УДК 1:316.334.3:004.056

Блинникова Анна Валерьевна,
к.филос.н., доцент;
Иркутский государственный университет,
г. Иркутск, Россия
ORCID: 0000-0001-8553-2679

КУЛЬТУРА ЦИФРОВОЙ БЕЗОПАСНОСТИ КАК НОВЫЙ ФУНДАМЕНТ ОБЩЕСТВЕННОГО КОНТРОЛЯ

Аннотация: В статье представлен анализ культуры цифровой безопасности как основы устойчивости электронной демократии. Автор исследует траекторию смещения акцентов от адаптивного обучения к активному общественному контролю и вызреванию новой политической субъектности. Ключевая идея работы состоит в том, что уязвимость демократии обусловлена дефицитом у граждан «цифрового габитуса». В реалиях «надзорного капитализма» это провоцирует эрозию ценностных оснований. Исследователь вводит дефиниции «цифрового габитуса» и «культуры цифровой безопасности», аргументируя императивность смены парадигмы с элементарной грамотности на концепцию «цифрового гражданства». Работа обосновывает, что цифровая гигиена представляет собой инструмент протекции от алгоритмического патернализма и выступает непременным актом сохранения автономии личности в контексте тотальной цифровизации.

Ключевые слова: культура цифровой безопасности, цифровая демократия, общество риска, надзорный капитализм, социальный контроль, цифровой габитус, субъектность, цифровое гражданство

Anna V. Blinnikova,
PhD (Candidate of Philos. Sci.), Associate Professor;
Irkutsk State University, Irkutsk, Russia
ORCID: 0000-0001-8553-2679

DIGITAL SECURITY CULTURE AS THE NEW FOUNDATION OF PUBLIC CONTROL

Abstract: The article presents an analysis of digital security culture as a foundation for the resilience of electronic democracy. The author explores the trajectory of a shift in focus from adaptive learning to active public oversight and the maturation of a new form of political subjectivity. The central idea of the work is that the vulnerability of democracy stems from a deficit of "digital habitus" among citizens. In the realities of "surveillance capitalism," this provokes an erosion of value foundations. The researcher introduces definitions

of "digital habitus" and "digital security culture," arguing for the imperative of a paradigm shift from basic literacy to the concept of "digital citizenship." The work substantiates that digital hygiene constitutes an instrument of protection against algorithmic paternalism and serves as an indispensable act of preserving individual autonomy in the context of total digitalization.

Keywords: digital security culture, digital democracy, risk society, surveillance capitalism, social control, digital habitus, agency, digital citizenship

Введение

Беспрецедентная динамика процессов цифровизации общества актуализирует неотложный поиск новых оснований для укрепления устойчивости демократических институтов и необходимой переоценки политической субъектности гражданина [1]. В условиях системного перехода к парадигме «общества контроля» и глобального доминирования феномена «надзорного капитализма» [2] традиционные механизмы гражданского участия и демократической делиберации сталкиваются с беспрецедентными экзистенциальными и политико-институциональными вызовами. Объективная реальность свидетельствует, что функция контроля и надзора пропорционально растет с увеличением степени цифровизации всех сфер общественной жизни. Электронное голосование, краудсорсинговые платформы коллективного принятия решений и системы цифровой обратной связи, исходно концептуализированные в качестве инструментов расширения пространства гражданской свободы и демократической коммуникации, парадоксальным образом трансформируются в скрытые, латентные инструменты алгоритмического управления, централизованного контроля и глубокого социального профилирования населения.

Центральная проблема, выносимая на обсуждение в рамках данного цикла исследований, заключается в критическом разрыве между нарастающей технологической сложностью цифровых инфраструктур и архаичностью социокультурных установок рядовых пользователей. Опираясь на предшествующие теоретические посылы и эмпирические исследования [3], автор выдвигает гипотезу о том, что ключевым фактором структурной уязвимости институтов электронной демократии является отсутствие аутентичного **цифрового габитуса,** *данный феномен рассматривается как система устойчивых когнитивных и поведенческих предрасположенностей субъекта, формируемых в процессе длительного взаимодействия с алгоритмическими средами, которая определяет границы его цифровой видимости, уровень критического доверия к интерфейсам и степень готовности к добровольному самораскрытию данных.* Жизнеспособность и долгосрочная устойчивость демократии детерминируется не только формализованными конституционными законами и правовыми нормами, но и глубоко укоренившимися

габитуальными привычками и автоматизированными поведенческими паттернами граждан в глобальной сетевой среде [4].

