НАУЧНО-ТЕОРЕТИЧЕСКИЙ ЖУРНАЛ «ВОПРОСЫ НАУКИ И ОБРАЗОВАНИЯ» № 15 (200) 2025

ИЗДАТЕЛЬСТВО НАУЧНЫЕ ПУБЛИКАЦИИ
КОНФЕРЕНЦИИ • ЖУРНАЛЫ • МОНОГРАФИИ
2015

ВОПРОСЫ НАУКИ И ОБРАЗОВАНИЯ

ELECTRONIC JOURNAL • ДЕКАБРЬ 2025 № 15 (200)

SCIENTIFIC-PRACTICAL JOURNAL
НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ
САЙТ ЖУРНАЛА: HTTPS:/SCIENTIFICPUBLICATION.RU
ИЗДАТЕЛЬСТВО: HTTPS://SCIENTIFICPUBLICATIONS.RU
Реестровая запись ЭЛ № ФС 77–65699

Google scholar

НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА
eLIBRARY.RU

ISSN 2542-081X
9 772542 081007

ISSN 2542-081X (Online)

Вопросы науки и образования

№ 15 (200), 2025

Москва
2025

ISSN 2542-081X (Online)

Вопросы науки и образования

№ 15 (200), 2025

НАУЧНО-ТЕОРЕТИЧЕСКИЙ ЖУРНАЛ
HTTPS://SCIENTIFICPUBLICATION.RU
EMAIL: TEL9203579334@YANDEX.RU

Издается с 2016 года.
Журнал зарегистрирован Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)
Реестровая запись ПИ № ФС77 – 65699

ISSN 2542-081X

Содержание

СОЗДАНИЕ ВИРТУАЛЬНЫХ КОПИЙ ФИЗИЧЕСКИХ ОБЪЕКТОВ ДЛЯ МОНИТОРИНГА ИХ СОСТОЯНИЯ И ТЕСТИРОВАНИЯ СЦЕНАРИЕВ РАБОТЫ В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ

Амандурдыев И.[1], Аманмырадова О.А.[2], Аннамырадов Х.Б.[3]

[1]Амандурдыев Исмайыл – преподаватель;
[2]Аманмырадова Огулджан Аманмырадовна – студент
[3]Аннамырадов Хангулы Батырович – студент;
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *данное исследование рассматривает концептуальные и практические аспекты создания виртуальных копий физических объектов, известных как цифровые двойники, для непрерывного мониторинга их технического состояния и имитационного моделирования рабочих сценариев. В работе анализируются механизмы синхронизации данных между реальным оборудованием и его цифровым эквивалентом в режиме реального времени с использованием технологий промышленного интернета вещей (IIoT) и предиктивной аналитики. Особое внимание уделяется возможностям тестирования гипотетических ситуаций и аварийных сценариев в безопасной виртуальной среде, что позволяет предотвращать критические сбои и оптимизировать производительность без остановки производственных процессов. Автор исследует методы обработки больших массивов сенсорных данных и алгоритмы машинного обучения, обеспечивающие высокую точность прогнозирования остаточного ресурса оборудования. В заключении обосновывается эффективность применения цифровых реплик для повышения операционной гибкости и снижения затрат на техническое обслуживание сложных инженерных систем.*

Ключевые слова: *цифровой двойник, виртуальная копия, мониторинг состояния, режим реального времени, имитационное моделирование, предиктивная аналитика, интернет вещей, техническое обслуживание, промышленная автоматизация, диагностика.*

Создание виртуальных копий физических объектов, или цифровых двойников, представляет собой передовую технологию синхронизации материального мира с цифровым пространством. В отличие от традиционного компьютерного моделирования, такая копия является динамической системой, которая живет и развивается вместе со своим физическим прототипом. Использование потоковых данных позволяет виртуальной модели с высокой точностью отражать текущие параметры работы оборудования, такие как температура, давление или частота вибраций. Это создает прозрачную среду для оперативного контроля, где каждое изменение в реальном мире мгновенно фиксируется программным обеспечением. Цифровой двойник становится надежным инструментом визуализации скрытых процессов, происходящих внутри сложных механизмов.

Технологической основой для функционирования виртуальных реплик является промышленный интернет вещей (IIoT), объединяющий тысячи интеллектуальных сенсоров в единую сеть. Эти датчики непрерывно собирают информацию о состоянии объекта и передают её через защищенные каналы связи в аналитическую платформу. Высокая скорость передачи данных обеспечивает работу системы в режиме реального времени, что критически важно для предотвращения аварийных ситуаций. Программные алгоритмы обрабатывают входящий трафик, очищают его от шумов и преобразуют в понятные инженеру показатели эффективности. Таким образом, физический объект получает «цифровой голос», позволяющий системе управления понимать его текущие потребности.

Важнейшим преимуществом использования цифровых копий является возможность проведения испытаний и тестирования сценариев в безопасной виртуальной среде.

Инженеры могут моделировать воздействие экстремальных нагрузок или имитировать отказы отдельных узлов, не рискуя целостностью реального дорогостоящего оборудования. Это позволяет заранее отработать алгоритмы реагирования на нештатные ситуации и обучить персонал действиям в кризисных условиях. Результаты таких симуляций используются для оптимизации регламентов эксплуатации и повышения общей живучести системы. Виртуальный полигон становится незаменимым инструментом для отработки стратегий «что, если», значительно сокращая время принятия управленческих решений.

Мониторинг состояния в режиме реального времени на базе цифровых двойников позволяет перейти от планового технического обслуживания к ремонту по фактическому состоянию. Система анализирует износ компонентов и выявляет малейшие отклонения в работе, которые могут свидетельствовать о зарождающемся дефекте. Предиктивная аналитика использует исторические данные и методы машинного обучения для точного прогнозирования момента выхода оборудования из строя. Это дает возможность заранее заказать необходимые запчасти и запланировать ремонтные работы на время технологических перерывов. В результате существенно снижаются затраты на содержание техники и минимизируются убытки от внеплановых простоев.

Внедрение цифровых реплик в энергетическом секторе позволяет оптимизировать работу турбин, генераторов и распределительных сетей. Виртуальная копия электростанции учитывает не только внутренние параметры агрегатов, но и внешние факторы, такие как погодные условия и колебания спроса на энергию. Моделирование различных режимов генерации помогает находить точки максимального КПД, снижая удельный расход топлива и объем вредных выбросов. Диспетчеры могут видеть цифровую проекцию всей сети, что облегчает балансировку мощностей и предотвращает перегрузки. Интеллектуальный

контроль энергетической инфраструктуры становится залогом стабильности и безопасности современного мегаполиса.

В аэрокосмической отрасли цифровой двойник сопровождает каждое воздушное судно от этапа сборки до вывода из эксплуатации. Виртуальная модель накапливает информацию о каждом совершенном полете, воздействии турбулентности и циклах взлета-посадки для конкретного экземпляра планера и двигателя. Это позволяет проводить индивидуальную оценку ресурса самолета, учитывая специфику его использования в различных климатических зонах. Данные с цифровых двойников передаются разработчикам для внесения корректировок в конструкцию новых моделей техники. Высокая детализация виртуальной реплики гарантирует, что ни одно повреждение не останется незамеченным службами наземного контроля.

Проектирование и эксплуатация морских судов также выигрывают от использования технологий виртуальных копий. Цифровой двойник корабля помогает оптимизировать прокладку маршрутов, учитывая гидродинамические характеристики корпуса и погодные условия в океане. Мониторинг работы судовой энергетической установки в реальном времени позволяет экипажу своевременно реагировать на изменения в работе механизмов. В случае серьезной поломки в открытом море береговые службы могут использовать виртуальную модель для дистанционной консультации и поиска способа устранения неисправности. Цифровизация флота повышает безопасность мореплавания и снижает нагрузку на окружающую среду за счет экономии топлива.

Сложность реализации цифровых двойников требует использования передовых облачных вычислений и технологий обработки больших данных. Для создания точной копии необходимо объединить конструкторскую документацию, результаты математического моделирования и потоки данных с сенсоров в единый информационный поток. Искусственный интеллект играет ключевую роль в

интерпретации этих данных, выявляя сложные зависимости между различными параметрами системы. Использование технологий дополненной реальности (AR) позволяет техническим специалистам видеть виртуальные подсказки поверх реального оборудования во время ремонта. Синергия различных ИТ-технологий превращает цифровой двойник в полноценную интеллектуальную экосистему.

Заключение

В заключении следует подчеркнуть, что создание виртуальных копий физических объектов является ключевым элементом Индустрии 4.0 и цифровой экономики. В будущем ожидается появление глобальных сетей цифровых двойников, которые будут взаимодействовать между собой для оптимизации целых отраслей промышленности. Развитие технологий искусственного интеллекта сделает виртуальные модели более автономными и способными к самостоятельному принятию решений по оптимизации процессов. Защита данных и обеспечение кибербезопасности цифровых реплик станут важнейшими задачами для разработчиков программного обеспечения. Цифровой двойник — это мост в будущее.

Список литературы

1. *Алексеев В.В.* Технологии построения цифровых двойников сложных технических систем. М.: Наука, 2024.
2. *Борисов А.М., Григорьев С.П.* Мониторинг и диагностика оборудования в концепции Индустрии 4.0. СПб.: Политехника, 2023.
3. *Волков Д.И.* Виртуальное тестирование и отработка сценариев работы промышленного оборудования // Датчики и системы. 2024. № 3. С. 15–28.
4. *Семенов К.А.* Информационные модели реального времени в задачах автоматизации. Екатеринбург: УрФУ, 2022.
5. *Tao F., Zhang M., Nee A.Y.C.* Digital Twin Driven Smart Manufacturing. London: Academic Press, 2019.

АВТОМАТИЗАЦИЯ СИСТЕМ КИБЕРФИЗИЧЕСКОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ ТЕХНОЛОГИИ БЛОКЧЕЙН

Аннамырадова Ш.[1], Бахтияров З.[2], Башимов Б.М.[3]

[1]Аннамырадова Шемшат – преподаватель,
[2]Бахтияров Зафарбек – студент,
[3]Башимов Башим Мейлисович – студент,
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *данное исследование направлено на изучение методов интеграции технологии блокчейн в системы обеспечения безопасности киберфизических объектов для предотвращения несанкционированного доступа и фальсификации данных. В работе рассматриваются архитектурные решения, позволяющие использовать децентрализованный реестр для хранения контрольных сумм программного обеспечения, журналов событий и конфигураций промышленных контроллеров. Особое внимание уделяется разработке самовыполняющихся алгоритмов (смарт-контрактов), которые автоматически блокируют скомпрометированные узлы сети при обнаружении аномальной активности или нарушении целостности данных. Автор исследует влияние распределенной структуры на устойчивость системы к атакам типа «отказ в обслуживании» и возможности обеспечения прослеживаемости всех управляющих команд в сложных иерархических сетях. В заключении формулируются принципы построения доверенной среды взаимодействия между автономными устройствами, способствующие повышению общей живучести критически важной инфраструктуры.*

Ключевые слова: *киберфизическая безопасность, блокчейн, децентрализованное управление, смарт-контракты, целостность данных, промышленный интернет вещей, киберустойчивость, распределенный реестр,*

аутентификация устройств, информационная безопасность.

Автоматизация систем киберфизической безопасности на основе технологии распределенного реестра представляет собой новый подход к защите промышленных и муниципальных объектов. В отличие от традиционных централизованных систем, где взлом главного сервера дает злоумышленнику контроль над всей сетью, блокчейн распределяет информацию о безопасности между всеми участниками. Это создает среду, в которой каждое устройство проверяет подлинность действий своих «соседей», исключая возможность незаметного внесения вредоносных изменений в логику работы контроллеров. Такая архитектура превращает пассивную защиту в активную систему коллективной безопасности, способную сохранять работоспособность даже при компрометации отдельных узлов.

Основным инструментом автоматизации безопасности выступают смарт-контракты — программные коды, которые записываются в блокчейн и выполняются автоматически при наступлении определенных условий. В киберфизических системах они могут использоваться для проверки прав доступа к критическим функциям оборудования или для автоматической изоляции сегментов сети при обнаружении аномального трафика. Например, если датчик начинает передавать данные, выходящие за рамки физически возможных значений, смарт-контракт может мгновенно заблокировать выполнение команд от этого источника и уведомить оператора. Это исключает задержки, связанные с человеческим фактором, и позволяет локализовать угрозу в течение долей секунды.

Использование технологии блокчейн гарантирует неизменность журналов событий и записей о состоянии системы, что критически важно для расследования инцидентов. Любая команда, отправленная на исполнительный механизм, фиксируется в распределенном реестре с цифровой подписью отправителя и временной

меткой. Попытка удалить или изменить запись о несанкционированном действии станет очевидной для всей сети, так как копия реестра хранится на множестве независимых узлов. Это создает высокий уровень ответственности и прозрачности в управлении сложными объектами, позволяя точно восстановить хронологию событий в случае аварии или попытки диверсии.

Децентрализованная аутентификация устройств позволяет решить проблему подмены оборудования (атаки типа «человек посередине») в распределенных сетях автоматизации. Каждое устройство при подключении к сети получает уникальный цифровой идентификатор, записанный в блокчейн. Перед выполнением любой критической операции узлы проводят взаимную проверку подлинности, используя криптографические ключи. Поскольку реестр идентификаторов распределен, у атакующего нет единой точки входа для массовой подмены адресов устройств. Это обеспечивает надежную защиту каналов связи между полевыми датчиками, шлюзами и облачными платформами управления.

Концепция блокчейна также позволяет автоматизировать управление обновлениями программного обеспечения (прошивок) для тысяч распределенных устройств. Контрольные суммы (хеши) эталонных версий программ записываются в блокчейн, и каждое устройство перед установкой обновления сверяет полученный файл с записью в реестре. Это предотвращает загрузку вредоносного кода через скомпрометированные серверы обновлений. Автоматическая проверка целостности на уровне железа гарантирует, что в системе выполняется только проверенное и авторизованное программное обеспечение, что является фундаментом киберфизической безопасности.

Устойчивость к атакам, направленным на отказ в обслуживании, повышается за счет отсутствия единого центра управления, который можно было бы перегрузить трафиком. В распределенной сети блокчейн запросы могут обрабатываться множеством узлов, что делает систему

управления более живучей. Даже если значительная часть сети выйдет из строя в результате кибератаки, оставшиеся узлы смогут поддерживать базовые функции безопасности и координировать действия по восстановлению. Это особенно важно для систем жизнеобеспечения «умных городов» и объектов энергетики, где непрерывность управления является жизненно необходимой.

Внедрение блокчейна в системы автоматизации требует решения проблемы масштабируемости и ограниченных вычислительных ресурсов полевых устройств. Традиционные алгоритмы консенсуса, используемые в публичных сетях, требуют больших мощностей и создают значительные задержки, что недопустимо для реального времени. Поэтому в промышленной автоматизации применяются частные блокчейны с облегченными алгоритмами подтверждения транзакций. Это позволяет достичь необходимой скорости обработки данных при сохранении всех преимуществ децентрализованной безопасности, обеспечивая время отклика в пределах миллисекунд.

Экономическая эффективность автоматизации безопасности на основе блокчейна складывается из минимизации ущерба от киберпреступлений и снижения затрат на аудит. Автоматическая проверка подлинности и целостности данных избавляет от необходимости содержания огромного штата специалистов по информационной безопасности для ручного мониторинга систем. Прозрачность и прослеживаемость всех процессов упрощают получение страховых выплат и прохождение сертификации на соответствие международным стандартам безопасности. Инвестиции в современную криптографическую защиту окупаются за счет стабильной работы предприятия и защиты интеллектуальной собственности.

Интеграция блокчейна с искусственным интеллектом открывает возможности для создания систем «самозалечивающейся» безопасности. Нейронные сети могут анализировать поток транзакций в блокчейне для выявления

скрытых паттернов атак, а смарт-контракты — реализовывать контрмеры на основе этих выводов. Такое сочетание технологий позволяет системе не только защищаться от известных угроз, но и адаптироваться к новым видам кибератак в автономном режиме. Будущее киберфизической безопасности связано с созданием глобальных доверенных сетей, где информация об угрозах распространяется между предприятиями мгновенно и анонимно.

Заключение

В заключении следует подчеркнуть, что блокчейн является не просто технологией хранения данных, а новым каркасом для построения доверия в цифровом мире. Автоматизация безопасности на его основе позволяет исключить человеческий фактор и создать системы, защищенные на уровне самой архитектуры. По мере развития стандартов промышленного интернета вещей, использование распределенных реестров станет обязательным требованием для критически важных объектов. Переход к децентрализованной защите обеспечит новый уровень надежности киберфизических систем, делая их устойчивыми к вызовам цифровой эпохи и гарантируя безопасность общества в будущем.

Список литературы

1. *Беляев А.И.* Проектирование безопасных робототехнических систем: учебное пособие. Москва: Издательство МГТУ им. Н.Э. Баумана, 2024.
2. *Григорьев С.Н., Волков М.П.* Сенсорные системы в коллаборативной робототехнике. Санкт-Петербург: Политех-Пресс, 2023.
3. *Егоров В.В.* Методы ограничения усилий коботов при физическом взаимодействии с персоналом // Робототехника и техническая кибернетика. 2024. № 1. С. 32–45.
4. *Левин Д.А.* Автоматизация сборочных процессов на базе коботов. Екатеринбург: УрФУ, 2022.

5. *Haddadin S., Croft E.* Physical Human-Robot Interaction // Springer Handbook of Robotics. 2016. P. 1835–1874.

