

— расширению возможностей человека?

— инклюзии слабо представленных слоев населения?

— уменьшению экономического, социального, гендерного, этнического неравенства?

Ответы на эти вопросы вытекают из целей нашего приложения: оно как раз направлено на расширение возможностей человека и инклюзию.

7.4. Повлияет ли цифровое решение на окружающую среду?

Нет.

7.4.1. (Если да) Как можно уменьшить это влияние?

Неактуально.

7.5. Какова вероятность того, что решение усиливает цифровое неравенство?

Эта вероятность есть. Для того чтобы ее избежать, мы будем принимать меры, описанные в ответе на вопрос 2.9.1.

7.6. Если вы используете в работе ИИ, оценивались ли данные на предвзятость?

Нет.

7.7. Что вы сделали, чтобы избежать предвзятости?

Неактуально.

БЛОК 8. ДОСТУПНОСТЬ И ИНКЛЮЗИВНОСТЬ

8.1. Следуете ли вы стандарту WCAG 2.0 при разработке интерфейсов и при верстке?

Мы не знаем, что есть такой стандарт.

8.2. Есть ли аналоговая замена цифровому решению?

Для записи на прием в государственные учреждения и взаимодействия с НКО — да. Для сервиса поиска доступных коммерческих учреждений — нет.

8.3. Если вы используете языковые модели для коммуникации с пользователем (например, чат-боты):

— Предупреждаете ли вы пользователя, что с ним говорит не человек?

Да.

— Переадресовывается ли вопрос специалисту-человеку, если чат-бот не может решить проблему?

Да.

— Кто несет ответственность за решения, принятые ИИ?

Планируется, что чат-бот будет давать ответы на простые вопросы. Решения будет принимать сам пользователь.

БЛОК 9. ДАННЫЕ

Объем данных

9.1. Можно ли достичь целей проекта, используя меньший объем данных?

Нет. Данные геолокации нужны для определения ближайших доступных кафе, кинотеатров, магазинов и т. п., данные о диагнозе — для получения актуальной и персонализированной информации о вариантах соцподдержки и других полезных услугах.

9.2. Можно ли достичь целей проекта, используя псевдонимизированные или анонимизированные данные?

Неактуально.

Контроль доступа

9.3. Используете ли вы данные, с помощью которых можно идентифицировать человека (персональные данные)?

У наших пользователей бывают очень редкие диагнозы. Мы осознаем, что некоторые данные о здоровье в случае утечки можно соотнести с субъектом этих данных. Поэтому мы сразу относимся к данным о здоровье как к персональным. Наш отдел информационной безопасности делает все, чтобы не допустить утечек.

9.3.1. (Если да) Как контролируется доступ к данным?

Этим занимается отдел ИБ.

9.4. У кого из членов команды есть доступ к данным?

У тимлида разработчиков.

9.5. Собираетесь ли вы передавать данные в другие организации? В какие? На каких условиях?

Мы сами не передаем данные в другие организации. Однако если пользователь, например, записывается через наше приложение на прием к врачу, он соглашается на передачу данных в поликлинику.

9.6. Есть ли у вас обязательство публиковать данные в открытом доступе (или, наоборот, не публиковать их)?

Такого обязательства у нас нет, но с согласия пользователя мы можем включить его в статистику того, как часто приложение использовалось для записи в социальные службы или на прием к врачу.

9.7. Проводилось ли тестирование устойчивости системы к взломам?

Протестируем, когда будет создана сама система.

9.8. Какие положительные и отрицательные последствия могут быть у публикации всего корпуса данных или его части?

Неактуально.

Анонимизация данных

9.9. Проверяли ли вы процессы сбора, хранения и обработки данных на соответствие методическим рекомендациям Роскомнадзора?

Нет, но проверка планируется.

9.10. Если в проекте используются анонимизированные данные, ответьте на следующие вопросы.

— Можете ли вы продемонстрировать, что данные были анонимизированы в максимально возможной степени?

Да, это могут сделать наши специалисты по ИБ.

— Можно ли соотнести данные с другими дата-сетами, которые сделают возможной идентификацию субъекта данных?

Нет.

— Какие меры вы приняли, чтобы этого не допустить?

Меры по контролю доступа, которые зафиксированы в регламенте по управлению данными.

9.11. У кого из команды есть доступ к ключу шифрования, с помощью которого можно соотнести псевдонимизированные данные с их субъектами?

Ни у кого.

БЛОК 10. РИСКИ

10.1. К каким негативным последствиям может привести внедрение цифрового решения?

В случае утечки данных может сложиться ситуация, когда данные могут быть использованы неправомерно.

10.2. Перевешивают ли эти негативные последствия те риски, которые возникнут, если проект не будет реализован?

Нет.

10.3. Может ли цифровое решение усугубить социальное, гендерное или этническое неравенство?

Нет.

10.3.1. (Если да) Есть ли механизмы, которые помогут вам этого избежать?

Неактуально.

10.4. Может ли цифровое решение вызвать возмущение граждан?

Нет.

10.5. Можно ли с помощью данных, которые вы используете, узнать что-то о частной жизни граждан?

Да.

10.6. Есть ли риск, что проект приведет к дискриминации определенных людей или группы людей?

Нет.

10.7. Все ли группы граждан, которых касается проект, в равной степени представлены в корпусе данных?

Неактуально.

10.8. Можете ли вы представить ситуацию, в которой результаты вашего проекта будут использоваться незаконно?

Это может произойти в случае утечки данных, но мы делаем все, чтобы ее не допустить.

10.9. Что самое плохое может произойти в результате использования (в том числе противоправного) вашего цифрового решения (скандал на местном/региональном/российском/международном уровне)?

Самый плохой вариант развития событий — утечка персональных данных о здоровье пользователей приложения. Мы предполагаем, что это риск скандала регионального уровня, однако если среди пользователей приложения будут публичные персоны, скандал может стать общероссийским. Еще один серьезный риск, если окажется, что мы не сможем в полной мере гарантировать добросовестность партнеров. Это сильно скомпрометирует и наш проект, и подобные социальные проекты в целом.

Классификация рисков

10.10. Есть ли классификация рисков?

Да, стандартная классификация «высокий риск — средний риск — низкий риск».

10.11. Сведены ли они в отдельный документ (реестр/карту рисков)?

Да.

10.12. Определена ли категория критических рисков?

Да.

Стратегии и инструменты управления рисками

10.13. Есть ли стратегия управления рисками?

Пока нет.

10.14. Можете ли вы рассказать, какие инструменты управления рисками вы используете?

Да, оценку влияния и оценку вероятности.

10.15. Есть ли план мероприятий по снижению рисков?

В процессе разработки.

10.16. Есть ли сотрудник, ответственный за управление рисками?

Да.

БЛОК 11. СОБЛЮДЕНИЕ ЗАКОНОДАТЕЛЬСТВА

11.1. Обсуждали ли вы цифровое решение с юристами вашей организации?

Да, в команде проекта работают два юриста.

11.2. Обсуждали ли вы цифровое решение с отделом информационной безопасности?

Да.

11.3. Какие законы и нормативные акты применимы к вашему проекту?

Федеральный закон от 17.07.1999 № 178-ФЗ «О государственной социальной помощи» (с учетом внесенных изменений);

Федеральный закон от 27.07.2010 № 210-ФЗ (ред. от 30.12.2020) «Об организации предоставления государственных и муниципальных услуг» (с изм. и доп., вступ. в силу с 01.01.2021);

Федеральный закон от 24.11.1995 № 181-ФЗ «О социальной защите инвалидов в Российской Федерации» (с учетом внесенных изменений).

11.4. Проверили ли вы решение на соответствие:

— Федеральному закону от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»?

Да.

— Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных»?

Да.

11.5. Придерживаетесь ли вы стандартов Ethically Aligned Design (IEEE) и ISO/IEC JTC 1/SC 42 Artificial Intelligence?

Нет.

КОММЕНТАРИЙ: ЗОНЫ РОСТА

Эксперты, проанализировав ответы на опросник, выделили очевидные болевые точки проекта (критические зоны отмечены красным цветом; важные, но не критические области — желтым). К красным зонам эксперты предложили краткие комментарии.

ЗОНА РОСТА «КОМАНДА»

4.2. Есть ли в команде DPO (Data Protection Officer)?

— Нет. В нашей организации нет такой должности.

Даже если такой должности нет в организации, можно выбрать человека в команде, имеющего достаточный уровень квалификации и достаточное количество времени, который будет выполнять функции DPO, совмещая их с другими задачами.

4.3. Есть ли четкое распределение ролей среди сотрудников, работающих с данными?

— Нет.

Рекомендуется распределить роли среди специалистов по данным, работающих в команде, и отразить это в соответствующих документах. Важно, чтобы все участники команды понимали не только свою роль, но и роли коллег по проекту, чтобы была возможность оперативно решать возникающие проблемы/вызовы.

4.5. Есть ли в команде человек, ответственный за сохранение данных?

— Нет.

Критически важно выделить эту функцию, в том числе для демонстрации всем заинтересованным в проекте сторонам (внутренним и внешним).

ЗОНА РОСТА «КОММУНИКАЦИИ»

6.7. Могут ли пользователи отправить запрос на изменение своих данных или отозвать их?

— Нет. Пока у нас нет такого механизма, мы не подумали об этом.

Это критически важный элемент управления данными. Он поддерживает автономию пользователя (возможность самостоятельно принимать решения о своих ПДн) и, соответственно, повышает доверие к сервису.

6.9. Разработаны ли стратегии коммуникации на случай кризисной ситуации?

— Сейчас четко видим две группы реальных рисков. Первая — плохая координация между сервисом и ведомством или учреждением, которое предоставляет услуги. Например, система записи к врачам в каких-то поликлиниках не будет достаточно связана с приложением, и человека, который записался к врачу через приложение, не примут в поликлинике в выбранное при записи время. Вторая — недобросовестность со стороны коммерческих партнеров. Например, в киноцентре номинально будет туалет для людей на колясках, но на практике он не будет работать или не будет достаточно приспособлен для них. Наша основная стратегия — своевременно реагировать на жалобы и исключать из приложения недобросовестных партнеров.

Недобросовестных коммерческих партнеров действительно можно удалить из приложения на основании поданных жалоб. Однако у команды не разработаны стратегии коммуникации для государственных партнеров, чьи услуги безальтернативны. Проектной группе нужно быть готовой к тому, что им придется решать проблемы с каждой конкретной организацией путем переговоров. Чтобы этого избежать, нужно провести очень тщательную подготовительную работу по заключению договоренностей. Еще один риск, который упустила команда проекта, — отсутствие или недостаточное число коммерческих структур, готовых стать партнерами. Без них приложение будет малополезно для целевой группы. Команде необходимо продумать механизм привлечения партнеров.

ЗОНА РОСТА «ОБЩЕСТВЕННЫЕ ЦЕННОСТИ»

7.6. Если вы используете в работе ИИ, оценивались ли данные на предвзятость?

— Нет.

Предвзятость алгоритмов — один из самых распространенных рисков. Существуют инструменты, которые помогут выявить предвзятость и минимизировать ее (например, AI Fairness от IBM).

ЗОНА РОСТА «ДОСТУПНОСТЬ И ИНКЛЮЗИВНОСТЬ»

8.1. Следуете ли вы стандарту WCAG 2.0 при разработке интерфейсов и при верстке?

— Мы не знаем, что есть такой стандарт.

Команде разработчиков неизвестны международные стандарты инклюзивного и этичного дизайна, которыми необходимо руководствоваться при создании приложения для уязвимой группы населения. Это может значительно снизить доступность приложения для целевой группы, таккак двигательные ограничения могут сопровождаться другими особенностями, которые не позволяют с удобством пользоваться обычными интерфейсами.

ЗОНА РОСТА «ДАННЫЕ»

9.3.1. Как контролируется доступ к данным?

