IJTIMOIY-GUMANITAR SOHADA ILMIY-INNOVATSION TADQIQOTLAR

ILMIY METODIK JURNALI

ISSN 3060-5059

VOL.3 № 5 2026

SHAXSNING AXBOROT XAVFSIZLIGI IJTIMOIY FALSAFA PREDMETI SIFATIDA

Burnashev Rinat Faritovich
Samarqand davlat chet tillar instituti, dotsent

Annotatsiya

Maqolada shaxsning axborot xavfsizligi raqamli transformatsiya sharoitida shakllanayotgan ijtimoiy-falsafiy fenomen sifatida talqin qilinadi. Antropotsentrik yondashuv asoslanib, unda shaxs xavfsizlik tizimining markaziy subyekti sifatida namoyon bo‘ladi. Michel Foucault, Jürgen Habermas hamda Manuel Castells g‘oyalari asosida insonning avtonomiyasi, identifikatsiyasi va maxfiyligiga ta’sir etuvchi raqamli muhitning hokimiyat, kommunikativ va tarmoq mexanizmlari tahlil qilinadi. Shaxs, davlat, jamiyat va texnologiyalar o‘rtasidagi o‘zaro aloqani ifodalovchi konseptual model taklif qilinib, unda xavfsizlik ijtimoiy, huquqiy va texnologik omillar bilan belgilanadigan dinamik jarayon sifatida talqin etiladi.

Kalit so‘zlar: shaxsning axborot xavfsizligi, raqamli subyektlik, ijtimoiy falsafa, raqamli jamiyat, axborot muhiti, raqamli identiklik, algoritmik nazorat, shaxsiy ma’lumotlar, kommunikatsiya, raqamli madaniyat, maxfiylik, shaxs avtonomiyasi.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЛИЧНОСТИ КАК ПРЕДМЕТ СОЦИАЛЬНОЙ ФИЛОСОФИИ

Бурнашев Ринат Фаритович
Самаркандский государственный институт иностранных языков, доцент

Аннотация

В статье информационная безопасность личности рассматривается как социально-философский феномен, формирующийся в условиях цифровой трансформации общества. Обосновывается антропоцентрический подход, в котором личность выступает центральным субъектом системы безопасности. На основе идей М. Фуко, Ю. Хабермаса и М. Кастельса анализируются властные, коммуникативные и сетевые механизмы цифровой среды, влияющие на автономию, идентичность и приватность человека. Предложена концептуальная модель взаимодействия личности, государства, общества и технологий, в рамках которой безопасность понимается как динамический процесс, обусловленный социальными, правовыми и технологическими факторами.

Ключевые слова: информационная безопасность личности, цифровая субъектность, социальная философия, цифровое общество, информационная среда, цифровая идентичность, алгоритмический контроль, персональные данные, коммуникация, цифровая культура, приватность, автономия личности.

INFORMATION SECURITY OF THE INDIVIDUAL AS A SUBJECT OF SOCIAL PHILOSOPHY

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

Abstract

The article examines personal information security as a socio-philosophical phenomenon emerging in the context of the digital transformation of society. An anthropocentric approach is substantiated, in which the individual is viewed as the central subject of the security system. Based on the ideas of M. Foucault, J. Habermas, and M. Castells, the study analyzes the power, communicative, and network mechanisms of the digital environment that influence human autonomy, identity, and privacy. A conceptual model of interaction between the individual, the state, society, and technologies is proposed, within which security is understood as a dynamic process determined by social, legal, and technological factors.

Keywords: personal information security, digital subjectivity, social philosophy, digital society, information environment, digital identity, algorithmic control, personal data, communication, digital culture, privacy, personal autonomy.

В условиях стремительной цифровой трансформации современного общества происходит качественное изменение положения личности в системе социальных отношений. Информационно-коммуникационные технологии перестают быть лишь инструментом деятельности и становятся самостоятельной средой формирования социальной реальности, в которой конструируются идентичность, формы коммуникации, модели поведения и механизмы социального контроля. Расширение цифровых платформ, сетевых сервисов и алгоритмических систем управления приводит к усилению влияния информационной среды на повседневную жизнь человека, его ценностные ориентации, способы взаимодействия и формы социальной активности. В этих условиях личность всё чаще оказывается включённой в сложные процессы цифрового наблюдения, обработки персональных данных и опосредованного алгоритмами управления, что трансформирует характер её автономии и субъектности.

