СОЦИАЛЬНАЯ ФИЛОСОФИЯ

Статья поступила в редакцию: 26.10.2026
Статья принята к публикации: 01.11.2026
Статья опубликована: 15.11.2026

УДК 004.056+316.42+17.02

DOI: 10.32743/UniSoc.2026.138.11.23650

Информационная безопасность личности в условиях цифровой трансформации: экзистенциальные риски и ценностные противоречия

Бурнашев Ринат Фаритович
доц.
Самаркандский государственный институт иностранных языков
Республика Узбекистан, г. Самарканд
E-mail: burnashev1982@gmail.com

Тилляева Мадина Махсудовна
студент
Самаркандский государственный институт иностранных языков
Республика Узбекистан, г. Самарканд
E-mail: madinatillyaeva927@gmail.com

Personal information security in the context of digital transformation: existential risks and value contradictions

Burnashev Rinat Faritovich
Associate Professor
Samarkand State Institute of Foreign Languages
Republic of Uzbekistan, Samarkand

Tillyaeva Madina Makhsudovna
student
Samarkand State Institute of Foreign Languages Samarkand
Republic of Uzbekistan

Аннотация

Целью исследования является выявление экзистенциальных рисков и ценностных противоречий информационной безопасности личности в цифровом обществе, уточнение критериев её оценки и обозначение возможностей их эмпирической проверки. Исследование носит теоретико-методологический характер; эмпирические данные не собирались. Применены социально-философский, экзистенциально-феноменологический, аксиологический и сравнительно-концептуальный методы. Обосновано различие между

Библиографическое описание: Бурнашев Р.Ф., Тилляева М.М. Информационная безопасность личности в условиях цифровой трансформации: экзистенциальные риски и ценностные противоречия // Universum: общественные науки : электрон. научн. журн. 2026. 11(138). URL: https://7universum.com/ru/social/archive/item/23650

технической защищённостью информации и сохранением условий самостоятельного действия личности. Выделены риски утраты аутентичности, ограничения автономии, цифрового отчуждения и экзистенциальной неопределённости, а также противоречия между свободой и контролем, приватностью и открытостью, автономией и персонализацией, ответственностью человека и автоматизацией решений. Предложены четыре взаимосвязанных критерия: онтологический (признание человека субъектом, не сводимым к цифровому профилю), гносеологический (критическая оценка информации), аксиологический (приоритет достоинства, свободы и приватности) и праксеологический, или социально-практический (реальная осуществимость защиты прав и пересмотра решений). Уточнено, что онтологический статус личности не измеряется непосредственно: проверке подлежат его институциональные проявления – доступ к объяснению, исправлению данных и человеческому пересмотру значимых решений. Для последующего исследования предложено сочетать анализ правил и практик обжалования автоматизированных решений с заданиями на цифровую и медиаграмотность и интервью пользователей разных групп. Сформулированные индикаторы являются исследовательскими предложениями, а не результатами проведённого измерения.

Abstract

The article examines existential risks and value contradictions of personal information security in the digital society, refines the criteria for its assessment, and outlines possible empirical tests. This is a theoretical and methodological study; no empirical data were collected. Socio-philosophical, existential-phenomenological, axiological, and comparative-conceptual approaches are employed. A distinction is drawn between protecting information systems and preserving the conditions for individuals to act autonomously. Four risks are identified: loss of authenticity, restricted autonomy, digital alienation, and existential uncertainty. The main value tensions involve freedom and control, privacy and openness, autonomy and algorithmic personalization, and human responsibility and automated decisions. The proposed framework comprises four criteria: ontological (recognition of the person as a subject irreducible to a digital profile), epistemological (critical assessment of information), axiological (priority of dignity, freedom, and privacy), and praxeological or socio-practical (effective access to remedies and decision review). The ontological status of personhood cannot be measured directly; empirical inquiry can instead examine its institutional manifestations, including access to explanations, data correction, and human reconsideration of consequential decisions. Future studies could combine analysis of automated-decision appeals with digital and media literacy tasks and interviews across user groups. These indicators constitute a proposal for future validation, not findings from completed fieldwork.

Ключевые слова: информационная безопасность личности, цифровая трансформация, экзистенциальные риски, автономия, аутентичность, субъектность, ценностные противоречия.

Keywords: personal information security, digital transformation, existential risks, autonomy, authenticity, subjectivity, value contradictions.