В данной работе ***культура цифровой безопасности*** *трактуется, как комплексный социокультурный режим субъектности, выходящий за рамки технической кибергигиены и включающий рефлексивное дистанцирование от алгоритмического управления, а также способность субъекта осознанно конструировать баланс между приватностью и функциональностью в условиях «надзорного капитализма»*. Культуру цифровой безопасности необходимо воспринимать в качестве основного фундамента для укрепления доверия к электронным институтам и государственным платформам, без которого любые технические средства и инструменты защиты информации (криптографическое шифрование, технология блокчейна) неизбежно обесцениваются преодолимым «человеческим фактором» и социальной инженерией [5].

Теоретико-методологические основания исследования.

Статья входит в цикл исследований, в рамках которых цифровая среда рассматривается как пространство конструирования новой субъектности. Особое аналитическое внимание уделяется качественному переходу от традиционных образовательных практик, механически воспроизводящих архаичную фигуру «прозрачного пользователя» и «цифрового верноподданного», к инновационной модели цифрового гражданства, способного к критической метарефлексии над алгоритмическими диспозитивами и структурами власти [6].

Методологический подход объединяет несколько взаимодополняющих уровней анализа: на социологическом уровне применяется теоретический аппарат П. Бурдье для полноценной интерпретации социального механизма принятия наблюдающих технологий как процесса целенаправленного конструирования габитуса «прозрачного субъекта» [5]. Социально-философский уровень анализа строится на основе концепции «общества риска» У. Бека [2], а также на теории психополитики Бён-Чхоль Хана [10], описывающей качественный переход от внешнего насильственного принуждения к режимам добровольной прозрачности и самораскрытия. На политико-онтологическом уровне исследование опирается на концепцию обществ контроля Ж. Делёза [7] и анализ симулякров Ж. Бодрийяра [4].

Методологическая новизна состоит в антропологически ориентированном подходе, где ***культура цифровой безопасности*** осмысляется как эмансипаторная практика, а ***цифровой габитус*** — как объект целенаправленного педагогического проектирования. Новизна работы состоит в переходе от технократического детерминизма к антропологически ориентированному анализу.

Результаты

Отправной точкой анализа выступает классическая теория У. Бека [2], в которой поздняя современность интерпретируется как перманентный режим обращения с непредсказуемыми опасностями, порожденными самой технологической модернизацией. В цифровом обществе риска монопольное знание о риске само по себе становится ключевым политическим ресурсом. В контексте цифрового общества риска монопольное знание о природе и масштабах риска само по себе трансформируется в ключевой политический и экономический ресурс. В данной аналитической конфигурации принципиально важное значение приобретает введенное У. Беком понятие «отношений определения» — специфических властно-правовых конфигураций и механизмов, которые жестко кодифицируют и закрепляют правила легальной идентификации, математического измерения и социального признания системных угроз и рисков в цифровой среде [2].

Радикальное переосмысление классической модели дисциплинарного паноптикума М. Фуко в реалиях XXI века предлагает философ Бён-Чхоль Хан [10], проводя детальный анализ исторических изменений в структуре и механизмах власти, он отмечает: «Кризис свободы в современном обществе заключается в том, что мы начинаем интерпретировать инструменты принуждения и контроля в качестве проявления собственной свободы и автономии» [10]. В архитектуре цифрового паноптикума современный индивид оказывается парадоксально расщеплен в своей субъектности: он функционирует одновременно в качестве инициативного и творческого актора, и в качестве объекта перманентного электронного надзора. Активно коммуницируя и делясь персональной информацией в социальных сетях, он добровольно и с энтузиазмом отказывается от собственной приватности и информационной автономии. Трансформируется и сама архитектура современной власти, которая она перестает опираться на традиционный запретительный страх и физическое насилие, а вместо этого функционирует посредством смарт-логики сетевого соблазна, геймификации и принудительной позитивности, формируя перманентную «диктатуру прозрачности». Данный процесс начинается со школьного возраста, когда учащиеся создают цифровые портфолио, и продолжается во взрослой жизни через конструирование развернутых цифровых социальных профилей гражданина.

Перенос теоретических наработок П. Бурдье в плоскость цифровых взаимодействий позволяет детально описать «цифровой габитус» как систему инкорпорированных ментальных схем, задающих автоматические, неосознанные реакции на манипулятивные интерфейсы и механическое согласие с кабальными условиями обработки персональных данных [5], [6]. Хроническая и структурная недостаточность цифрового культурного капитала неизбежно формирует уязвимый и конформистский габитус, в рамках которого пользователь систематически низводится до состояния

пассивного «прозрачного объекта», поставляющего ценное сырье для предиктивной аналитики и алгоритмического управления. Экономический и политический горизонт этой масштабной трансформации исчерпывающе раскрывается посредством концепции Ш. Зубофф [8]: «Надзорный капитализм в одностороннем порядке заявляет монопольные права на человеческий опыт в качестве бесплатного сырья для технической конвертации в поведенческие данные и алгоритмы управления» [8]. Фундаментальное правовое и экзистенциальное право на приватность и информационную автономию отчуждается и превращается в ликвидный экономический ресурс для взращивания корпоративного капитала прогнозирования и социального контроля.