Особую актуальность приобретает усиление механизмов цифрового контроля, алгоритмического управления и информационного воздействия. Современные цифровые технологии не только обеспечивают удобство коммуникации и доступ к информации, но и формируют новые формы власти, основанные на анализе данных, прогнозировании поведения и управлении вниманием. Алгоритмические системы, социальные сети, цифровые платформы и государственные информационные системы создают сложную инфраструктуру влияния, в рамках которой человек становится объектом постоянного наблюдения, оценки и регулирования. Это приводит к возникновению новых рисков, связанных с утратой приватности, манипуляцией сознанием, фрагментацией идентичности и усилением асимметрии информационной власти. В связи с этим возрастает необходимость философского осмысления информационной безопасности личности не только как технической или правовой категории, но как комплексного социально-философского феномена, отражающего глубинные изменения в структуре взаимодействия человека, общества, государства и цифровых технологий.

Анализ степени научной разработанности проблемы показывает, что в современной научной литературе преобладают преимущественно технические и правовые подходы к исследованию информационной безопасности. Основное внимание уделяется вопросам защиты данных, криптографическим методам, нормативно-правовому регулированию и обеспечению киберустойчивости информационных систем. При этом личность в большинстве исследований рассматривается как объект защиты, а не как активный субъект, формирующий и переживающий риски цифровой среды. Социально-философские модели, способные объяснить информационную безопасность как сложный феномен взаимодействия власти, коммуникации, социальных структур и технологий, разработаны недостаточно. Исследования, посвящённые проблемам власти, коммуникации и цифровых сетей, как правило, существуют разрозненно, не образуя единого концептуального пространства. В результате отсутствует целостная теоретическая рамка, позволяющая осмыслить информационную безопасность личности в контексте трансформации социальных отношений в цифровую эпоху.

В этой связи возникает научная проблема, заключающаяся в отсутствии целостной философской модели, объясняющей информационную безопасность личности как результат взаимодействия множества факторов — властных механизмов, коммуникативных процессов, социальных структур и технологических систем. Существующие подходы, ориентированные на отдельные аспекты проблемы, не позволяют в полной мере раскрыть системный характер угроз и показать роль личности как центрального элемента в структуре обеспечения безопасности. Необходимость интеграции различных теорий обусловлена тем, что цифровая среда формирует не только технические, но и антропологические, социальные и этические вызовы, затрагивающие фундаментальные основания человеческого существования.

Целью настоящего исследования является социально-философское обоснование концептуальной модели взаимодействия личности, государства, общества и цифровых технологий в процессе обеспечения информационной безопасности. Достижение поставленной цели предполагает рассмотрение информационной безопасности не как статического состояния защищённости, а как динамической системы отношений, в которой ключевую роль играет личность как носитель цифровой субъектности, прав, свобод и ценностей.

В соответствии с поставленной целью в исследовании решаются следующие задачи: раскрывается природа цифровой субъектности личности как новой формы социального бытия,

формирующейся в условиях информационного общества; обосновывается центральная роль личности в системе информационной безопасности, где именно человек выступает носителем идентичности, информации и социальных связей; выявляются властные, коммуникативные и сетевые механизмы формирования угроз, проявляющиеся через алгоритмический контроль, информационное воздействие и цифровую стратификацию; показывается системный и динамический характер безопасности, обусловленный постоянным изменением технологической среды и социальных практик.

Объектом исследования выступает информационная безопасность в условиях цифрового общества как комплексный социальный феномен, формирующийся на пересечении технологий, социальных институтов и культурных практик. Предметом исследования является социально-философская модель взаимодействия личности, общества, государства и цифровых технологий, определяющая условия, механизмы и формы обеспечения информационной безопасности.

