УДК 33 DOI: 10.14451/1.228.319

Цифровые технологии как угроза демократии: предпосылки и практики

© 2023 **Суздалева Наталья Николаевна**
старший преподаватель кафедры Менеджмент. Санкт-Петербургский филиал Финансового университета при Правительстве РФ.
E-mail: NNSuzdaleva@fa.ru

© 2023 **Алексеева Алёна Николаевна**
Студент 1 курса магистратуры. Университет ИТМО.
E-mail: alksv_aln@mail.ru

Ключевые слова: демократия, цифровизация, диджитализация, слежение, криптоактивы, монополизация.

В статье представлены различные аспекты негативного воздействия цифровизации на демократические процессы и процедуры в большинстве стран. Обращается внимание на значительное экономическое усиление тех компаний, которые побеждают в конкурентной борьбе благодаря автоматизации, повышению качества, рациональности операционных процессов. Также сделан акцент на проявившиеся практики применения цифровых технологий для ослабления демократии и достижения личных целей вопреки общественным интересам. В таком контексте важными следует признать скрытое и тотальное открытое слежение, анонимные финансовые инструменты и т. д.

На сегодняшний день в мире происходит интенсивный процесс цифровизации, то есть повышение роли создаваемых виртуальных копий и моделей, процессов и объектов реального мира, что позволяет достичь большого количества положительных эффектов. Это снижает затраты рабочего времени сотрудников предприятий, усиливает контроль за различными хозяйственными операциями, улучшает операционные процессы.

Актуальность исследования повышается в условиях потенциального негативного воздействия цифровых технологий на демократические процессы. Можно привести большое количество примеров использования последних достижений науки и техники для удовлетворения личных мотивов, а не достижения всеобщих интересов.

Сама по себе цифровизация проявляется в усилении эффективности коммуникационного процесса, автоматизации рутинных физических и интеллектуальных задач, ряде других эффектов, достигаемых благодаря использованию новых методов формирования и использования цифровых сред.

В качестве предпосылок негативного воздействия цифровых технологий на развитие демократии и демократических институтов следу-

ет указать следующие аспекты. Прежде всего, цифровизация, как и другие формы повышения эффективности определенных процессов, приводит к тому, что бизнес-модель конкретного предприятия усиливается. При этом благодаря высокой производительности, которую можно достичь путем разработки и внедрения адекватного программного комплекса на предприятии, происходит значительное улучшение рыночных позиций. Причем благодаря развитию технологий, внедрению новых инноваций рост у перспективных предприятий происходит очень быстро. Это означает, что повышается риск монополизации тех или иных сегментов хозяйственной системы страны. Высокой остается вероятность, что только одно предприятие относительно быстро победит в конкурентной борьбе и поглотит других участников рынка. Однако такая монополизация способствует не только определенным дисбалансам в экономической системе страны, но и приводит к ряду негативных эффектов в контексте демократии.

Ведь рост экономической силы приводит к тому, что у корпорации появляется больше возможностей навязывать свое видение по политическим вопросам. Например, такие компании могут финансировать благотворительные инициативы, прямо направлять средства в избирательные фонды кандидатов, использовать средства другим образом для влияния на политическое движение страны. Например, в США бизнес имеет право финансово поддерживать партии. Очевидно, что если количество участников на рынке является значительным, то можно ожидать относительно равномерную поддержку различных позиций. Однако если происходит монополизация, то у отдельной политической группы усиливается имущественное положение, а значит и возможность рекламировать и продвигать свою политическую силу.

Фактически происходят аналогичные процессы, наблюдаемые в период индустриализации в западных странах. В это время формировались различные трасты, монополии, другие формы дисбалансов на рынке, которые приводили к существенному влиянию на политический ландшафт.

Кроме монополизации и чрезмерной концентрации экономической силы компаний, победивших в конкурентной борьбе за счет активного применения цифровизации, еще одной предпосылкой выступает значительная аналитическая сила лиц, применяющих актуальные методы анализа данных, например, методы больших данных. Аналитику, использующему такой ресурс, раскрываются явления и тренды, не очевидные для стороннего наблюдателя. Проявляется корреляция процессов, которые на первый взгляд кажутся не связанными между собой. Воздействием на один процесс можно добиться непредсказуемых для третьих лиц результатов.