Введение

Цифровая трансформация меняет познание, общение и формирование идентичности. Поисковые системы, рекомендательные алгоритмы, платформы и генеративный искусственный интеллект выступают посредниками между человеком и обществом. Они отбирают содержание и предлагают пользователю способы действия. Расширение коммуникации сопровождается асимметрией влияния. Технологический подход связывает безопасность с конфиденциальностью, целостностью и доступностью информации. Однако даже технически защищённая система способна ограничивать свободу суждений посредством интерфейсных манипуляций и непрозрачного отбора альтернатив. В работе Р. Бурнашева информационная безопасность личности рассматривается как социально-философская проблема, выходящая за пределы сохранности данных [1]. В настоящем исследовании этот тезис уточняется через оценку возможности осмысленного несогласия, исправления цифрового профиля и пересмотра решений, затрагивающих права человека. Теоретическую основу составляют концепции дисциплинарной власти М. Фуко [2] и коммуникативного обоснования норм Ю. Хабермаса [3]. Проблемы этической ответственности при использовании искусственного интеллекта рассмотрены М. Кукельбергом [4], а изменение условий человеческого существования в гиперсвязанной среде раскрывается в «Манифесте онлайф», подготовленном исследовательской группой под редакцией Л. Флориди [5]. М. Хайдеггер подчёркивал: «Сущность техники вовсе не является чем-то техническим» [6]; для данной статьи это означает необходимость анализировать социальный способ применения техники, а не только её устройство. К. Кярки исследует неравенство возможностей противодействовать цифровому отвлечению [7]; Ж.-П. Сартр связывает свободу с ответственностью за выбор [8]. Б. Ваассен анализирует зависимость личной автономии от непрозрачности алгоритмических решений [9], Ш. Валлор – ограничения предсказательных технологий как моделей человеческого будущего [10], Ш. Зубофф – экономическую логику надзорного капитализма [11]. Цель статьи – уточнить критерии безопасности, не сводимые к защите данных, и предложить способы их эмпирической проверки. Рабочая гипотеза состоит в том, что информационная безопасность личности предполагает институционально обеспеченную возможность самостоятельного выбора и оспаривания значимых решений.

Материалы и методы

Исследование является теоретико-методологическим. Материалом послужили философские работы о свободе, технике и власти, а также публикации об алгоритмических решениях и цифровом внимании. Социально-философский подход использован для анализа отношений власти между человеком и цифровыми институтами; экзистенциально-феноменологический – для разграничения аутентичного выбора и адаптации к навязанным альтернативам; аксиологический – для выявления конфликтов свободы, безопасности и приватности; сравнительно-концептуальный – для сопоставления технических и субъектно-антропологических критериев. В качестве аналитического приёма применена модель «угроза

– механизм цифрового воздействия – затронутая ценность – доступное средство защиты». Это позволяет отличать характеристику платформы от последствий для способности личности действовать самостоятельно.

Единицей теоретического анализа выступает ситуация цифрового взаимодействия, в которой решение алгоритмической системы может повлиять на жизненные возможности человека. Опросы, интервью, наблюдения и анализ административных дел в рамках статьи не проводились; описываемые далее ситуации имеют характер мысленных примеров, а предложенные индикаторы требуют самостоятельной эмпирической апробации. Поэтому выводы относятся к концептуальной обоснованности критериев, а не к установленной распространённости рисков.