— Этим занимается отдел ИБ.

Наличие отдела ИБ и его добросовестная работа не гарантируют абсолютную защиту от утечек данных. Все члены команды должны знать, какие существуют риски при работе с чувствительными данными, и понимать, какие действия (пусть даже неосознанные) могут поставить под угрозу безопасность данных.

ЗОНА РОСТА «РИСКИ»

10.13. Есть ли стратегия управления рисками?

— Пока нет.

Стратегия управления рисками должна быть сформирована на раннем этапе разработки проекта и пересматриваться по мере его реализации.

Результаты тестовой работы с опросником говорят о том, что он может быть полезен для выявления этических болевых точек на ранней стадии проекта. Безусловно, фреймворк не дает абсолютной гарантии этичности сервиса, однако он поможет команде прояснить вопросы, которые могут оставаться в тени при разработке продукта. Кроме того, сам процесс заполнения опросника даст возможность не только структурировать видение сервиса с этической точки зрения, но и тщательнее проанализировать риски, наметить пути их снижения.

6.4 ПЕРВЫЕ ШАГИ

Время чтения — 5 минут

Автор раздела:

М. В. Туманова

Предложенный выше фреймворк — это инструмент, требующий обсуждения и тщательной проработки в команде. Его цель — провести аналитическую работу над этическими рисками, поставить вопросы и выявить зоны роста. Следующим этапом должно стать применение полученных выводов на практике.

Создание этичного цифрового решения предполагает выполнение ряда шагов, описанных ниже. Их последовательность можно менять, если этого требует логика разработки. Некоторые шаги могут повторяться, например при создании различных прототипов одного решения или при внесении изменений в прототип.

Шаг 1. Продумайте и сформулируйте **цели создания цифрового решения** (подробнее см. блок 2 в разделе 6.3).

Шаг 2. Проанализируйте **альтернативы**: дальнейшее развитие услуги/функции без цифрового решения или дальнейшее развитие услуги/функции с цифровым решением. Зафиксируйте преимущества и недостатки каждого варианта. (Подробнее см. блок 7 в разделе 6.3.)

Шаг 3. Оцените **два вида рисков** при внедрении цифрового решения: 1) риск ошибочного получения услуги / исполнения функции; 2) риск ошибочного неполучения услуги / неисполнения функции.

Шаг 4. На основании шагов 2 и 3 **обоснуйте** необходимость разработки цифрового решения в данный момент.

Шаг 5. Изучите существующие **этические документы и кодексы**, касающиеся разработки и использования цифровых технологий, как глобальные, так и более узкие (национальные, отраслевые, технические). Выберите подходы и принципы, которые необходимо будет использовать при создании и эксплуатации цифрового решения.

Шаг 6. Проанализируйте **обратную связь от пользователей**, привлеките стейкхолдеров для выявления их этических ценностей и учета их интересов в новом цифровом решении. (См. также блок 5 в разделе 6.3.)

Шаг 7. Определите, как понимают этичное использование нового цифрового решения его заказчики, разработчики и владельцы. Разработайте **общее понимание** и зафиксируйте его в документах, чтобы избежать в дальнейшем конфликта ценностей. Максимально четко и подробно укажите все этические требования к цифровому решению и его ограничения в документации для разработчика.

Шаг 8. Убедитесь, что приоритетом при разработке решения является **благополучие пользователя**. Цифровое решение не должно содержать в себе этические дилеммы.

Шаг 9. Определите **зоны ответственности** заказчиков, разработчиков, владельцев и пользователей решения, закрепите их в документации.

Шаг 10. Доведите этические принципы и требования до каждого в команде разработки сервиса, при необходимости проведите обучение. Назначьте ответственного сотрудника, который будет **фокусировать внимание команды на этических вопросах**. (См. также блок 4 в разделе 6.3.)

Шаг 11. Убедитесь, что после разработки и внедрения цифрового решения **будут сохранены альтернативные (нецифровые) способы** получения услуги или осуществления функции.

Шаг 12. Обеспечьте соответствие цифрового решения требованиям **информационной безопасности**. Решение должно обеспечивать полную защиту от утечек данных (принцип zero tolerance), любая утечка должна рассматриваться как ЧП и служить поводом к переработке решения и/или правил работы с ним.

Шаг 13. Определите **минимальные ПДн пользователя**, которые будут нужны для работы вашего цифрового решения, избегайте накопления излишних ПДн. Определите, каких именно данных, получаемых при идентификации пользователя через ЕСИА, Единую биометрическую систему и другие системы, вашему сервису будет достаточно. (См. также блок 9 в разделе 6.3.)

Шаг 14. Установите **правила обработки, хранения, уничтожения ПДн**. Определите, будут ли обезличенные данные пользователя передаваться другим организациям, если да — то каким и на каких условиях. Предоставьте пользователю информацию о том, кто имеет доступ к его ПДн, предусмотрите для него простую и понятную процедуру регулирования этого доступа.

Шаг 15. Используемые в цифровом решении **алгоритмы должны быть прозрачными и понятными** для пользователя (решение не должно быть «черным ящиком»). Применяйте требования по соблюдению этичности на каждом уровне работы цифрового решения, вплоть до самых рутинных операций. Если в решении используется робот или чат-бот, предусмотрите информирование об этом пользователя каждый раз, когда начинается общение с роботом или чат-ботом.

Шаг 16. Привлеките тестировщиков («белых хакеров»), чтобы найти уязвимости сервиса. Соберите фокус-группу пользователей и узнайте их мнение о работе сервиса. Убедитесь, что сервис доступен для всех категорий граждан, нет дискриминации и ограничений. Проведите **оценку воздействия** сервиса на пользователя.

Шаг 17. Предусмотрите способы **повышения доверия** пользователя к сервису: независимый аудит, открытость, публикацию протоколов, фиксацию и признание ошибок. Разработайте информационно-разъяснительные материалы для будущих пользователей, проведите информационную кампанию, чтобы снизить сопротивление и привлечь пользователей к новому сервису. (См. также блок 6 в разделе 6.3.)

ВЫВОДЫ. НА ЧТО ОПЕРЕТЬСЯ ПРИ ОЦЕНКЕ ЦИФРОВОГО СЕРВИСА

В повседневной работе госслужащий постоянно принимает решения. Несмотря на жесткие рамки, в первую очередь регуляторные, у него все же есть определенная свобода действий. В случае создания цифровых инструментов перед госслужащим встает вопрос выбора концепции, дизайна, способа обработки данных и т. д. Поскольку государственные цифровые решения влияют на большое количество людей и организаций, важно, чтобы этот выбор был сделан осознанно, с учетом максимального количества возможных рисков, в том числе и этических.

Принять этичное решение при разработке цифрового сервиса или инструмента помогает ценностно ориентированный подход, основной принцип которого — доверие. Как и во многих других областях управления, при разработке и внедрении цифровых сервисов доверие граждан складывается из открытости процесса, справедливости решений и добросовестности людей, которые их принимают. Фреймворки и чек-листы помогают организовать процесс принятия решений так, чтобы следовать этим ценностям. Эти инструменты помогают задуматься об этических вопросах, которые могли остаться незамеченными при разработке цифрового решения.

7. ОТВЕТСТВЕННОСТЬ РАЗРАБОТЧИКА

«Нам нужен программист: а — небалованный, бэ — доброволец, цэ — чтобы согласился жить в общежитии...» — «Дэ, — подхватил бородатый, — на сто двадцать рублей». — «А как насчет крылышек? — спросил я. — Или, скажем, сияния вокруг головы?»

А. и Б. Стругацкие.
Понедельник начинается в субботу

7.1 ГРАНИ ОТВЕТСТВЕННОСТИ: ЗАКАЗЧИК, РАЗРАБОТЧИК, ПОЛЬЗОВАТЕЛЬ

Время чтения — 15 минут

ИТ-специалисты, стараясь создать работающий сервис, склонны недооценивать важность этической составляющей. Государственный заказчик зачастую не считает необходимым прямо указывать в техническом задании этические требования, разработчик-исполнитель не выходит за рамки ТЗ — и в результате этика цифрового сервиса «теряется» в процессе его разработки.

Наверное, трудно спорить с тем, что государственные цифровые сервисы пока далеки от совершенства. Системные проблемы, такие как неудобство, нестабильная работа, уязвимости, правовая неотрегулированность, затрудняют их использование, приводят к потерям времени и прямому

ущербу для граждан. Тестирование сервиса, которое выполняется в процессе разработки, не может гарантировать его длительную и безупречную работу в различных условиях, не всегда должным образом изучаются и учитываются потребности разных клиентов.

Все больше государственных услуг переходит в цифровой формат, появляются новые услуги, ставшие возможными только в цифровой среде, государство все более активно использует возможности мобильных приложений и интернета вещей. При всей очевидной пользе для граждан (например, выплаты нуждающимся можно оформлять проактивно), этот тренд вызывает много опасений.

Роль госслужащих становится более значимой, их ответственность растет (подробнее см. раздел 1), но при этом многие государственные цифровые решения этически несовершенны еще на уровне планирования и проектирования (особенно связанные с отслеживанием передвижения, распознаванием лиц и т. д.), их проверкой и оценкой никто не занимается. Ведь даже безукоризненно сделанные цифровые продукты вызывают целый ряд этических вопросов, а большинству государственных продуктов в России, даже самым лучшим, далеко до совершенства.

«Много лет не имела системного решения распространенная проблема: из-за ошибочного присвоения одному физлицу двух и более ИНН у него возникают налоговые задолженности. Попытки обращения в госорганы не приводили к решению проблемы. Сотрудники ФНС на местах видели явную ошибку, но фактически оставались заложниками сложившейся системы, не имея возможности ни устранить ошибку, ни повлиять на доработку системы.

Другая проблема связана с внедрением электронной подписи (ЭП). От действий мошенников, которые ее подделывают, страдают и государство, оплачивая возврат НДС по отчетности, оформленной с фальшивыми ЭП, и граждане, теряющие свою собственность[309]. Лишь в 2020 году на портале „Госуслуги“ появился сервис, который позволяет гражданину проверить, какие сертификаты электронных подписей ему выдавались. Де-юре граждане и организации могут обжаловать возникающие проблемы в суде. Де-факто судебной системе не хватает компетенций для работы с такими делами. Это фундаментальная институциональная проблема».

Константин Синюшин,
управляющий партнер The Untitled Ventures

Авторы раздела:

С. С. Коротких

К. С. Синюшин

[309] Скобелев В. МВД предложило лишать свободы за подделку электронной подписи // РКБ. URL: https://www.rbc.ru/technology_and_media/18/05/2021/60a3e8759a7947e88055018b

Хорошим выходом из ситуации могла бы стать система независимого аудита государственных цифровых сервисов, а также наделение разработчика особой ответственностью и публикация протоколов испытаний сервиса. Каждый случай некорректной работы приложений, который имеет последствия для жизни и деятельности людей, должен обсуждаться, государство не должно закрывать на них глаза. Необходима работающая система сдержек и противовесов. Во всех странах, где развивается цифровая экономика, возникают похожие проблемы (см. разделы 2.1 и 2.2), но там, где есть независимые институты, цифровые сервисы полнее учитывают интересы разных сторон и вызывают больше доверия.

Частный заказчик может заказать внешний аудит работ, выполненных частным подрядчиком. Госорганизация в России сама заказывает, производит (или принимает у внешнего разработчика), тестирует, внедряет в работу, сама проверяет разработку, не предусматривая внешнего независимого аудита. В итоге всегда есть риск запустить цифровой сервис с серьезными недоработками. Но даже если они проявились после его запуска, культура непризнания ошибок в госсекторе приводит к замалчиванию проблем и усложняет их устранение[310].