Конкретным институциональным полигоном ранней материализации и социальной нормализации этих глубинных структурных процессов выступает сфера образования. Форсированное внедрение в образовательную практику цифровых образовательных платформ управления обучением (LMS), алгоритмов биометрического мониторинга и автоматизированного прокторинга, а также тотального электронного учета и регистрации учебной деятельности институционализирует непрерывную практику формирования цифровых следов и расширенных профилей обучающихся. Образовательная ИКТ-инфраструктура постепенно трансформируется в жесткий властный диспозитив, который со школьного возраста систематически приучает формирующегося субъекта к состоянию постоянного, асимметричного и отчуждающего наблюдения в качестве безальтернативной нормы социальной жизни [9].

В этой точке возникает выраженная и асимметричная эпистемологическая ситуация, когда учащийся оказывается абсолютно прозрачен и видим для централизованной контролирующей системы, тогда как внутренняя механика, логика и критерии функционирования самих оценивающих алгоритмов остаются закрытыми и непроницаемыми. Ситуацию существенно усугубляет повсеместное распространение «теневой» и незащищенной ИТ-инфраструктуры, когда использование сотрудниками образовательных учреждений и учащимися незащищенных публичных мессенджеров и коммерческих облачных сервисов хранения данных для передачи конфиденциальной информации нормализует фатальное пренебрежение приватностью в угоду ситуативному комфорту и удобству. Существующие педагогические методики и образовательные подходы, сведенные к механическому и поверхностному освоению программного обеспечения, не способны сформировать развитого когнитивного иммунитета и критической резистентности к алгоритмическому вторжению и манипуляции. Подобная конфигурация образовательной среды успешно легитимирует системы контроля и воспроизводит специфический тип субъектности «цифрового верноподданного» [10], идеально адаптированного к пассивному

выживанию при надзорном капитализме, но абсолютно не готового к суверенному отстаиванию гражданских прав и политических свобод.

Покидая стены школы, человек вступает в пространство публичной политики и общественного контроля как носитель уже деформированного, конформистского цифрового габитуса. Инкорпорированная привычка игнорировать риски компрометации данных автоматически переносится на использование государственных сервисов и платформ электронной демократии. Острый и критический дефицит навыков распознавания технологических симулякров и цифровых подделок делает учреждения гражданского общества беззащитными и уязвимыми перед таргетированным фишингом, астротурфингом и теневой подменой легитимных государственных интерфейсов. Технологическая непрозрачность и черный ящик правительственных платформ обратной связи порождают биполярную и дисфункциональную реакцию: это либо наивное, безусловное и некритическое доверие к «объективности» и нейтральности машинных алгоритмов, либо радикальное, луддитское отторжение и отказ от любых цифровых процедур и инноваций. Обе эти крайние позиции эффективно блокируют продуктивный и конструктивный демократический дискурс. В конечном счете гражданин оказывается интегрированным в архитектуру цифрового паноптикума не в желаемом качестве суверенного субъекта общественного контроля и надзора, а в качестве предсказуемого и управляемого объекта предиктивного администрирования и поведенческого программирования. Пользователь часто не сопоставляет и не осознает, что его прошлые действия, интернет-активность и поведенческие паттерны зафиксированы на цифровых носителях и способны повлиять на будущие решения и действия административных и коммерческих систем (трудоустройство, выдача кредита, допуск в учреждение и т.д.).

Полученные результаты исследования позволяют интерпретировать дефицит культуры цифровой безопасности не в качестве узкотехнической проблемы, а в качестве глубокого симптома и проявления фундаментальной неисправности и дисфункции цифровой модерности. Поскольку формальные правовые нормы о защите персональных данных создают лишь иллюзорный контур защиты и безопасности, не становясь при этом частью внутренней мотивации, ценностной структуры и поведенческого репертуара индивида. Из логического анализа следует необходимость в радикальном институциональном и педагогическом повороте и переходу от узкой модели «подготовленного пользователя» к комплексной модели цифрового гражданства, предполагающей развитую способность к критической метарефлексии над внутренним устройством цифровых сред и артикуляции права на «эпистемологический суверенитет» [11]. Образовательное пространство в современную эпоху трансформируется в ключевую и определяющую арену борьбы за будущее

общественного контроля и демократии. Инерционный консервативный сценарий ведет к окончательному закреплению «уязвимого габитуса» и превращению гражданского участия в управляемую имитацию и симуляцию. Альтернативный сценарий предполагает включение принципов цифровой приватности и этики данных в базовый образовательный стандарт в качестве обязательных компетенций цифрового гражданства.