ЭВОЛЮЦИЯ И АРХИТЕКТУРА КВАНТОВЫХ КОМПЬЮТЕРОВ

Атаев Ы.[1], Мухиев С.[2], Годыков П.[3]

[1]Атаев Ыхлас – преподаватель,
[2]Мухиев Селим – преподаватель,
[3]Годыков Перман – преподаватель,
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *квантовые компьютеры представляют собой следующую ступень в эволюции вычислительных систем, использующих принципы квантовой механики для решения задач, недоступных классическим компьютерам. Ключевым элементом квантовой архитектуры является кубит (квантовый бит), который, в отличие от классического бита, может существовать в суперпозиции состояний 0 и 1 одновременно. Эволюция этой технологии началась с теоретических работ 1980-х годов, а сегодня сосредоточена на создании физических кубитов на основе различных технологий, включая сверхпроводящие цепи, захваченные ионы и фотонные системы. Архитектура квантовых компьютеров включает массив кубитов, систему управления ими (контроллеры) и средства для считывания состояний, требуя крайне низких температур и идеальной изоляции для поддержания когерентности.*

Ключевые слова: *квантовые компьютеры, квантовая механика, кубит, суперпозиция, когерентность, сверхпроводящие кубиты, захваченные ионы, квантовая архитектура.*

Эволюция квантовых компьютеров представляет собой один из самых значительных технологических скачков со

времен изобретения транзистора. Эти системы обещают радикально изменить подходы к криптографии, разработке материалов, фармакологии и искусственному интеллекту, используя фундаментальные законы квантовой механики.

История квантовых вычислений берет начало в 1980-х годах, когда физики, такие как Пол Бениофф и Ричард Фейнман, предложили идею создания машин, которые могли бы использовать квантовые эффекты для моделирования природных систем. Фейнман утверждал, что моделировать квантовые системы на классических компьютерах неэффективно.

Ключевым концептуальным прорывом стало изобретение кубита (квантового бита). В отличие от классического бита, который может принимать только одно из двух состояний (0 или 1), кубит может находиться в суперпозиции обоих состояний одновременно. Это свойство является основой экспоненциального роста вычислительной мощности.

Другой критически важный квантовый феномен, используемый в архитектуре, — это квантовая запутанность. Когда два или более кубита запутываются, их состояния становятся взаимозависимыми, независимо от физического расстояния между ними. Это позволяет выполнять параллельные вычисления.

Теоретические основы были подкреплены алгоритмическими открытиями: алгоритм Шора (для факторизации больших чисел, угрожающий современной криптографии RSA) и алгоритм Гровера (для ускоренного поиска в неструктурированных базах данных). Эти алгоритмы продемонстрировали потенциал квантовых систем.

Современная эволюция квантовых компьютеров сосредоточена на создании физических, устойчивых кубитов. Не существует единой доминирующей технологии; исследования ведутся по нескольким параллельным направлениям, каждое со своими преимуществами и недостатками.

Один из наиболее развитых подходов — сверхпроводящие кубиты, используемые IBM и Google. Эти кубиты создаются на основе микроволновых резонаторов и требуют экстремально низких температур (милликельвины), близких к абсолютному нулю, для поддержания когерентности.

Архитектура сверхпроводящих систем включает плоские чипы с кубитами, размещенными в специальном криостате — рефрижераторе растворения. Управление и считывание кубитов осуществляется с помощью сложной системы микроволновых импульсов и коаксиальных кабелей.

Другой ведущий подход — захваченные ионы. В этой архитектуре кубиты представлены отдельными атомами (ионами), которые удерживаются в вакууме с помощью электромагнитных полей. Ионы возбуждаются и считываются с помощью лазеров.

Системы захваченных ионов, такие как IonQ, демонстрируют более высокую когерентность (дольшее время сохранения квантового состояния) и высокую связность (возможность взаимодействовать практически с любым другим кубитом в массиве), что упрощает выполнение сложных квантовых алгоритмов.

Фотонные квантовые компьютеры используют фотоны (частицы света) в качестве кубитов. Вычисления выполняются с помощью оптических элементов, таких как светоделители и интерферометры. Преимущество этого подхода — возможность работы при комнатной температуре.

Кубиты на основе кремниевых спинов представляют собой попытку интегрировать квантовые технологии в существующую полупроводниковую промышленность. Они используют спин отдельных электронов в кремнии. Хотя эта технология находится на более ранней стадии, она обладает потенциалом для массового масштабирования.

Ключевым архитектурным вызовом для всех типов кубитов является декогеренция — потеря кубитом своего квантового состояния из-за взаимодействия с окружающей средой. Это ограничивает время, в течение которого могут выполняться полезные вычисления.

Для борьбы с декогеренцией разрабатываются системы коррекции квантовых ошибок. Эти системы требуют использования большого количества физических кубитов для кодирования одного надежного, "логического" кубита. Это усложняет архитектуру и требует большего масштаба.

Архитектура современных квантовых компьютеров является многоуровневой. Она включает физический уровень (кубиты), уровень управления (контроллеры, электроника, криогеника) и программный уровень (языки программирования, такие как Qiskit или Cirq, и алгоритмы).

На программном уровне происходит эволюция от моделей NISQ (Noisy Intermediate-Scale Quantum) — шумных компьютеров среднего масштаба с ограниченным количеством кубитов — к моделям с исправлением ошибок. NISQ-компьютеры, как правило, используются для приближенных расчетов.

Важным направлением является создание квантовых сетей и квантового Интернета. Это позволит связывать несколько квантовых процессоров для увеличения их общей вычислительной мощности и обмена квантовой информацией (квантовая связь).

Эволюция идет по пути увеличения количества кубитов (масштабирование) и повышения качества кубитов (улучшение когерентности и снижение частоты ошибок). Оба параметра критически важны для достижения квантового превосходства (способности решать задачи, недоступные классике).

Влияние квантовых компьютеров на бизнес-трансформацию огромно. Они могут оптимизировать логистику (задача коммивояжера), ускорять открытие новых лекарств (моделирование молекул) и создавать новые, более эффективные финансовые модели.

Заключение

Таким образом, эволюция квантовых компьютеров — это сложный, многогранный процесс, в котором сочетаются физические инновации, архитектурное проектирование и

разработка новых алгоритмов, направленный на создание вычислительной парадигмы будущего.

Список литературы

1. *Nielsen M.A., & Chuang I.L.* (2010). Quantum Computation and Quantum Information. 10th Anniversary Edition. Cambridge University Press.
2. *Ladd T.D., Jelezko F., Laflamme R., Nakamura Y., Monroe C., & O'Brien J.L.* (2010). Quantum Computing. Nature, 464(7289), 45–53.
3. *Devitt S.J., Munro W.J., & Nemoto K.* (2013). Quantum Error Correction for Beginners. Reports on Progress in Physics, 76(7), 076001.
4. *Krantz P., Kjaergaard M., Yan F., Orlando T.P., Gustavsson S., & Oliver W.D.* (2019). A Quantum Engineer’s Guide to Superconducting Qubits. Applied Physics Reviews, 6(2), 021318.
5. *Monroe C., & Kim J.* (2013). Scaling the Ion Trap Quantum Processor. Science, 339(6119), 560–563.
6. *Смирнов С.А., Иванов Д.В.* Интеграция данных компьютерного зрения и лидаров для беспилотного транспорта // Журнал технической кибернетики. 2024. № 2. С. 45–58.
7. *Thrun S., Burgard W., Fox D.* Probabilistic Robotics. Cambridge: MIT Press, 2005.
8. *Хорошев А.М.* Методы семантической сегментации в задачах городской навигации // Вестник робототехники. 2023. Т. 12. № 4. С. 112–125.
9. *Дубровин И.А.* Алгоритмы навигации мобильных роботов в динамических средах. Москва: Наука, 2023.
10. *Карпов В.Э.* Основы адаптивного управления робототехническими комплексами. Санкт-Петербург: БХВ-Петербург, 2022.

ПРИМЕНЕНИЕ ДЕЦЕНТРАЛИЗОВАННЫХ РЕЕСТРОВ ДЛЯ ОБЕСПЕЧЕНИЯ НЕИЗМЕННОСТИ ЛОГОВ СОБЫТИЙ В ПРОМЫШЛЕННЫХ СЕТЯХ

Атаева Б.[1], Бадышев Э.П.[2], Байлыев Б.Я.[3]

[1]Атаева Багул – преподаватель;
[2]Бадышев Эмир Перхадович – студент;
[3]Байлыев Батыр Ялкапович – студент;
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *данное исследование посвящено анализу методов использования технологий децентрализованных реестров для решения задачи обеспечения достоверности и неизменности журналов регистрации событий в современных промышленных сетях. В работе рассматриваются недостатки традиционных централизованных систем логирования, такие как уязвимость к преднамеренному удалению или модификации записей администраторами с избыточными правами или внешними злоумышленниками. Особое внимание уделяется механизмам криптографического связывания записей и распределенного хранения хеш-сумм логов на множестве узлов сети, что исключает возможность незаметного внесения правок в историю работы оборудования. Автор исследует влияние интеграции блокчейн-платформ на производительность промышленных протоколов передачи данных и предлагает подходы к оптимизации структуры реестра для работы в условиях ограниченных вычислительных ресурсов полевых устройств. В заключении обосновывается роль неизменных логов как фундаментальной основы для проведения точных технических расследований инцидентов и обеспечения юридически значимого аудита деятельности цифровых предприятий.*

Ключевые слова: *децентрализованные реестры, блокчейн, журналы событий, промышленная безопасность,*

целостность данных, киберфизические системы, аудит безопасности, промышленный интернет вещей, криптография, сетевой мониторинг.

Применение децентрализованных реестров в промышленных сетях обусловлено необходимостью создания абсолютно доверенной среды для регистрации всех технологических событий. В классических системах автоматизации данные о действиях операторов или сбоях оборудования записываются в базу данных, которая находится под управлением центрального сервера. Это создает единую точку отказа и теоретическую возможность для манипуляции данными, если злоумышленник получит права суперпользователя. Децентрализованный реестр лишен этого недостатка, так как информация о каждом событии дублируется и проверяется всеми участниками сети, что делает подделку записей физически невозможной.

Технология блокчейн обеспечивает неизменность логов за счет использования криптографического связывания блоков данных. Каждая новая запись в журнале содержит в себе зашифрованный отпечаток (хеш) предыдущей записи, формируя непрерывную цепочку. Если кто-то попытается изменить старую запись, это приведет к несоответствию всех последующих отпечатков, и система мгновенно зафиксирует нарушение целостности. В промышленных условиях это позволяет гарантировать, что информация о параметрах давления, температуры или об аварийных сигналах не была подкорректирована для скрытия ошибок эксплуатации или неисправностей оборудования.

Распределенное хранение журналов событий на нескольких независимых узлах промышленной сети значительно повышает живучесть системы безопасности. Даже в случае физического уничтожения или кибератаки на один из серверов, полная и достоверная копия журнала сохраняется на других устройствах. Это особенно важно для критически важных объектов, таких как электростанции или химические комбинаты, где информация о последних

минутах работы перед аварией является бесценной для установления причин происшествия. Синхронизация данных между узлами происходит автоматически, обеспечивая постоянную актуальность распределенного архива без участия человека.

Интеграция децентрализованных реестров в промышленные сети требует адаптации под требования реального времени. Стандартные процедуры подтверждения транзакций, используемые в глобальных сетях, могут вносить недопустимые задержки. В специализированных индустриальных блокчейнах применяются алгоритмы облегченного консенсуса, которые позволяют фиксировать события в реестре в течение миллисекунд. Это дает возможность использовать блокчейн не только для долгосрочного архивирования, но и для оперативного контроля за выполнением управляющих команд непосредственно в процессе производства, гарантируя, что каждая команда была получена и выполнена именно тем устройством, которому она предназначалась.

Использование смарт-контрактов позволяет автоматизировать процесс аудита журналов событий и реагирования на выявленные нарушения. Программный код, встроенный в реестр, может непрерывно анализировать входящие логи на предмет подозрительных закономерностей или несанкционированных действий. Например, если в журнале зафиксирована попытка изменения настроек контроллера в неурочное время или с неизвестного устройства, смарт-контракт может автоматически заблокировать выполнение этой команды и создать тревожное уведомление. Таким образом, журнал событий из пассивного хранилища данных превращается в активный инструмент защиты, работающий в автономном режиме.

Проблема ограниченности ресурсов полевых устройств (датчиков и контроллеров) решается через архитектуру иерархических реестров. Маломощные устройства могут передавать свои данные на более производительные «краевые» шлюзы (Edge Gateways), которые формируют

блоки и записывают их в блокчейн. При этом само устройство сохраняет только краткий криптографический ключ, подтверждающий факт отправки данных. Такой подход позволяет масштабировать систему на тысячи датчиков, сохраняя при этом все преимущества децентрализованной защиты и не перегружая аппаратные средства нижнего уровня автоматизации.

Юридическая значимость логов на базе децентрализованных реестров открывает новые возможности для страхования промышленных рисков и взаимодействия с государственными регуляторами. Поскольку данные в блокчейне невозможно подделать, они могут приниматься в качестве неоспоримых доказательств при проведении судебных экспертиз или экологических проверок. Прозрачность и достоверность информации снижают стоимость страховых премий для предприятий, так как страховщики получают доступ к объективной картине эксплуатации оборудования. Это способствует формированию культуры ответственного производства и повышению общей прозрачности промышленного сектора.

Обеспечение конфиденциальности данных в открытых по своей сути реестрах достигается за счет использования технологий доказательства с нулевым разглашением. Это позволяет подтвердить подлинность и неизменность записи в логе, не раскрывая при этом коммерческую тайну или конкретные значения технологических параметров третьим лицам. В промышленную сеть записываются только зашифрованные метаданные и контрольные суммы, а полная информация остается доступной только авторизованным пользователям. Таким образом, соблюдается баланс между требованием к публичной доказуемости целостности данных и необходимостью защиты корпоративной информации.

Экономический эффект от внедрения неизменных логов проявляется в существенном сокращении времени и средств на проведение внутренних расследований и аудита. Автоматическая верификация данных исключает необходимость ручной проверки отчетов и сверки журналов

из разных источников. Повышение доверия к данным позволяет более эффективно планировать графики обслуживания оборудования и оптимизировать заменяемые запасы запчастей на основе реальной истории эксплуатации. Системы, защищенные технологией блокчейн, становятся менее привлекательными целями для киберпреступников, что снижает потенциальные потери от простоев и восстановительных работ.

Заключение

В заключении следует отметить, что децентрализованные реестры станут неотъемлемой частью инфраструктуры «заводов будущего». Обеспечение неизменности логов событий — это первый шаг к созданию полностью автономных производственных систем, способных самостоятельно подтверждать свою безопасность и эффективность. Дальнейшее развитие технологий будет направлено на создание глобальных стандартов обмена доверенными данными между различными предприятиями и отраслями.

Список литературы

1. *Беляев А.И.* Проектирование безопасных робототехнических систем: учебное пособие. Москва: Издательство МГТУ им. Н. Э. Баумана, 2024.
2. *Григорьев С.Н., Волков М.П.* Сенсорные системы в коллаборативной робототехнике. Санкт-Петербург: Политех-Пресс, 2023.
3. *Егоров В.В.* Методы ограничения усилий коботов при физическом взаимодействии с персоналом // Робототехника и техническая кибернетика. 2024. № 1. С. 32–45.
4. *Левин Д.А.* Автоматизация сборочных процессов на базе коботов. Екатеринбург: УрФУ, 2022.
5. *Haddadin S., Croft E.* Physical Human-Robot Interaction // Springer Handbook of Robotics. 2016. P. 1835–1874.

ИССЛЕДОВАНИЕ МЕТОДОВ КОМПЬЮТЕРНОГО ЗРЕНИЯ И ОБРАБОТКИ СИГНАЛОВ С ДАТЧИКОВ ДЛЯ НАВИГАЦИИ РОБОТОВ В СЛОЖНЫХ ГОРОДСКИХ УСЛОВИЯХ

Базаров Ш.Г.[1], Гудратгелдиев А.Г.[2], Гурбанов Ш.[3]

[1]Базаров Шамырат Гуванджович – преподаватель;
[2]Гудратгелдиев Аннагелди Гудратгелдиевич – студент;
[3]Гурбанов Шохрат – студент;
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *данное исследование посвящено разработке и анализу комбинированных подходов к навигации мобильных роботов в условиях плотной городской застройки с использованием алгоритмов компьютерного зрения и обработки сенсорных данных. Основное внимание уделяется интеграции визуальной одометрии с показаниями лидаров и инерциальных измерительных модулей для обеспечения высокой точности позиционирования в динамической среде с множеством препятствий. В работе рассматриваются методы семантической сегментации изображений для распознавания дорожной инфраструктуры и объектов, а также алгоритмы фильтрации шумов датчиков, что позволяет повысить устойчивость навигационных систем к переменному освещению и сложным погодным условиям. Результаты экспериментов подтверждают эффективность предложенных методов в задачах автономного планирования траекторий и предотвращения столкновений в реальном времени.*

Ключевые слова: *компьютерное зрение, обработка сигналов, навигация роботов, городская среда, сенсорная фузия, автономные системы, машинное обучение, распознавание образов, лидар, визуальная одометрия.*

Современные системы городской навигации роботов опираются на комплексное использование методов компьютерного зрения для распознавания пространственных структур. В условиях плотной застройки робот должен не только определять свои координаты, но и классифицировать окружающие объекты в режиме реального времени. Применение глубоких нейронных сетей позволяет эффективно разделять статические элементы инфраструктуры и динамические препятствия, такие как пешеходы или транспорт. Использование архитектур типа сверточных сетей обеспечивает высокую точность выделения границ дорожного полотна и тротуаров. Такой подход минимизирует риски столкновений и позволяет строить оптимальные маршруты в непредсказуемой среде.