> **«У нас в госсекторе владельцев продукта просто нет. Считается, что они должны быть со стороны исполнителя. В результате заказчик не может сформулировать нормально, чего он хочет, а у исполнителя нет стимула сделать все супер. С другой стороны, как только государственные служащие чувствуют, что у них есть какие-то компетенции, они начинают пытаться делать все сами. И это тоже большая проблема».**
>
> **Дарья Двинских, независимый эксперт**

Заказчик, разработчик, пользователь — все они в разной степени несут ответственность за этичную работу цифрового сервиса. По мнению авторов доклада, значительная доля ответственности лежит на заказчике, который еще на этапах формирования ТЗ, тестирования, приемки может и должен предусмотреть этические проблемы и риски своего проекта, а затем на этапе сопровождения — исправлять допущенные ошибки.

Степень ответственности заказчика в госсекторе выше, чем в коммерческом секторе, поскольку государство одновременно выступает здесь и как заказчик, и как регулятор. К тому же в отличие от коммерческих сервисов у гражданина-пользователя, как правило, нет выбора: он не может пойти в другую организацию, чтобы получить водительское удостоверение, материнский капитал или свидетельство о праве собственности на недвижимость.

[310] Типичную ситуацию замалчивания проблемы вместо ее решения на примере утечек персональных данных россиян в государственных цифровых сервисах см.: Бегтин И. Что делать в ситуации, когда за приватность граждан никто не отвечает? // Ivan's Begtin Newsletter on digital, open and preserved government. URL: https://begtin.substack.com/p/13

«Существует фундаментальная проблема недоверия к государству как равноправному субъекту взаимоотношений с гражданином. Государство зачастую ставит гражданина перед фактом: появился новый сервис, в существующий внесены изменения. В качестве примера — перевод правоустанавливающих документов в электронный вид с недостаточной защитой интересов граждан — владельцев собственности. Как было раньше? У человека был подлинник правоустанавливающего документа, у госучреждения — информация об этом документе; человек мог защитить свои права с помощью этого документа, а в случае утери — получить дубликат. Сейчас право собственности не подтверждено бумажным документом и хранится в электронном виде, так что гражданин рискует даже не узнать об изменениях (например, в случае мошенничества)».

Константин Синюшин,
управляющий партнер The Untitled Ventures

Разработчик на этапах разработки и тестирования должен предлагать заказчику технические решения с учетом этических рисков, наращивать свои цифровые компетенции и помогать заказчику стать более знающим, осведомленным, не ссылаясь на то, что, раз этого не было в ТЗ, «значит, меня не касается». Государственный сектор предъявляет к разработчикам дополнительные требования: использовать методы безопасного программирования[311], особенно внимательно относиться к использованию открытого кода (популярная в бизнесе практика не всегда подходит для государственных сервисов), осознавать свою моральную ответственность за разработки, которые повлияют на жизнь многих, если не всех граждан страны.

Глобальная задача заказчика — составить ТЗ с учетом потребностей всех заинтересованных сторон, не нарушая при этом этические принципы[312]. Во взаимодействии заказчика и разработчика важно регламентировать моменты, которые могут затрагивать чьи-либо интересы.

При постановке задачи и создании цифрового решения у заказчика есть ряд обязанностей.

Детально обсудить условия контракта. Создать четкое ТЗ, подробно описать результат. Внести в ТЗ решения этического плана, например минимизацию объема собираемых пользовательских данных и периода их хранения, принципы и правила уничтожения данных по истечении срока хранения или при закрытии проекта и т. д.

[311] При создании нового цифрового сервиса желательно руководствоваться ГОСТ Р 58412-2019 «Защита информации. Разработка безопасного программного обеспечения».

[312] Помочь в этом призван фреймворк в разделе 6.2. Вопросы фреймворка помогут еще на первых этапах создания цифрового сервиса выявить его слабые места, продумать взаимодействие с пользователями и выявить интересы всех сторон, чтобы затем учесть все эти факторы в ТЗ. Уже разработанные сервисы также можно оценить с по-мощью фреймворка, чтобы выявить потенциальные риски и запланировать необходимые доработки.

Разграничить зоны ответственности. Ответственность за жизненный цикл разработки системы (создание, внедрение, обслуживание, выключение и даже полную разборку системы) несет разработчик. Он должен заранее описать не только процессы внедрения и обслуживания, но также и отключения (демонтажа) системы, в том числе действия с данными, содержащимися в системе.

Определить чувствительность типов данных и уровни доступа к информации, условия работы с ней, роли заказчика и разработчика по отношению к данным.

Создать пользовательское соглашение. Проинформировать пользователя о том, как и с помощью каких систем будут использоваться (храниться, передаваться) его данные. При реализации решения важно предусмотреть информирование пользователя на понятном ему языке (простые тексты без канцеляризмов, наглядные схемы)[313].

Пользоваться только лицензионным программным обеспечением. Оговорить, какое программное обеспечение может использоваться при импортозамещении. Выбор программных и аппаратных решений может влиять на технические возможности разработчика и создавать ограничения, например в сфере ИБ.

Обсудить возможные риски еще на стадии разработки и принять меры для их предотвращения (возможно, внести изменения в ТЗ). Это особенно важно для тех систем, которые управляют жизненно важным производством или существенно влияют на здоровье и благополучие людей. При необходимости проводить широкое общественное обсуждение, привлекая экспертов и регуляторов, которые должны оценить риски и угрозы в зоне их ответственности.

Предусмотреть альтернативный способ, например, получения услуги, который позволит гражданину отказаться от использования цифрового сервиса без ущерба для себя (то есть обеспечить инклюзивность). Для разработки подобных решений госслужащие должны обладать достаточными компетенциями в этических вопросах.

Поддерживать взаимодействие с пользователями на этапе эксплуатации, регулярно проводить клиентские исследования, чтобы улучшать сервис с учетом обратной связи и опыта использования.

Далее на примере, разработанном одним из авторов раздела, будет показано, каким образом при создании экспертной платформы для органов государственной власти может быть применен на практике этичный подход к сбору и обработке персональных данных пользователей (в данном случае — отраслевых экспертов).

[313] См.: Четыре принципа Apple // Medium. URL: https://medium.com/macoclock/the-four-core-privacy-principles-for-apple-according-to-craig-federighi-96d2f5690321

ПРОЕКТ «РАЗРАБОТКА ЭКСПЕРТНОЙ ПЛАТФОРМЫ ДЛЯ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ»

Экспертная платформа создавалась с целью обеспечить быстрое, четкое и качественное взаимодействие сотрудников органа государственной власти (ОГВ) и пользователей — отраслевых экспертов, способных давать квалифицированную и оперативную обратную связь в своей предметной области. Для разработки решения заказчик нанял подрядчика.

На этапах разработки и тестирования платформы подрядчику понадобился доступ как к ПДн экспертов, так и к данным ОГВ, которые необходимы для работы экспертов с информацией. С точки зрения этики заказчик должен выявить чувствительные данные, которые требуют большей защиты; разграничить уровни доступа к данным (секретный характер, ограниченный доступ, общего пользования); определить правила предоставления данных третьим лицам; зафиксировать эти уровни в договоре с подрядчиком о неразглашении конфиденциальной информации.

Популярный подход заказчиков и разработчиков — собирать максимум доступных данных. В случае экспертной платформы это могут быть не только ФИО, контактные данные, сведения об образовании, но и паспортные данные, место фактического проживания, сведения о предыдущем опыте работы, перечень публикаций и многое другое.

С точки зрения этики разработчик должен собирать только самую необходимую информацию. Поэтому в ходе глубинных интервью с пользователями разработчик выяснил, какая минимальная информация ему необходима для запуска продукта (достаточно ФИО, адреса электронной почты и резюме). В дальнейшем заказчик заключил пользовательское соглашение с экспертами, в котором указал типы данных и цели их сбора и обработки.

В чем проявляется этичный подход сторон?

1. **Четко разграничены зоны ответственности заказчика и исполнителя.**
2. **Определяется чувствительная информация и уровень доступа к разным типам данных в зависимости от степени их чувствительности.**
3. **Собирается минимум ПДн пользователей.**
4. **Перечень необходимых данных определяется на этапе разработки исходя из задачи сервиса/продукта.**
5. **Пользователь получает подробное объяснение, какие именно данные и с какими целями собираются.**
6. **При обновлении условий обновляется пользовательское соглашение, пользователей информируют, спрашивают их согласие.**
7. **Пользователь может обозначить свои права и интересы в ходе взаимодействия с заказчиком и разработчиком.**

Пользователь (государственных цифровых сервисов) тоже несет ответственность за происходящее в цифровом мире. Правила кибергигиены давно известны, но пользователи до сих пор оставляют в общедоступных местах пароли, сообщают незнакомым людям коды из СМС, не глядя нажимают «Согласен», переходят по подозрительным ссылкам и т. п.

Государству предстоит повышать цифровую грамотность граждан, обучать их цифровой самозащите. Курсы кибергигиены стали трендом, существуют программы дополнительного образования для школьников.

Международный центр компетенций в Республике Татарстан организует курсы по кибергигиене для детей 13–17 лет. Подростки изучают проблемы безопасности в интернете, учатся обращаться с ПДн, распознавать угрозы и противодействовать им.

Однако граждане обычно не имеют ресурсов, времени, знаний, чтобы полностью обеспечивать свою кибербезопасность. Для большинства людей слишком сложно и трудозатратно каждый раз, передавая государству или бизнесу свои данные, выяснять, достаточные ли меры принимаются для их сохранности, постоянно следить, не взял ли кто-то от их имени кредит и не поменялся ли собственник их квартиры. Кроме того, даже продвинутый пользователь не может предотвратить утечки данных, на условия хранения которых он никак не влияет (см. об этом раздел 2.1).

«Человек может быть некомпетентен в вопросах этики, информационной безопасности, может думать, что персональные данные — это только фамилия, имя, отчество и все. Маленькая галочка „Согласен на обработку персональных данных“ — такая формальность, которая никак не помогает человеку осознать, какие данные и кому он отдает, как они будут храниться, как использоваться, какие риски он на себя принимает. Ответственность оператора данных здесь — прозрачно и понятно объяснять гражданину, в чем его риски, последствия и нюансы использования его данных, поместить эту информацию так, чтобы человеку было просто ее найти. Тогда человек, прежде чем оставить свой номер телефона и другую информацию о себе, сможет задуматься и принять осознанное решение».

Ксения Ткачева, директор Центра подготовки РКЦТ

Когда гражданин не понимает, как защищать свои права, он видит в новых возможностях не пользу, а угрозу. (Подробнее о доверии граждан к государству и «цифре» см. раздел 3.) Это скрытая бомба социального взрыва, и если он произойдет, восстановить доверие будет практически невозможно. Отметим, что в восприятии людей виновным в таком результате будет именно государство.

«Без учета этических норм и постоянной коррекции сервисов в соответствии с ними быстрая цифровая трансформация способов взаимодействия госслужащих (как между собой, так и с гражданами и юридическими лицами) может привести не к удобному сервисному государству, а к отторжению нового инструментария».

Анатолий Дюбанов, РЦТ Новосибирской области

7.2 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Время чтения — 7 минут

Авторы раздела:

А. А. Пьянченко

М. В. Туманова

Обеспечение информационной безопасности — одна из ключевых задач заказчика и разработчика[314]. Сложно говорить о цифровой этике, когда, несмотря на обширную нормативную базу в сфере ИБ, постоянно происходят утечки данных. Нулевая толерантность к нарушению требований ИБ — первый шаг к этичным цифровым сервисам.

Низкий уровень защиты данных — одна из системных проблем сферы ИБ, и это становится серьезным препятствием в развитии технологий. Чем сложнее ИТ-системы, чем больше они влияют на жизнь человека, на общество, на инфраструктуру, тем важнее защита и обеспечение бесперебойной работы систем.

