

Безбородов Данил Павлович,
курсант 223 учебной группы 2 факультета,
филиал Военно-учебного научного центра
Военно-воздушных сил «Военно-воздушной академии»
имени профессора Н. Е. Жуковского и Ю. А. Гагарина в г. Челябинск

Попов Юрий Леонидович,
филиал Военно-учебного научного центра
Военно-воздушных сил «Военно-воздушной академии»
имени профессора Н. Е. Жуковского и Ю. А. Гагарина в г. Челябинск

Иванов Денис Александрович,
филиал Военно-учебного научного центра
Военно-воздушных сил «Военно-воздушной академии»
имени профессора Н. Е. Жуковского и Ю. А. Гагарина в г. Челябинск

ВЛИЯНИЕ НА ЛИЧНОСТЬ ИНТЕРНЕТ ВЕЩЕЙ

Аннотация: Статья посвящена исследованию многогранного влияния интернет вещей (IoT) на формирование и трансформацию современной личности. Рассматриваются как положительные аспекты, такие как повышение эффективности, удобства и персонализации различных аспектов жизни, так и негативные последствия, связанные с проблемами конфиденциальности, зависимости от технологий, усилением контроля и манипуляций. Анализируются механизмы воздействия IoT на поведение, познавательные процессы, социальные связи и самооценку. Особое внимание уделяется этическим вопросам, связанным с алгоритмическим управлением и влиянием автоматизированных систем на принятие решений человеком. В заключение предлагаются рекомендации по осознанному использованию IoT для минимизации рисков и максимизации потенциала для развития личности в цифровом обществе.

Ключевые слова: интернет вещей, алгоритмическое управление, личность, риски, интернет.

Сегодня практически каждый гаджет может работать без прямого физического контакта с человеком. Чайник с дистанционным включением, кофеварка, которая автоматически готовит кофе по утрам, самостоятельное регулирование температуры в комнате кондиционером и многие другие девайсы способны жить своей жизнью. Человек здесь нужен только для настройки или программирования, максимум для подачи команд со смартфона. В остальном же все работает автоматически или по установленным алгоритмам. Такие возможности «умных» устройств относятся к системе интернет вещей, которая нацелена на максимальную автоматизацию выполнения действий без участия человека [1].

Интернет вещей (IoT) – это одна из самых быстрорастущих технологий современности. Умные дома, носимые устройства, промышленные датчики и connected-автомобили уже стали частью нашей повседневной жизни. Однако с увеличением количества подключённых устройств растёт и риск потери данных.

В настоящее время выделяют следующие примеры IoT-устройств:

- Умные дома (термостаты, камеры, лампы);
- Носимые устройства (фитнес-трекеры, умные часы);
- Промышленные датчики (мониторинг оборудования, логистика);
- Connected-автомобили (навигация, диагностика) [1].



Интернет вещей (IoT) имеет в себе как полезные, так и негативные стороны. Рассмотрим каждую из сторон по подробнее:

1. Полезные стороны использования Интернет вещей (IoT):

1. Повышение эффективности и производительности:

- Автоматизация рутинных задач освобождает время и ресурсы для более важных дел.
- Оптимизация процессов в промышленности, сельском хозяйстве, логистике за счет сбора и анализа данных в реальном времени.

2. Удобство и комфорт:

- Умные дома с автоматизированным управлением освещением, отоплением, бытовой техникой.

- Носимые устройства для мониторинга здоровья и физической активности.

3. Повышение безопасности:

- Умные системы видеонаблюдения и сигнализации для защиты домов и предприятий.
- Датчики мониторинга состояния окружающей среды для предупреждения о стихийных бедствиях.

4. Персонализация:

- Адаптация продуктов и услуг к индивидуальным потребностям пользователей.
- Индивидуальные планы тренировок и диеты на основе данных от носимых устройств.

5. Новые возможности для бизнеса:

- Разработка новых продуктов и услуг на основе данных от IoT устройств.
- Улучшение клиентского сервиса за счет проактивного мониторинга оборудования.

6. Улучшение здравоохранения:

- Удаленный мониторинг пациентов с хроническими заболеваниями.
- Быстрая диагностика и реагирование на критические ситуации.

7. Улучшение образования:

- Интерактивные учебные материалы и персонализированные образовательные программы.
- Мониторинг успеваемости студентов и выявление проблем на ранних стадиях.

2. Негативные стороны использования Интернет вещей (IoT):

1. Проблемы конфиденциальности:

- Сбор огромных объемов данных о пользователях, что может быть использовано для слежки и манипуляций.