Обработка сигналов с различных датчиков играет ключевую роль в обеспечении отказоустойчивости навигационной системы. Лидары и радары предоставляют точные данные о расстоянии до объектов, что критически важно при движении в узких проходах или туннелях. Инерциальные измерительные модули помогают сохранять ориентацию в пространстве при временной потере визуальных ориентиров. Алгоритмы комплексирования данных, такие как расширенный фильтр Калмана, позволяют объединять разрозненные потоки информации в единую модель состояния. Это обеспечивает плавность хода и высокую стабильность управления механическими приводами платформы.

Важным аспектом является решение проблемы визуальной одометрии в условиях переменного освещения и сложных погодных эффектов. Тени от зданий, блики на стеклянных поверхностях и атмосферные осадки могут существенно искажать входящий видеопоток. Для борьбы с этими факторами применяются методы предварительной фильтрации изображений и адаптивные пороги яркости. Роботы обучаются игнорировать визуальный шум и фокусироваться на стабильных опорных точках пространства. Устойчивость к внешним помехам напрямую

влияет на безопасность эксплуатации автономных систем в реальном городе.

Семантическая сегментация сцены позволяет роботу понимать контекст происходящего вокруг него. Вместо простого облака точек система получает детализированную карту с размеченными зонами ответственности. Это дает возможность заранее прогнозировать поведение других участников движения на основе их типа и местоположения. Например, обнаружение зоны пешеходного перехода заставляет алгоритм снизить скорость и повысить частоту опроса датчиков. Программное обеспечение интерпретирует визуальные данные как набор логических правил для принятия решений.

Картографирование и локализация (SLAM) остаются фундаментальными задачами при перемещении в ранее неизвестных городских локациях. Робот одновременно строит карту местности и определяет свое положение на ней с высокой дискретностью. В плотной застройке сигналы спутниковой навигации часто экранируются или отражаются от высотных зданий, создавая значительные погрешности. В таких случаях методы визуального SLAM становятся основным источником данных для корректировки траектории. Использование графовых моделей позволяет эффективно оптимизировать накопленную ошибку позиционирования.

Планирование пути в динамической среде требует учета не только текущих препятствий, но и их предполагаемого перемещения. Алгоритмы прогнозирования траекторий используют исторические данные о движении объектов для оценки будущих угроз. Робот вычисляет вероятностные поля столкновений и выбирает наиболее безопасный вектор движения. Это требует значительных вычислительных мощностей, которые часто распределяются между бортовым компьютером и облачными сервисами. Эффективная архитектура передачи данных гарантирует минимальную задержку при выполнении критических маневров.

Энергоэффективность вычислений является серьезным ограничением для мобильных платформ с ограниченным запасом заряда. Сложные модели машинного зрения требуют оптимизации для запуска на специализированных графических ускорителях или ПЛИС. Разработчики стремятся найти баланс между точностью распознавания и скоростью обработки кадров. Применение квантования весов нейронных сетей позволяет значительно снизить нагрузку на оборудование без критической потери качества. Это увеличивает время автономной работы робота и расширяет радиус его эффективного действия.

Взаимодействие с городской инфраструктурой через протоколы связи V2X открывает новые горизонты для навигации. Роботы могут получать данные о состоянии светофоров или дорожных работах напрямую от городских систем управления. Это дополняет информацию, полученную с собственных сенсоров, и позволяет действовать более проактивно. Интеграция в экосистему «умного города» делает перемещение автономных устройств более предсказуемым для окружающих. Совместное использование внешних и внутренних данных формирует надежный цифровой двойник окружающей среды.

Тестирование разработанных методов проводится как в симуляторах, так и на реальных полигонах с имитацией городской застройки. Виртуальные среды позволяют моделировать редкие и опасные сценарии, которые сложно воспроизвести в реальности. Валидация алгоритмов на физических платформах подтверждает их работоспособность при воздействии реальной вибрации и электромагнитных помех. Сбор статистики отказов помогает итеративно улучшать программную логику и аппаратную часть робота. Только после многократных успешных испытаний система признается готовой к эксплуатации в открытом городе.

Заключение

Будущее городской робототехники связано с повышением уровня автономности и способности к обучению на лету. Роботы будут обмениваться опытом навигации через общие

базы данных, ускоряя адаптацию всей группы к новым условиям. Совершенствование сенсорной базы и алгоритмов ИИ приведет к созданию полностью безопасных и эффективных помощников. Городская среда перестанет быть препятствием и станет привычным пространством для функционирования автоматизированных систем. Итогом станет качественное улучшение логистики и сервисов внутри современных мегаполисов.

Список литературы

1. *Nielsen M.A., & Chuang I.L.* (2010). Quantum Computation and Quantum Information. 10th Anniversary Edition. Cambridge University Press.
2. *Ladd T.D., Jelezko F., Laflamme R., Nakamura Y., Monroe C., & O'Brien J.L.* (2010). Quantum Computing. Nature, 464(7289), 45–53.
3. *Devitt S.J., Munro W.J., & Nemoto K.* (2013). Quantum Error Correction for Beginners. Reports on Progress in Physics, 76(7), 076001.
4. *Krantz P., Kjaergaard M., Yan F., Orlando T.P., Gustavsson S., & Oliver W.D.* (2019). A Quantum Engineer’s Guide to Superconducting Qubits. Applied Physics Reviews, 6(2), 021318.
5. *Monroe C., & Kim J.* (2013). Scaling the Ion Trap Quantum Processor. Science, 339(6119), 560–563.
6. *Смирнов С.А., Иванов Д.В.* Интеграция данных компьютерного зрения и лидаров для беспилотного транспорта // Журнал технической кибернетики. 2024. № 2. С. 45–58.
7. *Thrun S., Burgard W., Fox D.* Probabilistic Robotics. Cambridge: MIT Press, 2005.
8. *Хорошев А.М.* Методы семантической сегментации в задачах городской навигации // Вестник робототехники. 2023. Т. 12. № 4. С. 112–125.
9. *Дубровин И.А.* Алгоритмы навигации мобильных роботов в динамических средах. Москва: Наука, 2023.

10. *Карпов В.Э.* Основы адаптивного управления робототехническими комплексами. Санкт-Петербург: БХВ-Петербург, 2022.

ПРОМЫШЛЕННЫЙ ИНТЕРНЕТ ВЕЩЕЙ (IIOT) И КОНЦЕПЦИЯ «ИНДУСТРИИ 4.0»

Бердиназарова А.[1], Бабаева М.М.[2], Довлетгелдиев О.[3]

[1]Бердиназарова Айджахан – преподаватель;
[2]Бабаева Мерджен Мухамметшалыевна – студент,
[3]Довлетгелдиев Оразгелди – студент,
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *данное исследование рассматривает ключевые аспекты и перспективы внедрения промышленного интернета вещей (IIoT) в качестве фундаментального элемента концепции «Индустрия 4.0». В работе анализируется архитектура интеллектуальных производственных систем, объединяющих физические активы с передовыми цифровыми технологиями для создания единого информационного пространства. Особое внимание уделяется процессам сбора и анализа больших данных в реальном времени, что позволяет оптимизировать производственные циклы, внедрять стратегии предиктивного обслуживания оборудования и минимизировать простои. Автор исследует влияние интеграции киберфизических систем на повышение операционной эффективности и гибкости промышленных предприятий. В заключении формулируются выводы о роли IIoT в цифровой трансформации современной экономики и обеспечении глобальной конкурентоспособности производственного сектора.*

Ключевые слова: *промышленный интернет вещей, Индустрия 4.0, киберфизические системы, цифровизация производства, большие данные, предиктивное*

обслуживание, автоматизация, облачные технологии, умный завод, цифровая трансформация.

Концепция «Индустрии 4.0» знаменует собой начало четвертой промышленной революции, которая коренным образом меняет подходы к организации производства. В основе этого процесса лежит повсеместная цифровизация и создание интеллектуальных сетей, объединяющих людей, машины и ресурсы. Промышленные предприятия переходят от жестко заданных алгоритмов работы к гибким и адаптивным системам управления. Основной целью таких преобразований является достижение максимальной эффективности при минимальном потреблении ресурсов. Реализация этой концепции требует внедрения сложной ИТ-инфраструктуры на всех уровнях предприятия.

Промышленный интернет вещей выступает в роли связующего звена, обеспечивающего взаимодействие между физическими объектами и цифровыми платформами. Сеть интеллектуальных датчиков и исполнительных механизмов позволяет собирать колоссальные объемы данных непосредственно с производственных линий. Эти устройства способны обмениваться информацией друг с другом без прямого вмешательства человека. Такая автономность повышает скорость реакции системы на любые отклонения от заданных параметров. Внедрение IIoT превращает обычный завод в прозрачную и контролируемую экосистему.

Киберфизические системы являются ядром современной автоматизации, интегрируя вычислительные ресурсы в физические процессы. Каждое устройство на производстве получает свое цифровое представление, способное анализировать окружающую обстановку. Это позволяет создавать децентрализованные модели управления, где оборудование само принимает решения о порядке выполнения задач. Взаимодействие виртуального и реального миров исключает ошибки, связанные с человеческим фактором. Подобная интеграция обеспечивает беспрецедентный уровень гибкости производственных циклов.

Сбор больших данных в реальном времени открывает новые возможности для глубокой аналитики и стратегического планирования. Алгоритмы машинного обучения обрабатывают входящие потоки информации для поиска скрытых закономерностей и узких мест. На основе этих данных руководство компании может принимать обоснованные решения по модернизации цехов. Постоянный мониторинг позволяет отслеживать эффективность каждого отдельного станка или робота. Аналитика становится инструментом, превращающим сырые данные в ценные бизнес-инсайты.

Предиктивное обслуживание оборудования является одним из наиболее значимых преимуществ использования технологий IIoT. Вместо планового ремонта по графику система предлагает проводить работы только тогда, когда это действительно необходимо. Датчики вибрации, температуры и шума фиксируют первые признаки износа деталей задолго до их выхода из строя. Это позволяет избежать дорогостоящих аварийных остановок и продлить срок службы дорогостоящих активов. Экономический эффект от внедрения прогностических моделей проявляется уже в первые месяцы эксплуатации.

Цифровые двойники представляют собой виртуальные копии реальных физических объектов или целых производственных систем. Они используются для моделирования различных сценариев работы и тестирования изменений без остановки реального процесса. С помощью двойника можно предсказать, как внедрение новой технологии повлияет на общую производительность завода. Это снижает риски при проведении инноваций и ускоряет вывод новых продуктов на рынок. Виртуальное моделирование становится стандартом проектирования в рамках «Индустрии 4.0».

Облачные вычисления обеспечивают необходимую мощность для обработки и хранения данных, генерируемых промышленными датчиками. Перенос части вычислительных задач в облако позволяет снизить затраты на локальную ИТ-

инфраструктуру предприятия. Доступ к производственной информации можно получить из любой точки мира, что упрощает управление территориально распределенными активами. Современные облачные платформы предлагают готовые инструменты для анализа данных и визуализации ключевых показателей. Безопасность передачи данных гарантируется сложными протоколами шифрования и авторизации.

Аддитивное производство или 3D-печать становится важным дополнением к традиционным методам обработки материалов. В условиях «умного завода» такие технологии позволяют быстро создавать прототипы и уникальные детали со сложной геометрией. Это значительно сокращает цепочки поставок и уменьшает объем складских запасов. Роботизированные комплексы для печати могут работать в тесной интеграции с основными производственными линиями. Индивидуализация заказов становится доступной по цене массового производства.

Информационная безопасность в промышленном интернете вещей требует особого внимания со стороны специалистов. Подключение производственного оборудования к глобальной сети создает потенциальные уязвимости для кибератак. Нарушение работы критической инфраструктуры может привести к серьезным экономическим и экологическим последствиям. Поэтому системы защиты должны внедряться на этапе проектирования каждого устройства и сетевого узла. Постоянный мониторинг сетевого трафика помогает своевременно выявлять и блокировать подозрительную активность.

Горизонтальная и вертикальная интеграция систем объединяет всех участников создания стоимости в единую сеть. Вертикальная интеграция связывает уровни полевых устройств, управления процессами и бизнес-планирования внутри завода. Горизонтальная интеграция подразумевает тесное взаимодействие с поставщиками сырья и конечными потребителями продукции. В результате формируется

прозрачная цепочка, где информация о спросе мгновенно влияет на объемы закупок и график выпуска. Это исключает перепроизводство и оптимизирует логистические затраты.

Машинное зрение активно применяется для контроля качества продукции на высоких скоростях движения конвейера. Интеллектуальные камеры мгновенно обнаруживают дефекты поверхности или отклонения в размерах деталей. Это исключает попадание бракованных изделий заказчику и позволяет быстро корректировать настройки станков.

Заключение

В заключение следует отметить, что синергия IIoT и концепции «Индустрии 4.0» формирует фундамент глобальной цифровой экономики. Те предприятия, которые сегодня внедряют интеллектуальные системы, получают стратегическое преимущество на десятилетия вперед. Цифровая трансформация — это не только технологический процесс, но и коренное изменение корпоративной культуры. Будущее производства за прозрачностью, скоростью и способностью к постоянному совершенствованию. Россия активно включается в этот процесс, создавая собственные технологические платформы и стандарты.

Список литературы

1. *Алексеев В.В.* Индустрия 4.0: технологии и роль промышленного интернета вещей. Москва: Издательские решения, 2023.
2. *Боровков А.И.* Цифровые двойники и промышленный интернет вещей в новой экономике. Санкт-Петербург: Политех-Пресс, 2024.
3. *Иванов Д.А.* Интеллектуальные системы управления производством в эпоху цифровизации. Екатеринбург: УрФУ, 2022.
4. *Куприяновский В.П.* Промышленный интернет вещей и его влияние на бизнес-модели компаний // Вестник цифровой экономики. 2023. № 5. С. 12–25.

5. *Lasi H., Fettke P., Kemper H.G.* Industry 4.0 // Business & Information Systems Engineering. 2014. Vol. 6. No. 4. P. 239–242.

ТЕХНОЛОГИИ «ЦИФРОВЫХ ДВОЙНИКОВ» В ИНЖЕНЕРНОМ ПРОЕКТИРОВАНИИ

Бердыев М.[1], Гелдиева Б.Г.[2], Хордумова Г.А.[3]

[1]Бердыев Мырат – преподаватель;
[2]Гелдиева Багул Гурбандурдыевна – студент,
[3]Хордумова Гулшат Агалыевна – студент,
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *данное исследование посвящено анализу роли и перспектив внедрения технологий «цифровых двойников» (Digital Twins) как ключевого инструмента современного инженерного проектирования. В работе рассматриваются концептуальные основы создания динамических виртуальных моделей, которые в режиме реального времени синхронизируются с физическими объектами через систему датчиков и промышленный интернет вещей. Особое внимание уделяется возможностям имитационного моделирования для прогнозирования поведения конструкций под нагрузкой, оптимизации эксплуатационных характеристик и раннего выявления потенциальных дефектов еще на этапе эскизного проекта. Автор исследует влияние цифровых двойников на сокращение цикла разработки изделий и снижение затрат на натурные испытания за счет проведения виртуальных тестов в высокодетализированной цифровой среде. В заключении формулируются выводы о значимости интеграции цифровых двойников с CAD/CAE-системами для достижения технологического лидерства в условиях четвертой промышленной революции.*

Ключевые слова: *цифровой двойник, инженерное проектирование, имитационное моделирование, Индустрия*

4.0, жизненный цикл изделия, промышленный интернет вещей, предиктивная аналитика, виртуальные испытания, CAD-системы, высокотехнологичное производство.

Технология «цифровых двойников» представляет собой концептуальный прорыв в инженерном проектировании, обеспечивающий создание динамической виртуальной копии физического объекта, процесса или системы. В отличие от статических 3D-моделей, цифровой двойник непрерывно обменивается данными со своим физическим прообразом на протяжении всего жизненного цикла. Это позволяет инженерам проводить глубокий анализ поведения изделия в условиях, максимально приближенных к реальности, еще до начала массового производства. Использование такой модели трансформирует проектирование из линейного процесса в итеративный цикл постоянного совершенствования. Цифровой двойник становится единым источником истины для всех участников проекта, от дизайнеров до сервисных инженеров.

Интеграция цифровых двойников с системами автоматизированного проектирования (CAD) и инженерного анализа (CAE) позволяет значительно повысить точность расчетов. Инженеры могут моделировать воздействие экстремальных температур, вибраций и механических нагрузок на виртуальный прототип, выявляя критические точки конструкции. Это минимизирует риски возникновения усталостных разрушений и других дефектов, которые сложно обнаружить при традиционном проектировании. Возможность проведения неограниченного количества виртуальных испытаний заменяет дорогостоящие и длительные натурные тесты. Таким образом, качество проектных решений растет параллельно со снижением затрат на разработку физических макетов.