Научная новизна исследования заключается в разработке системного социально-философского подхода к осмыслению информационной безопасности личности. В работе обоснована необходимость трактовки информационной безопасности личности как самостоятельной философской категории, отражающей новые антропологические, этические и социокультурные вызовы цифровой эпохи. Показано, что личность должна рассматриваться как центральный элемент системы обеспечения безопасности, вокруг которого выстраиваются отношения между государством, обществом и технологическими структурами. Выявлены ключевые социокультурные и этические противоречия, возникающие в процессе защиты личности в информационном пространстве, включая соотношение между контролем и свободой, безопасностью и автономией, публичностью и приватностью. Сформирована концептуальная модель взаимодействия личности, государства, общества и цифровых технологий, раскрывающая безопасность как динамическую систему отношений, изменяющуюся под влиянием развития цифровой среды и трансформации социальных практик.

Методологическая основа исследования выстраивается в рамках социально-философского анализа, ориентированного на выявление глубинных закономерностей взаимодействия личности, общества, государства и цифровых технологий в условиях формирования информационного общества. Исследование опирается на системный и междисциплинарный подход, позволяющий рассматривать информационную безопасность личности не как изолированную техническую проблему, а как сложный социальный феномен, включённый в сеть институциональных, коммуникативных и технологических отношений. Системный подход обеспечивает целостное понимание структуры информационной безопасности, её элементов и взаимосвязей, а также позволяет выявить динамический характер трансформаций, происходящих в цифровой среде. Междисциплинарность проявляется в интеграции философских, социологических, правовых и культурологических перспектив, что создаёт условия для комплексного осмысления исследуемого явления.

Важное место в методологической структуре работы занимает структурно-функциональный анализ, направленный на выявление ролей и функций ключевых акторов системы информационной безопасности — личности, государства, общества и технологических платформ. Данный подход позволяет рассмотреть информационную безопасность как совокупность взаимосвязанных элементов, каждый из которых выполняет определённые функции в процессе поддержания устойчивости цифровой среды. В рамках исследования применяется также метод концептуального моделирования, ориентированный на построение теоретической конструкции, отражающей характер взаимодействия социальных и технологических факторов, формирующих условия защищённости личности в информационном пространстве.

Методологическая специфика исследования заключается в синтезе классических и современных социально-философских теорий, позволяющих раскрыть многомерную природу информационной безопасности личности. В качестве теоретических оснований используются концепции Мишеля Фуко, Юргена Хабермаса и Мануэля Кастельса, которые в совокупности создают целостную аналитическую рамку для осмысления властных, коммуникативных и сетевых механизмов функционирования цифрового общества.

Подход Мишеля Фуко позволяет рассматривать информационную безопасность через призму властных отношений, проявляющихся в формах наблюдения, контроля и дисциплинарного воздействия. В контексте цифровой эпохи власть приобретает распределённый характер и

реализуется через алгоритмические системы, базы данных, цифровые платформы и информационные инфраструктуры. В этом смысле продуктивной является мысль Фуко о том, что «власть повсюду; не потому, что она всё охватывает, а потому, что она исходит отовсюду» [1, с. 49], что позволяет интерпретировать цифровые технологии как среду множественных и рассредоточенных механизмов контроля. Использование методологии Фуко даёт возможность рассматривать цифровые технологии как инструменты дисциплинарных практик, формирующих новые формы регулирования поведения и идентичности. Особое значение приобретает анализ персональных данных как объекта контроля и управления, поскольку именно через их сбор, обработку и интерпретацию осуществляется современное информационное воздействие на личность. В этом контексте сохраняет актуальность и положение Фуко о том, что «знание и власть непосредственно предполагают друг друга» [2, с. 130], что позволяет рассматривать информационные ресурсы и данные как важнейший инструмент формирования современных структур власти и контроля.