Результаты исследования

В условиях цифровой трансформации современного общества происходит существенное изменение характера человеческой субъектности, выражающееся в преобразовании механизмов познания, коммуникации, самоидентификации и принятия решений. Субъектность в данном контексте понимается как способность личности осознавать основания собственных действий, соотносить их с индивидуальными ценностями, осуществлять самостоятельный выбор и принимать ответственность за его последствия. Цифровизация не обязательно ослабляет данную способность, поскольку современные информационные технологии расширяют доступ к знаниям, образовательным ресурсам и различным формам общественного участия. Вместе с тем персонализированные цифровые платформы и алгоритмические системы предоставляют пользователю не нейтральную совокупность сведений, а предварительно отобранную информационную картину действительности. В подобных условиях самостоятельный выбор источников информации и критическое осмысление получаемых сведений становятся необходимыми предпосылками обеспечения информационной безопасности личности. Предлагается различать цифровой профиль и личностную идентичность. Первый представляет собой поддающуюся вычислительной обработке совокупность сведений, присвоенных признаков и прогнозных оценок; вторая связана с продолжающимся рефлексивным самоопределением человека. Это различие существенно в контексте надзорного капитализма, при котором поведенческие данные могут использоваться для прогнозирования и формирования будущих действий [11]. Алгоритмический профиль способен влиять на доступ к услугам и возможностям, но не должен приобретать статус окончательного суждения о человеке. Авторский тезис заключается в том, что онтологическая угроза возникает не от самого существования профиля, а при институциональном отождествлении профиля с личностью: когда человек не может исправить значимые сведения, получить объяснение решения или добиться рассмотрения своей индивидуальной ситуации. Тем самым субъектно-антропологическое понимание информационной безопасности [1] дополняется указанием на проверяемые условия сохранения субъектного статуса. Социально-философский анализ позволяет выделить четыре взаимосвязанные группы экзистенциальных рисков цифровой трансформации. Утрата аутентичности означает подмену собственных мотивов и жизненных целей ориентацией на показатели рейтинга и одобрения; ограничение автономии – сужение пространства осознанных альтернатив вследствие непрозрачной настройки рекомендаций;

цифровое отчуждение – ослабление возможности непосредственно влиять на условия взаимодействия, заданные платформой; экзистенциальная неопределённость – затруднение установления различия между событием, интерпретацией и синтетическим изображением действительности. Эти риски необходимо различать по механизмам: рейтинг влияет на мотивацию, алгоритмическая селекция – на доступные варианты, платформенные правила – на способность участвовать в их изменении, а синтетический контент – на доверие к знанию. Такая типология не означает, что каждый пользователь переживает все четыре риска: их наличие и выраженность зависят от контекста и требуют эмпирической проверки.

Воздействие цифровых технологий на личность не является исключительно негативным или технологически предопределённым. Расширение доступа к альтернативным источникам способно укреплять самостоятельность мышления, тогда как непрозрачное управление вниманием – ослаблять её. Ж.-П. Сартр писал: «человек осуждён быть свободным» [8, с. 327]. Применительно к цифровой среде этот тезис не означает, будто любой выбор пользователя уже свободен: ответственность человека нельзя обсуждать вне доступного ему набора альтернатив и возможности понять последствия своих действий. Поэтому предлагаемое различение состоит в следующем: формальная возможность нажать кнопку подтверждения ещё не равнозначна содержательной автономии, если значимая информация скрыта или отказ фактически невозможен. Именно такое расхождение между формальным и содержательным выбором образует особый экзистенциальный аспект информационного риска.

Ценностные противоречия цифрового общества особенно заметны в соотношении свободы и информационного контроля. Мониторинг может повышать безопасность и предотвращать злоупотребления, однако без соразмерных ограничений наблюдение способно стимулировать самоцензуру и зависимость человека от внешней оценки. М. Фуко, характеризуя дисциплинарную власть, использовал формулу «Видимость – это ловушка» [2]. Применение этой идеи к цифровым платформам требует оговорки: цифровая среда не тождественна дисциплинарным учреждениям, а наблюдение может преследовать законные защитные цели. Авторская позиция заключается в том, что критерием допустимости мониторинга служит не его наличие само по себе, а сочетание определённости цели, соразмерности вмешательства, информированности пользователя и доступности независимого пересмотра спорного применения контроля. Противоречие между приватностью и информационной открытостью проявляется в том, что расширение публичной коммуникации одновременно увеличивает возможности участия и риски использования персональных сведений. Противоречие между автономией и алгоритмической персонализацией состоит в двойственном эффекте рекомендаций: они облегчают поиск информации, но могут закреплять привычный набор вариантов. Наконец, автоматизация решений повышает скорость обработки обращений, но усложняет распределение ответственности за ошибочный результат. Концепция надзорного капитализма Ш. Зубофф объясняет экономическую заинтересованность платформ в прогнозировании поведения на основе собираемых данных [11]. Однако не всякая персонализация равнозначна манипуляции: социально-философская оценка должна устанавливать, насколько человек информирован о принципах отбора, может изменить настройки и располагает реальными способами возражения.