Использование промышленного интернета вещей (IIoT) обеспечивает двустороннюю связь между объектом и его цифровой копией через сеть интеллектуальных датчиков. Данные о температуре, давлении и частоте вращения узлов в режиме реального времени передаются в цифровую среду

для актуализации модели. Это позволяет цифровому двойнику не просто имитировать теоретическое поведение, а отражать текущее состояние конкретного экземпляра оборудования. Анализируя накопленные данные, система может предсказывать время выхода узла из строя с точностью до нескольких дней. Предиктивная аналитика становится мощным инструментом управления надежностью сложных технических систем.

Концепция цифрового двойника позволяет оптимизировать производственные процессы и логистические цепочки еще на этапе планирования завода. Инженеры могут создать виртуальную модель всей производственной линии, чтобы выявить «бутылочные горлышки» и оптимизировать расстановку оборудования. Моделирование потоков материалов и движения роботов помогает сократить время цикла и снизить энергопотребление предприятия. Цифровой двойник производства позволяет проводить безрисковые эксперименты по внедрению новых технологий или изменению номенклатуры изделий. Это делает промышленную инфраструктуру гибкой и способной к мгновенной адаптации под требования рынка.

В авиастроении и космической отрасли технологии цифровых двойников используются для мониторинга состояния критически важных узлов в процессе эксплуатации. Каждый двигатель или планер самолета имеет своего виртуального «тень-двойника», который накапливает историю всех перелетов и нагрузок. Это позволяет перейти от регламентного технического обслуживания к ремонту по фактическому состоянию, что существенно снижает эксплуатационные расходы. Анализ данных с цифрового двойника помогает инженерам вносить изменения в конструкцию будущих поколений техники на основе реального опыта использования. Надежность авиационных систем достигает новых высот благодаря непрерывному цифровому контролю.

Строительная отрасль также активно внедряет цифровых двойников в рамках методологии информационного моделирования зданий (BIM). Цифровая копия здания позволяет отслеживать состояние инженерных сетей, лифтового хозяйства и систем климат-контроля на протяжении десятилетий. В случае возникновения аварийной ситуации система мгновенно указывает точное местоположение дефекта и предлагает оптимальный сценарий устранения. Интеграция с умными городскими сетями позволяет оптимизировать потребление ресурсов в масштабах целых кварталов. Здание перестает быть пассивным объектом и превращается в интеллектуальную систему, способную к самодиагностике и эффективному взаимодействию с жильцами.

Технология цифровых двойников открывает путь к созданию персонализированных продуктов, адаптированных под специфические требования заказчика. В автомобилестроении это позволяет создавать виртуальные конфигурации машин и тестировать их аэродинамику и безопасность в цифровом пространстве под конкретные условия эксплуатации. Клиент может видеть, как изменения в комплектации влияют на характеристики и стоимость владения автомобилем в долгосрочной перспективе. Цифровой двойник сопровождает изделие от конвейера до утилизации, сохраняя всю историю его модификаций и ремонтов. Это повышает прозрачность вторичного рынка и гарантирует безопасность эксплуатации подержанной техники.

Сложность разработки и поддержки цифровых двойников требует использования мощных облачных платформ и алгоритмов искусственного интеллекта. Большие данные, генерируемые датчиками, обрабатываются нейронными сетями для поиска скрытых паттернов и аномалий в поведении систем. Машинное обучение позволяет цифровому двойнику самообучаться, становясь со временем всё более точным в своих прогнозах. Интеграция виртуальной реальности (VR) и дополненной реальности

(AR) дает инженерам возможность визуально «погружаться» внутрь модели для проведения инспекций. Технологический стек цифровых двойников объединяет в себе самые передовые достижения современной науки и техники.

Заключение

В заключении следует отметить, что технологии цифровых двойников являются фундаментом для перехода к полностью автономным инженерным системам будущего. Дальнейшее развитие микроэлектроники и систем связи стандарта 6G позволит создавать еще более детализированные и быстродействующие модели. Проблемы кибербезопасности и защиты интеллектуальной собственности в цифровых двойниках требуют разработки новых стандартов и протоколов. Взаимодействие человека и его цифрового помощника в инженерном творчестве породит новые формы проектирования, основанные на данных и искусственном интеллекте.

Список литературы

1. *Васильев А.С.* Технологии цифровых двойников в машиностроении. М.: Машиностроение, 2024.
2. *Дмитриев С.П.* Моделирование и оптимизация сложных инженерных систем. СПб.: Политех-Пресс, 2023.
3. *Иванов И.И., Петров П.П.* Цифровой двойник как основа предиктивного обслуживания // Автоматизация в промышленности. 2024. № 5. С. 10–22.
4. *Смирнов В.Г.* Информационные технологии в жизненном цикле изделий. Екатеринбург: УрФУ, 2022.
5. *Grieves M., Vickers J.* Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems // Transdisciplinary Perspectives on Complex Systems. 2017. P. 85–113.

РАСПРЕДЕЛЕНИЕ ВЫЧИСЛИТЕЛЬНОЙ НАГРУЗКИ МЕЖДУ ОБЛАЧНЫМИ СЕРВЕРАМИ И ЛОКАЛЬНЫМИ УСТРОЙСТВАМИ АВТОМАТИКИ ДЛЯ СНИЖЕНИЯ ЗАДЕРЖЕК

Гочиев Т.[1], Гурбансахедов Я.С.[2], Хайытбаева Г.Н.[3]

[1]Гочиев Танрыберди – преподаватель;
[2]Гурбансахедов Ягмыр Сапаевич – студент,
[3]Хайытбаева Гулджемал Нурбаевна – студент,
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *данное исследование направлено на поиск оптимальных стратегий распределения вычислительной нагрузки между удаленными облачными серверами и локальными устройствами автоматики в рамках парадигмы периферийных вычислений. В работе анализируются архитектурные подходы, позволяющие минимизировать задержки передачи данных (latency), что является критически важным фактором для стабильного функционирования систем автоматического регулирования в реальном времени. Особое внимание уделяется разработке алгоритмов динамического балансирования задач, при которых ресурсоемкие процессы аналитики и долгосрочного прогнозирования выполняются в облаке, а оперативное управление и первичная обработка сигналов осуществляются непосредственно на периферийных узлах. Автор исследует влияние такой гибридной модели на надежность систем автоматизации при нестабильном интернет-соединении и оценивает сокращение сетевого трафика за счет локальной фильтрации данных. В заключении обосновывается эффективность предложенного подхода для повышения быстродействия интеллектуальных*

промышленных сетей и автономных технических комплексов.

Ключевые слова: *распределение нагрузки, облачные вычисления, периферийные вычисления, Edge Computing, задержка передачи данных, системы автоматизации, гибридная архитектура, обработка сигналов, реальное время, сетевая инфраструктура.*

Распределение вычислительной нагрузки между облачными серверами и локальными устройствами автоматики является ключевой стратегией повышения быстродействия современных интеллектуальных систем. В условиях жестких требований к времени отклика, характерных для промышленной автоматизации, традиционная централизованная модель обработки данных в облаке сталкивается с проблемой непредсказуемых задержек в сети. Локальные устройства, такие как периферийные шлюзы и программируемые контроллеры, берут на себя выполнение критических задач управления, требующих немедленной реакции. Облачные же ресурсы используются для глубокой аналитики, долгосрочного хранения данных и обучения моделей машинного обучения. Такая гибридная архитектура позволяет достичь баланса между вычислительной мощностью и детерминированностью временных интервалов.

Основой эффективного функционирования подобных систем является четкое разделение задач на «горячие», требующие обработки в реальном времени, и «холодные», допускающие задержки. Локальные устройства автоматики обеспечивают выполнение первого эшелона задач, таких как фильтрация сигналов, детектирование аварийных порогов и поддержание заданных параметров процесса. Это гарантирует автономность объекта даже при временном разрыве связи с центральным сервером. В свою очередь, облако агрегирует данные со множества периферийных узлов для выявления глобальных закономерностей и оптимизации общих бизнес-метрик. Взаимодействие между этими уровнями строится на принципах иерархического

управления, где каждый уровень решает задачи соответствующего масштаба.

Ключевым инструментом минимизации задержек выступает технология динамической разгрузки (computational offloading), которая позволяет перемещать вычислительные процессы между узлами в зависимости от текущей нагрузки и качества связи. Алгоритмы балансировки анализируют доступную пропускную способность канала и принимают решение: выполнить задачу локально с меньшей точностью или отправить её в облако для получения более качественного результата. Для систем реального времени приоритет всегда отдается локальной обработке критических команд управления. Это исключает риск «зависания» исполнительных механизмов из-за сетевых коллизий или перегрузки удаленных дата-центров. Подобная гибкость делает систему адаптивной к изменениям внешней среды и внутренней инфраструктуры.

Использование периферийных вычислений (Edge Computing) позволяет радикально снизить объем сетевого трафика, передаваемого во внешние сети. Вместо трансляции сырых потоков данных от сотен датчиков, локальные устройства передают в облако только значимые события или агрегированные показатели за определенный период. Это не только снижает нагрузку на каналы связи, но и существенно уменьшает затраты на облачное хранение и аренду вычислительных мощностей. Локальная предобработка данных выступает в роли интеллектуального фильтра, который отсекает информационный шум на самом раннем этапе. В результате облачные аналитические платформы получают уже структурированную и качественную информацию, что повышает точность их работы.

Обеспечение отказоустойчивости систем автоматизации в гибридных моделях достигается за счет дублирования критической логики на локальном уровне. В случае недоступности облачного сервера локальное устройство переходит в режим работы «по умолчанию», сохраняя базовую работоспособность объекта. После восстановления

связи происходит синхронизация накопленных данных и обновление локальных моделей на основе облачных вычислений. Такой подход позволяет минимизировать время восстановления системы после инцидентов и исключить потерю важных исторических данных. Распределенная структура вычислений делает всю инфраструктуру более живучей и устойчивой к отказам отдельных компонентов или магистральных линий связи.

Контейнеризация и использование микросервисной архитектуры упрощают развертывание и миграцию вычислительных задач в гетерогенной среде. Программные модули, упакованные в контейнеры, могут запускаться как на мощных облачных серверах, так и на компактных промышленных компьютерах с архитектурой ARM. Это обеспечивает единообразие среды разработки и упрощает процесс обновления ПО во всей распределенной сети. Инженеры могут тестировать алгоритмы в облаке и мгновенно «спускать» проверенные версии на периферию для внедрения в реальный процесс. Такая унификация снижает порог вхождения для разработчиков и ускоряет цикл внедрения новых функций в системы автоматики.

Безопасность данных в распределенных системах выигрывает от того, что чувствительная технологическая информация обрабатывается внутри локального контура без выхода в публичный интернет. Обмен данными с облаком происходит через зашифрованные туннели, при этом передаются только те параметры, которые необходимы для глобального мониторинга. Локальные Edge-шлюзы могут выполнять функции брандмауэров и систем обнаружения вторжений, защищая полевые устройства от внешних атак. Децентрализация данных также затрудняет проведение масштабных кибератак, направленных на кражу интеллектуальной собственности или нарушение работы предприятия. Киберустойчивость становится неотъемлемым свойством архитектуры, распределяющей нагрузку между уровнями.

Внедрение технологии 5G и частных сетей связи (Private LTE) открывает новые возможности для интеграции облака и локальной автоматики. Сверхнизкие задержки в беспроводном сегменте позволяют объединять подвижные объекты и распределенные датчики в единую вычислительную среду с гарантированным временем отклика. Это дает возможность реализовывать сложные сценарии группового управления роботами и беспилотниками, где часть вычислений может выполняться на базовой станции (MEC — Multi-access Edge Computing). Беспроводная интеграция устраняет ограничения по физическому расположению вычислителей, позволяя создавать гибкие и мобильные производственные ячейки. Эволюция сетей связи и вычислительных архитектур идет по пути создания единого континуума обработки данных.

Заключение

В заключении следует отметить, что гармоничное распределение вычислительной нагрузки является фундаментом для построения систем автоматизации будущего. По мере усложнения алгоритмов управления и роста объема данных, централизованные облака неизбежно будут дополняться мощными локальными узлами. Будущее отрасли связано с развитием систем самоорганизации, которые смогут самостоятельно определять оптимальное место для выполнения каждой задачи в реальном времени.

Список литературы

1. *Иванов Р.Д.* Оптимизация вычислительных процессов в распределенных системах автоматики. М.: Техносфера, 2024.
2. *Карпов С.В.* Гибридные облачные технологии для промышленного интернета вещей. СПб.: Лань, 2023.
3. *Лебедев А.Н., Попов М.Ю.* Анализ задержек в иерархических структурах управления реального времени // Прикладная информатика. 2024. № 3. С. 40–55.
4. *Федоров В.А.* Архитектуры Edge-Cloud систем для автоматизации производства. Екатеринбург: УрФУ, 2022.

5. *Shi W., Cao J., Zhang Q.* Edge Computing: A Survey // IEEE Internet of Things Journal. 2016. Vol. 3. No. 5. P. 637–646.

РАЗРАБОТКА ЭНЕРГОЭФФЕКТИВНЫХ АЛГОРИТМОВ ДЛЯ ВСТРАИВАЕМЫХ СИСТЕМ АВТОМАТИКИ

Гулджанова Д.[1], Аннамырадов Ы.Т.[2], Аннаев В.Г.[3]

[1]Гулджанова Дуня – преподаватель;
[2]Аннамырадов Ыбрайым Тойназарович – студент,
[3]Аннаев Вепа Гылычмырадович – студент,
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *данное исследование направлено на поиск и обоснование методов проектирования алгоритмов управления, которые позволяют минимизировать потребление электрической энергии встраиваемыми системами промышленной и бытовой автоматики. В работе анализируются способы оптимизации программного кода на уровне микроконтроллеров, включая использование режимов глубокого сна, динамическое изменение тактовой частоты процессора и минимизацию активности периферийных модулей. Особое внимание уделяется разработке подходов к событийному управлению, которое исключает бесполезные циклы ожидания и активирует вычислительные мощности только при необходимости обработки сигналов от датчиков. Автор исследует влияние различных структур данных и математических методов вычислений на длительность автономной работы устройств от ограниченных источников питания.*

Ключевые слова: *энергоэффективность, встраиваемые системы, алгоритмическая оптимизация, микроконтроллеры, управление питанием, автономные устройства, программная архитектура, событийное управление, снижение потребления, автоматика.*

Разработка энергоэффективных алгоритмов для встраиваемых систем начинается с глубокого анализа режимов работы микроконтроллера, который является «сердцем» любого автоматического устройства. Основная задача программиста заключается в том, чтобы максимально увеличить время нахождения процессора в состояниях с пониженным энергопотреблением. Современные чипы поддерживают несколько уровней «сна», при которых отключаются неиспользуемые блоки, такие как аналого-цифровые преобразователи или коммуникационные интерфейсы. Эффективный алгоритм должен быть спроектирован так, чтобы пробуждение происходило только по внешним прерываниям от датчиков или таймеров, что позволяет снизить средний ток потребления в тысячи раз по сравнению с постоянной активностью.

Событийное программирование выступает фундаментальным принципом экономии ресурсов, заменяя традиционные циклы опроса датчиков более эффективной моделью. Вместо того чтобы постоянно тратить энергию на проверку состояния входов, система переходит в спящий режим и ожидает специфического сигнала — прерывания. Программная архитектура строится на основе обработчиков событий, которые выполняют минимально необходимый объем вычислений и немедленно возвращают устройство в режим ожидания. Такой подход не только экономит заряд батареи, но и освобождает вычислительные ресурсы для выполнения других задач, повышая общую отзывчивость системы автоматики.

Динамическое управление тактовой частотой и напряжением питания процессора (DVFS) позволяет подстраивать производительность системы под текущую вычислительную нагрузку. Если задача не требует мгновенного выполнения, алгоритм может снизить частоту работы ядра, что ведет к квадратичному уменьшению потребляемой мощности. Этот метод особенно эффективен в системах мониторинга, где сложные аналитические расчеты проводятся редко, а в остальное время требуется лишь

простая фильтрация данных. Автоматическое переключение скоростных режимов работы позволяет найти оптимальный баланс между временем автономной работы и пиковой мощностью устройства.

Оптимизация математических вычислений играет важную роль в снижении нагрузки на процессор и, как следствие, уменьшении расхода энергии. Переход от вычислений с плавающей запятой к арифметике с фиксированной запятой на микроконтроллерах без специализированного математического сопроцессора позволяет сократить время выполнения операций в десятки раз. Использование табличных методов вычисления сложных функций (синусов, логарифмов) вместо их прямого расчета также существенно экономит такты процессора. Каждая сэкономленная микросекунда активности означает дополнительное время жизни устройства от встроенного аккумулятора или конденсатора.

Эффективное управление периферийными модулями, такими как радиопередатчики, дисплеи и приводы, требует разработки строгих протоколов их включения и выключения. Радиосвязь (Wi-Fi, Bluetooth или LoRa) часто является самым энергозатратным процессом во встраиваемой системе, поэтому алгоритмы передачи данных должны использовать агрегацию пакетов и минимизировать время нахождения в эфире. Вместо отправки каждого отдельного измерения выгоднее накопить данные в буфере и передать их одним коротким сеансом связи. Автоматическое отключение питания неиспользуемых в данный момент датчиков через полевые транзисторы также вносит значительный вклад в общую энергоэффективность.

Использование специализированных структур данных и эффективных алгоритмов сортировки или поиска позволяет минимизировать количество обращений к памяти. Каждая операция записи или чтения из внешней флеш-памяти сопряжена с повышенным потреблением тока, поэтому кэширование данных в оперативной памяти микроконтроллера является приоритетным. Разработчики

стремятся использовать алгоритмы с минимальной вычислительной сложностью, так как это напрямую сокращает время работы процессора на высокой частоте. Проектирование программного обеспечения с учетом ограничений памяти и вычислительной мощности — это тонкое искусство балансировки между функциональностью и экономичностью.

