ПРОБЛЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННОМ МИРЕ

Тутин Н. В., Марудин А.А., студенты

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Бархатков А.И. – канд. фил. наук, доцент

В работе рассматривается проблема информационной безопасности через призму социально-философского анализа. Проанализирован переход от техноцентричного понимания ИБ к антропоцентричному, где главным объектом защиты становится когнитивная свобода и цифровая идентичность личности. В исследовании сопоставляются традиционные и современные подходы к защите данных, а также обосновывается необходимость формирования новой культуры цифрового доверия в условиях алгоритмизации общества.

Стремительное развитие цифровой культуры и формирование информационного общества (в терминах Д. Белла и М. Кастельса) фундаментально изменили характер взаимодействия человека с окружающей реальностью. Информация перестала быть просто транслируемым сообщением, превратившись в ключевой фактор конструирования социальной реальности и управления массами [1]. В этой связи проблема информационной безопасности выходит далеко за рамки сугубо технической (программной или аппаратной) дисциплины, приобретая ярко выраженное философское, этическое и экзистенциальное измерение. Сетевые структуры проникают во все сферы человеческой жизнедеятельности, размывая границы между физическим и виртуальным мирами. Цифровая среда больше не является внешним инструментом; она стала средой обитания, формирующей наши ценности, убеждения и способы познания.

Традиционно информационная безопасность рассматривалась как триада «конфиденциальность, целостность, доступность» данных. Однако сегодня философский дискурс смещает фокус с «железа и кода» на самого человека.

Во-первых, актуализируется проблема трансформации понятия приватности. В условиях тотальной цифровизации и развития технологий Больших данных человек оставляет непрерывный «цифровой след». Философская дилемма современности заключается в поиске баланса между потребностью общества в безопасности (что часто ведет к усилению контроля и цифровому надзору) и фундаментальным правом личности на неприкосновенность частной жизни. Утечка персональных данных сегодня — это не просто потеря информации, это вторжение в экзистенциальное пространство личности, угроза ее цифровой идентичности. Каждое действие в сети, от поисковых запросов до геолокации, фиксируется, анализируется и монетизируется транснациональными корпорациями. Человек оказывается в ситуации цифрового паноптикума, где невидимое наблюдение модифицирует его поведение, приводя к самоцензуре и утрате спонтанности.

Особого внимания в контексте защиты данных заслуживает философская концепция «права на забвение». В традиционной культуре забвение было естественным механизмом социальной и психологической адаптации, однако цифровая память перманентна. Информационная безопасность личности сегодня должна подразумевать возможность полного удаления своего цифрового следа и суверенный контроль над тем, какая информация остается доступной в глобальной сети. Невозможность «стереть» устаревшие данные или ошибки прошлого создает беспрецедентное давление на человека, фактически лишая его свободы на личностную трансформацию и переосмысление собственного опыта в цифровой среде.

Во-вторых, информационная безопасность тесно связана с гносеологической (познавательной) безопасностью. В эпоху «постправды», дипфейков и алгоритмических лент новостей возникает угроза искажения картины мира. Алгоритмы социальных сетей, стремясь максимизировать вовлеченность пользователя, помещают его в так называемые «информационные пузыри» и «эхо-камеры». В результате субъект лишается доступа к альтернативным точкам зрения, что ведет к радикализации мнений и социальной поляризации. Истина в цифровой среде утрачивает свою объективность, становясь продуктом консенсуса алгоритмов ранжирования. Манипуляция массовым сознанием через информационные сети ставит под вопрос способность человека к критическому мышлению и автономному принятию решений. Защита от дезинформации становится важнейшим элементом сохранения когнитивной свободы субъекта.

В-третьих, делегирование функций безопасности системам искусственного интеллекта порождает проблему «черного ящика». Когда ИИ определяет уровень доверия к пользователю или выявляет потенциальные угрозы, возникает этическая дилемма: кто несет моральную ответственность за ошибочные алгоритмические решения [2]? Философия техники предупреждает об опасности технологического детерминизма, при котором человек становится заложником собственных защитных систем. Перенос субъектности с человека на машину в вопросах безопасности создает риск

дискриминации на основе скрытых алгоритмических предвзятостей. Обществу необходимо разрабатывать концепцию «объяснимого ИИ», чтобы сохранить человеческий контроль над инфраструктурой безопасности.

Таким образом, технические средства являются лишь базовым уровнем обеспечения информационной безопасности. Подлинная защищенность в XXI веке требует философского осмысления «инфосферы» (по Л. Флориди) [3] и формирования новой цифровой этики. Безопасность должна рассматриваться не как система запретов, а как среда, гарантирующая неприкосновенность личности, достоверность познания и свободу воли в условиях тотальной цифровизации.

Список использованных источников:

1. Кастельс, М. Информационная эпоха: экономика, общество и культура / М. Кастельс ; пер. с англ. под науч. ред. О. И. Шкаратана. – М. : ГУ ВШЭ, 2000. – 608 с.

2. Алексеева, И. Ю. Информационные вызовы национальной и международной безопасности / И. Ю. Алексеева // Вопросы философии. – 2013. – № 5. – С. 49–53.

3. Floridi, L. The Fourth Revolution: How the Infosphere is Reshaping Human Reality / L. Floridi. – Oxford : Oxford University Press, 2014. – 272 p.