Предложенные ценностные противоречия нельзя разрешить ни простым увеличением контроля, ни отказом от цифровых услуг. Требуется оценивать, какие именно интересы затронуты, допускается ли менее ограничительное средство обеспечения безопасности и предусмотрен ли пересмотр решения. В этой связи предлагается трёхуровневое различение: техническая безопасность защищает данные и работу систем; процедурная безопасность обеспечивает объяснимость, предсказуемость и оспоримость значимых решений; экзистенциальная безопасность характеризует сохранение способности человека определять собственные цели. Указанные уровни не заменяют друг друга: целостность базы данных ещё не подтверждает справедливость решения, а формально установленная процедура обжалования не гарантирует её фактической доступности. На основании проведённого анализа предлагается четыре взаимосвязанных критерия информационной безопасности личности. Онтологический критерий означает признание человека действующим субъектом, личность которого принципиально не исчерпывается цифровым профилем. Его нельзя свести к измерению «количества субъектности»: косвенными признаками институционального признания человека выступают возможность ознакомиться со значимыми сведениями о себе, исправить ошибочную запись, получить понятное объяснение решения и представить индивидуальные обстоятельства при его пересмотре. Гносеологический критерий характеризует способность отличать факт от интерпретации и синтетического контента, проверять источники и понимать ограничения алгоритмических рекомендаций; предполагаемые индикаторы – результаты ситуационных заданий, а не только самооценка грамотности. Аксиологический критерий выражает нормативную согласованность цифровой практики с достоинством, свободой, приватностью и ответственностью; он предполагает оценку соразмерности вмешательства и ясности правил обработки данных. Праксеологический (социально-практический) критерий характеризует действительную осуществимость защиты интересов: наличие понятной процедуры обращения, достижимость уполномоченного человека, разумность сроков ответа и результативность пересмотра. Таким образом, онтологический критерий фиксирует принцип несводимости человека к профилю и условия признания его субъектом, а праксеологический – то, насколько эти условия реализуются в конкретных действиях и институтах.

Предложенная система критериев предполагает проверку на разных уровнях. Онтологический и аксиологический критерии имеют прежде всего нормативно-философское содержание: эмпирические данные не способны окончательно доказать или опровергнуть ценность человеческого достоинства и субъектности, но позволяют установить, насколько цифровые практики соответствуют этим требованиям. Гносеологический и праксеологический критерии допускают более непосредственную проверку через наблюдаемые действия, результаты ситуационных заданий и документируемые процедуры. В этом состоит методологическое уточнение авторского подхода: не следует отождествлять провозглашённое право с возможностью его использования, а осведомлённость о цифровых угрозах – с умением распознать их в конкретной ситуации. Для косвенной проверки онтологического критерия целесообразно провести сравнительный анализ публично доступных правил автоматизированного принятия решений и практик обращения пользователей. Единицами наблюдения могут быть случаи, в которых алгоритмическая

оценка влияет на доступ к услуге или существенную возможность. Предлагаемые показатели: информирование о факте автоматизации; наличие процедуры ознакомления и исправления данных; возможность сообщить индивидуальные обстоятельства; доступность человеческого рассмотрения. Фиксация этих признаков позволяет оценить институциональные условия признания субъектности, но не измеряет онтологический статус человека как таковой.

Праксеологический критерий предлагается проверять по фактическому ходу обжалования: доступности инструкции и канала обращения, времени до содержательного ответа, доле обращений, получивших мотивированное рассмотрение, и доле решений, изменённых после проверки человеком. Знаменатель каждого показателя должен быть явно указан (например, число поданных обращений, а не всех решений). Если доступны только правила сервиса, допустим вывод лишь о формальных гарантиях, но не об эффективности их реализации. Важно также учитывать отказы пользователей от обжалования вследствие сложности процедуры. Гносеологический критерий может изучаться с помощью одинаковых ситуационных заданий на проверку источника, распознавание синтетического контента, настройку приватности и оценку достоверности алгоритмического ответа. Результаты целесообразно сопоставлять между группами пользователей с разным возрастом, образованием и опытом взаимодействия с цифровыми сервисами, не отождествляя эти характеристики с уровнем компетентности заранее. Аксиологический критерий требует качественного анализа того, как участники обосновывают допустимость наблюдения, приоритет приватности и распределение ответственности за автоматизированную ошибку.

В качестве возможного дизайна следующего этапа предложена последовательность: анализ документов и обезличенных обращений, затем ситуационные задания и полуструктурированные интервью, после чего – сопоставление формальных гарантий с описанным опытом пользователей. Перед проведением исследования необходимы добровольное информированное согласие, минимизация персональных данных и проверка применимого правового режима: процедуры оспаривания различаются в зависимости от страны, отрасли и вида решения. Приведённый план не является описанием уже собранного массива или завершённого пилотного исследования.