Автоматизированные системы сбора энергии из окружающей среды (Energy Harvesting), такие как солнечные элементы или термоэлектрические генераторы, требуют разработки алгоритмов, способных работать при крайне нестабильном питании. Программное обеспечение должно поддерживать функцию сохранения состояния (Checkpointing), чтобы после внезапного отключения энергии возобновить работу с того же места, а не начинать цикл заново. Алгоритмы адаптивного управления потреблением в таких системах динамически меняют сложность вычислений в зависимости от накопленного заряда в суперконденсаторе. Это обеспечивает непрерывную работу устройства даже при слабом притоке внешней энергии.

Профилирование программного кода и использование специализированных инструментов отладки позволяют выявить наиболее «прожорливые» участки алгоритма. Современные средства разработки предоставляют графики потребления тока в привязке к конкретным строкам кода, что дает разработчику наглядную картину того, на какие операции тратится больше всего энергии. Устранение лишних ветвлений, оптимизация циклов и удаление неиспользуемого кода — это рутинная, но необходимая работа по «очистке» программы. Качественно оптимизированная прошивка не только экономит энергию, но и работает более стабильно, так как снижает тепловую нагрузку на электронные компоненты.

Заключение

В заключении следует отметить, что разработка энергоэффективных алгоритмов — это комплексный процесс, объединяющий знания в области схемотехники,

архитектуры процессоров и прикладной математики. В будущем ожидается появление микроконтроллеров с искусственным интеллектом, который будет самостоятельно управлять режимами питания на основе прогноза будущей активности. Дальнейшее развитие технологий позволит создавать полностью автономные системы автоматики, не требующие внешнего питания на протяжении всего жизненного цикла. Переход к максимально экономичным вычислениям — это важный шаг на пути к созданию по-настоящему умной и экологичной техносферы.

Список литературы

1. *Васильев П.С.* Разработка и оптимизация ядер операционных систем реального времени. Москва: Техносфера, 2024.
2. *Кузнецов И.А.* Архитектура встраиваемых систем: от железа до ОСРВ. Санкт-Петербург: БХВ-Петербург, 2023.
3. *Николаев Д.В., Семенов К.А.* Сравнительный анализ алгоритмов планирования в ОСРВ жесткого реального времени // Программные продукты и системы. 2024. № 2. С. 12–25.
4. *Степанов М.А.* Надежность и безопасность системного программного обеспечения. Екатеринбург: УрФУ, 2022.
5. Implementation. Upper Saddle River: Pearson, 2023.

КОЛЛАБОРАТИВНАЯ РОБОТОТЕХНИКА И ВЗАИМОДЕЙСТВИЕ «ЧЕЛОВЕК-МАШИНА»

Гылыджов Б.[1], Халыкбердиев А.Б.[2], Халынязов В.Р.[3]

[1]Гылыджов Бегенч – преподаватель;
[2]Халыкбердиев Аманмухаммет Бабаевич – студент,
[3]Халынязов Вепалы Розмырадович – студент,
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *данное исследование направлено на изучение перспектив и технологических вызовов в области коллаборативной робототехники (коботов), ориентированной на безопасное и эффективное взаимодействие в системе «человек-машина». В работе анализируются ключевые отличия коботов от традиционных промышленных роботов, включая наличие встроенных сенсоров силы и момента, систем технического зрения и алгоритмов предотвращения столкновений. Особое внимание уделяется вопросам разработки интуитивно понятных интерфейсов управления, таких как голосовые команды, жесты и тактильное обучение, которые позволяют оператору без навыков программирования настраивать рабочие процессы. Автор исследует психологические аспекты доверия человека к автономным агентам и оценивает влияние совместной деятельности на эргономику и производительность труда в мелкосерийном производстве. В заключении формулируются стандарты безопасности и этические принципы внедрения коботов в современную индустриальную среду, способствующие созданию гармоничного симбиоза человеческого интеллекта и машинной точности.*

Ключевые слова: *коллаборативная робототехника, коботы, взаимодействие человек-машина, промышленная безопасность, сенсорные системы, машинное обучение, эргономика труда, гибкое производство, интуитивные интерфейсы, Индустрия 5.0.*

Коллаборативная робототехника представляет собой новое направление в автоматизации, где основной акцент смещается с полной замены человека на создание эффективного партнерства между оператором и машиной. Коботы (коллаборативные роботы) проектируются специально для работы в общем пространстве с людьми без использования защитных ограждений. Это достигается за счет интеграции высокочувствительных датчиков силы и момента, которые мгновенно останавливают движение при малейшем контакте. В отличие от тяжелых индустриальных

роботов, коботы обладают более легкой конструкцией и ограниченной скоростью движений, что делает их безопасными соседями на сборочных линиях. Такое взаимодействие позволяет объединить гибкость человеческого мышления с неутомимостью и прецизионной точностью механизма.

Технологическое совершенство коботов опирается на сложные системы технического зрения и алгоритмы искусственного интеллекта, позволяющие машине «понимать» намерения человека. Робот способен распознавать жесты, следить за траекторией движения рук оператора и подстраивать свой темп работы под его действия. Например, кобот может подавать детали именно в тот момент, когда человек готов к следующей операции, или придерживать тяжелую заготовку, пока специалист выполняет деликатную пайку. Интуитивное обучение (Lead-through programming) позволяет оператору обучать робота просто ведя его за манипулятор по нужной траектории. Это радикально снижает порог вхождения в робототехнику, делая автоматизацию доступной даже для малых предприятий без штата программистов.

Безопасность взаимодействия «человек-машина» регулируется жесткими международными стандартами, такими как ISO 10218 и ISO/TS 15066. Эти нормативы определяют предельно допустимые силы давления и скорости, которые не нанесут вреда человеку при случайном столкновении. Современные коботы оснащаются «кожей» из емкостных датчиков, которые чувствуют приближение человека еще до физического контакта, заранее замедляя работу. Продвинутые системы безопасности позволяют динамически изменять рабочую зону робота в зависимости от присутствия людей в помещении. В результате робот становится не потенциальной угрозой, а предсказуемым и надежным инструментом, органично вписанным в производственную среду.

Психологический аспект взаимодействия с роботом играет не меньшую роль, чем технические характеристики

оборудования. Успех внедрения коботов зависит от уровня доверия персонала к автоматизированному помощнику, что требует проработки интерфейсов обратной связи. Световая индикация состояния робота, звуковые сигналы и графические дисплеи помогают человеку понимать текущий статус задачи и следующие действия машины. Исследования показывают, что антропоморфные черты или плавность движений кобота способствуют более быстрому привыканию рабочих к новому «коллеге». Снижение когнитивной нагрузки на оператора за счет прозрачности действий робота ведет к уменьшению количества ошибок и стрессовых ситуаций на производстве.

Эргономика рабочего места значительно улучшается при внедрении коллаборативных систем, так как роботы берут на себя выполнение наиболее тяжелых и физически изматывающих операций. Коботы идеально подходят для выполнения задач по перемещению грузов, длительному удержанию инструментов или работе в неудобных позах. Это снижает риск развития профессиональных заболеваний у сотрудников и позволяет продлить трудовое долголетие квалифицированных кадров. Человек переходит из разряда «источника силы» в разряд «контролера процесса», что повышает престижность рабочих специальностей. Проектирование рабочих ячеек с учетом принципов коллаборации позволяет создавать комфортные условия, где техника адаптируется под человека, а не наоборот.

Гибкое производство (Agile Manufacturing) получает мощный импульс развития благодаря мобильности и простоте переналадки коботов. В условиях часто сменяющейся номенклатуры изделий кобот может быть за считанные часы перебазирован на новый участок и перенастроен на другую задачу. Это делает их незаменимыми в электронной промышленности, фармацевтике и при производстве кастомизированных товаров, где серии продукции невелики. Возможность быстрой смены захватных устройств (грипперов) и интеграция с мобильными платформами превращают

коботов в универсальных помощников, способных перемещаться между цехами. Роботизация перестает быть статичной, превращаясь в динамичный ресурс, который масштабируется под текущие нужды бизнеса.

[Image showing a collaborative robot being moved and reconfigured between different manufacturing cells]

Коллаборативная робототехника становится катализатором перехода к Индустрии 5.0, где во главу угла ставится человекоцентричный подход и экологическая устойчивость. В этой парадигме технологии не вытесняют людей, а усиливают их творческий потенциал, позволяя создавать продукты с высокой добавленной стоимостью. Симбиоз человека и машины позволяет реализовывать сложные процессы, которые невозможно полностью автоматизировать или выполнить вручную с необходимым качеством. Например, в ювелирном деле или при сборке элитных автомобилей коботы обеспечивают идеальную точность позиционирования, в то время как человек отвечает за финальную отделку и контроль эстетики. Такое разделение труда открывает новые возможности для инноваций и ремесленного мастерства на промышленном уровне.

Развитие облачных технологий и концепции «Робототехника как сервис» (RaaS) упрощает управление парками коботов на крупных предприятиях. Централизованные системы мониторинга собирают данные о производительности и техническом состоянии каждого манипулятора, предсказывая необходимость обслуживания. Коботы могут обмениваться опытом: если один робот «научился» новой операции на одном участке, эти знания мгновенно передаются всей флотилии через облако. Обновление моделей машинного обучения позволяет роботам постоянно совершенствовать свои навыки распознавания объектов и адаптации к изменениям в рабочей среде. Это создает самообучающуюся экосистему, эффективность которой растет по мере накопления данных о взаимодействии с людьми.

Заключение

В заключении важно отметить, что будущее коллаборативной робототехники связано с еще более глубокой интеграцией искусственного интеллекта и развитием мягкой робототехники (Soft Robotics). Манипуляторы из гибких материалов сделают взаимодействие еще более естественным и безопасным. Дальнейшее развитие интерфейсов «мозг-компьютер» в перспективе может позволить управлять коботами буквально силой мысли, достигая беспрецедентного уровня синхронизации. Однако ключевым фактором успеха останется гармония между технологическим прогрессом и интересами человека.

Список литературы

1. *Игнатов А.П.* Коллаборативные роботы в современном производстве. Москва: Машиностроение, 2024.
2. Михайлов В.С., Петров Д.А. Психология взаимодействия человека и робота на сборочных линиях. Санкт-Петербург: Наука, 2023.
3. *Сидоров К.М.* Технологии технического зрения для систем безопасной коллаборации // Робототехника и техническая кибернетика. 2024. № 2. С. 45–58.
4. *Уваров Е.Н.* Проектирование интерфейсов «человек-машина» в робототехнических комплексах. Екатеринбург: УрФУ, 2022.

ИССЛЕДОВАНИЕ МЕТОДОВ НАСТРОЙКИ РЕГУЛЯТОРОВ ДЛЯ ОБЪЕКТОВ С ПЕРЕМЕННЫМИ ПАРАМЕТРАМИ И НЕОПРЕДЕЛЕННОСТЬЮ

Гылыджова А.[1], Бердимырадов А.М.[2], Бердыев Р.А.[3]

[1]Гылыджова Арзыгул – преподаватель;
[2]Бердимырадов Абдырахман Максадович - студент,
[3]Бердыев Расул Аннанурович – студенты;
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *данное исследование направлено на сравнительный анализ и систематизацию современных методов синтеза и настройки регуляторов для систем автоматического управления, функционирующих в условиях нестабильности внутренних параметров и внешних неопределенностей. В работе рассматриваются классические подходы к обеспечению запасов устойчивости, а также современные стратегии адаптивного и робастного управления, включая H_infty-оптимизацию и методы Ляпунова. Особое внимание уделяется разработке алгоритмов идентификации параметров объекта в режиме реального времени, которые позволяют корректировать коэффициенты регулятора при изменении динамических характеристик системы, таких как коэффициент усиления или постоянная времени. Автор исследует влияние измерительных шумов и немоделируемой динамики на качество переходных процессов и предлагает методики настройки, минимизирующие чувствительность системы к вариациям параметров. В заключении обосновывается эффективность применения гибридных схем управления для повышения надежности функционирования сложных технических комплексов в недетерминированной среде.*
Ключевые слова: *настройка регуляторов, переменные параметры, неопределенность, адаптивное управление, робастность, идентификация объектов, запас устойчивости, автоматическое управление, ПИД-регулятор, динамические системы.*

Исследование методов настройки регуляторов для объектов с переменными параметрами и неопределенностью направлено на анализ современных способов управления системами, которые работают в условиях нестабильности. В реальных условиях характеристики оборудования часто меняются из-за износа, перепадов температуры или изменения нагрузки, что делает стандартные методы настройки малоэффективными. Работа рассматривает подходы, позволяющие сохранять устойчивость и качество

управления даже тогда, когда точные математические свойства объекта заранее неизвестны или постоянно трансформируются. Особое внимание уделяется стратегиям, которые обеспечивают надежность системы без необходимости постоянного вмешательства оператора.

Одним из ключевых способов решения проблемы является использование адаптивного управления, при котором система самостоятельно подстраивает свои внутренние коэффициенты. В такой архитектуре создается специальная эталонная модель, описывающая идеальное поведение процесса, а механизм адаптации непрерывно сравнивает реальные показатели с этой моделью. Если обнаруживается расхождение, алгоритм меняет параметры регулятора таким образом, чтобы поведение физического объекта максимально соответствовало идеальному. Это позволяет технике «привыкать» к новым условиям эксплуатации и компенсировать негативные факторы в режиме реального времени.

Другим важным направлением является робастное управление, которое проектируется с расчетом на работу в некотором диапазоне возможных отклонений. Вместо того чтобы менять свои параметры в процессе работы, робастный регулятор изначально создается достаточно «сильным», чтобы выдерживать изменения характеристик объекта в определенных границах. Это обеспечивает высокую стабильность и гарантирует, что система не выйдет из-под контроля при резком изменении внешних условий. Главная задача инженера в данном случае — найти баланс между устойчивостью к помехам и быстродействием системы, чтобы она не стала слишком медленной.

Для того чтобы адаптация была успешной, необходимо использовать методы идентификации параметров в реальном времени. Эти алгоритмы анализируют входящие и исходящие сигналы, чтобы вычислить текущие физические свойства объекта, такие как инерционность или коэффициент усиления. На основе полученных данных система управления понимает, насколько сильно изменились условия работы, и

передает эту информацию блоку настройки. Важно обеспечить высокую точность этих вычислений, так как ошибка в определении параметров может привести к неправильной настройке и потере качества управления всем технологическим процессом.

Использование нечеткой логики позволяет настраивать регуляторы, основываясь на человеческом опыте и лингвистических правилах, а не только на строгих формулах. Такой подход эффективен для очень сложных объектов, для которых трудно составить точное математическое описание. В адаптивных нечетких системах правила управления могут меняться автоматически, подстраиваясь под текущую ситуацию. Это делает управление более «интеллектуальным» и гибким, позволяя успешно справляться с неопределенностью там, где классические математические методы оказываются бессильны из-за высокой сложности процессов.

Наличие скрытых задержек и неучтенных динамических свойств в системе создает дополнительные сложности при настройке. Если время реакции объекта меняется непредсказуемо, это может вызвать опасные колебания. Для борьбы с этим применяются специальные блоки предсказания, которые учитывают запаздывание сигналов и позволяют регулятору действовать на опережение. Исследование показывает, что правильный учет фазовых сдвигов и временных задержек является критическим фактором для обеспечения безопасности при работе высокоточных станков и автоматизированных производственных линий.

Математический аппарат функций устойчивости Ляпунова служит инструментом для проверки того, что система всегда будет возвращаться в состояние равновесия. При проектировании законов настройки инженеры стремятся доказать, что при любых изменениях параметров энергия системы будет стремиться к минимуму, а не бесконечно расти. Это гарантирует безопасность эксплуатации даже в самых тяжелых режимах работы. Современные

вычислительные методы позволяют автоматизировать этот анализ, что значительно ускоряет создание надежных регуляторов для многомерных технических комплексов со множеством взаимосвязанных параметров.

Практическое внедрение таких алгоритмов на базе промышленных контроллеров требует учета ограничений по памяти и скорости вычислений. Сложные математические операции по идентификации и адаптации должны выполняться очень быстро, чтобы не вносить дополнительных задержек в контур управления. Оптимизация программного кода и использование эффективных вычислительных схем позволяют реализовывать передовые методы настройки даже на стандартном оборудовании. Важным аспектом является также защита от накопления ошибок в алгоритмах обучения, что достигается за счет введения специальных зон нечувствительности к малым помехам.

Экономическая выгода от использования продвинутых методов настройки заключается в повышении производительности и снижении эксплуатационных расходов. Системы, которые умеют адаптироваться к изменениям, требуют гораздо меньше времени на пусконаладочные работы и повторную калибровку. Уменьшение отклонений от заданного режима работы позволяет экономить сырье, электроэнергию и снижать количество бракованной продукции. Кроме того, мягкое и точное управление продлевает срок службы дорогостоящих исполнительных механизмов, предотвращая их преждевременный износ из-за ударов или вибраций.

Заключение

В заключении отмечается, что изучение методов настройки в условиях неопределенности открывает путь к созданию полностью автономных и интеллектуальных заводов. В будущем ожидается интеграция нейронных сетей и методов машинного обучения для формирования еще более совершенных законов адаптации. Развитие этих технологий позволит создавать системы, которые не только

компенсируют изменения параметров, но и способны самостоятельно восстанавливаться после частичных отказов оборудования. Сочетание классической теории управления и современного искусственного интеллекта станет основой для нового поколения надежной и эффективной автоматики.