Методологические положения Юргена Хабермаса применяются для анализа информационной безопасности в контексте коммуникативных процессов и трансформации публичной сферы. В условиях цифровой среды коммуникация становится ключевым фактором формирования общественного сознания, ценностных ориентаций и моделей поведения. С позиций теории коммуникативного действия информационная безопасность рассматривается как состояние, связанное с качеством и рациональностью коммуникации, возможностью достижения взаимопонимания и согласования интересов различных социальных акторов. Хабермас подчёркивал, что «коммуникативное действие направлено на достижение взаимопонимания» [3, с. 362], что особенно значимо в условиях цифровой публичной сферы, где формируются новые формы общественного диалога. Цифровая среда существенно трансформирует публичное пространство, создавая как новые возможности для участия в общественной дискуссии, так и риски манипуляции информацией, искажения смыслов и фрагментации коммуникации. В этой связи особое значение приобретают правовые и этические нормы, выступающие механизмами согласования интересов и регулирования взаимодействия в цифровом пространстве, что соответствует идее Хабермаса о том, что устойчивость социального порядка основывается на нормативно закреплённых формах рационального согласия [4, с. 127].

Подход Мануэля Кастельса, основанный на теории сетевого общества, позволяет осмыслить информационную безопасность в логике сетевых структур, в которых происходит перераспределение власти, ресурсов и информационных потоков. В рамках данной концепции цифровая реальность рассматривается как система взаимосвязанных сетей, охватывающих экономику, политику, культуру и повседневную жизнь. Кастельс отмечал, что «наши общества всё больше структурируются вокруг оппозиции между Сетью и Я» [5, с. 431], указывая на напряжённое взаимодействие между глобальными информационными потоками и личной идентичностью. Это приводит к формированию новых форм социальной организации, в которых личность становится частью глобальных информационных процессов и сетевых взаимодействий. Особое внимание уделяется понятию сетевой идентичности, формирующейся под влиянием цифровых коммуникаций и социальных платформ. Использование методологии Кастельса позволяет выявить особенности взаимодействия государства, общества и технологий в цифровой реальности, а также показать, каким образом сетевые структуры влияют на распределение рисков и угроз информационной безопасности личности. Существенным является и положение Кастельса о том, что «власть сети сильнее власти над сетью» [6, с. 56], что подчёркивает трансформацию традиционных механизмов социального управления в условиях цифровой эпохи.

Построение концептуальной модели исследования осуществляется на основе синтеза трёх теоретических направлений, отражающих ключевые измерения цифровой реальности: власть, коммуникацию и сеть. Перспектива Фуко раскрывает механизмы контроля и дисциплинарного воздействия, Хабермаса — процессы коммуникации и согласования интересов, Кастельса — структурную организацию сетевых взаимодействий. Их объединение позволяет сформировать целостную теоретическую конструкцию, в которой информационная безопасность рассматривается как результат взаимодействия различных социальных и технологических факторов. В качестве основополагающего принципа построения модели используется антропоцентрический подход, в рамках которого личность рассматривается как центральный элемент системы. Именно вокруг личности выстраиваются отношения власти, коммуникации и сетевых взаимодействий,

формирующие условия её защищённости или уязвимости в цифровом пространстве.

Для анализа динамики информационной безопасности личности в исследовании вводится ряд аналитических критериев, позволяющих оценить степень устойчивости и эффективности функционирования системы. К числу таких критериев относятся уровень цифровой грамотности, определяющий способность личности осознанно взаимодействовать с информационной средой и противостоять манипулятивным воздействиям; зрелость социальных институтов, обеспечивающих нормативное регулирование и защиту прав в цифровом пространстве; эффективность правового регулирования, направленного на защиту персональных данных, обеспечение приватности и ограничение злоупотреблений информационной властью; а также уровень этической ответственности технологических акторов, включая разработчиков цифровых платформ, операторов данных и информационные корпорации. Использование данных критериев позволяет рассматривать информационную безопасность как динамический процесс, зависящий от взаимодействия социальных, культурных, правовых и технологических факторов и изменяющийся по мере развития цифрового общества.

В результате проведённого исследования информационная безопасность личности была переосмыслена и концептуализирована как самостоятельная социально-философская категория, отражающая качественно новый уровень взаимодействия человека с цифровой средой [7, с. 243]. В традиционных подходах безопасность рассматривалась преимущественно как защита информации, технических систем и каналов передачи данных. Однако в условиях цифровой трансформации акцент постепенно смещается от защиты информационных ресурсов к защите субъекта, который становится центральным носителем и одновременно объектом информационных процессов. В этой связи информационная безопасность приобретает антропологическое и аксиологическое измерение, поскольку напрямую связана с сохранением автономии личности, устойчивости её идентичности, права на приватность и свободу самовыражения. Таким образом, безопасность перестаёт быть исключительно технической задачей и становится условием сохранения целостности личности в цифровом обществе.