- Риск утечки персональных данных в результате хакерских атак.

2. Проблемы безопасности:

- Уязвимости IoT устройств для хакерских атак, которые могут привести к краже данных, удаленному управлению устройствами и даже физическому вреду.

- Возможность использования IoT устройств для организации DDoS атак.

3. Зависимость от технологий:

- Чрезмерная зависимость от автоматизированных систем может привести к снижению навыков и способностей человека.

- Проблемы с адаптацией в случае сбоев в работе IoT устройств.

4. Потеря контроля:

- Передача принятия решений автоматизированным системам, что может привести к потере контроля над собственной жизнью.

- Влияние алгоритмов на поведение и выбор человека.

5. Увеличение неравенства:

- Доступ к преимуществам IoT может быть ограничен для людей с низким доходом.
- Риск создания цифрового разрыва между теми, кто может использовать IoT, и теми, кто не может.



6. Этические проблемы:

- Вопросы ответственности за действия автономных систем.
- Дискриминация на основе алгоритмов машинного обучения.

7. Экологические проблемы:

- Производство и утилизация большого количества электронных устройств.
- Потребление энергии IoT устройствами.

8. Экономические проблемы:

- Высокие затраты на внедрение и обслуживание IoT систем.
- Риск потери рабочих мест из-за автоматизации.

Важно помнить, что преимущества и недостатки IoT тесно связаны друг с другом [3].

Интернет вещей (IoT) выходит за рамки простого сбора и передачи данных, он все чаще становится платформой для алгоритмического управления, где автоматизированные системы влияют на принятие решений человеком.

Выделяют следующие механизмы влияния на личность со стороны интернет вещей (IoT):

1. Навязчивые подсказки и рекомендации: IoT устройства, анализируя наши данные и поведение, предлагают персонализированные рекомендации, касающиеся всего: от выбора продуктов и развлечений до режима сна и физических упражнений.

2. Автоматизация принятия решений: Умные дома автоматически регулируют температуру, освещение и даже заказывают продукты, опираясь на заданные параметры и машинное обучение. Аналогично, подключенные автомобили предлагают маршруты и даже берут на себя управление в критических ситуациях..

3. "Темные шаблоны" и манипулятивные интерфейсы: Некоторые IoT устройства и приложения могут использовать "темные шаблоны" в дизайне интерфейса, подталкивая пользователей к определенным действиям, например, к покупкам или подпискам.

4. Алгоритмическая предвзятость: Алгоритмы машинного обучения, лежащие в основе многих IoT систем, могут быть предвзятыми, отражая предрассудки, присутствующие в данных, на которых они обучались.

5. Усиление эхо-камер и фильтрация информации: Алгоритмы персонализации могут создавать "эхо-камеры", окружая нас информацией, которая подтверждает наши существующие убеждения, и фильтруя альтернативные точки зрения.

Выделяют следующие последствия воздействующие на личность со стороны интернет вещей (IoT):

1. Снижение автономии и самоопределения: Постоянное влияние алгоритмов на наши решения может подрывать чувство контроля над собственной жизнью и приводить к снижению самооценки.

2. Утрата навыков принятия решений: Делегирование все большего числа решений автоматизированным системам может привести к утрате навыков критического мышления, анализа информации и самостоятельного принятия решений.

3. Формирование алгоритмической идентичности: Наши цифровые следы, собираемые IoT устройствами, формируют нашу "алгоритмическую идентичность", которая может влиять на то, как нас воспринимают другие люди и как мы воспринимаем самих себя.

4. Усиление манипуляций и контроля: Возможность использования IoT для манипулирования поведением человека, например, через таргетированную рекламу или социальный инжиниринг, представляет серьезную угрозу для свободы и демократии.

Выделяют следующие вызовы и перспективы, для того, чтобы смягчить негативные последствия алгоритмического управления и усилить позитивные, необходимо:

5. Разработать этические принципы для разработки и использования IoT систем:



Необходимо установить четкие границы и ограничения на сбор и использование персональных данных, а также обеспечить прозрачность и подотчетность алгоритмов.

6. Повышать цифровую грамотность населения: Людям необходимо понимать, как работают алгоритмы, как они влияют на их решения и как защитить свою конфиденциальность.

7. Создавать механизмы контроля и регулирования: Необходимо разрабатывать законодательство и нормативные акты, которые бы регулировали использование IoT, обеспечивали защиту прав потребителей и предотвращали злоупотребления.