Заключение

Проведенный институциональный и социотехнологический анализ обнажает фундаментальное лицемерие современного этапа цифровизации публичной сферы. Декларируя максимальную открытость и эмпатичную «обратную связь» с гражданами, платформенное государство и транснациональные корпорации на деле осуществляют тотальный «административный и коммерческий захват» самой идеи гражданского участия и демократического контроля [3]. Институты общественного контроля, перенесенные на централизованные цифровые платформы, подвергаются глубокой стерилизации и нейтрализации, а острый политический диалог и коллективная рефлексия постепенно подменяются поверхностным клик-активизмом, реальный действенный надзор за властью и корпорациями сводится к оптимизации работы коммунальных служб через неполитические интерфейсы жалоб и обращений [7]. В отсутствие развитого цифрового габитуса и интериоризированной культуры безопасности электронная демократия неизбежно схлопывается в чистый симулякр [4], маскирующий тотальную асимметрию властных отношений и информационных иерархий.

Главный и наиболее острый вывод нашего исследования заключается в том, что современный общественный контроль в его цифровой форме незаметно превратился из инструмента сдерживания элит в эффективный механизм калибровки государственного и корпоративного надзора. Граждане, добровольно поставляющие данные о локальных проблемах и настроениях через удобные приложения, фактически работают бесплатными сенсорами предиктивных систем управления, лишаясь при этом субъектности и возможности влиять на стратегические решения.

Стоит отметить, что преодоление этой ловушки требует решительного отказа от сервисного восприятия цифровой среды. Культура цифровой безопасности должна быть переосмыслена не как набор инструкций по защите паролей, а как форма современного политического сопротивления избыточной прозрачности. Обретение «эпистемологического суверенитета» и формирование резистентного цифрового габитуса становятся главными условиями выживания гражданского общества. Научившись осознанно управлять границами собственной видимости в цифровом пространстве и целенаправленно саботировать манипулятивные алгоритмы «надзорного капитализма», общество сможет вернуть

институту контроля его исходную и подлинную демократическую сущность, превратив цифровые платформы из опасных инструментов слежения в реальные и действенные рычаги ограничения публичной власти.

Использованные источники:

1. Абрамов Ю. Ф. [и др.] Эколого-информационный глобализм и перспективы развития образования // Байкальский психологический и педагогический журнал. — 2004. — № 1–2. — С. 12–18.
2. Бек У. Общество риска. На пути к другому модерну / пер. с нем. В. Седельника, Н. Федоровой. — Москва : Прогресс-Традиция, 2000. — 384 с.
3. Блинникова А.В. Сравнительный анализ моделей цифровизации общественного контроля: институциональные основы и взаимодействие в гражданском обществе // Политика и Общество. 2026. № 1. С. 252-264. DOI: 10.7256/2454-0684.2026.1.77013
4. Бодрийяр Ж. Симулякры и симуляция / пер. с фр. А. Качалова. — Москва : Постум, 2023. — 320 с.
5. Бурдье П. Практический смысл / пер. с фр. ; общ. ред. пер. и послесл. Н. А. Шматко. — Санкт-Петербург : Алетейя, 2001. — 562 с.
6. Бурдье П. Социология социального пространства / пер. с фр. ; отв. ред. Н. А. Шматко. — Москва : Ин-т эксперим. социологии ; Санкт-Петербург : Алетейя, 2007. — 288 с.
7. Делёз Ж. Postscriptum к обществам контроля // Переговоры. 1972–1990 / пер. с фр. В. Ю. Быстрова. — Санкт-Петербург : Наука, 2004. — С. 226–233.
8. Зубофф Ш. Эпоха надзорного капитализма. Битва за человеческое будущее на новых рубежах власти / пер. с англ. А. Ф. Васильева. — Москва : Изд-во Института Гайдара, 2022. — 784 с.
9. Политическая онтология цифровизации и государственная управляемость : монография / под ред. Л. В. Сморгунова. — Москва : Аспект Пресс, 2022. — 351 с.
10. Блинникова А.В. Воспитание «цифрового верноподданного»: роль образовательной среды в легитимации систем социального контроля (опыт КНР и РФ) // Журнал монетарной экономики и менеджмента. 2026. № S1. С. 190-196. DOI: 10.26118/2782-4586.2024.10.67.001
11. Хан Б.-Ч. Общество усталости / пер. с нем. Г. Хайдаровой. — Москва : АСТ, 2024. — 128 с.