На основе социально-философского и междисциплинарного анализа была разработана концептуальная модель четырёхуровневого взаимодействия, объясняющая информационную безопасность как результат системной взаимосвязи личности, цифровых технологий, общества и государства (см. рис. 1). Научная новизна данной модели заключается в том, что впервые в рамках комплексного подхода информационная безопасность личности рассматривается как продукт взаимодействия этих четырёх взаимосвязанных уровней, образующих целостную систему. В отличие от традиционных технократических концепций, в центре разработанной схемы помещена личность как носитель цифровой субъектности. Это позволяет рассматривать защиту информации не только как техническую задачу, но и как гуманистическую, ценностно-правовую проблему, затрагивающую фундаментальные основы человеческой свободы и социальной идентичности.

Рисунок 1. Субъектно-ориентированная концептуальная модель взаимодействия

личности, государства, общества и цифровых технологий

Центральный уровень модели представлен личностью как цифровой субъектностью, включающей персональные данные, цифровую идентичность, автономию и свободу. Именно на этом уровне формируется основное содержание информационной безопасности, поскольку утрата контроля над персональными данными, искажение цифрового образа или ограничение автономии напрямую затрагивают социальное и психологическое благополучие человека. Личность в цифровом пространстве становится не только потребителем информации, но и источником данных, участником коммуникации и объектом алгоритмического анализа, что усиливает её уязвимость и одновременно повышает значимость защиты.

Внешние уровни модели образуют систему факторов, воздействующих на личность и определяющих степень её защищённости. Первый из них — цифровые технологии — представляет собой пространство власти и алгоритмического управления. Технологические платформы, системы обработки данных и алгоритмы анализа поведения формируют новую инфраструктуру контроля, в рамках которой осуществляется сбор, интерпретация и использование персональной информации. Второй уровень — общество — выступает пространством коммуникации, норм и ценностей, в котором формируются культурные установки, модели поведения и социальные ожидания, влияющие на восприятие безопасности и приватности. Третий уровень — государство — представляет собой пространство правового регулирования, где закрепляются нормативные механизмы защиты персональных данных, прав и свобод личности в информационной среде [8, с. 39].

Анализ показал, что в цифровой среде формируются специфические властные механизмы, которые существенно влияют на состояние информационной безопасности личности. В рамках интерпретации Мишеля Фуко они проявляются в виде алгоритмического контроля, цифрового надзора и концентрации информационной власти в руках крупных технологических структур и институциональных акторов. Алгоритмические системы позволяют не только фиксировать действия пользователя, но и прогнозировать его поведение, формируя условия скрытого управления и регулирования. Цифровой надзор становится повседневной практикой, встроенной в социальные сети, платформенные сервисы и государственные информационные системы. Концентрация информационной власти проявляется в накоплении больших массивов данных, что усиливает асимметрию между субъектом и институтами, обладающими доступом к информации.

Наряду с властными механизмами значительную роль в формировании информационной безопасности играют коммуникативные процессы, которые можно рассматривать в контексте теории Юргена Хабермаса. В цифровой среде формируется новая публичная сфера, основанная на сетевой коммуникации, обмене информацией и участии в общественном диалоге. Однако данная сфера характеризуется не только расширением возможностей коммуникации, но и ростом рисков, связанных с манипуляцией информацией, распространением недостоверных сведений и искажением общественного дискурса. В этих условиях особую роль приобретают нормы, регулирующие коммуникацию, а также культура диалога и рационального обсуждения, которые выступают важным фактором обеспечения информационной безопасности. Безопасность в данном случае проявляется не только как защита данных, но и как способность общества поддерживать конструктивное и ответственное коммуникативное пространство.