> **«Первый шаг к повышению этичности в цифровой сфере — снижение толерантности к утечкам. Сейчас отношение граждан и профессионального сообщества к постоянным утечкам данных остается несерьезным: защитой данных занимаются спустя рукава, требования ИБ часто выполняют „для галочки“. Недостаточно принимать новые документы, внедрять новые стандарты, необходимо обеспечить возможность их выполнения. Нулевая толерантность (zero tolerance) проявляется в жестком регулировании, выполнении всех возможных обязательных и дополнительных требований ИБ, в расследованиях инцидентов с выявлением виновных, в серьезных наказаниях за кражу данных и халатное отношение к ИБ».**
>
> **Павел Готовцев, координатор российской Рабочей группы IEEE по тематике «Этика и искусственный интеллект»**

Безопасность обработки ПДн контролируется Роскомнадзором, Федеральной службой по техническому и экспортному контролю (ФСТЭК) и ФСБ. Несмотря на большое количество документов и требований, на практике проверки проводятся точечно, нередко никто не несет ответственности за выявленные нарушения, а некоторые из них появляются как результат непродуманных требований регулятора.

Обеспечение ИБ[315] — отдельный бизнес-процесс, который должен регламентироваться специальными документами. В частности, в них описывается **работа с инцидентами**[316]: выявление, оповещение,

[314] Этот раздел не претендует на сколь-нибудь полное освещение темы ИБ в госсекторе, в нем нет обзора нормативной базы в сфере ИБ в России и мире и рекомендуемых технических и организационных решений.

[315] Информационная безопасность организации сертифицируется по международному стандарту ISO/IEC 27000:2016. URL: https://www.iso.org/ru/standard/73906.html

[316] Управление инцидентами информационной безопасности // SearchInform. URL: https://searchinform.ru/informatsionnaya-bezopasnost/dlp-sistemy/upravlenie-intsidentami-informatsionnoj-bezopasnosti/

регистрация, реагирование, расследование и т. п. В отношении обработки и хранения ПДн существует ряд требований, установленных законодательством[317]. Так, любая ИС должна быть классифицирована, после чего для нее определяются модель угроз, модель нарушителя и устанавливается соответствующий класс криптографической защиты.

В российском законодательстве появилось новое понятие — критическая информационная инфраструктура[318] (КИИ). Внесены поправки в Уголовный кодекс; теперь нарушение требований ИБ, касающееся КИИ (неправомерное воздействие, неправомерный доступ или нарушение правил эксплуатации, если оно повлекло причинение вреда КИИ), карается не в административном, а в уголовном порядке: принудительными работами, штрафом или даже лишением свободы до шести лет[319].

Чтобы технический заказчик или разработчик и цифровая команда могли оценить, насколько продукт или сервис учитывает этические аспекты, прежде всего нужно убедиться, что продукт разработан в соответствии с нормативными требованиями. Для этого необходимо пройти процедуру сертификации ФСТЭК и ФСБ, исследовать код на отсутствие недекларируемых или недокументируемых возможностей, оценить эффективность защиты, пройти аттестацию на соответствие требованиям безопасности. В случае создания ГИС такая процедура, кроме прочего, обеспечивает «алиби» при каких-то недостатках или случайных сбоях в работе системы. Ответственность при инциденте уже не будет целиком возложена на владельца системы, ее будет нести и регулятор, который сертифицировал систему.

«Всегда существуют неписаные нормы, здравый смысл, основанный на представлении о том, как не следует делать. Чтобы не допустить ошибку, разработчик должен отслеживать тенденции развития своей отрасли, участвовать в тематических выставках, конференциях, обмениваться мнениями с коллегами. На таких мероприятиях часто обсуждаются этические вопросы: насколько удобен или неудобен для граждан тот или иной сервис, какой эффект вызовет широкое внедрение той или иной технологии».

Андрей Пьянченко, заместитель директора — директор программ ФГАУ НИИ «Восход»

[317] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»; Постановление Правительства РФ от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»; приказ ФСТЭК от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», приказ ФСТЭК от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

[318] Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_220885/

[319] УК РФ. Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации // КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/

При разработке цифровых продуктов для коммерческих структур аттестация ФСТЭК:

- необходима, если компания предоставляет какой-либо государственный сервис;
- возможна, если компания обрабатывает ПДн (проводится оценка соответствия по приказу ФСТЭК от 18.02.2013 № 21, которая может быть проведена в форме аттестации).

Помимо юридической ответственности (например, за нарушение требований ФСТЭК или ФСБ по обеспечению ИБ) возможно наступление ответственности другого рода: политической (для руководителей высокого звена), репутационной (для организации и государства в целом, см. подробнее раздел 3), организационной (например, недостижение КПЭ из-за социальных и экономических последствий принятых решений). Даже в случае выполнения всех требований возможны ситуации, не предусмотренные НПА[320]. Действия в таких ситуациях сильно зависят от этических принципов заказчика и разработчика.

Сразу после анонсирования скорого запуска нового банковского сервиса — снятия наличных в банкомате с чужой карты с помощью QR-кода, который генерирует и отправляет своему знакомому владелец карты, — возник вопрос оценки рисков. Массовое распространение такой услуги может спровоцировать рост кибермошенничества[321]. Среди других возможных негативных последствий — снижение доверия к государству (как регулятору, допустившему проблему), к банковскому сектору и к проведению банковских операций с применением цифровых технологий.

Если государственные органы, как регуляторы или операторы, собирающие данные в больших количествах, не следят за их этичным сбором, обработкой, хранением, недостаточно защищают от утечек, не ограничивают способы их использования, то есть риск, что эти данные будут использованы против граждан. Тем самым государство и отдельные организации создают предпосылки для будущих случаев мошенничества, в то время как существует понятный подход «собирать как можно меньше данных» (подробнее см. разделы 4.1 и 4.2), чтобы в случае утечки ущерб также был минимальным.

[320] По словам вице-президента «Ростелекома» по ИБ Игоря Ляпунова, «когда-то уникальные хакерские технологии сегодня становятся все более распространенными, и стандартные средства защиты, применяемые в госструктурах и субъектах КИИ, оказываются бессильными». См.: НКЦКИ и «Ростелеком-Солар» рассказали об атаках иностранных проправительственных кибергруппировок на российские органы власти // CNews. URL: https://www.cnews.ru/news/line/2021-05-18_nktski_i_rostelekomsolar

[321] Колобова М. Код в мешке: банки разрешат снимать деньги с чужой карты // Известия. URL: https://iz.ru/1164100/mariia-kolobova/kod-v-meshke-banki-razreshat-snimat-dengi-s-chuzhoi-karty

7.3 ВНЕДРЕНИЕ ЭТИЧЕСКИХ НОРМ В ОРГАНИЗАЦИОННУЮ КУЛЬТУРУ

Автор раздела:

М. В. Крель

Время чтения — 12 минут

Недостаточно написать регламентирующие документы и использовать технические средства защиты, требуются еще и изменения в организационной культуре. Как известно, строгость законов компенсируется необязательностью их исполнения[322], а высокая толерантность к неэтичным решениям губит многие благие намерения. При разработке цифровых решений вопросы этики могут составлять отдельный слой в «дорожной карте»; там фиксируются задачи и результаты, декомпозированные из стратегии организации и целей ее развития.

Руководитель играет ключевую роль во внедрении этических норм. Он может повысить уровень этичности в своей организации или в команде, не дожидаясь инструкций сверху. Руководитель — ролевая модель для сотрудников, он подает пример своими поступками и решениями, задает формальные и неформальные правила поведения. При этом, если руководитель говорит о важности этики, но сам поступает неэтично или двусмысленно, люди поверят действиям больше, чем словам. Поэтому без поддержки руководителя, без его личного примера изменения культуры обречены на молчаливое сопротивление или даже провал. Расхождение между словами и делами также может привести к имитации изменений вместо их реальной реализации.

Чтобы заняться вопросами этики и попытаться изменить культуру в организации, у руководства есть несколько отправных точек.

- Обратная связь (не обязательно негативная) от потребителей, клиентов, партнеров, поставщиков решений. Иногда поставщики технологических платформ, решений или экосистем повышают уровень культуры и стандартов, технических и этических.
- Обратная связь от собственных сотрудников, особенно тех, кто напрямую взаимодействует с клиентами.
- Решение руководителя, основанное на его личных ценностях.

Проект внедрения этических норм в организации может пугать масштабом и отсутствием измеряемых результатов, поэтому задачу следует решать поэтапно, шаг за шагом уменьшая неопределенность исходной ситуации и формулируя конкретные цели, способы их достижения и промежуточные результаты для контроля.

[322] Крылатое выражение «Строгость российских законов смягчается необязательностью их исполнения» встречается в разных вариантах; обычно его приписывают М. Е. Салтыкову-Щедрину или другим русским классикам XIX века, см. обзор в Википедии: URL: https://ru.wikipedia.org/wiki/Строгость_российских_законов_смягчается_необязательностью_их_исполнения

Для начала необходимо:

- назначить ответственного за тему этики, провести инвентаризацию ролей (кто может курировать вопросы цифровой этики) и сформировать рабочую группу;
- составить список инструментов и каналов обратной связи: собрать «голос клиента»[323] и честную информацию о доверии, качестве услуг и других факторах для постановки целей и понимания проблемных областей;
- изучить периметр нынешних правил организации в сфере ИБ и защиты данных (использование ИС, работа с данными без ИС, ограничения в использовании персональных гаджетов на рабочем месте и т. п.);
- изучить нормативные документы, регулирующие процессы и взаимодействие с гражданами в тех процессах, в которых планируется внедрять изменения в части этики;
- оценить доступные ресурсы (технические, финансовые и т. д.);
- составить карту заинтересованных сторон (всех, кто влияет на предлагаемое изменение или на кого влияет изменение: групп граждан, смежные организации, поставщиков услуг и т. д.).

Инвентаризация выявит зоны ближайшего развития, поможет спланировать методы оценки первых изменений и следующие шаги. Изучение обратной связи покажет дистанцию между существующим и желательным состоянием организации в той части, которая касается этики в «цифре». Может выясниться, что разрыв большой: низок уровень доверия граждан, их осведомленности, удобства в получении услуг; этика в принятии решений находится на низком уровне или отсутствует. В таком случае потребуется много усилий и серьезная трансформация[324]. Проще улучшить уже существующие сервисы и платформы, оцифровать уже оказываемые услуги. Гораздо сложнее оценивать решения, которые разрабатываются или планируются к разработке, а в случае трансформационных проектов[325] эффекты не могут быть предсказуемыми на 100%[326].

На следующем этапе руководителю необходимо выявить и сформулировать 3–4 самые значимые ценности (желаемое будущее), связанные с культурой и этикой внутри организации и по отношению к клиентам. Хорошо, если в их число входят уважение к гражданам и к собственным сотрудникам. Сформулировать ценности помогут ответы на вопросы:

- Что такое этика для нашей организации на каждом управленческом уровне?

[323] Подробнее о клиентских исследованиях см.: Основные инструменты клиентоцентричного подхода // Клиентоцентричный подход в государственном управлении: навигатор цифровой трансформации / под ред. О. В. Линник, А. В. Ожаровского, М. С. Шклярук. М.: РАНХиГС, 2020. URL: https://cx.cdto.ranepa.ru/5-1-ehtapy-proektirovaniya-klientocentrichnogo-produkta

[324] Подробнее о трансформации оргкультуры и работе с изменениями оргкультуры см. также: Потеев П. М., Крель М. В. Культура цифровой трансформации // Учебник 4CDTO: «О цифровизации и цифровой трансформации». М., 2020.