Список литературы

1. *Игнатов А.П.* Коллаборативные роботы в современном производстве. Москва: Машиностроение, 2024.
2. *Михайлов В.С., Петров Д.А.* Психология взаимодействия человека и робота на сборочных линиях. Санкт-Петербург: Наука, 2023.
3. *Сидоров К.М.* Технологии технического зрения для систем безопасной коллаборации // Робототехника и техническая кибернетика. 2024. № 2. С. 45–58.
4. *Уваров Е.Н.* Проектирование интерфейсов «человек-машина» в робототехнических комплексах. Екатеринбург: УрФУ, 2022.
5. *Peshkin M., Colgate J.E.* Cobots: Robots for Collaboration with Human Operators // IEEE Transactions on Robotics and Automation. 1999. Vol. 15. No. 4. P. 711–723.

ВНЕДРЕНИЕ СЕНСОРНЫХ СЕТЕЙ НА ПРОИЗВОДСТВЕ ДЛЯ СОЗДАНИЯ ГИБКИХ И САМООРГАНИЗУЮЩИХСЯ АВТОМАТИЗИРОВАННЫХ ЛИНИЙ

Джелилова Г.[1], Атаева Г.А.[2], Азадова Г.А.[3]

[1]Джелилова Гулнар – преподаватель;
[2]Атаева Гулджерен Алламырадовна – студент,
[3]Азадова Гулдессе Азадовна – студент,
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *данное исследование посвящено анализу архитектуры и практического применения беспроводных*

сенсорных сетей в качестве фундаментального элемента гибких и самоорганизующихся автоматизированных линий на современном производстве. В работе рассматриваются механизмы динамической перенастройки производственных процессов на базе интеллектуальных датчиков, обеспечивающих децентрализованное управление и высокую адаптивность к изменяющимся технологическим задачам в рамках концепции «Индустрии 4.0». Особое внимание уделяется методам интеграции сенсорных данных в системы принятия решений для минимизации простоев и оптимизации энергопотребления промышленного оборудования. Автор исследует влияние распределенных сетей на повышение отказоустойчивости систем и общую эффективность производственных циклов. В заключении формулируются рекомендации по внедрению масштабируемых протоколов связи для создания высокотехнологичных и автономных «умных заводов».
Ключевые слова: *сенсорные сети, самоорганизация, промышленная автоматизация, гибкое производство, Индустрия 4.0, адаптивное управление, интернет вещей, киберфизические системы, цифровая трансформация, умный завод.*

Данное исследование направлено на анализ процессов внедрения беспроводных и проводных сенсорных сетей как фундаментального инструмента для создания адаптивных производственных систем. В работе рассматриваются механизмы построения гибких автоматизированных линий, способных к самоорганизации и динамической перенастройке в зависимости от текущих производственных задач и состояния оборудования. Особое внимание уделяется протоколам передачи данных и алгоритмам децентрализованного управления, которые обеспечивают бесперебойную связь между отдельными узлами системы в условиях промышленных помех. Автор оценивает влияние интеллектуальных сенсорных сетей на снижение эксплуатационных затрат и повышение общей эффективности производственных циклов. Итогом работы

является обоснование перехода от жестких иерархических структур к распределенным саморегулирующимся сетям в рамках концепции цифрового предприятия.

Промышленная революция 4.0 требует перехода от статичных производственных схем к динамическим структурам, способным мгновенно реагировать на изменения спроса. Сенсорные сети становятся «нервной системой» современного завода, объединяя разрозненные станки в единый интеллектуальный организм. Каждое устройство в такой сети обладает определенной долей автономности и может координировать свои действия с соседними узлами. Это позволяет создавать линии, которые самостоятельно оптимизируют нагрузку и перераспределяют задачи при выходе из строя одного из компонентов. Гибкость таких систем обеспечивает высокую выживаемость производства в условиях неопределенности.

Основой самоорганизующихся линий является распределенный сбор данных с тысяч датчиков, контролирующих физические параметры процессов. Интеллектуальные узлы сети не просто транслируют сигнал, но и проводят его первичную обработку непосредственно на месте возникновения. Это значительно снижает нагрузку на центральные серверы и уменьшает задержки в контуре управления. Масштабируемость таких сетей позволяет легко добавлять новые производственные модули без необходимости полной перепрошивки всей системы. Сенсоры автоматически обнаруживают друг друга и устанавливают связи согласно заданным протоколам взаимодействия.

Протоколы связи в промышленных сенсорных сетях должны обладать повышенной устойчивостью к электромагнитным шумам и физическим препятствиям. Использование технологий Mesh-сетей позволяет сигналам находить альтернативные пути доставки информации в случае блокировки прямого канала. Каждый датчик в такой топологии выступает не только как источник данных, но и как ретранслятор для соседних устройств. Это гарантирует

доставку критически важных команд управления даже в самой сложной цеховой среде. Энергоэффективность протоколов позволяет беспроводным датчикам работать годами без замены элементов питания.

Интеграция сенсорных сетей с исполнительными механизмами роботов создает условия для функционирования самоорганизующихся конвейеров. Роботизированные ячейки могут самостоятельно запрашивать необходимые компоненты со склада, основываясь на данных от датчиков наличия материалов. Система способна автоматически изменять последовательность технологических операций для минимизации простоев оборудования. Человек в этой схеме переходит от прямого управления к роли высокоуровневого супервизора и постановщика задач. Автоматизация становится не только полной, но и по-настоящему разумной и адаптивной.

Алгоритмы машинного обучения, внедренные в программное обеспечение сенсорных сетей, позволяют предсказывать возможные сбои на основе аномалий в данных. Постоянный мониторинг вибрации, тока и температуры двигателей дает возможность выявить предотказное состояние задолго до поломки. Информация о необходимости обслуживания автоматически передается в систему планирования ресурсов предприятия. Это исключает внезапные остановки линии и позволяет проводить технические работы в наиболее подходящие моменты времени. Точность прогнозов растет по мере накопления данных о работе оборудования в различных режимах.

Безопасность передачи данных в распределенных сетях является критическим фактором для обеспечения непрерывности бизнеса. Защита от несанкционированного доступа реализуется на уровне аппаратного шифрования и строгой аутентификации каждого нового узла. Децентрализованная природа сети делает её менее уязвимой к точечным атакам по сравнению с традиционными клиент-серверными архитектурами. Постоянное обновление

встроенного ПО (прошивок) через беспроводные каналы позволяет оперативно закрывать обнаруженные уязвимости. Информационная устойчивость становится залогом физической безопасности производственного процесса.

Визуализация данных, полученных из сенсорных сетей, помогает инженерам оперативно оценивать общую эффективность оборудования (OEE). Интерактивные панели отображают состояние каждого датчика и узла автоматизированной линии в режиме реального времени. На основе этих метрик принимаются решения о необходимости оптимизации отдельных участков или всей производственной цепочки. Использование технологий дополненной реальности позволяет техникам видеть показания скрытых датчиков прямо на корпусе оборудования. Это значительно ускоряет диагностику и сокращает время на обучение нового персонала.

Внедрение гибких линий на базе сенсорных сетей существенно сокращает время выхода новых продуктов на рынок (Time-to-Market). Перенастройка оборудования на выпуск другого типа изделий происходит программным путем без необходимости физического демонтажа узлов. Это открывает путь к массовому производству индивидуализированных заказов по стоимости стандартной продукции. Малые партии товаров становятся экономически выгодными благодаря отсутствию длительных этапов переналадки. Предприятие приобретает уникальную конкурентную способность, быстро адаптируясь к трендам и запросам потребителей.

Заключение

В заключении можно утверждать, что сенсорные сети являются фундаментом для перехода к полностью автономным фабрикам будущего. Создание самоорганизующихся линий — это не просто технологический апгрейд, а качественный скачок в методологии управления производством. Объединение физического мира машин с миром цифровой аналитики создает синергетический эффект для всей промышленности.

Дальнейшее развитие технологий будет направлено на миниатюризацию сенсоров и повышение интеллекта на периферийных устройствах. Россия имеет значительный потенциал для разработки и внедрения собственных стандартов в области промышленных сенсорных сетей.

Список литературы

1. *Игнатов А.М.* Интеллектуальные сенсорные сети в задачах промышленной автоматизации. М.: Техносфера, 2024.
2. *Леонтьев С.В.* Архитектура самоорганизующихся систем управления производством. СПб.: Политех-Пресс, 2023.
3. *Матвеев Е.Н.* Беспроводные технологии в индустриальном интернете вещей // Автоматика и телемеханика. 2024. № 4. С. 56–72.
4. *Павлов Д.К.* Методы повышения отказоустойчивости распределенных сенсорных сетей. Казань: Бук, 2022.
5. *Wang S., Wan J., Li D.* The internet of things for smart manufacturing // Engineering. 2016. Vol. 2. No. 4. P. 488–496.

РОБОТИЗИРОВАННАЯ АВТОМАТИЗАЦИЯ ПРОЦЕССОВ В ИТ-ИНФРАСТРУКТУРЕ

Кулиев Э.[1], Джумаева Г.К.[2], Кесаева Г.Ч.[3]

[1]Кулиев Эзиз – преподаватель;
[2]Джумаева Гулнара Курбандурдыевна - студент,
Кесаева Гулджерен Чарыевна – студент,
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *данное исследование посвящено анализу эффективности внедрения технологий роботизированной автоматизации процессов (RPA) в структуру управления современными ИТ-системами. В работе рассматриваются механизмы использования программных роботов для автоматизации рутинных и повторяющихся задач администрирования, таких как управление учетными*

записями, мониторинг доступности ресурсов и развертывание обновлений программного обеспечения. Особое внимание уделяется интеграции RPA с системами управления ИТ-сервисами (ITSM) для ускорения обработки заявок пользователей и снижения нагрузки на первую линию технической поддержки. Автор исследует влияние роботизации на минимизацию человеческих ошибок при выполнении критических операций и оценивает экономическую эффективность замены ручного труда цифровыми сотрудниками. В заключении формулируются рекомендации по масштабированию RPA-решений для создания гибкой и высокопроизводительной ИТ-инфраструктуры, способной к быстрой адаптации под запросы бизнеса.
Ключевые слова: *роботизированная автоматизация процессов, RPA, ИТ-инфраструктура, цифровая трансформация, автоматизация администрирования, ITSM, программные роботы, оптимизация ресурсов, управление сервисами, эффективность ИТ.*

Роботизированная автоматизация процессов (RPA) в ИТ-инфраструктуре представляет собой технологию использования программных роботов для имитации действий человека при работе с различными интерфейсами. В отличие от традиционной автоматизации через скрипты, RPA взаимодействует с приложениями на уровне пользовательского интерфейса, что позволяет объединять разрозненные системы без изменения их исходного кода. Это решение становится критически важным для компаний, использующих устаревшее программное обеспечение (Legacy), которое не поддерживает современные протоколы интеграции API. Программные роботы способны выполнять задачи по расписанию или по триггеру, обеспечивая непрерывность сервисных процессов в режиме 24/7. Роботизация освобождает квалифицированных системных инженеров от монотонной работы, позволяя им сосредоточиться на стратегическом развитии ИТ-ландшафта.

Внедрение RPA в процессы системного администрирования значительно повышает скорость и точность управления учетными записями пользователей. Роботы автоматически обрабатывают запросы на создание новых профилей, сброс паролей и изменение прав доступа в различных корпоративных справочниках. Это исключает задержки, вызванные человеческим фактором, и гарантирует соблюдение политик безопасности при каждом изменении. Синхронизация данных между кадровыми системами и Active Directory происходит мгновенно, что особенно важно при массовом приеме или увольнении сотрудников. Автоматизированный контроль доступа снижает риски несанкционированного проникновения в систему из-за несвоевременно удаленных учетных записей.

Мониторинг доступности ресурсов и первичная диагностика инцидентов являются идеальными сценариями для применения роботизированных помощников. Программный робот может непрерывно проверять работоспособность критических сервисов и при обнаружении сбоя выполнять базовые сценарии восстановления, такие как перезагрузка службы. Если стандартные методы не помогают, робот автоматически собирает логи и передает структурированный отчет профильному специалисту второй линии поддержки. Это позволяет сократить время восстановления сервисов (MTTR) и минимизировать негативное влияние инцидентов на бизнес-пользователей. Интеллектуальный мониторинг превращает реактивную модель поддержки в проактивную систему управления надежностью.

Управление конфигурациями и развертывание обновлений программного обеспечения с помощью RPA обеспечивает идентичность настроек на сотнях серверов одновременно. Роботы последовательно выполняют команды установки, проверяют зависимости и фиксируют результаты в журналах аудита без риска пропустить важный шаг. Это решение позволяет автоматизировать рутинные задачи патч-менеджмента, которые часто откладываются из-за высокой

трудоемкости. Программная автоматизация гарантирует, что все узлы инфраструктуры находятся в актуальном состоянии и соответствуют стандартам безопасности. Точность выполнения операций роботами исключает появление «дрейфа конфигураций», который часто становится причиной трудноуловимых ошибок.

Интеграция RPA с системами управления ИТ-сервисами (ITSM) позволяет полностью автоматизировать жизненный цикл типовых заявок от момента поступления до закрытия. Робот анализирует содержание тикета, классифицирует его и выполняет необходимые действия в соответствующих ИТ-системах без участия диспетчера. После завершения задачи бот информирует пользователя об успешном выполнении и закрывает заявку в системе учета. Такой подход разгружает службу Service Desk на 30–50%, позволяя персоналу заниматься более сложными и творческими задачами. Скорость обработки запросов при этом увеличивается в десятки раз, что напрямую влияет на лояльность сотрудников компании.

Роботизация процессов резервного копирования и восстановления данных обеспечивает дополнительный уровень гарантии сохранности корпоративной информации. Роботы могут автоматически проверять целостность созданных архивов и проводить регулярные тестовые восстановления в изолированных средах. В случае обнаружения поврежденного бэкапа система немедленно инициирует повторное копирование и уведомляет администратора о потенциальной проблеме. Автоматизация отчетности по состоянию хранилищ данных делает процесс управления бэкапами прозрачным и легко проверяемым в ходе аудитов. Это минимизирует вероятность потери данных при реальных авариях из-за незамеченных вовремя ошибок копирования.

[Image showing the comparison between manual IT administration steps and a streamlined RPA-driven process]

Масштабируемость ИТ-инфраструктуры в облачных средах требует динамического управления мощностями,

которое эффективно реализуется через RPA-сценарии. Роботы могут отслеживать нагрузку на веб-серверы и автоматически развертывать дополнительные экземпляры в часы пик, а затем сворачивать их для экономии бюджета. Такой «автоскейлинг» на базе роботов позволяет учитывать сложные условия, которые сложно настроить стандартными облачными инструментами. Программные роботы управляют квотами ресурсов и оповещают владельцев систем о необходимости оптимизации затрат. Это делает использование облачной инфраструктуры более рациональным и предсказуемым для финансового департамента.

Обеспечение информационной безопасности выигрывает от внедрения RPA за счет автоматизации процессов сканирования уязвимостей и управления сертификатами. Роботы могут ежедневно проверять тысячи узлов на соответствие требованиям безопасности и автоматически блокировать подозрительные порты или соединения. Процесс обновления SSL-сертификатов, который часто приводит к простоям при ручном управлении, полностью делегируется ботам, отслеживающим сроки действия. Роботизированный аудит журналов безопасности позволяет выявлять аномалии в поведении пользователей, которые могут указывать на кибератаку. Скорость реакции робота на угрозу значительно превышает возможности человека, что критично для предотвращения утечек данных.

Заключение

В заключении следует отметить, что роботизированная автоматизация является неизбежным этапом эволюции современных ИТ-департаментов к модели «Инфраструктура как код» (IaC). В будущем ожидается синергия RPA с искусственным интеллектом, что приведет к появлению самозалечивающихся (Self-healing) систем управления. Программные роботы станут более умными, способными принимать решения в ситуациях с высокой степенью неопределенности на основе накопленного опыта.

Список литературы

1. *Иванов С.С.* Роботизация бизнес-процессов и ИТ-инфраструктуры: учебное пособие. Москва: Альпина Паблишер, 2024.
2. *Козлов Д.В.* Технологии RPA в управлении корпоративными сервисами. Санкт-Петербург: Питер, 2023.
3. *Мартынов А.А., Петров В.В.* Оценка эффективности внедрения RPA-ботов в ИТ-департаментах // Вестник цифровой экономики. 2024. № 4. С. 12–25.
4. *Сидоров К.М.* Автоматизация системного администрирования на базе интеллектуальных роботов. Екатеринбург: УрФУ, 2022.
5. *Taulli T.* The Robotic Process Automation Handbook: A Guide to Implementing RPA Systems. New York: Apress, 2020.