Существенное влияние на состояние информационной безопасности оказывает и сетевая структура современного общества, что находит отражение в концепции Мануэля Кастельса. Глобальные цифровые сети становятся основной средой существования личности, в которой формируются социальные связи, профессиональная активность и культурная идентичность. Включённость в сетевые процессы расширяет возможности самореализации, но одновременно усиливает уязвимость субъекта, поскольку персональные данные, коммуникации и цифровая идентичность оказываются встроенными в сложную систему глобальных информационных потоков. Сетевая структура общества формирует условия, при которых риски и угрозы распространяются быстрее и приобретают транснациональный характер, а защита личности требует координации усилий различных социальных институтов [9, с. 42].

Разработанная концептуальная модель интегрирует технологические, образовательные, организационные, правовые и этические механизмы, которые ранее рассматривались преимущественно разрозненно. Такой синтез обеспечивает целостное представление о современных стратегиях защиты персональных данных и цифровой идентичности, а также

позволяет рассматривать информационную безопасность как многомерное явление, включающее не только технические, но и социальные, культурные и нормативные аспекты. В рамках данной модели показано, что устойчивость системы безопасности определяется не отдельными мерами, а согласованным взаимодействием всех уровней — личности, общества, государства и технологий.

Одним из ключевых результатов исследования является обоснование динамического характера информационной безопасности личности. Впервые показано, что в условиях цифровой трансформации безопасность не может рассматриваться как статическое состояние, а представляет собой процесс, зависящий от ряда взаимосвязанных факторов. К их числу относятся уровень цифровой грамотности личности, определяющий способность осознанно взаимодействовать с информационной средой; зрелость социальных институтов, обеспечивающих защиту прав и формирование культуры безопасного поведения; эффективность правового регулирования, направленного на защиту персональных данных и обеспечение прозрачности использования информации; а также этическая ответственность разработчиков и операторов цифровых систем, влияющая на характер функционирования технологической среды. В совокупности эти факторы формируют изменяющуюся структуру рисков и возможностей, в рамках которой информационная безопасность личности становится результатом постоянного взаимодействия социальных, правовых и технологических процессов.

Обсуждение

Представленная концептуальная модель демонстрирует, что безопасность в цифровом обществе формируется не в рамках одного институционального или технологического пространства, а на пересечении нескольких фундаментальных измерений социальной реальности. Информационная безопасность личности возникает как результат сложного взаимодействия властных механизмов, коммуникативных процессов и сетевых структур, в которых осуществляется современное социальное бытие человека. Властное измерение проявляется через системы наблюдения, контроля и регулирования, встроенные в цифровую инфраструктуру; коммуникативное — через процессы обмена информацией, формирования общественного мнения и конструирования смыслов; сетевое — через глобальные информационные потоки и цифровые платформы, формирующие новую архитектуру социальных связей. Такое пересечение создаёт многомерное пространство, в котором безопасность личности становится результатом динамического баланса между различными социальными силами и институциональными практиками.

В рамках предложенной модели принципиально переосмысляется роль личности. Если в традиционных технократических концепциях она выступала преимущественно объектом защиты, то в разработанной философской интерпретации личность занимает центральное положение как активный субъект системы информационной безопасности. Именно человек является носителем цифровой идентичности, источником персональных данных, участником коммуникации и одновременно объектом воздействия цифровых технологий. Переход от понимания личности как пассивного объекта защиты к её рассмотрению в качестве центрального субъекта системы позволяет изменить саму логику осмысления безопасности. Она начинает рассматриваться не только как совокупность внешних защитных мер, но и как условие сохранения автономии, идентичности и способности к свободному социальному взаимодействию. Такой подход придаёт исследованию гуманистическую направленность, подчёркивая, что ключевой задачей обеспечения безопасности является не только защита информации, но и защита человеческого достоинства, свободы и права на самореализацию в цифровом пространстве.

Полученные результаты позволяют выявить ряд фундаментальных противоречий, характеризующих цифровую эпоху и определяющих сложность обеспечения информационной безопасности личности. Одним из наиболее значимых является противоречие между свободой и контролем. Цифровые технологии расширяют возможности доступа к информации, самовыражения и участия в общественной жизни, однако одновременно усиливают механизмы наблюдения, сбора данных и алгоритмического регулирования. Власть в цифровой среде приобретает рассредоточенный характер и проявляется в повседневных практиках, встроенных в функционирование платформ и сервисов. Это создаёт ситуацию, в которой расширение свободы сопровождается ростом контроля, что делает проблему безопасности не только технической, но и глубоко социально-философской.