8. Развивать "гуманно-ориентированный" дизайн IoT систем: Необходимо создавать IoT устройства и приложения, которые ставят в центр внимания потребности и интересы человека, а не только эффективность и автоматизацию [4].

Преимущества, которые IoT предлагает для личностного роста и развития.

1. Повышение цифровой грамотности и критического мышления:

- Изучайте принципы работы IoT: Разберитесь, как IoT устройства собирают и используют ваши данные, какие алгоритмы лежат в их основе. Ищите достоверную информацию из разных источников.

- Развивайте критическое мышление: Не принимайте на веру все рекомендации и предложения, поступающие от IoT устройств. Анализируйте информацию, учитывайте контекст и собственные предпочтения.

2. Активное управление конфиденциальностью:

- Внимательно читайте политику конфиденциальности: Перед использованием IoT устройства или приложения тщательно изучите, какие данные собираются, как они используются и с кем ими делятся.

- Настраивайте параметры конфиденциальности: Максимально ограничивайте сбор данных, отключайте функции, которые вам не нужны, и контролируйте доступ приложений к вашим личным данным.

3. Обеспечение безопасности IoT устройств:

- Регулярно обновляйте программное обеспечение: Устанавливайте последние обновления безопасности, чтобы устранить уязвимости.

- Изменяйте пароли по умолчанию: Сразу после установки IoT устройства измените пароль по умолчанию на сложный и уникальный.

4. Осознанное использование автоматизации:

- Не полагайтесь полностью на автоматизацию: Сохраняйте контроль над важными решениями и не позволяйте алгоритмам принимать их за вас.

- Регулярно проверяйте результаты работы автоматизированных систем: Убедитесь, что они работают корректно и не приводят к нежелательным последствиям.

5. Поддержание баланса между виртуальным и реальным миром:

- Устанавливайте лимиты на использование IoT устройств: Ограничивайте время, проводимое с технологиями, чтобы избежать зависимости и сохранить баланс с реальной жизнью.

- Уделяйте время общению с людьми в реальном мире: Поддерживайте живые социальные связи и не позволяйте технологиям заменить реальное общение.

6. Развитие навыков саморегуляции и самоконтроля:

- Определяйте свои цели и приоритеты: Сознательно выбирайте, как использовать IoT устройства для достижения своих целей и реализации своих ценностей.

- Развивайте навыки самоконтроля: Учитесь противостоять соблазнам, связанным с использованием IoT, и не позволяйте технологиям управлять вашим поведением.

7. Активное участие в формировании цифрового будущего:



- Поддерживайте инициативы, направленные на защиту конфиденциальности и безопасности в цифровом мире.
- Выражайте свою точку зрения по вопросам регулирования IoT и использования данных.

Следуя этим рекомендациям, вы сможете минимизировать риски, связанные с использованием IoT, и максимально использовать его потенциал для личного роста, развития и улучшения качества жизни в цифровом обществе. Осознанное использование технологий – это ключ к созданию более гуманного и справедливого цифрового будущего [4].

Интернет вещей открывает огромные возможности для автоматизации и улучшения качества жизни, но также создаёт новые вызовы в области безопасности данных. Только совместные усилия производителей, регуляторов и пользователей помогут создать безопасную экосистему Интернета вещей. Эксперты прогнозируют, что в ближайшее десятилетие всё больше устройств будут выполнять рутинные задачи и взаимодействовать между собой не только в рамках «умного дома» или интернета, а в рамках районов и целых городов [2].

Список литературы:

1. Что такое интернет вещей и как он влияет на жизнь потребителей // SUPA. Электронный источник. -URL: <https://supa.ru/blog/posts/chto-takoe-intiernet-vieshchiei-i-kak-on-vliiaiet-na-zhizn-potriebitieliei?ysclid=m8bra9jis337014401> (05.03.2025)
2. Людмила Клейменова. Что такое интернет вещей и как он устроен // РБК Тренды. Электронный источник. -URL: <https://trends.rbc.ru/trends/industry/5db96f769a7947561444f118> (12.03.2025)
3. Вебер, Р. Х., & Weber, R. (2010). Интернет вещей: новые вызовы безопасности и конфиденциальности. Обзор компьютерного законодательства и безопасности, × 26 × (1), 23-30.
4. Уитакер Р. и Дитворст Б. Дж. (2021). Неприятие алгоритмов и моральное лицензирование: почему мы недооцениваем алгоритмы и переоцениваем человеческие советы. Журнал экспериментальной психологии: Общие, × 150 × (2), 245.