ТЕХНОЛОГИИ ВИРТУАЛЬНОЙ И ДОПОЛНЕННОЙ РЕАЛЬНОСТИ В ПРОМЫШЛЕННОЙ АВТОМАТИЗАЦИИ

Кулыева Б.[1], Ходжамырадов М.М.[2], Гурбандурдыева О.М.[3]

[1]Кулыева Багты – преподаватель;
[2]Ходжамырадов Мухаммедалы Мерданович - студент,
[3]Гурбандурдыева Огулшат Мейлисовна – студент,
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *данное исследование посвящено анализу применения технологий виртуальной и дополненной реальности как инструментов повышения эффективности процессов промышленной автоматизации. В работе рассматриваются способы интеграции цифровых двойников*

производственных линий с визуальными интерфейсами, позволяющими персоналу взаимодействовать с оборудованием в интерактивном режиме. Особое внимание уделяется сценариям удаленного обслуживания, где дополненная реальность обеспечивает наложение сервисных инструкций на реальные объекты, и обучению операторов в безопасных симуляционных средах. Автор исследует влияние иммерсивных технологий на сокращение времени пусконаладочных работ, снижение количества ошибок при сборке сложных узлов и минимизацию простоев оборудования. В заключении формулируются технические требования к аппаратным средствам и программным платформам для успешного внедрения виртуальных инструментов в контур управления современным цифровым предприятием.
Ключевые слова: *виртуальная реальность, дополненная реальность, промышленная автоматизация, цифровой двойник, удаленное обслуживание, обучение персонала, человеко-машинный интерфейс, визуализация данных, интеллектуальное производство, техническое зрение.*

Технологии виртуальной и дополненной реальности становятся важным звеном в развитии концепции цифрового производства, обеспечивая наглядную связь между виртуальными данными и физическим оборудованием. Виртуальная реальность позволяет создавать точные копии цехов и производственных площадок еще до момента их строительства, что дает возможность инженерам оптимизировать расположение станков и логистических путей. В таких средах можно проводить виртуальную пусконаладочную работу, выявляя ошибки в алгоритмах управления и механические коллизии в безопасном цифровом пространстве. Это значительно ускоряет ввод реальных систем в эксплуатацию и снижает риски поломок дорогостоящей техники на начальных этапах.

Дополненная реальность находит широкое применение непосредственно на рабочих местах, предоставляя операторам актуальную информацию без необходимости

отвлекаться на бумажные инструкции или экраны мониторов. С помощью специальных очков или мобильных устройств важные показатели — такие как температура, давление или текущая скорость вращения валов — накладываются прямо на корпус соответствующего агрегата. Это превращает обычное зрение специалиста в мощный инструмент мониторинга, позволяющий мгновенно замечать отклонения от нормы. Интеграция дополненной реальности с датчиками систем автоматизации создает новый уровень ситуационной осведомленности персонала на сложных объектах.

Удаленное техническое обслуживание на базе дополненной реальности позволяет квалифицированным экспертам консультировать ремонтные бригады на местах, находясь за тысячи километров от объекта. С помощью функции «видеть то, что вижу я», эксперт может рисовать графические подсказки и метки в поле зрения рабочего, указывая, какие именно детали нужно заменить или какие задвижки повернуть. Это радикально снижает затраты компаний на командировки и сокращает время простоя оборудования в случае критических сбоев. Информация передается в режиме реального времени через защищенные каналы связи, что обеспечивает оперативность и конфиденциальность проводимых работ.

Обучение персонала в виртуальной реальности становится стандартом для опасных и высокотехнологичных производств, где цена ошибки крайне велика. В виртуальных тренажерах сотрудники могут многократно отрабатывать последовательность действий при возникновении пожара, утечки газа или аварийного отключения систем. Программное обеспечение фиксирует каждое движение ученика, анализирует скорость реакции и правильность принимаемых решений, формируя детальный отчет о готовности специалиста к самостоятельной работе. Такой подход полностью исключает риск травматизма в процессе обучения и позволяет готовить кадры для работы на уникальном оборудовании без остановки основного производственного процесса.

Концепция цифровых двойников получает новое измерение благодаря визуализации через средства виртуальной реальности, позволяя анализировать работу всего завода как единого организма. Инженеры могут «проходить» сквозь стены зданий или заглядывать внутрь закрытых механизмов, чтобы оценить состояние узлов, не разбирая их физически. Синхронизация данных между реальным объектом и его цифровой копией происходит мгновенно, что дает возможность моделировать последствия различных сценариев управления. Визуальное представление сложных потоков данных делает аналитику более доступной для понимания, помогая руководству принимать обоснованные стратегические решения.

Внедрение дополненной реальности в процессы складской логистики повышает точность и скорость комплектации заказов. Системы «выбора по лучу» (Vision Picking) подсказывают складским работникам кратчайший маршрут к нужному стеллажу и подсвечивают необходимый товар в виртуальном поле зрения. Это исключает ошибки, связанные с человеческим фактором, и освобождает руки персонала от сканеров и накладных. Автоматизация учета товаров происходит в момент их идентификации камерой очков, что обеспечивает абсолютную прозрачность складских остатков в реальном времени. Подобные технологии позволяют эффективно справляться с большими объемами заказов при ограниченном количестве персонала.

Программная архитектура для работы виртуальных интерфейсов требует высокой производительности и сверхмалых задержек при передаче данных. Даже небольшое расхождение между движениями человека и обновлением картинки в виртуальной реальности может вызвать дискомфорт и снизить эффективность работы. Использование передовых графических движков и специализированных протоколов связи позволяет достичь плавности визуализации, необходимой для профессиональных задач. Интеграция иммерсивных технологий с облачными вычислительными мощностями

дает возможность обрабатывать огромные трехмерные модели зданий и агрегатов без потери детализации.

Безопасность использования дополненной реальности в цехах требует разработки специальных эргономичных стандартов, чтобы виртуальные объекты не перекрывали реальные опасности. Проектировщики интерфейсов должны соблюдать баланс между информативностью и прозрачностью, чтобы рабочий всегда видел движущиеся части механизмов и предупреждающие знаки. Сами устройства (шлемы и очки) должны быть сертифицированы для работы в условиях повышенной запыленности, влажности и вибрации. Вопросы кибербезопасности также выходят на первый план, так как перехват управления визуальным потоком данных может привести к дезинформации персонала и созданию аварийных ситуаций.

Экономический эффект от внедрения технологий виртуальной и дополненной реальности складывается из прямой экономии времени и повышения качества производственных операций. Сокращение цикла разработки новых продуктов и ускорение подготовки кадров дают предприятиям серьезное конкурентное преимущество. Снижение вероятности брака при сборке за счет визуальных подсказок напрямую влияет на прибыльность и удовлетворенность заказчиков.

Заключение

В заключении важно отметить, что технологии виртуальной и дополненной реальности перестают быть развлечением, превращаясь в обязательный атрибут современной промышленной автоматизации. Будущее связано с развитием искусственного интеллекта, который будет автоматически распознавать объекты и генерировать нужные визуальные подсказки без участия человека. Мы движемся к созданию единого информационного пространства, где грань между физическим миром и цифровыми данными будет практически стерта.

Список литературы

1. *Андреев В.К.* Автоматизация инженерных систем современных мегаполисов. Москва: Стройиздат, 2024.
2. *Кузнецов Л.А.* Концепции и технологии Smart City: учебное пособие. Санкт-Петербург: Лань, 2023.
3. *Николаев С.П., Федоров А.И.* Интеллектуальное управление водными и энергетическими ресурсами города // Энергосбережение и водоподготовка. 2024. № 1. С. 15–28.
4. *Соколова М.В.* Системы мониторинга и безопасности умной городской среды. Екатеринбург: УрФУ, 2022.
5. *Townsend A.M.* Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia. New York: W. W. Norton & Company, 2013.

ПРОЕКТИРОВАНИЕ КОБОТОВ, СПОСОБНЫХ БЕЗОПАСНО РАБОТАТЬ СОВМЕСТНО С ПЕРСОНАЛОМ НА СБОРОЧНЫХ ПРЕДПРИЯТИЯХ

Менлиева А.[1], Халлыева М.М.[2], Халылова Г.Я.[3]

[1]Менлиева Айлар – преподаватель;
[2]Халлыева Махриджемал Мередовна - студент,
[3]Халылова Гулдане Язмуратовна – студент,
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *данное исследование рассматривает инженерные и методические аспекты проектирования коллаборативных роботов (коботов), специально предназначенных для интеграции в рабочие процессы сборочных предприятий без использования защитных физических барьеров. В работе анализируются конструктивные решения, обеспечивающие пассивную и активную безопасность: использование легких материалов, отсутствие острых углов, а также внедрение специализированных сенсоров силы, момента и емкостных датчиков приближения. Особое внимание уделяется*

разработке программных алгоритмов ограничения скорости и усилия, которые в режиме реального времени корректируют траекторию движения робота при обнаружении человека в зоне выполнения операции. Автор исследует методы интуитивного программирования и интерфейсы тактильного обучения, позволяющие персоналу быстро перенастраивать коботов под новые задачи сборки. В заключении обосновывается эффективность применения коботов для снижения травматизма на производстве и повышения операционной гибкости при выполнении мелкосерийных заказов.
Ключевые слова: *коллаборативные роботы, коботы, безопасное проектирование, сборочное производство, датчики силы, активная безопасность, интерфейс человек-машина, тактильное обучение, Индустрия 5.0, промышленная автоматизация.*

Проектирование коботов для сборочных предприятий начинается с реализации концепции «безопасности по конструкции», которая предполагает минимизацию потенциального вреда при случайном контакте. Инженеры используют сглаженные формы манипулятора, закрытые сочленения без зон защемления и энергопоглощающие покрытия. Масса подвижных частей кобота значительно ниже, чем у традиционных роботов, что снижает инерцию и позволяет мгновенно остановить механизм при столкновении. Это создает фундамент доверия между рабочим персоналом и автоматизированным помощником, позволяя им работать плечом к плечу над общими задачами. Безопасность на физическом уровне дополняется интеллектуальными системами контроля за окружающей средой.

Система активной безопасности базируется на многоуровневой сети сенсоров, встроенных в каждое сочленение робота. Датчики силы и момента (Force/Torque sensors) непрерывно измеряют внешние воздействия, позволяя коботу отличать технологическое сопротивление при сборке от случайного касания человеком. При

превышении заданного порога усилия робот переходит в режим экстренной остановки или податливости, «уходя» от контакта. Дополнительные лазерные сканеры или 3D-камеры могут формировать невидимый защитный периметр, при пересечении которого кобот автоматически замедляет движение. Такая эшелонированная защита гарантирует исключение травматизма даже в условиях высокой плотности рабочих мест на сборочном участке.

Интеграция коботов в сборочные линии требует разработки интуитивно понятных методов программирования, доступных рабочим без профильного образования в ИТ. Метод «обучения показом» (Lead-through programming) позволяет оператору вручную перемещать манипулятор по нужным точкам, фиксируя траекторию и действия захвата. Робот запоминает последовательность движений и воспроизводит их с высокой точностью, что критично для операций ввинчивания, склейки или установки компонентов. Графические интерфейсы на планшетных компьютерах позволяют визуализировать процесс и вносить корректировки в логику работы через простые блок-схемы. Это сокращает время переналадки с одного изделия на другое с дней до считанных минут.

Сборочные предприятия часто сталкиваются с проблемой вариативности деталей, что требует от коботов наличия систем технического зрения для точного позиционирования. Камеры, установленные на фланце робота, позволяют ему самостоятельно идентифицировать положение заготовки на конвейере и корректировать захват. Алгоритмы машинного обучения помогают роботу распознавать дефекты деталей на лету, выполняя функции контроля качества в процессе сборки. Это избавляет человека от необходимости монотонного визуального осмотра и гарантирует, что в готовое изделие не попадет некондиционный компонент. Коллаборация становится не просто совместным трудом, а интеллектуальным процессом взаимного дополнения навыков.

Эргономика сборочного поста при участии кобота проектируется таким образом, чтобы робот выполнял физически тяжелые или неудобные операции, а человек — задачи, требующие сложной моторики и принятия решений. Робот может удерживать массивный корпус прибора, обеспечивая оптимальный угол для монтажа внутренних плат сотрудником. Это снижает нагрузку на опорно-двигательный аппарат человека и позволяет организовать рабочее место с учетом принципов бережливого производства. Совместная работа повышает общую производительность поста, так как время такта синхронизируется между человеком и машиной. Правильное распределение ролей в паре «человек-кобот» является залогом успеха внедрения автоматизации.

Внедрение коботов позволяет сборочным предприятиям эффективно работать в условиях высокой кастомизации продукции и мелкосерийного производства. Традиционная автоматизация часто экономически неоправданна при частой смене номенклатуры изделий из-за дороговизны перенастройки оборудования. Коботы же легко перемещаются между рабочими станциями и могут быть быстро перепрофилированы с одной задачи на другую. Мобильные платформы позволяют коботам самостоятельно передвигаться по цеху, подключаясь к различным сборочным ячейкам в зависимости от текущего плана выпуска. Такая гибкость превращает производственные мощности в динамичную систему, способную мгновенно реагировать на запросы рынка.

Вопрос психологического принятия роботов персоналом является важной частью проектирования системы взаимодействия. Коботы оснащаются визуальными индикаторами состояния (световыми кольцами), которые цветом сигнализируют о текущем режиме: работа, ожидание человека или неисправность. Использование плавных, предсказуемых траекторий движения снижает уровень тревожности у сотрудников, работающих в непосредственной близости от манипулятора.

Проектировщики стремятся сделать действия робота прозрачными и понятными для окружающих, создавая эффект «коллеги», а не бездушного автомата. Обучение персонала основам безопасной работы с коботами повышает культуру производства и вовлеченность сотрудников в процессы модернизации.

Техническое обслуживание и диагностика коботов на сборочных предприятиях максимально упрощены за счет модульной конструкции и встроенных систем самодиагностики. Большинство узлов манипулятора могут быть заменены за короткое время без использования специализированного инструмента. Облачные платформы мониторинга позволяют отслеживать износ приводов и предсказывать необходимость замены смазки или компонентов до того, как произойдет отказ. Это обеспечивает высокий коэффициент технической готовности оборудования и исключает внеплановые остановки сборочных линий. Предиктивный подход к сервису в сочетании с надежностью современных коботов делает их эксплуатацию экономически прозрачной и эффективной.

Заключение

В заключении следует подчеркнуть, что проектирование коботов для безопасной работы — это междисциплинарная задача на стыке механики, электроники и когнитивной психологии. Будущее сборочных предприятий связано с созданием полностью адаптивных сред, где группы людей и роботов координируют свои действия через общие цифровые платформы. Развитие технологий мягкой робототехники и тактильной обратной связи позволит сделать контакт еще более естественным и безопасным. Мы движемся к эпохе Индустрии 5.0, где технологии возвращают человека в центр производственного процесса, усиливая его возможности мощью интеллектуальных машин. Коллаборативная робототехника станет стандартом де-факто для современной промышленности, обеспечивая гармоничное развитие техносферы.

Список литературы

1. *Беляев А.И.* Проектирование безопасных робототехнических систем: учебное пособие. Москва: Издательство МГТУ им. Н. Э. Баумана, 2024.
2. *Григорьев С.Н., Волков М.П.* Сенсорные системы в коллаборативной робототехнике. Санкт-Петербург: Политех-Пресс, 2023.
3. *Егоров В.В.* Методы ограничения усилий коботов при физическом взаимодействии с персоналом // Робототехника и техническая кибернетика. 2024. № 1. С. 32–45.
4. *Левин Д.А.* Автоматизация сборочных процессов на базе коботов. Екатеринбург: УрФУ, 2022.
5. *Haddadin S., Croft E.* Physical Human-Robot Interaction // Springer Handbook of Robotics. 2016. P. 1835–1874.

УМНОЕ УПРАВЛЕНИЕ ГОРОДСКИМ ОСВЕЩЕНИЕМ, ТРАФИКОМ И РАСПРЕДЕЛЕНИЕМ ЭНЕРГОРЕСУРСОВ НА ОСНОВЕ АНАЛИЗА БОЛЬШИХ ДАННЫХ

Мередов Ы.[1], Мамметовезова Э.Д.[2], Мырадова З.С.[3]

[1]Мередов Ымамкасым – преподаватель;
[2]Мамметовезова Эджеш Дортгулыевна – студент,
[3]Мырадова Зохре Сазакмаммедовна – студент,
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *данное исследование рассматривает возможности применения аналитики больших данных (Big Data) для создания комплексных систем управления ключевыми аспектами городской среды: уличным*

освещением, транспортными потоками и распределением энергоресурсов. В работе анализируются методы сбора и интеграции массивов данных от гетерогенных источников — сенсоров IoT, GPS-трекеров, метеорологических станций и интеллектуальных приборов учета. Особое внимание уделяется разработке прогностических моделей, позволяющих адаптировать яркость городского освещения в зависимости от присутствия людей, оптимизировать работу светофоров для снижения заторности на 30% и динамически перераспределять нагрузку в энергетических сетях (Smart Grid) для предотвращения пиковых перегрузок. Автор исследует влияние предиктивного анализа на снижение энергопотребления муниципальных объектов (до 45% в секторе освещения) и повышение общей безопасности городской инфраструктуры.
Ключевые слова: *большие данные, умный город, Smart City, интеллектуальное освещение, управление трафиком, распределение энергоресурсов, интернет вещей, предиктивная аналитика, устойчивое развитие, городская инфраструктура.*

Разработка интеллектуальных систем управления в рамках Smart City требует глубокой интеграции информационных потоков и перехода от реактивного управления к проактивному. Использование больших данных позволяет городской администрации не просто фиксировать инциденты, а предсказывать их появление, будь то пробки на дорогах или аварии в электросетях. Программные алгоритмы анализируют историческую ретроспективу и текущие показатели, создавая динамическую модель города, которая постоянно адаптируется под нужды населения. Это обеспечивает более рациональное использование бюджетных средств и природных ресурсов, минимизируя антропогенное воздействие на экологию.