Не менее значимым является противоречие между коммуникацией и манипуляцией.

Цифровая среда формирует новую публичную сферу, открывающую широкие возможности для диалога, обмена мнениями и участия в общественных процессах. Однако вместе с этим возникают риски информационного воздействия, искажения смыслов и манипулирования общественным сознанием. Масштабируемость цифровых коммуникаций усиливает влияние информационных потоков на восприятие реальности, а это делает человека более уязвимым перед воздействием дезинформации и скрытых стратегий влияния. В таких условиях информационная безопасность личности оказывается тесно связанной с качеством коммуникации, уровнем критического мышления и культурой информационного взаимодействия.

Третье ключевое противоречие связано с двойственной природой сетевых структур. С одной стороны, глобальные цифровые сети создают условия для интеграции, расширяют социальные связи, открывают доступ к знаниям и новым формам самореализации. С другой стороны, включённость в сетевое пространство повышает уязвимость личности, поскольку её цифровая идентичность, данные и коммуникации становятся частью глобальных информационных потоков. Сетевая логика организации общества усиливает взаимозависимость субъектов и одновременно снижает степень индивидуального контроля над собственной информацией. В результате личность оказывается в ситуации, где участие в сети становится условием социальной активности, но одновременно источником новых рисков.

Предложенная системная философская модель демонстрирует ряд существенных преимуществ по сравнению с традиционными подходами к анализу информационной безопасности. Прежде всего, она позволяет преодолеть узкотехническое понимание безопасности, ограниченное задачами защиты информации и инфраструктуры. В рамках данной модели безопасность рассматривается как многомерное социальное явление, формирующееся на пересечении технологических, правовых, коммуникативных и культурных процессов. Это расширяет исследовательскую перспективу и позволяет выявить глубинные причины возникновения угроз, связанные не только с техническими уязвимостями, но и с трансформацией социальных отношений.

Важным достоинством модели является интеграция гуманистического измерения в анализ информационной безопасности. Рассмотрение личности как центрального элемента системы позволяет подчеркнуть ценностный характер проблемы, связанный с защитой автономии, идентичности и права на свободное участие в социальной жизни. В этом контексте безопасность приобретает значение не только как инструмент защиты, но и как условие устойчивого развития цифрового общества, основанного на балансе между технологическим прогрессом, правовыми механизмами и этическими принципами. Таким образом, разработанная концептуальная модель создаёт теоретическую основу для более глубокого понимания природы информационной безопасности личности и открывает возможности для дальнейших исследований, направленных на осмысление роли человека в условиях цифровой трансформации социальной реальности.

Заключение

Проведённое исследование позволило сформулировать ряд обобщающих выводов, раскрывающих содержание и значение информационной безопасности личности в условиях цифровой трансформации общества. В работе обосновано, что информационная безопасность личности представляет собой не только прикладную или техническую категорию, но прежде всего системный социально-философский феномен, отражающий глубинные изменения в структуре взаимодействия человека, общества, государства и технологий. Она формируется в пространстве сложных взаимосвязей, где пересекаются властные механизмы, коммуникативные процессы и сетевые структуры, определяющие характер современной социальной реальности. В этой связи безопасность личности должна рассматриваться как результат динамического взаимодействия различных социальных и технологических факторов, влияющих на сохранение автономии, идентичности и свободы субъекта в цифровом мире.

Анализ показал, что именно на пересечении власти, коммуникации и сетевых взаимодействий формируется современная архитектура информационной безопасности. Властные механизмы проявляются в формах цифрового контроля, алгоритмического управления и концентрации информационных ресурсов; коммуникативные процессы определяют характер публичной сферы, способы согласования интересов и уровень доверия в обществе; сетевые структуры задают пространственные и функциональные параметры существования личности в глобальной информационной среде. В совокупности данные измерения создают сложную систему, в которой безопасность перестаёт быть исключительно технической задачей и приобретает

антропологическое, этическое и социально-философское содержание.

