УДК 004.89:17

ЭТИЧЕСКИЕ ВОПРОСЫ ИСПОЛЬЗОВАНИЯ АЛГОРИТМОВ ПОВТОРНОЙ ИДЕНТИФИКАЦИИ ЧЕЛОВЕКА НА ИЗОБРАЖЕНИЯХ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ

М. Д. КАРЕЛИНА
(Представлено: канд. техн. наук, доц. С. А. ИГНАТЬЕВА)

В статье рассмотрены технологии распознавания и повторной идентификации человека, основанные на применении алгоритмов искусственного интеллекта. Проанализированы области их практического использования, а также выявлены основные этические риски, связанные с обработкой биометрических данных, нарушением приватности и возможными ошибками идентификации. Целью данной работы является изучение этических аспектов использования технологий повторной идентификации человека в современном цифровом обществе.

Развитие цифровых технологий изменяет привычное представление о том, что такое личное пространство и анонимность. Современные системы видеонаблюдения уже не просто фиксируют происходящее, но и способны анализировать и распознавать людей. Одна из таких технологий называется повторной идентификацией (Re-Identification или ReID). Она позволяет определить, что на разных видеозаписях изображён один и тот же человек, даже если он изменил одежду, находится в другом месте или при других условиях освещения. Иными словами, это технология, которая позволяет «узнавать» человека в потоке других людей, используя алгоритмы искусственного интеллекта.

Такие системы применяются в самых разных сферах: в обеспечении общественной безопасности, в транспорте, в торговых центрах, на предприятиях и даже в образовательных учреждениях. Они помогают находить пропавших людей, предотвращать преступления и повышать уровень защиты на массовых мероприятиях. Тем не менее, наряду с очевидными преимуществами такие технологии поднимают важные этические вопросы – от границ допустимого наблюдения до рисков вмешательства в личную жизнь и возможности их недобросовестного применения.

Главный этический вопрос связан с тем, что человек теряет контроль над своими изображениями. Камеры фиксируют миллионы лиц ежедневно, и большинство людей даже не знает, что их изображения могут храниться, анализироваться и использоваться для сопоставления с другими записями. Это вызывает вопрос: остаётся ли у человека право на анонимность в современном обществе, где за каждым шагом может следить камера?

Конституция Республики Беларусь гарантирует каждому «право на защиту от незаконного вмешательства в его частную жизнь» [1]. Государство обязано создавать условия для защиты персональных данных и безопасности личности. Законодательство классифицирует информацию о частной жизни и персональные данные как сведения ограниченного доступа, сбор и обработка которых допускается только с согласия субъекта или на иных законных основаниях [2, 3]. По официальным данным МВД, к 2025 году в Беларуси уже установлено около 60 тыс. «умных» камер видеонаблюдения, которые способны «отслеживать человека, распознавать лица, читать номерные знаки» [4]. В таких условиях возможность оставаться анонимным в общественных местах фактически утрачена.

Многие исследователи отмечают, что постоянное наблюдение может привести к так называемой самоцензуре [5]. Под этим понимается ситуация, когда человек начинает ограничивать своё поведение – не потому, что нарушает закон, а потому что боится, что его действия будут неправильно поняты или зафиксированы системой наблюдения. Такое состояние снижает ощущение свободы и формирует психологическое давление: даже в безопасной обстановке человек чувствует себя под контролем.

Кроме того, постоянное наблюдение может повлиять на социальную динамику в обществе. Люди начинают вести себя более сдержанно, избегают нестандартных поступков и проявлений индивидуальности. Это может привести к снижению уровня доверия между гражданами, ослаблению общественной активности и даже к самоизоляции. В долгосрочной перспективе такие изменения способны трансформировать общественные нормы и повлиять на демократические процессы.

Ещё одной важной проблемой является отсутствие прозрачности. Люди, даже при наличии уведомления о видеонаблюдении, зачастую не информируются о том, какая информация собирается, с какой целью и как долго она хранится. назначении. В результате возникает недоверие к таким системам и организациям, которые их используют. Без понимания принципов работы технологии у граждан создаётся ощущение несправедливости и вторжения в личную жизнь.