[325] О трансформационном эффекте цифровых проектов см.: Условия оценки трансформационного эффекта // Стратегия цифровой трансформации: написать, чтобы выполнить / под ред. Е. Г. Потаповой, П. М. Потеева, М. С. Шклярук. М.: РАНХиГС, 2021. URL: https://strategy.cdto.ranepa.ru/6-3-usloviya-ocenki-transformacionnogo-ehffekta

[326] Для оценки этических рисков рекомендуется использовать фреймворк, описанный в разделе 6.2.

- Каковы этические ценности организации? Что самое важное для организации в части этики? Как эти ценности могут конфликтовать между собой?
- Как проявляется конфликт ценностей (как понять, что мы попали в него) и как его решать?

Также рекомендуется сформулировать 3–4 способа поведения, которое следует поощрять, и 3–4 способа дискредитации этических ценностей (для этого на мозговом штурме можно сформулировать «вредные советы»). Все способы формирования и дискредитации ценностей должны быть понятно описаны, чтобы сотрудники в любой момент могли сами оценить свои действия. Чем конкретнее формулировка, тем больше сотрудников сможет следовать новым правилам.

Пример проявления ценности «уважение к гражданам» — предоставление прозрачного и максимально простого способа получения услуги. Если гражданин ради получения услуги проходит непредсказуемый для него «квест», вынужден догадываться, что делать дальше, процесс оказания услуги для него непрозрачен, то это скорее дискредитирует ценность, нежели формирует ее. Противоречия между заявленными ценностями и действиями сотрудников разрушают доверие граждан к органу власти.

К конфликтам ценностей и способов поведения следует относиться как к неотъемлемой части сложной задачи. Например, ценность «уважение к сотрудникам» может войти в противоречие с необходимостью сверхурочной работы ради реагирования на запросы граждан. Такой конфликт ценностей требует выработки правил его разрешения с учетом интересов как граждан, так и сотрудников организации. При этом выбор варианта действий в конфликтной ситуации не должен зависеть только от специалиста по этике или только от руководителя. Необходимо на уровне руководства согласовать систему принятия этических решений с правилами и механизмами[327], общими для всех сотрудников, вовлеченных в трансформацию.

Вопросами этики можно заниматься стратегически, на уровне управления организацией (главная роль у руководителя), и тактически, на операционном уровне. В этом случае этический выбор сужается до конкретных областей, и разработчику или госзаказчику необходим один или несколько сотрудников, глубоко погруженных в тему цифровой этики. (Так, DPO решает задачи организации, связанные с обработкой ПДн, подробнее см. раздел 4.2.) Нельзя допускать, чтобы контроль за этичностью превратился в повод для наказаний.

Главный по этике (назовем его так) должен иметь:

- необходимые полномочия для взаимодействия напрямую с руководителем, для принятия решений в ходе разработки (в том числе право вето), внесения предложений, эскалации рисков;

[327] Например, такая система создана для разрешения конфликта интересов DPO — сотрудника, ответственного за обработку персональных данных в организации, см. подробнее об этом в разделе 4.2.3.

- опыт кросс-функционального взаимодействия, поскольку этические вопросы цифровых технологий связаны со многими бизнес-процессами организации, а в идеале станут частью ее культуры;
- опыт работы на стыке психологии и технологий (технические специалисты при оценке этичности уделяют больше внимания технологической стороне, часто недооценивая психологические аспекты);
- знание специфики организации и понимание, какие области этики могут стать ее зоной развития.

В Республике Татарстан работает единая экосистема, в которую входят министерство цифрового развития государственного управления, информационных технологий и связи, Центр цифровой трансформации (проектный офис, он же государственный заказчик), Центр информационных технологий (государственная ИТ-компания). Есть и должностные лица, обязательные в такой команде; уполномоченный по делам ИИ следит за соблюдением кодекса этики при разработке ресурсов, в том числе ориентированных на проактивное оказание услуг с применением ИИ, машинного зрения и т. д.; замминистра отвечает за ИБ и сохранность ПДн.

Команда минцифры Татарстана сотрудничает с ИТ-компаниями — разработчиками и представителями бизнес-сообщества, готовыми оказывать услуги гражданам. ИТ-специалисты разрабатывают основы безопасности при пользовании системами оказания госуслуг, с помощью «белых хакеров» выявляют случаи мошенничества при получении госуслуг. Вместе они ищут такие варианты, которые не повредят честным людям, имеющим право на получение услуги, и при этом остановят мошенников.

Регулярно (не реже раза в месяц) на встречах ресурсных комитетов рассматриваются выявленные потребности и заявки коллег из других ОГВ, помимо поиска решений в рамках экосистемы оцениваются риски для пользователей, граждан, госорганов и т. д. Конкретные случаи разбирают на архитектурном совете с участием представителей ОГВ и ИТ-компаний муниципалитетов.

Сотрудникам важно понимать смысл и пользу изменений: бессмысленная работа демотивирует, осмысленная, напротив, дает стимул действовать. Поэтому на всех этапах проекта измеряют уровень доверия, уровень удовлетворенности услугами до и после внедрения изменений, в том числе для определения скорости и масштаба изменений. Также необходимо доносить до сотрудников, как именно изменения повлияли на их работу и на жизнь граждан, в чем этические ценности стали проявляться заметнее.

В качестве ориентира можно рекомендовать такой список документов для разработки:

- ценности организации, способы поведения, правила разрешения конфликтов ценностей;
- состав рабочей группы по этике, ее задачи, полномочия и ответственность ее лидера;

- устав и «дорожная карта» проекта с четким образом желаемого состояния и промежуточными результатами;
- для процессов оказания услуг: карта пути пользователя с анализом обратной связи и проблемными областями;
- план обучения сотрудников новым правилам работы;
- методики оценки изменений, показатели для оценки результатов (уровень доверия, удовлетворенности и другие важные параметры);
- план коммуникаций со всеми заинтересованными сторонами на всех этапах проекта.

Уровень цифровой этики зависит от уровня цифровой грамотности. Не зная, как работают цифровые сервисы, к каким последствиям приводят те или иные действия в цифровом пространстве, сотрудник организации может неумышленно создавать этические риски еще на этапе разработки (недооценивать риски, серьезность ситуации и последствия своих шагов) или, наоборот, перестраховываться и не делать то, что необходимо. (Подробнее об этических рисках и проблемах см. раздел 2.)

Обучение сотрудников может быть общим и специализированным. Обучение общей цифровой и этической грамотности необходимо для синхронизации уровня сотрудников, имеющих разное образование, разные представления о хорошем и плохом. Перед началом обучения нужно согласовать его программу с ценностями и принципами организации. Тогда команда будет говорить об этике цифровых решений на одном языке. Специализированное обучение требуется специалистам конкретных направлений (например, DPO).

«Цифровые технологии подрывают устоявшиеся социальные отношения. И проблема нашего времени в том, что таких подрывных технологий уже несколько, они синергетически друг с другом взаимодействуют, так что изменения происходят экспоненциально. Раньше подрывные технологии, например одомашнивание скота, вводились на протяжении длительного времени. Одомашнили — и после этого тысячи лет все было нормально. Сейчас у нас каждый год что-то происходит; изменения настолько катастрофические, что люди не могут их осмыслить. И задача государства как регулятора общественных отношений заключается в том, чтобы, во-первых, общество успокаивать, а во-вторых, позаботиться о том, чтобы люди не остались за бортом перемен. Для этого необходимо развивать образование и повышать квалификацию тех, кто сейчас работает».

Роман Душкин, директор по науке и технологиям Агентства Искусственного Интеллекта

Привыкать к новому всегда сложно, даже если это перемены к лучшему. Следует двигаться маленькими шагами, постепенно, начиная с простых действий, но без длительных перерывов. Внедряя новые правила и нормы, важно не перегружать людей чрезмерными требованиями, иначе возмож-

ны сопротивление и имитация изменений. Большой объем непонятных задач создает риск отказаться от реализации проекта еще на старте, а попытки взяться за все задачи сразу приведут к тому, что не будет реализована ни одна из них.

ВЫВОДЫ. КТО ОТВЕЧАЕТ ЗА ЭТИКУ

Когда государство разрабатывает и внедряет цифровые проекты, ответственность за последствия неэтичных цифровых решений лежит и на госзаказчике (ведомстве, заказавшем разработку, ГИС), и на разработчике (компании или команде, создающей решение). Ответственность гражданина ограничена уровнем его доступа к ИС и сервисам. Также важна роль государства как регулятора, который вводит соответствующие нормы для заказчиков и разработчиков и контролирует их выполнение.

Основные сферы ответственности сторон, вовлеченных в создание и использование цифровых решений, описаны в таблице 3.

Таблица 3. Ответственность участников цифровых проектов

Чья ответственность	Минимальные требования	Желательный уровень
Заказчик (и государство в целом)	› Совершенствовать законодательство и контролировать его соблюдение › Обсуждать и согласовывать ТЗ с внешними специалистами › Определить статус информации › Определить зоны ответственности по обработке данных (кто работает с данными: разработчики или госорган?) › Обеспечить защиту данных › Сохранять аналоговые пути получения услуг › Обучать граждан работе с цифровыми сервисами	› Определять и транслировать ценности и принципы цифровой этики › Собирать информацию о слабых сторонах решений › Внедрять нулевой уровень терпимости к утечкам и нарушениям › Использовать данные, не приводящие к дискриминации › Внедрять подход минимального и обоснованного сбора данных › Внедрять культуру принятия и исправления ошибок (вместо замалчивания)
Разработчик/ исполнитель	› Соблюдать нормы законодательства › Обеспечить защиту данных › Понимать границы своих компетенций, привлекать специалистов в тех областях, где компетенций не хватает, эскалировать риски по дефициту компетенций	› Использовать данные, не приводящие к дискриминации › Проводить глубинные интервью › Совершенствовать практику работы с кодом и публиковать открытый код
Пользователь (гражданин)	› Ознакомиться с инструкциями и правилами › Понимать границы своих цифровых компетенций › Повышать свою ИТ- и кибергигиену	› Давать обратную связь › Осознавать риски, связанные с цифровой беспечностью › Занимать проактивную позицию по отношению к цифровым решениям

8. ЭТИКА В ГОССЕКТОРЕ: ЗАРУБЕЖНЫЙ ОПЫТ

— Послушай, — сказал Форд, все еще погруженный в рекламную брошюру, — какую они штуку придумали. «Новое поколение роботов и компьютеров НЧК, разработанных сириусианской кибернетической корпорацией».
— НЧК? — переспросил Артур. — Что это такое?
— Настоящие Человеческие Качества.

Д. Адамс. Автостопом по галактике

Время чтения — 15 минут

Правительства развитых стран уделяют серьезное внимание этике применения цифровых технологий в государственном управлении. Создано немало интересных документов, руководств и кодексов, наработана практика их использования. Не претендуя на исчерпывающий обзор, предлагаем познакомиться с наиболее полезным, с нашей точки зрения, опытом. Эти опробованные подходы помогут сделать работу с цифровыми технологиями более этичной.

ВЕЛИКОБРИТАНИЯ

Один из лучших примеров методического обеспечения работы госорганов — Великобритания, где существует портал GOV.UK с максимально подробной и удобной информацией по всем направлениям деятельности государственных служб. На этом портале, в частности, опубликовано **Руководство по этичному использованию данных** в органах власти

и в государственном секторе в целом[328]. Руководство содержит общие этические принципы (открытость, ответственность, честность), а также специфичные принципы работы с данными. Для каждого из таких принципов приводятся конкретные шаги по реализации на практике. Приведем два примера.

Проанализируйте качество и полноту данных. Результат внедрения новых технологий зависит от качества данных и методов, которыми они получены. Необходимо убедиться в том, что данные для проекта являются точными, репрезентативными, что они хорошего качества, соразмерно используются и что вы понимаете их ограниченность.