Теоретическая значимость исследования заключается в формировании новой философской модели информационной безопасности, основанной на антропоцентрическом принципе и системном подходе. Предложенная концепция позволяет переосмыслить традиционные представления о безопасности, сместив акцент с защиты информации на защиту личности как носителя цифровой субъектности. Тем самым расширяется предметное поле социальной философии, в которое включаются вопросы цифровой идентичности, информационной автономии, алгоритмического контроля и сетевых форм социальной организации. Разработанная модель способствует более глубокому пониманию природы современных социальных трансформаций и создаёт теоретическую основу для дальнейших исследований в области философии информационного общества.

Практическая значимость исследования определяется возможностью применения предложенной модели в сфере формирования цифровой политики и стратегий обеспечения информационной безопасности. Рассмотрение личности как центрального элемента системы позволяет учитывать не только технологические и правовые аспекты защиты данных, но и гуманистические, культурные и образовательные факторы. Полученные результаты могут быть использованы при разработке концепций государственной цифровой политики, направленных на защиту прав и свобод личности в информационном пространстве, а также при формировании комплексных программ цифровой безопасности. Особую роль в данном контексте играет развитие образовательных инициатив, ориентированных на повышение уровня цифровой грамотности, формирование культуры ответственного обращения с информацией и развитие критического мышления, что способствует снижению уязвимости личности в условиях цифровой среды.

Перспективы дальнейших исследований связаны с углублённым философским осмыслением новых вызовов, возникающих в процессе цифровой трансформации общества. Одним из приоритетных направлений является развитие этической философии цифровых технологий, ориентированной на анализ моральных оснований разработки и использования алгоритмических систем, искусственного интеллекта и цифровых платформ. Важное значение имеет исследование феномена цифровой субъектности в контексте проблем социальной справедливости, неравенства доступа к информационным ресурсам и трансформации социальных ролей. Не менее актуальным представляется дальнейшее развитие философии цифрового контроля, направленной на изучение механизмов наблюдения, управления и регулирования поведения в информационной среде, а также на выявление баланса между безопасностью и свободой в условиях усиливающейся цифровой зависимости. Таким образом, представленное исследование закладывает основу для формирования нового направления социально-философского анализа, в центре которого находится личность как ключевой субъект и ценностный ориентир информационной безопасности в цифровую эпоху.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Низовцев Д.Б. Проблема власти в работах Мишеля Фуко // Вестник Северного (Арктического) федерального университета. Серия: Гуманитарные и социальные науки. — 2015. № 4. — С. 49–57.
2. Грозина Н.А. Генеалогия субъекта в философии Фуко // Вестник Новосибирского государственного университета. Серия: Философия. — 2007. — Т. 5. — № 1. — С. 130–135.
3. Кудряшова М. Коммуникативное действие как ключевой механизм социальной интеграции: история вопроса // Проблемы современного мира глазами молодежи. — 2016. — С. 362–367.
4. Фливберг Б. Хабермас и Фуко — теоретики гражданского общества // Социологические исследования. — 2000. — Т. 2. — С. 127–136.
5. Кастельс М. Информационная эпоха: экономика, общество и культура / пер. с англ.; под науч. ред. О.И. Шкаратана. — М.: ГУ ВШЭ, 2000. — 608 с.
6. Кастельс М. Мануэль Кастельс о власти и коммуникации в сетевом обществе (сводный реферат) // Социальные сети и виртуальные сетевые сообщества. — 2013. — № 2013. — С. 56–69.
7. Бурнашев Р.Ф. Информационная безопасность как новая философская категория цифровой эпохи // Научный вестник Наманганского государственного университета. — 2024.№ 12.С. 243–248.
8. Бурнашев Р.Ф. Личность как центральный субъект информационной безопасности в условиях цифровой трансформации // Восточный журнал истории, политики и права Национального университета Узбекистана имени М. Улугбека. — 2026. — Т. 6. — № 2. — С. 39–51.
9. Бурнашев Р.Ф., Торгаутова Ш.А. Информационная безопасность в условиях сетевого общества: философский анализ концепции М. Кастельса // Universum: общественные науки. — 2026. — Т. 1.