С этической точки зрения большое значение имеет и качество работы самих алгоритмов. Ошибки в системах распознавания могут привести к неправильной идентификации человека. Например, система

может ошибочно распознать человека, который не имеет отношения к событию, зафиксированному камерой. В реальной жизни подобные сбои могут привести к самым разным последствиям – от простых недоразумений до серьёзных ложных обвинений [6]. Кроме того, исследования показывают, что алгоритмы могут работать по-разному с людьми разных внешностей, возраста или пола. Это связано с тем, что модели искусственного интеллекта обучаются на ограниченных наборах данных и иногда отражают предвзятости, присутствующие в обществе. Например, программа может хуже распознавать лица женщин или людей с определённым типом внешности.

Таким образом, технологии повторной идентификации не только технический, но и социально-нравственный феномен. Они затрагивают вопрос доверия между человеком и обществом. Чтобы такие системы использовались во благо, необходимо соблюдать принципы прозрачности, ответственности и уважения к личной свободе.

Первым шагом к этически ответственному использованию технологий распознавания является информирование. Граждане должны знать, где и зачем применяется видеонаблюдение, кто хранит данные и как долго они сохраняются. Простое предупреждение о наличии системы уже создаёт основу доверия и снижает риск недопонимания. Второй важный шаг – это ограничение объёма собираемых данных. Не всегда необходимо сохранять изображение лица; иногда достаточно общих признаков, таких как одежда или силуэт. Соблюдение принципа минимизации данных снижает риски их неправомерного использования.

Третий аспект связан с безопасностью хранения и обработки информации. Биометрические данные должны быть защищены от несанкционированного доступа, утечек и неправильного использования. Это требует строгих технических мер, включая шифрование, контроль доступа и удаление устаревших данных. Также важно, чтобы каждый, кто работает с такими системами, понимал свою ответственность и проходил специальное обучение по правилам обращения с персональными данными.

Наконец, необходимо развивать общественную дискуссию. Технологии не должны внедряться незаметно. Важно обсуждать их преимущества и риски, искать баланс между безопасностью и личной свободой. Общество должно участвовать в принятии решений о том, где и как допустимо использование систем распознавания и наблюдения. Участие граждан в определении допустимых сфер и форм использования подобных систем способствует формированию доверия и справедливому регулированию личных данных.

Этическое будущее цифровых систем зависит от того, насколько осознанно и ответственно они будут применяться. Технологии распознавания человека могут быть полезными инструментами, если они служат интересам общества, а не становятся средством тотального контроля. Необходимо формировать культуру цифровой этики – систему ценностей, в основе которой лежит уважение к личности, её праву на частную жизнь и достоинство. Только в этом случае инновации будут восприниматься как шаг вперёд, а не как угроза свободе.

ЛИТЕРАТУРА

1. Конституция Республики Беларусь: от 15 марта 1994 г. № 2875-XII [Электронный ресурс]. – Режим доступа: https://etalonline.by/document/?regnum=V19402875 – Дата доступа: 26.09.2025.
2. Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» [Электронный ресурс]. – Режим доступа: https://etalonline.by/document/?regnum=H10800455 – Дата доступа: 26.09.2025.
3. Закон Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» [Электронный ресурс]. – Режим доступа: https://etalonline.by/document/?regnum=H12100099 – Дата доступа: 26.09.2025.
4. Умных видеокамер, которые следят за беларусами, за 5 лет стало больше в 600 раз [Электронный ресурс]. – Режим доступа: https://devby.io/news/umnyh-videokamer-stalo-bolshe-v-600-raz - Дата доступа: 27.09.2025.
5. Volosevici D., Isbasoiu G.D. Surveillance as a Socio-Technical System: Behavioral Impacts and Self-Regulation in Monitored Environments [Электронный ресурс]. – Режим доступа: https://www.mdpi.com/2079-8954/13/7/614 – Дата доступа: 28.09.2025.
6. Facial Recognition Leads To False Arrest Of Black Man In Detroit [Электронный ресурс]. – Режим доступа: https://www.npr.org/2020/06/24/882683463/facial-recognition-leads-to-false-arrest-of-black-man-in-detroit – Дата доступа: 28.09.2025.