Обсуждение результатов исследования

Техническая защищённость не равнозначна защищённости человеческой автономии. Конфиденциальность исключает неправомерное раскрытие данных, но не манипулятивное получение согласия на их обработку; целостность записи не гарантирует обоснованности решения, которое на ней построено; доступность сервиса не означает доступности обжалования. Предложенное трёхуровневое различение технической, процедурной и экзистенциальной безопасности позволяет установить точку возникновения риска: в обработке данных, в правилах принятия решения или в ограничении осмысленного самоопределения. При этом нарушения одного уровня не всегда свидетельствуют о нарушениях остальных, что делает необходимой раздельную оценку. Рассмотрим условную ситуацию: автоматизированная система отказывает гражданину в доступе к значимой услуге, опираясь на ошибочный цифровой профиль. Даже если база защищена от утечки, нарушение может возникнуть на двух иных уровнях. Онтологический риск проявится в том, что профиль

фактически признаётся исчерпывающим описанием человека; праксеологический – в отсутствии доступного канала исправления сведений и пересмотра отказа. Если же сервис позволяет объяснить решение, исправить данные и обратиться к ответственному специалисту, один и тот же алгоритм создаёт иные условия для реализации субъектности. Пример является аналитической конструкцией, а не описанием конкретного случая.

Б. Ваассен обосновывает значимость непрозрачности алгоритмов именно в ситуациях, когда решения влияют на существенные жизненные возможности человека [9]. К. Кярки показывает, что возможности управлять вниманием и сопротивляться цифровому отвлечению распределены между пользователями неравномерно [7]. Из сопоставления этих выводов следует проверяемое предположение: одинаковый интерфейс может создавать неодинаковый риск для разных социальных групп, а тяжесть последствий алгоритмической ошибки зависит не только от технических характеристик модели, но и от доступности разъяснений и человеческого пересмотра. В русле дискурсивной этики Ю. Хабермаса легитимность цифровых правил предполагает возможность их публичного обоснования перед теми, кого они затрагивают [3]. Для оценки платформ и автоматизированных сервисов этот тезис переводится в три вопроса: известны ли пользователю основания значимого решения; может ли он представить возражения; предусмотрен ли субъект, ответственный за мотивированный ответ? Сочетание отрицательных ответов позволяет говорить о риске институционального исключения человека из процедуры, даже если обработка данных технически корректна. Вместе с тем прозрачность алгоритма не является достаточным условием справедливости: объяснение может быть формально доступным, но непонятным человеку без специальной подготовки. Поэтому человекоцентричность предполагает не только публикацию правил, но и проверку их практической понятности и применимости.

Заключение

Проведённый теоретико-методологический анализ позволяет рассматривать информационную безопасность личности как сочетание технической защищённости, процедурных гарантий и сохранения условий самостоятельного самоопределения. Авторское уточнение состоит в разграничении наличия формального выбора и возможности содержательно влиять на затрагивающие человека цифровые решения. Обоснована типология четырёх экзистенциальных рисков и предложена четырёхкритериальная модель оценки: онтологический критерий фиксирует принцип несводимости человека к цифровому профилю, гносеологический – способность критически работать с информацией, аксиологический – соответствие практик фундаментальным ценностям, праксеологический – фактическую доступность способов защиты и пересмотра. Указанные измерения связаны между собой, но не совпадают: признание субъектного статуса не тождественно эффективности процедуры его защиты. Предложены направления эмпирической апробации модели: изучение регламентов и результатов обжалования автоматизированных решений, анализ ситуационных заданий на цифровую и медиаграмотность и сопоставление опыта разных групп пользователей. Эти исследования в рамках статьи не проводились, поэтому заявленные критерии и индикаторы рассматриваются как теоретически обоснованная программа проверки, а не как эмпирически подтверждённая шкала. Дальнейшая работа

должна оценить пригодность индикаторов, контекстные ограничения их применения и возможные расхождения между формальными гарантиями и реальным опытом пользователя.