Применение принципа:

- проверка источника данных;
- исключение лишних данных, которые не нужны для конкретной цели;
- обнаружение и удаление ошибок в данных;
- обезличивание данных;
- экспертная проверка алгоритма;
- перевод данных в открытый, доступный для передачи формат;
- подготовка методологии к опубликованию в интернете;
- подготовка простого и понятного широкому читателю объяснения модели.

Оцените политические последствия. Необходимо непрерывно мониторить использование информации, полученной на основе данных. Команды разработки и внедрения, будучи экспертами по корректному использованию моделей данных, должны контролировать это использование с помощью эффективных механизмов подотчетности.

Применение принципа:

- мониторинг корректности и этичности задач проекта на всем его протяжении;
- пересмотр задач проекта, если потребности пользователей изменились;
- организация обучения и долговременной поддержки пользователей;
- привлечение общественного контроля;
- публикация результатов проекта.

Применение каждого принципа в работе конкретного служащего оценивается по пятибалльной шкале, например: 0 баллов — данные,

[328] Data Ethics Framework // GOV.UK. URL: https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework-2020

Авторы раздела:


И. В. Данилин


И. В. Кириченко


К. С. Костюкова


Е. В. Романова


М. В. Туманова


Э. П. Шавлай


Н. В. Шелюбская

используемые в проекте, плохого качества, неподходящие, ненадежные, нерепрезентативные; 5 баллов — данные, используемые в проекте, являются репрезентативными, точными и т. д.

Для решения конкретных задач по работе с данными на сайте есть отдельные руководства, например руководство по обезличиванию данных[329] или руководство по обеспечению воспроизводимости выводов[330].

В автономном правительстве Шотландии создана национальная **экспертная группа по цифровой этике**[331], цель которой — разработка основополагающих принципов создания и внедрения новых технологий, установление критериев, которым должны отвечать все цифровые продукты и услуги. В экспертную группу входят не только ИТ-специалисты, но и эксперты в области общественных наук, творчества и медиа, философии и права. На сайте правительства опубликована **Шотландская стратегия в сфере искусственного интеллекта**[332], построенная на принципах надежности, этичности и инклюзивности. Правительство также проводит открытые конференции по вопросам этичного внедрения цифровых технологий в работу государственных служб[333]. В центре внимания — сохранение доверия граждан.

ГЕРМАНИЯ

При федеральном правительстве Германии работает **Комиссия по этике данных**[334], задача которой — разработка этических принципов для защиты личности, сохранения единства общества и развития информационных технологий. Опубликовано «Мнение комиссии по этике данных»[335], в котором прослежены взаимосвязи между нормами этики и действующим законодательством, описана роль государства в регулировании межотраслевой экосистемы данных, утверждены требования к данным и алгоритмам.

Комиссия также предоставила рекомендации для стратегии федерального правительства в области ИИ[336]. В частности, рекомендовано добавить

[329] Anonymisation: managing data protection risk code of practice // Information Commissioner's Office. URL: https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf

[330] Reproducible Analytical Pipelines // GOV.UK. URL: https://dataingovernment.blog.gov.uk/2017/03/27/reproducible-analytical-pipeline/

[331] National Expert Group on Digital Ethics // Scottish Government. URL: https://www.gov.scot/groups/national-expert-group-on-digital-ethics/

[332] Scotland's Artificial Intelligence Strategy // Scottish Government. URL: https://www.gov.scot/binaries/content/documents/govscot/publications/strategy-plan/2021/03/scotlands-ai-strategy-trustworthy-ethical-inclusive/documents/scotlands-artificial-intelligence-strategy-trustworthy-ethical-inclusive/scotlands-artificial-intelligence-strategy-trustworthy-ethical-inclusive/govscot%3Adocument/scotlands-artificial-intelligence-strategy-trustworthy-ethical-inclusive.pdf

[333] Digital ethics: a framework for trust // Scottish Government. URL: https://consult.gov.scot/digital-directorate/digital-ethics/

[334] Datenethikkommission // Bundesministerium der Justiz und für Verbraucherschutz. URL: https://www.bmjv.de/DE/Themen/FokusThemen/Datenethikkommission/Datenethikkommission_EN_node.html

[335] Opinion of the Data Ethics Commission // Bundesministerium der Justiz und für Verbraucherschutz. URL: https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_EN_lang.pdf?__blob=publicationFile&v=3

[336] Recommendations of the Data Ethics Commission for the Federal Government's Strategy on Artificial Intelligence // Bundesministerium der Justiz und für Verbraucherschutz. URL: https://www.bmjv.de/SharedDocs/Downloads/DE/Ministerium/ForschungUndWissenschaft/DEK_Empfehlungen_englisch.pdf?__blob=publicationFile&v=3

в стратегию два основных этических положения: следовать демократическим этическим и правовым принципам на протяжении всего процесса разработки и применения ИИ; повышать способность граждан и общества действовать осознанно.

ФРАНЦИЯ

Во Франции создан **Национальный комитет по цифровой этике**[337]. В него входят как ИТ-специалисты, работающие в государственных или частных исследовательских организациях, так и философы, врачи, юристы и другие эксперты. Национальный комитет подготовил по поручению премьер-министра заключения по этическим вопросам, связанным с использованием конкретных цифровых приложений, таких как: 1) разговорные агенты (чат-боты); 2) автономные автомобили; 3) программы медицинской диагностики с использованием ИИ.

В стране работает Национальная комиссия по информатике и свободам[338] — независимый административный орган, состоящий из 17 комиссаров (представителей органов власти разного уровня, экспертов). На сайте комиссии опубликованы права гражданина применительно к цифровым технологиям и способы защиты этих прав[339], а также Хартия поддержки для профессионалов в сфере цифровых технологий[340]. В процессе разработки закона «О цифровой республике» комиссия проанализировала этические и социальные проблемы, возникающие в связи с новыми технологиями, и подготовила отчет «Как люди могут сохранить преимущество? Отчет по этическим вопросам, связанным с алгоритмами и искусственным интеллектом»[341].

ШВЕЦИЯ

В Швеции действует **Комитет по технологическим инновациям и этике**[342]. Его задача — выявлять проблемы, связанные с внедрением цифровых технологий, и предлагать правительству изменения нормативных правовых актов. Комитет публикует на своей странице статьи об отдельных цифровых технологиях[343] и разрабатывает специальные инструменты, которые должны помочь госслужащим соблюдать этические нормы в работе[344]. Кроме того, в Швеции существует специальный контрольно-

[337] French National Committee for Digital Ethics // AI-Regulation.com. URL: https://ai-regulation.com/the-french-national-committee-for-digital-ethics/

[338] Commission nationale de l'informatique et des libertés (CNIL).

[339] Les droits pour maîtriser vos données personnelles! // CNIL. URL: https://www.cnil.fr/fr/les-droits-pour-maitriser-vos-donnees-personnelles

[340] La CNIL publie sa charte d'accompagnement des professionnels // CNIL. URL: https://www.cnil.fr/fr/la-cnil-publie-sa-charte-daccompagnement-des-professionnels

[341] Comment permettre à l'homme de garder la main? Les enjeux éthiques des algorithmes et de l'intelligence artificielle / Synthèse du débat public animé par la CNIL dans le cadre de la mission de réflexion éthique confiée par la loi pour une République numérique — Commission nationale de l'informatique et des libertés, Decembre 2017. URL: https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf

[342] Kommittén för teknologisk innovation och etik. URL: https://www.kometinfo.se/in-english/about-us/

[343] Publikationer // Kommittén för teknologisk innovation och etik. URL: https://www.kometinfo.se/rapporter-och-dokument/

[344] Verktyg för självutvärdering av ansvarsfull teknikutveckling — bakgrundsrapport // Kommittén för teknologisk innovation och etik. URL: https://www.kometinfo.se/publikation/verktyg-for-sjalvutvardering-av-ansvarsfull-teknikutveckling-bakgrundsrapport/#.YGRI6a8zZPY

надзорный орган, курирующий **вопросы этики в исследованиях**[345]. Чтобы использовать в работе ПДн людей, исследователь должен подать заявку в этот орган и пройти этическую экспертизу.

ФИНЛЯНДИЯ

С первых шагов развития новых цифровых технологий власти Финляндии подчеркивали необходимость соблюдения принципов справедливости и инклюзивности, превращения цифровых инструментов в доступное общественное благо. При обсуждении проблем ИИ на первое место выдвигается его влияние на общественную мораль и ценности. **Финский центр искусственного интеллекта**[346] публикует результаты исследований, дискуссии и мнения экспертов по вопросам внедрения технологий ИИ в жизнь. Правительство Финляндии опубликовало исследование «Этическая информационная политика в эпоху ИИ»[347], в котором сформулирован главный принцип развития технологий — «в интересах государства, бизнеса и людей».

Финское законодательство в сфере цифровых технологий отличается проработанностью и акцентом на персональную ответственность за возможные проблемы в эксплуатации сервисов. **Закон Финляндии о биобанках**[348] многие страны использовали в качестве образца при формировании своей нормативной базы.

КАНАДА

Правительство Канады приняло **Цифровую хартию**, в которой заявило о доверии как основе цифрового мира: «В этом цифровом мире канадцы должны быть уверены в том, что их конфиденциальность защищена, что их данные не будут использоваться неправомерно и что компании, работающие в этом пространстве, просто и прямо общаются со своими пользователями. Это доверие служит фундаментом, на котором будет построена наша цифровая экономика, основанная на данных»[349].

НИДЕРЛАНДЫ

В Нидерландах действует **Цифровое правительство** Нидерландов[350], которое поставило своей целью содействовать госслужащим, политикам и разработчикам ИТ в повышении качества цифровых услуг, в том числе в создании этичных алгоритмов и установлении правил обработки персональных данных. Цифровое правительство заявляет: «Каждая ситуация индивидуальна. Этические дилеммы в работе с данными не могут быть решены простым определением того, как должны действовать

[345] Värnar människan i forskning. URL: https://etikprovningsmyndigheten.se/

[346] Finnish Center for Artificial Intelligence. URL: https://fcai.fi/

[347] Government report on information policy and artificial intelligence. URL: https://vm.fi/documents/10623/7768305/VM_Tiepo_selonteko_070219_ENG_WEB.pdf

[348] Biobank Act 688/2012. URL: https://www.finlex.fi/en/laki/kaannokset/2012/en20120688_20120688.pdf

[349] Canada's Digital Charter: Trust in a digital world // Government of Canada. URL: https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html

[350] Digitale Overheid. URL: https://www.nldigitalgovernment.nl/about-digital-government/

органы исполнительной власти. Невозможно составить правила для каждой ситуации. Лучше сформулировать общие принципы и решить, как именно мы как правительство будем ответственно обращаться с данными. Затем на учебных курсах мы можем практиковаться в применении этих принципов, используя реальные примеры»[351].

ЯПОНИЯ

Власти Японии были озабочены недостаточной защитой данных и тяжелыми последствиями утечек. Поэтому в 2020 году были ужесточены нормы **закона о защите личных данных**, который предусматривает уголовную ответственность для операторов ПДн за нарушение правил их обработки. В соответствии с новыми положениями закона каждый гражданин может потребовать удаления сведений о себе из любой базы данных[352].

Другая проблема, остро стоящая перед властями страны, — старение населения и связанный с этим «цифровой эйджизм», когда лица старшего возраста оказываются недостаточно вовлеченными в использование новых технологий. Решением стала организация специальных курсов по преодолению цифрового разрыва. Курсы организуются на государственных онлайн-платформах, преподавателями выступают молодые специалисты, что одновременно решает проблему занятости молодежи.