Другой предпосылкой следует признать фундаментальную невозможность обеспечить стопроцентную защищенность любой современной цифровой системы. В новостях постоянно появляется информация о потере данных клиентов коммерческими банками, социальными сетями, компаниями, активно использующими достижения цифровизации в своей бизнес-модели. При этом в процессе противодействия тех, кто хочет взломать систему и тех, кто ее защищает, обычно побеждает именно первая сторона. Это связано с тем, что ошибки возможны на самых различных уровнях. Не только код может содержать места, позволяющие получить доступ стороннему лицу, но и компоненты компьютерных систем, то есть физические объекты, могут иметь уязвимости в связи с недостаточно продуманной архитектурой [2].

Таким образом, можно выделить основные предпосылки негативного воздействия цифровизации на демократию: стимулирование монополизации, значительная аналитическая сила в случае использования современных методов анализа и фундаментальная неспособность обеспечить стопроцентную защиту цифровой среды от взлома.

На сегодняшний день появляется большое количество подходов и технологий, негативно воз-

действующих на демократические процедуры.

Практики и решения, негативно влияющие на развитие демократических институтов:

- Pegasus.
- Cambridge Analytica.
- Darkweb биржи.
- Тотальная открытая слежка.
- Анонимные криптоактивы.

Известным является случай использования анализа больших данных для лучшей коммуникации с целевой аудиторией в рамках политического процесса, что должно было привести к победе определенной партии (Cambridge Analytica) [3]. Суть подхода состояла в том, чтобы собирать огромный массив данных о различных пользователях сети Facebook (запрещена в России, принадлежит компании Meta — признана экстремистской и запрещена в РФ), после чего у аналитика появлялась возможность получить портрет каждого конкретного лица. Соответственно, представитель политической партии лучше понимал мотивы, особенности мышления, политические пристрастия и большое количество других особенностей человека или конкретной группы людей. Следовательно, это позволяло более точно настраивать коммуникационную политику в интернете, особенно на соответствующей интернет-площадке.

Использовались не только прозрачные методы взаимодействия с целевой аудиторией, например, рациональная аргументация и выделение причин, по которым то или иное лицо должно проголосовать за продвигаемого кандидата, но и активно применялись манипулятивные методы, воздействующие на эмоциональную составляющую человека, тем самым отключая рациональное восприятие.

Особенность анализа больших данных состоит в том, что накапливается огромный массив данных, после чего появляется возможность выявлять неочевидные связи между различными сторонами общественной жизни. Все это может приводить к тому, что выигрывать будут группы лиц, способные лучше манипулировать эмоциональным состоянием избирателей, а не политические лидеры, способные сформировать рациональную, эффективную, прозрачную стратегию дальнейшего развития страны.

Еще одной проблемой является существенное усиление скрытой слежки за гражданами, общественными деятелями, политическими лидерами. Это может происходить как на массовой, так и на индивидуальной основе. В контексте последнего следует упомянуть такую программу как Pegasus. Это шпионское программное обеспечение, позволяющее получать доступ к любому телефону, а также другим устройствам, без какого-либо уведомления лица, за которым происходит слежка [4]. Хотя израильская компания-производитель декларирует, что она продает программное обеспечение только государственным агентствам из развитых, устоявшихся демократий, но на практике происходит распространение программы и среди различных авторитарных режимов. Как результат, последние получают возможность следить за общественными деятелями, оппозиционерами, другими представителями политически-противоборствующей стороны.

Кроме этого, в развитых демократиях существует высокая вероятность того, что программное обеспечение будет использоваться не для борьбы с преступниками и террористами, а для тех же целей усиления своих позиций в политической борьбе. Не следует исключать человеческий фактор, постоянное желание получить материальное или другое преимущество путем использования всех доступных инструментов.

В контексте практик, способных негативно сказаться на демократическом развитии, следует упомянуть также криптоактивы. Обычно под этим термином понимают криптовалюты и прочие виды активов с применением технологии криптографирования.

В течение последних 50 лет в мире активно развивалась и формировалась современная финансовая архитектура. Если раньше всем были доступны анонимные финансовые продукты, то

на текущий момент они не предлагаются в большинстве стран мира. Лицо, желающее дать взятку в значительном размере, могло открыть счет в банке, разместить соответствующую сумму средств на нем, после чего передать данные о счете другому заинтересованному лицу. Последний должен был выполнить определенные действия в интересах взяткодателя, а после завершения таких действий и получения информации о счете взяточник посещал отделение банка, обычно в офшорной юрисдикции, получал деньги со счета на предъявителя.

Учитывая активное использование такого инструмента для сокрытия различных криминальных преступлений, в мире активно происходила трансформация протекающих в банках бизнес-процессов, в том числе были запрещены анонимные счета и депозиты. Все движение денежных средств могло быть легко отслежено благодаря постоянной проверке происхождения денежных средств в большинстве развитых стран. Усложнился и процесс перетекания финансовых ресурсов из офшорных юрисдикций в другие.