Список литературы

1. Бурнашев Р. Информационная безопасность личности как предмет социальной философии // Ijtimoiy-gumanitar sohada ilmiy-innovatsion tadqiqotlar. – 2026. – Т. 3. – С. 535–543.
2. Фуко М. Фуко М. Надзирать и наказывать. Рождение тюрьмы / Пер. с фр. В. Наумова под ред. И. Борисовой. С. 217. – М.: Ad Marginem, 1999.
3. Хабермас Ю. Моральное сознание и коммуникативное действие / Пер. с нем. С.В. Шачин, под ред. Д.В. Скляднева. С. 149. – СПб.: Наука, 2001.
4. Coeckelbergh M. Al ethics // Cambridge, MA: The MIT Press. Coeckelbergh, M. (2022),“Democracy, epistemic agency, and AI: Political epistemology in times of artificial intelligence,” Al Ethics. – 2020. – Т. 3. – P. 1–10.
5. Floridi L. Onlife Initiative. The onlife manifesto // The onlife manifesto: Being human in a hyperconnected era. – Cham: Springer International Publishing, 2014. – P. 7–13.
6. Хайдеггер М. Вопрос о технике / Пер. с нем. В.В. Бибихина // Хайдеггер М. Время и бытие: Статьи и выступления. – М.: Республика, 1993. – С. 221–237.
7. Kärki K. Digital Distraction, Attention Regulation, and Inequality: K. Kärki // Philosophy & Technology. – 2024. – Т. 37. – P. 1–21.
8. Сартр Ж.П. Экзистенциализм – это гуманизм: [сборник] / Жан Поль Сартр; [перевод с французского Т. Чугуновой, Н. Полторацкой]. – Москва: Издательство АСТ, 2025. – 160 с.
9. Vaassen B. AI, opacity, and personal autonomy // Philosophy & Technology. – 2022. – Т. 35. – P. 1–20.
10. Vallor S. The AI mirror: How to reclaim our humanity in an age of machine thinking. – Oxford University Press. – 2024. – 257 P.
11. Зубофф Ш. Эпоха надзорного капитализма: битва за человеческое будущее на новых рубежах власти / Пер. с англ. А.Ф. Васильева; под ред. Я. Охонько и А. Смирнова. – Москва: Издательство Института Гайдара, 2024. – 784 с.

References

1. Burnashev R. [Information security of the individual as a subject of social philosophy] // Ijtimoiy-gumanitar sohada ilmiy-innovatsion tadqiqotlar. – 2026. – Vol. 3. (In Russ.).
2. Fuko M. [Foucault M. Discipline and Punish. The Birth of the Prison] / Per. s fr. V. Naumova pod red. I. Borisovoj. – M.: Ad Marginem, 1999. – C. 217 (In Russ.).
3. Khabermas Yu. [Moral Consciousness and Communicative Action] / Per. s nem. S.V. Shachin, pod red. D.V. Sklyadneva. – SPb.: Nauka, 2001. – C. 149 (In Russ.).

4. Coeckelbergh M. Al ethics // Cambridge, MA: The MIT Press. Coeckelbergh, M. (2022),“Democracy, epistemic agency, and AI: Political epistemology in times of artificial intelligence,” Al Ethics. – 2020. – Vol. 3. – P. 1–10.
5. Floridi L. Onlife Initiative. The onlife manifesto // The onlife manifesto: Being human in a hyperconnected era. – Cham: Springer International Publishing, 2014. – P. 7–13.
6. Heidegger M. Vopros o tekhnike [The Question Concerning Technology]. In: Heidegger M. Vremya i bytie: stat’i i vystupleniya [Time and Being: Articles and Speeches]. Moscow: Respublika, 1993, P. 221–237. (In Russ.).
7. Kärki K. Digital Distraction, Attention Regulation, and Inequality: K. Kärki // Philosophy & Technology. – 2024. – Vol. 37. – P. 1–21.
8. Sartre J.-P. Ekzistentsializm – eto gumanizm [Existentialism Is a Humanism]. Moscow: AST,. – 2025. – 160 P. (In Russ.).
9. Vaassen B. AI, opacity, and personal autonomy // Philosophy & Technology. – 2022. – Vol. 35. – P. 1–20.
10. Vallor S. The AI mirror: How to reclaim our humanity in an age of machine thinking. – Oxford University Press. – 2024. – 257 P.
11. Zuboff Sh. Epokha nadzornogo kapitalizma: bitva za chelovecheskoe budushchee na novykh rubezhakh vlasti [The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power]. Moscow: Izdatel’stvo Instituta Gaidara,. – 2024. – 784 P. (In Russ.).