СИНГАПУР

Город-государство Сингапур известен высоким уровнем развития информационных технологий, которые считаются национальным приоритетом. С начала 2000-х годов город формирует и развивает институты **электронного правительства** (e-government), под эгидой которого взаимодействуют все государственные, коммерческие структуры и простые граждане[353]. В 2014 году была объявлена новая правительственная инициатива — проект **«Умная нация» (Smart Nation)**[354]. Проект предусматривает внедрение цифровых технологий в экономику (Digital Economy), государственные структуры (Digital Government) и общество в целом (Digital Society)[355]. Основной прорывной технологией при этом должен стать ИИ. В 2017 году Национальным исследовательским фондом Сингапура (National Research Foundation, NRF) была разработана национальная программа AI Singapore, задачей которой стало объединение усилий всех профильных организаций и исследовательских центров для достижения общенациональных целей[356].

---

[351] Focusing on legislation and public values // Digitale Overheid. URL: https://www.nldigitalgovernment.nl/overview/new-technologies-data-and-ethics/data-agenda-government/focusing-on-legislation-and-public-values/

[352] Comparative table of the current and amended provisions of the APPI // Personal Information Protection Commission, Japan. URL: https://www.ppc.go.jp/files/pdf/20200612_comparative_table_amended_APPI.pdf.

[353] eGov Masterplans // Govtech Singapore. URL: https://www.tech.gov.sg/media/corporate-publications/egov-master-plans#:~:text=eGAP%20I's%20purpose%20was%20to,Delivering%20integrated%20electronic%20services

[354] Smart Nation Sinapore. URL: https://www.smartnation.gov.sg/

[355] Pillars of Smart Nation // Smart Nation Sinapore. URL: https://www.smartnation.gov.sg/why-Smart-Nation/pillars-of-smart-nation

[356] AI Singapore // National Research Foundation. URL: https://www.nrf.gov.sg/programmes

КИТАЙ

Внимание к вопросам конфиденциальности в китайском обществе постепенно растет. В частности, с утечками и незаконным использованием данных борется Управление по вопросам киберпространства КНР. По мнению американских экспертов, регулирование обработки данных в Китае в настоящее время более жесткое, чем в США, но менее системное, чем в ЕС[357]. Китайская специфика выражается в более широком политическом и идеологическом контроле над интернетом и «видимости» пользователя для госструктур. С точки зрения западных ценностей это крайне неэтичная ситуация, но восточная традиция более терпимо относится к деанонимизации гражданина государством.

> **«Китайское общество полагает, что часто критикуемая система социального рейтинга имеет определенные плюсы. Акцент в ней делается не столько на наказания, сколько на поощрения (например, возможность забронировать место в гостинице без предоплаты, что важно с учетом растущего внутреннего туризма; получить беззалоговый кредит и т. п.). При этом большое внимание уделяется безопасности граждан — не только в политическом смысле, но и в части охраны правопорядка».**
>
> **Иван Данилин, заведующий отделом науки и инноваций ИМЭМО РАН**

Таким образом, в Китае формируется своего рода альтернативный подход к этике использования цифровых технологий, при котором неприемлемые для западного человека ограничения компенсируются социально-экономической инклюзией и повышением качества жизни.

ВЫВОДЫ. КУДА ДВИЖЕТСЯ МИР

Можно выделить три подхода, которые развитые страны используют при обращении к этическим проблемам цифровизации:

- создание нормативных и методических документов, описывающих общие принципы разработки и использования цифровых технологий и отдельные правила, обеспечивающие этичность цифрового продукта, такие как обезличивание данных, контроль качества данных, открытость алгоритмов и другие;
- создание специализированного органа (агентства, комитета, комиссии), уполномоченного осуществлять методическую поддержку в сфере этики и контроль соблюдения этических принципов при разработке цифровых технологий.
- стимулирование (через поощрение или принуждение) этического саморегулирования бизнеса — как контура предварительного контроля и/или условия выработки новых подходов и норм.

[357] Pernot-Leplay E. China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.? // Penn State Journal of Law & International Affairs. 2020. Vol. 8 (1). P. 49–117. URL: https://elibrary.law.psu.edu/cgi/viewcontent.cgi?article=1244&context=jlia

Проблема приватности, вероятно, будет обостряться по мере расширения и усложнения цифровых технологий. По мнению Европейской комиссии, это наиболее важная проблема цифровизации с точки зрения этики. Внимательное **отношение к приватности** вытекает из общих подходов ЕС к правам человека и к правам потребителей, а также вызвано беспокойством по поводу возможного несанкционированного доступа к данным представителей других стран, прежде всего тех, где размещены интернет-платформы США и где законодательство значительно либеральнее относится к нарушению приватности. Такая позиция руководства ЕС согласуется и с мнением самих европейцев, 12% из которых вообще не готовы доверять кому-либо персональную информацию[358].

Многие страны — лидеры в сфере развития цифровизации подчеркивают необходимость **обеспечения равного доступа к технологиям**. Инклюзивность является важной характеристикой любого этичного цифрового сервиса. Она абсолютно необходима там, где идет речь о предоставлении государственных услуг или пользовании общественными благами. ИИ и другие новые технологии сопряжены с высоким риском усугубления неравенства вследствие непреднамеренной предвзятости сервисов и решений, ожидаемых ограничений доступа к ним для меньшинств и беднейших слоев населения и других факторов.

Все это меняет идеологию регулирования цифровой этики: акцент смещается от формирования рамок использования новых технологий к обеспечению их этичности уже на стадии научно-технологических работ и вплоть до внедрения решений. Такая идеология предполагает рост участия пользователей и учет доминирующих общественных ценностей, в том числе через диалог с институтами гражданского общества.

Крупные развивающиеся страны следуют в фарватере западных подходов, но на их понимание цифровой этики влияют местные культурные установки, политические и экономические особенности и проблемы развития: государствоцентричный подход, примат социально-экономических соображений и стабильности над «абстрактными» ценностями (анонимность, свобода мнений, частично некорректное использование данных и т. п.).

В России регулирование этики цифровых технологий пока чаще всего выражается в увеличении количества разнообразных нормативных актов. Традиционно этичным считается то, что соответствует закону, хотя наиболее продвинутые компании делают успешные попытки саморегулирования. В ближайшей перспективе наиболее актуальными вопросами этичности цифровых технологий будут приватность, инклюзивность и проблемы, связанные с развитием ИИ.

[358] Shaping the digital transformation in Europe. European Commission DG Communications Networks, Content & Technology. September 2020. Final Report. P. 17. URL: https://ec.europa.eu/digital-single-market/en/news/shaping-digital-transformation-europe

9. ЗАКЛЮЧЕНИЕ. ЭТИКА КАК КОМПАС ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Авторы раздела:

И. Д. Димитров

К. Л. Киселева

Е. Г. Потапова

— Решение принимаешь ты один. Но помнить ты должен, что делаешь это также и за других, кто стоит за твоим плечом.

Джуд Уотсон. Ученик джедая. Осажденный Храм

Время чтения — 9 минут

Если рассматривать «цифру» не как цель, а как средство, как путь к укреплению общественного благосостояния, то этические вопросы оказываются ключевыми для успешного внедрения любых цифровых решений. Когда эти вопросы не получают ответов, а сервисы, возникающие в ходе такой беспечной цифровизации, не учитывают удобства и безопасность людей, у граждан возникает чувство недоверия к государству и системе в целом. И если представители власти не разъясняют им, каким образом будут гарантированы их права и свободы при появлении цифровых решений, недоверие будет лишь усиливаться.

В этом и предыдущем[1] исследованиях Центра подготовки РКЦТ, посвященных этике, мы описали широкий спектр этических рисков ЦТ. Один из самых критичных — риск цифровой эксклюзии, когда некоторые группы в обществе имеют ограниченный доступ к технологиям. Для этих групп повсеместная цифровизация означает либо полную утрату доступа к государственным и коммерческим сервисам, либо существенное снижение их доступности. Такой эффект противоречит задачам перехода на «цифру»: открывать новые возможности, ускорять и упрощать процессы.

[1] Этика и «цифра»: этические проблемы цифровых технологий. В 2 т. М.: РАНХиГС, 2020. URL: https://ethics.cdto.center/

«В начале 2020 года мы выпустили первый доклад об этике в цифровую эпоху. Мы разобрали в нем этические проблемы, которые возникают в разных отраслях с распространением цифровых технологий. Проблема состоит в том, что этику нельзя нормативно урегулировать. Госслужащие привыкли мыслить так: то, что нормативно урегулировано, мы делаем, а то, что по закону не требуется, — нет. Но этические вопросы нельзя решить таким образом, часто они не имеют единственно правильного решения».

Мария Шклярук, академический директор Центра подготовки руководителей и команд цифровой трансформации

За полтора года, прошедших с момента выхода нашего первого доклада, в мировой цифровой повестке наметилось несколько положительных трендов, связанных с этикой. Среди них — ограничение потенциально опасных технологий, развитие технологических, регуляторных и управленческих решений, способствующих созданию более этичных продуктов.

- В ряде стран стали запрещать или серьезно ограничивать применение технологий, если потенциальный вред от них превышает потенциальную пользу. Неэтичность обработки данных и внедрения технологий становится достаточным поводом для отказа от их использования, хотя бы временного.
- Создаются этические кодексы и нормативные документы в области ИИ и данных. Новые роли, такие как руководитель по этике ИИ или Data Protection Officer, появляются в офисах на Западе и (сравнительно редко) в России.
- Появляются (пока только в Европе) проекты нормативных документов, ограничивающие наиболее критические технологии, например системы социального рейтинга или видеонаблюдение с распознаванием лиц.
- Вопросы приватности и защиты данных, прежде интересовавшие только узких специалистов, разработчиков и юристов, становятся темой общественных дискуссий. В России появляются первые примеры масштабного удаления данных по окончании срока их использования, создаются более удобные формы отзыва пользовательских данных.
- Внедряются практики разработки на основании концепции Privacy by Design / by Default, в которых приватность предусматривается по умолчанию и с самого начала разработки продукта.
- Государства более-менее успешно предпринимают попытки ограничить власть ИТ-гигантов и дата-корпораций.

Однако этих первых сдвигов недостаточно. Для полноценного включения вопросов этики технологий в государственную повестку их обсуждение нужно выводить на более высокий, стратегический уровень.

В последний год обострилась борьба государств и компаний за власть и влияние. Россия должна не только наращивать свою технологическую,

интеллектуальную мощь, но и стремиться к цифровому суверенитету, чтобы сохранять за право на собственное мнение и возможность занимать сильную позицию в конструктивном диалоге мировых держав. Однако сохранение цифрового суверенитета невозможно, пока Россия замкнута (научно, технологически, экономически и культурно) в русскоговорящей зоне и ориентируется на копирование успешного опыта других стран вместо создания своего, уникального. Создателям цифровых продуктов нужно задаваться вопросами о перспективах, ставить перед собой более амбициозные цели, заглядывать в будущее. Есть много примеров удачных решений, несколько российских министерств и ведомств (ФНС, ФАС и др.) совершили прорыв, сделали то, чего нет в большинстве стран.

Текущая деятельность — это в основном распоряжения, отчеты, рутина, поэтому у сотрудников госорганов обычно нет времени на обдумывание этических вопросов. Государственные и муниципальные служащие — заложники планов и решений, принятых несколько лет назад, в то время как решения, принимаемые сегодня, определяют развитие страны на ближайшие годы.

Так что же дальше? Что позволит экономике страны вырасти не на 2–3%, а на 10–20%? Какие действия, связанные с социально-экономической политикой и ЦТ, помогут совершить этот скачок? Мы наблюдаем парадокс: чем больше всего оцифровывается, тем сильнее цифровой хаос.Возможно, потомки назовут этот период эпохой цифровой архаики. Метрик новой экономики и нового мира еще нет, их предстоит разработать; если государство хочет определять смыслы, оно должно их предлагать, обосновывать и активно продвигать (см. рисунок 19).