Появление криптоактивов снова восстанавливает проблему коррупции путем использования доступных анонимных инструментов. Хотя сам по себе Bitcoin не выступает анонимной валютой, современные методики позволяют выявить источник происхождения средств и получателя [1], но все же такие приемы как перемешивание обеспечивает сокрытие прямолинейных связей от отправителя к получателю. Также появляется большое количество криптовалют, которые действительно имеют такое свойство как реальная анонимность.

Учитывая это, повышается риск получения взятки политическими деятелями, представителями общественных организаций, членами избирательных комиссий. Конечно, это крайне негативно будет сказываться на практической реализации демократических процедур в большинстве стран мира. Под воздействием такого фактора лицо, предлагающее взятку различным субъектам избирательного процесса, может непосредственно влиять на результаты, которые будут опубликованы по завершению соответствующих процедур. Поэтому можно утверждать, что криптоактивы создают значительную угрозу для развития современной демократии.

Еще одной практикой, способной оказать деструктивное воздействие на состояние общества, в том числе и демократических процедур, является активное развитие различных бирж и магазинов в ДаркВебе. В процессе осуществления финансовых операций используются именно криптоактивы. В этом случае у любых граждан появляется возможность покупать поддельные документы, оружие, наркотические вещества, прочие запрещенные вещи. В случае дальнейшего развития таких сайтов можно ожидать существенного ухудшения общественных отношений, деградации демократических процессов, повышения уровня преступности, распространения других нежелательных явлений.

Для нормального функционирования общества важно, чтобы принимаемые законы соблюдались, а товары, исключенные из торгового оборота, не были доступны массовому потребителю. В противном случае может произойти изменение мотивов ежедневного поведения граждан. Если раньше они интересовались возможностями улучшить свое материальное положение, создать более безопасное и открытое общество, то в случае развития наркомании и других негативных явлений можно ожидать резкого изменения приоритетов и жизненных ценностей. Поэтому такое явление также негативно сказывается на развитии общества, в том числе и демократических процессов в них.

Проблемой, способной оказать воздействие на демократическое развитие общества, выступает тотальная и открытая слежка. В отдельных странах посредством слежения составляется социальный рейтинг гражданина, а камеры отслеживают его поведение в публичных местах. Очевидно, что накопление огромного массива данных способно скомпрометировать любого человека даже в том случае, если он не осуществляет никаких незаконных действий. Это следует из того, что большое количество фактов

можно использовать против лица, о котором они известны.

Тотальное проведение слежки негативно сказывается на дальнейшем развитии демократии в любой стране. Безусловно, это вполне оправданная мера, если речь идет о лицах, подозреваемых в преступной деятельности. Если на начальном этапе основные усилия будут концентрироваться на противодействии оппозиционерам, то для дальнейшего обеспечения работы «карательной машины» следует расширять перечень тех, против кого будут использоваться доступные инструменты преследования.

Кроме этого, тотальная слежка сама по себе приводит к тому, что граждане пытаются минимизировать свою активность, в том числе и политическую. Они понимают, что в случае необходимости все их секреты моментально станут известными стороннему наблюдателю. В таких условиях можно ожидать подавление демократических инициатив.

Таким образом, выявлено три основные предпосылки негативного воздействия цифровых технологий на развитие демократии в мире: быстрая монополизация отдельных сегментов хозяйственной системы из-за победы одного участника рынка в случае ключевой значимости цифровых технологий в бизнес-модели, фундаментальная невозможность обеспечить защиту цифровых систем от проникновения, а также значительная сила аналитика, использующего такие методы анализа как Биг Дата. В качестве практик и решений, негативно влияющих на развитие демократических институтов, указаны Pegasus, Cambridge Analytica, Darkweb-биржи, анонимные криптоактивы, тотальная открытая слежка.

Библиографический список

1. СК завел дело о взятках биткоинами за диссертации в МПГУ. — URL: https://www.rbc.ru/society/25/08/2021/61262ebe9a7947383e067c59 (дата обр. 11.11.2023).
2. Уязвимость в процессорах Intel и AMD позволяет обойти защиту от Spectre и Meltdown. — URL: https://backuprent.com/news/uyazvimost-v-protsessorah-intel-i-amd-pozvolyaet-oboyti-zaschitu-ot-spectre-i-meltdown.html (дата обр. 11.11.2023).
3. Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. — URL: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html (visited on 11/11/2023).
4. What is Pegasus spyware and how does it hack phones? — URL: https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones (visited on 11/11/2023).