«Залог успеха в развитии государства — способность мыслить стратегически, учитывая этические вопросы. Система управления — это не просто сбор и анализ статистических данных, это динамическая система с разными уровнями, возможностью прогнозирования разных вариантов действий. Важным компонентом системы управления является собственный образ будущего, ключевыми элементами системы должны стать образ человека и его этика. Мыслить краткосрочными промежутками — значит заведомо проиграть конкурентам, у которых есть стратегия на десятилетия. У России есть и возможности, и кадры, чтобы сформировать новые смыслы: не план развития на ближайшие три года, а стратегию на 50–100 лет».

Илия Димитров, омбудсмен по вопросам развития цифровой экономики

Невозможно и далее пренебрегать этикой в процессе ЦТ. Этика напрямую связана с доверием, а доверие — с успешностью страны в долгосрочной перспективе. В условиях турбулентности и глобальных потрясений государству критически важно иметь заранее выстроенные и основанные на доверии коммуникации с гражданами, понятные и этичные принципы принятия решений. Укрепление доверия к государственным

Рисунок 19. Компоненты техноэтики в госуправлении

цифровым сервисам — одна из ключевых задач любой стратегии ЦТ. И при создании стратегии, и при разработке конкретных цифровых решений государственным органам не обойтись без тщательного изучения пользовательского опыта. Механизмы обратной связи должны использоваться уже на этапе проектирования сервиса, так же как и фокус-группы, и тестирование прототипов. Открытый диалог с экспертным сообществом, внимательное отношение к ПДн и надежная защита приватности должны стать для владельцев цифровых продуктов базовыми принципами деятельности.

Кроме открытости, умения строить коммуникации и завоевывать доверие, в практике реализации этических принципов в области «цифры» важны и другие аспекты. В любых цифровых решениях, исходящих от государства, нужно заботиться об этичности систем на основе ИИ, сохранении аналоговых альтернатив цифровым сервисам, о доступности цифровых решений и в социально-экономическом, и в цифровом смысле, что предполагает совершенствование самих сервисов, инклюзивный подход к их дизайну, повышение цифровой грамотности граждан и рост их благосостояния.

В цифровом мире этика — научная дисциплина, которая изучает новые способы взаимодействия людей между собой и людей с машинами и пытается выяснить, что такое хорошо и что такое плохо в новых реалиях. Но этим она не исчерпывается. Этика в области цифровых решений — это еще и этичное поведение людей, принимающих эти решения, практика применения новых инструментов. Для государственного или муниципального служащего, вообще для всех, кто работает «на государство», этика в цифровом мире — это ежедневный выбор в пользу гражданина, защита его безопасности, поиск самого простого, быстрого и удобного способа удовлетворить его потребности, оставаясь почти незаметным. О том, как сделать этот выбор, мы постарались рассказать в докладе.

ПУБЛИКАЦИИ ЦЕНТРА ПОДГОТОВКИ РКЦТ

ГОСУДАРСТВО КАК ПЛАТФОРМА: ЛЮДИ И ТЕХНОЛОГИИ

Практическое пособие для тех, кто участвует в осуществлении цифровой трансформации государственного управления в России.

«Государство как платформа: люди и технологии» развивает идеи доклада «Государство как платформа», выпущенного фондом «Центр стратегических разработок» в мае 2018 года, и содержит конкретные рекомендации, как формировать ИТ-команды цифровой трансформации, а также описание компетенций и технологий, необходимых участникам команды.

www.ranepa.ru/images/News/2019-01/16-01-2019-GovPlatform.pdf

AGILE-ПОДХОД В ГОСУДАРСТВЕННОМ УПРАВЛЕНИИ

Методические рекомендации по применению гибких подходов в проектном управлении в органах государственной власти.

Навигатор цифровой трансформации позволяет сформировать единое понимание области применения гибких подходов для управления проектами цифровизации, дает практические рекомендации по использованию Agile при управлении проектами цифровизации в органах исполнительной власти, в том числе с учетом ограничений современной практики госуправления в РФ.

gosagile.cdto.ranepa.ru

МОДЕЛЬ КОМПЕТЕНЦИЙ КОМАНДЫ ЦИФРОВОЙ ТРАНСФОРМАЦИИ В СИСТЕМЕ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Обоснование ключевой роли модели компетенций для формирования успешных цифровых команд.

В детальном описании модели раскрыты ключевые личностные и профессиональные компетенции, описаны их характеристики и поведенческие индикаторы. Показано, почему приоритетом является кадровое обеспечение ЦТ: оно позволит реализовать проекты цифровой трансформации в органах власти на качественно новом уровне.

hr.cdto.ranepa.ru/cm

ОРГАНИЗАЦИОННЫЕ СТРУКТУРЫ И КОМАНДЫ ЦИФРОВОЙ ТРАНСФОРМАЦИИ В СИСТЕМЕ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Результаты изучения организационно-функциональных структур подразделений, ответственных за ЦТ в России, и лучших зарубежных практик.

Подробно анализируются особенности организационных структур в зависимости от их функций, численности и состава персонала, в частности цифровых команд. Представлено описание ключевых ролей системы управления и реализации цифровых проектов.

hr.cdto.ranepa.ru/os_0

Материалы о модели компетенций будут полезны прежде всего руководителям цифровой трансформации, кадровым службам, а также всем категориям госслужащих, специалистам, участвующим в разработке цифровых продуктов и услуг, читателям, интересующимся темой цифровой трансформации в государственном секторе.

САМОИЗОЛЯЦИЯ: РАБОТАЕМ, РУКОВОДИМ, ТРАНСФОРМИРУЕМ

Рекомендации по работе госслужащих в режиме удаленного доступа в условиях противодействия распространению новой коронавирусной инфекции.

В докладе представлены пошаговые алгоритмы, выделены приоритеты, освещен опыт перехода крупных и средних организаций и органов власти на удаленную работу. Собраны рекомендации как руководителей проектных команд, команд разработки продуктов, которые традиционно представляют собой распределенные команды, так и функциональных руководителей ФОИВ, которые уже получили и обобщили опыт перехода на удаленный режим работы.

udalenka.cdto.ranepa.ru

КЛИЕНТОЦЕНТРИЧНЫЙ ПОДХОД В ГОСУДАРСТВЕННОМ УПРАВЛЕНИИ

Рекомендации по внедрению клиентоцентричного подхода в организации в виде практико-ориентированного навигатора.

В навигаторе описаны около 50 инструментов изучения клиентского опыта, большинство из которых просты и доступны тем, кто впервые погружается в тему клиентоцентричности. Он отвечает на практические вопросы: какие инструменты подходят для разных проектов? Как обеспечить доступность продукта или услуги? Какие ГОСТы и стандарты нужно знать при создании клиентоцентричного продукта? С чего начать внедрение клиентоцентричного подхода в организации? Каждый может стать клиентоцентричным уже сейчас, освоив в повседневной работе один-два инструмента в качестве первого шага.

cx.cdto.ranepa.ru

СТРАТЕГИЯ ЦИФРОВОЙ ТРАНСФОРМАЦИИ: НАПИСАТЬ, ЧТОБЫ ВЫПОЛНИТЬ

Основные принципы создания и применения стратегических документов цифровой трансформации в органах власти и других госорганизациях.

Для государственных и муниципальных служащих доклад может стать удобным и полезным навигатором по разным аспектам разработки стратегии, поможет избежать ошибок, учесть опыт первопроходцев и выбрать свой путь. В книге описаны основные компоненты стратегии цифровизации и ЦТ, исследования, необходимые для ее создания, архитектурный подход к проектированию. На российских примерах показаны необходимые этапы разработки и реализации. Издание адресовано руководителям, кураторам, участникам проектов ЦТ, а также всем, кому интересна эта тема.

strategy.cdto.ranepa.ru

БЕРЕЖЛИВОЕ УПРАВЛЕНИЕ В ГОССЕКТОРЕ. КАК НАЛАДИТЬ ПРОЦЕССЫ

Рекомендации по внедрению современных подходов, основанные на лучших российских практиках в бизнесе и госсекторе.

Навигатор рассказывает о существующих инструментах, кейсах и результатах процессного подхода, плюсах и минусах разных методов и особенностях их внедрения. Адресован в первую очередь руководителям цифровой трансформации (РЦТ) и членам команд, которые занимаются процессной деятельностью. Навигатор будет интересен также сотрудникам процессных офисов (или подразделений, отвечающих за процессное управление в организации), которые хотят больше узнать о цифровой трансформации.

lean.cdto.ranepa.ru

О ЦЕНТРЕ ПОДГОТОВКИ РУКОВОДИТЕЛЕЙ И КОМАНД ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Центр создан в феврале 2019 года под эгидой Минкомсвязи и Минэкономразвития на базе Высшей школы государственного управления РАНХиГС. Финансирование Центра осуществляется в рамках национальной программы «Цифровая экономика».

Директор Центра — **Ксения Андреевна Ткачева**

Академический директор — **Мария Сергеевна Шклярук**

Центр проектирует и реализует образовательные программы для государственных и муниципальных служащих, ответственных за цифровую трансформацию и развитие российских органов власти. В 2021 году отбор для обучения в Центре пройдут 12 620 государственных и муниципальных служащих из 85 российских регионов. В их числе заместители федеральных министров, вице-губернаторы и заместители руководителей федеральных служб, руководители и участники проектных офисов цифрового развития, специалисты муниципальных органов власти. До конца 2024 года более 70 000 человек смогут пройти обучение по программам Центра.

Центр предлагает сотрудникам и руководителям коммерческих и государственных организаций индивидуальные проекты обучения под ключ по темам цифровой трансформации и цифровой экономики. Эксперты Центра разрабатывают **образовательные программы** и отдельные курсы с учетом конкретной сферы, предпочитаемого формата обучения, возраста и уровня подготовки аудитории, опираясь на большой опыт в проектировании и проведении образовательных программ.

Центр также ведет **исследовательскую работу** и разрабатывает аналитические и методические материалы. Эксперты Центра изучают вопросы цифровой трансформации госуправления, цифровых платформ и их экосистем, реализации проектов цифровой трансформации, проводят

исследования в области управления изменениями и этики цифровых технологий, включая этику данных, этику искусственного интеллекта, защиту приватности и цифровых прав граждан.

Одно из важных направлений работы Центра подготовки руководителей и команд цифровой трансформации — просветительская деятельность, **популяризация цифровой трансформации** как в сфере госуправления, так и в других областях.

- В 2020 году создана информационная система для руководителей цифровой трансформации федеральных и региональных органов власти **«База знаний РЦТ»**. Сотрудники 62 ФОИВ и 85 РОИВ систематически используют базу для подготовки к совещаниям с аппаратом Правительства, участия в федеральном рейтинге РЦТ и самообразования. База знаний содержит официальные документы, методические рекомендации, авторский контент Центра по темам цифровой трансформации, кейсы. Также в систему включены инструменты для формирования рейтинга РЦТ.
- В 2021 году Центр запустил открытый курс на платформе Stepik **«Цифровая трансформация. Быстрый старт»** по основам цифровой трансформации, проектного управления и сквозным технологиям для госслужащих, научного, образовательного сообщества и бизнеса. Темы курса: ИИ, AR/VR, блокчейн, квантовые технологии, робототехника, разработка цифровых сервисов. Курс создан при участии экспертов Центра, топ-менеджеров экосистемы Сбер, Ростелекома, ВТБ и других российских ИТ-компаний.
- На портале и в соцсетях Центра регулярно публикуются актуальные материалы для тех, кто интересуется вопросами цифровизации, реформами в сфере госуправления, оптимизацией управленческих процессов в разных областях.

ЭТИКА И «ЦИФРА»: ОТ ПРОБЛЕМ К РЕШЕНИЯМ

Аналитический доклад

Оригинал-макет: Надежда Каблукова
Дизайн и верстка: Наталья Балева
Корректоры: Марк Кантуров, Ольга Капполь
Источник фото: depositphotos

Сайт: https://ethics.cdto.center/