Умное управление городским освещением на основе Big Data позволяет радикально снизить затраты на электроэнергию, сохраняя при этом высокий уровень

безопасности. Современные LED-светильники, объединенные в сеть, способны менять интенсивность свечения в зависимости от плотности трафика, погодных условий и даже уровня естественной освещенности. Анализ данных о перемещении граждан помогает освещать только те участки, где это необходимо в конкретный момент времени, предотвращая световое загрязнение. Внештатные ситуации, такие как неисправность ламп, фиксируются системой автоматически, что исключает необходимость регулярных обходов и ускоряет обслуживание.

Интеллектуальные транспортные системы (ИТС) используют большие данные для борьбы с заторами и повышения эффективности общественного транспорта. Данные от камер видеонаблюдения, индукционных петель и смартфонов водителей позволяют алгоритмам регулировать фазы светофоров в реальном времени, увеличивая пропускную способность магистралей. Предиктивное моделирование помогает предсказывать возникновение пробок за 15–30 минут до их появления, предлагая водителям альтернативные маршруты через навигационные приложения. Это не только экономит время горожан, но и снижает объемы вредных выбросов в атмосферу, улучшая экологическую обстановку в жилых зонах.

Распределение энергоресурсов в концепции Smart Grid опирается на анализ потребления каждой домохозяйства и промышленного объекта. Большие данные позволяют балансировать спрос и предложение, интегрируя возобновляемые источники энергии (ВИЭ) в общую сеть без риска дестабилизации. Интеллектуальные сети автоматически перенаправляют потоки электричества в случае повреждения линий, минимизируя количество отключенных потребителей. Предиктивное обслуживание трансформаторных подстанций на основе анализа вибраций и температуры помогает заменять изношенные узлы до того, как они приведут к каскадному отключению. Энергосистема города становится более гибкой и устойчивой к экстремальным нагрузкам.

Централизованные платформы управления данными (City Operating Systems) объединяют разрозненные сведения от различных ведомств в единую картину. Это позволяет выявлять неочевидные корреляции: например, как изменение графиков работы общественного транспорта влияет на потребление электроэнергии в офисных центрах. Визуализация этих данных в виде интерактивных дашбордов помогает городским планировщикам принимать обоснованные решения о развитии инфраструктуры. Прозрачность данных повышает доверие граждан к власти, так как результаты оптимизации (например, снижение аварийности) становятся наглядными и измеримыми.

Безопасность систем управления в «умном городе» является критическим аспектом, требующим использования методов защиты на основе машинного обучения. Анализ аномалий в поведении городской сети позволяет выявлять попытки кибератак на ранних стадиях, предотвращая захват контроля над светофорами или энергообъектами. Шифрование данных и сегментация критических систем минимизируют последствия возможных инцидентов. Технологии блокчейн могут быть использованы для обеспечения целостности данных и прозрачности транзакций в сфере ЖКХ. Надежность цифрового контура «умного города» напрямую определяет безопасность его физической инфраструктуры.

Экономическая эффективность Smart City проектов подтверждается сокращением муниципальных расходов на 15–20% в течение первых лет после внедрения. Оптимизация освещения и теплоснабжения дает наиболее быструю отдачу, высвобождая средства для других социальных нужд. Снижение потерь ресурсов в сетях и повышение срока службы оборудования за счет предиктивного подхода делают город более привлекательным для частных инвестиций. Цифровизация услуг повышает собираемость платежей и снижает затраты на администрирование городских сервисов. Интеллектуальное управление становится не роскошью, а

необходимым условием финансовой устойчивости современного мегаполиса.

Социальный аспект автоматизации жизнеобеспечения заключается в создании более инклюзивной и комфортной городской среды. «Умные» светофоры могут автоматически продлевать время перехода для маломобильных групп граждан, обнаруживая их с помощью сенсоров. Общественный транспорт, работающий на основе данных о реальном спросе, становится более предсказуемым и удобным. Информирование жителей о качестве воздуха и воды через мобильные приложения способствует ведению здорового образа жизни. Город начинает «заботиться» о своих жителях, подстраиваясь под их индивидуальные потребности и обеспечивая высокий уровень психологического комфорта.

Проблемы внедрения технологий Smart City связаны с необходимостью стандартизации данных и обеспечения приватности граждан. Сбор огромных массивов информации требует четкого правового регулирования, чтобы исключить злоупотребления и слежку. Инфраструктурные затраты на установку миллионов датчиков и строительство сетей связи стандарта 5G являются значительным барьером для многих регионов. Однако долгосрочные выгоды перевешивают первоначальные вложения, делая цифровую трансформацию неизбежной.

Заключение

В заключении следует отметить, что управление городом на основе анализа больших данных — это путь к созданию по-настоящему устойчивой цивилизации. Будущее отрасли связано с использованием искусственного интеллекта для полностью автономного управления городскими подсистемами в рамках «цифровых двойников» городов. Мы движемся к эпохе, когда город будет функционировать как единый организм, способный к саморегуляции и постоянному развитию. Дальнейшее развитие технологий позволит сделать «умные» решения доступными не только для столиц, но и для малых городов. Интеллектуальное

управление — это мост в безопасное и процветающее будущее для миллионов людей.

Список литературы

1. *Андреев В.К.* Автоматизация инженерных систем современных мегаполисов. Москва: Стройиздат, 2024.
2. *Кузнецов Л.А.* Концепции и технологии Smart City: учебное пособие. Санкт-Петербург: Лань, 2023.
3. *Николаев С.П., Федоров А.И.* Интеллектуальное управление водными и энергетическими ресурсами города // Энергосбережение и водоподготовка. 2024. № 1. С. 15–28.
4. *Соколова М.В.* Системы мониторинга и безопасности умной городской среды. Екатеринбург: УрФУ, 2022.
5. *Townsend A.M.* Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia. New York: W.W. Norton & Company, 2013.

ИСПОЛЬЗОВАНИЕ ПРОГРАММНЫХ РОБОТОВ ДЛЯ ВЫПОЛНЕНИЯ РУТИННЫХ ЗАДАЧ И ИНТЕГРАЦИИ РАЗЛИЧНЫХ КОРПОРАТИВНЫХ СИСТЕМ

Мырадов Р.[1], Аннаева Э.А.[2], Багтыярова Л.[3]

[1]Мырадов Ресул – преподаватель;
[2]Аннаева Энеджан Агамырадовна - студент,
[3]Багтыярова Лейла – студент,
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *данное исследование направлено на анализ эффективности внедрения программных роботов (RPA) для автоматизации трудоемких рутинных операций и бесшовной интеграции разнородных корпоративных систем. В работе рассматриваются механизмы имитации действий пользователя программными агентами, что позволяет объединять информационные потоки между устаревшим ПО и современными облачными платформами без изменения*

их исходного кода. Особое внимание уделяется сценариям миграции данных, автоматической сверке отчетов и обработке типовых клиентских запросов в многослойных ИТ-ландшафтах крупных предприятий. Автор исследует влияние роботизации на снижение частоты ошибок, связанных с человеческим фактором, и оценивает потенциал высвобождения кадровых ресурсов для решения интеллектуальных и стратегических задач. В заключении формулируются принципы построения масштабируемой экосистемы цифровых сотрудников, способствующей повышению операционной гибкости и ускорению циклов обработки бизнес-информации.
Ключевые слова: *программные роботы, RPA, корпоративные системы, интеграция данных, рутинные задачи, автоматизация процессов, цифровая трансформация, операционная эффективность, бизнес-аналитика, программная инженерия.*

Технология программной роботизации (RPA) выступает ключевым инструментом цифровой трансформации, позволяя делегировать алгоритмам выполнение монотонных и часто повторяющихся бизнес-операций. Программные роботы имитируют действия человека в интерфейсах приложений, выполняя ввод данных, нажатие кнопок и перенос информации между окнами с абсолютной точностью. Это решение позволяет предприятиям оптимизировать временные затраты на такие задачи, как ввод первичной документации, формирование стандартных отчетов или сверка реестров. Внедрение цифровых сотрудников устраняет проблему «бутылочного горлышка» в административных процессах, где ручной труд традиционно замедлял общую скорость работы. Благодаря круглосуточному режиму функционирования роботы обеспечивают непрерывность бизнес-циклов вне зависимости от рабочего графика персонала.

Одной из наиболее востребованных функций программных роботов является бесшовная интеграция различных корпоративных систем в единое информационное

пространство. Зачастую крупные компании сталкиваются с проблемой разобщенности данных, когда информация заблокирована внутри старых Legacy-приложений, не имеющих современных интерфейсов связи (API). Роботы решают эту проблему, выступая связующим звеном, которое считывает данные из одной системы и переносит их в другую на уровне пользовательского интерфейса. Это избавляет организацию от необходимости инвестировать огромные средства в переписывание кода старых систем или покупку дорогостоящих интеграционных шин. Такой метод интеграции значительно дешевле и быстрее в реализации, что позволяет получить первые результаты уже через несколько недель после старта проекта.

Автоматизация рутинных задач в бухгалтерии и финансовом департаменте позволяет радикально снизить количество ошибок, вызванных невнимательностью или усталостью сотрудников. Роботы успешно справляются с проверкой контрагентов, автоматическим распределением платежей по счетам и формированием налоговой отчетности на основе данных из нескольких источников. При обнаружении расхождений система немедленно уведомляет ответственного специалиста, исключая возможность пропуска критической ошибки. Точность выполнения операций в финансовых процессах напрямую влияет на прозрачность отчетности и снижает риски наложения штрафов со стороны регуляторов. Высвобождение бухгалтеров от рутины позволяет им сосредоточиться на более глубоком анализе финансовой устойчивости предприятия.

В области управления персоналом программные роботы берут на себя весь цикл документального сопровождения сотрудников от момента найма до увольнения. Бот может автоматически собирать данные из присланных резюме, создавать учетные записи в корпоративных системах, формировать трудовые договоры и заказывать оборудование для нового специалиста. Это существенно сокращает период адаптации новичков и разгружает HR-менеджеров для

работы над корпоративной культурой и обучением персонала. Аналогично процессы увольнения или перевода сотрудников на другие должности обрабатываются роботами мгновенно, гарантируя своевременное обновление прав доступа и корректность начисления выплат. Роботизация делает взаимодействие сотрудника с кадровой службой быстрым, понятным и технологичным.

Службы технической и клиентской поддержки используют RPA для автоматической классификации и маршрутизации входящих обращений. Программный робот способен анализировать текст запроса, выявлять его суть и самостоятельно выполнять типовые действия, такие как разблокировка учетной записи или отправка статуса заказа. Если запрос требует участия человека, робот подготавливает всю необходимую контекстную информацию, избавляя оператора от поиска данных в разных базах. Это сокращает среднее время ответа и повышает удовлетворенность клиентов за счет мгновенной реакции на их проблемы. Роботы также могут проактивно информировать пользователей о плановых работах или изменениях в сервисе, снижая нагрузку на контакт-центр в пиковые часы.

Процессы закупок и управления цепочками поставок значительно ускоряются благодаря автоматическому мониторингу цен и наличия товаров у поставщиков. Роботы могут ежедневно парсить сайты партнеров, сравнивать предложения и автоматически формировать заказы при достижении критического остатка на складе. Это гарантирует бесперебойность производственных процессов и позволяет закупать материалы по наиболее выгодным ценам. В интеграции с ERP-системами роботы отслеживают статусы отгрузок и автоматически обновляют сроки поступления товаров в графиках производства. Такой уровень автоматизации минимизирует складские издержки и повышает общую эффективность управления товарными запасами.

[Image showing comparison between a manual data entry process and a robotized data migration workflow]

Безопасность данных при использовании RPA обеспечивается за счет строгого логирования каждого действия программного робота. В отличие от человека, робот не может передать данные третьим лицам или использовать информацию в личных целях, так как действует строго в рамках заданного алгоритма. Все учетные записи, используемые ботами, надежно защищены в специализированных хранилищах учетных данных (Vaults). Это позволяет проводить детальный аудит всех операций и точно восстанавливать последовательность действий в случае возникновения инцидентов. Использование роботов для работы с конфиденциальной информацией повышает уровень комплаенса и снижает риски инсайдерских утечек.

Масштабируемость роботизированных решений позволяет компаниям гибко реагировать на сезонные всплески активности без расширения штата. В периоды отчетности или массовых распродаж можно мгновенно запустить дополнительных виртуальных сотрудников, распределив нагрузку на облачные мощности. После спада активности лишние боты отключаются, что позволяет оптимизировать затраты на лицензии и вычислительные ресурсы. Такая эластичность бизнес-процессов делает компанию более устойчивой к рыночным колебаниям и агрессивным изменениям внешней среды. Руководство получает возможность управлять производительностью бэк-офиса так же эффективно, как и производственными мощностями.

Заключение

В заключении важно отметить, что будущее корпоративной автоматизации лежит в синергии RPA и искусственного интеллекта, что порождает концепцию интеллектуальной автоматизации (IA). Роботы будут не просто повторять действия, но и принимать решения на основе анализа неструктурированных данных, таких как сканы документов, изображения и голосовые сообщения. Постепенно компании придут к созданию полноценных цифровых экосистем, где роботы будут координировать действия друг друга для достижения общих бизнес-целей.

Список литературы

1. *Беляев С.А.* Роботизация корпоративных процессов: от теории к практике. М.: Инфра-М, 2024.
2. *Зайцев Д.К.* Методы бесшовной интеграции информационных систем на базе RPA-технологий. СПб.: Наука и техника, 2023.
3. *Королев М.В.* Автоматизация рутинных операций в ERP-системах с использованием программных ботов // Прикладная информатика. 2024. № 2. С. 18–31.
4. *Морозов П.А.* Цифровые сотрудники в современной ИТ-инфраструктуре. Екатеринбург: УрФУ, 2022.
5. *Willcocks L.P., Lacity M.C.* Service Automation, Robots and the Future of Work. Warwickshire: SB Publishing, 2016.

ПЕРИФЕРИЙНЫЕ ВЫЧИСЛЕНИЯ ДЛЯ СИСТЕМ РЕАЛЬНОГО ВРЕМЕНИ

Пирлиев К.[1], Азадов А.А.[2], Байрамова А.М.[3]

[1]Пирлиев Кувват – преподаватель;
[2]Азадов Акмухаммет Азадович - студент,
[3]Байрамова Айлар Мергеновна – студент,
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *данное исследование посвящено анализу архитектуры и преимуществ периферийных вычислений (Edge Computing) в контексте функционирования высоконагруженных систем реального времени. В работе рассматриваются механизмы децентрализованной обработки данных непосредственно в местах их возникновения, что позволяет радикально снизить задержки передачи сигналов и разгрузить центральные облачные хранилища. Особое внимание уделяется вопросам обеспечения детерминированности временных интервалов обработки информации, необходимых для стабильной*

работы критически важных приложений в области автономного транспорта, промышленной робототехники и смарт-энергетики. Автор исследует подходы к оптимизации алгоритмов машинного обучения для работы на устройствах с ограниченными вычислительными ресурсами и оценивает стратегии повышения кибербезопасности за счет локализации потоков данных. В заключении обосновывается роль периферийных вычислений как фундаментального элемента для реализации концепции Индустрии 4.0 и создания отказоустойчивых интеллектуальных экосистем.
Ключевые слова: *периферийные вычисления, системы реального времени, Edge Computing, задержка данных, промышленный интернет вещей, децентрализация, обработка данных, Индустрия 4.0, облачные технологии, киберфизические системы.*

Периферийные вычисления представляют собой парадигму децентрализованной обработки данных, при которой вычислительные ресурсы располагаются максимально близко к источникам информации — датчикам, контроллерам и исполнительным механизмам. В отличие от традиционной облачной модели, требующей передачи огромных массивов данных на удаленные серверы, Edge Computing позволяет анализировать сигналы локально. Это критически важно для систем реального времени, где время отклика должно измеряться миллисекундами, чтобы гарантировать стабильность технологических процессов. Использование периферийных узлов исключает зависимость от пропускной способности магистральных каналов связи и минимизирует риски, связанные с задержками в глобальной сети. Такая архитектура становится фундаментом для построения быстрых и отзывчивых цифровых экосистем.

Основным драйвером внедрения периферийных вычислений является необходимость обеспечения жесткой детерминированности временных интервалов в управлении сложными техническими объектами. В автономном транспорте или высокоскоростной робототехнике задержка в

несколько сотых секунды может привести к потере управления или аварии. Локальная обработка данных позволяет системе мгновенно принимать решения на основе анализа окружающей обстановки, не дожидаясь ответа от центрального дата-центра. Периферийные шлюзы выполняют первичную фильтрацию и агрегацию данных, отправляя в облако только важную итоговую информацию для долгосрочного хранения и глубокого анализа. Это превращает систему автоматизации в иерархическую структуру, где оперативные задачи решаются на месте, а стратегические — централизованно.

Использование Edge Computing существенно повышает кибербезопасность и конфиденциальность промышленных данных за счет локализации информационных потоков. Информация о критических параметрах работы предприятия не покидает защищенный периметр объекта, что снижает риск перехвата данных в процессе их передачи по публичным сетям. Локальные вычислители могут выполнять функции криптографической защиты и аутентификации устройств непосредственно в точке подключения. В случае массированной кибератаки на центральные серверы или потери связи с внешним миром, периферийные узлы продолжают поддерживать функционирование объекта в автономном режиме. Таким образом, децентрализация вычислений становится важным элементом обеспечения живучести критически важной инфраструктуры.

Оптимизация алгоритмов машинного обучения для работы на периферийных устройствах с ограниченными ресурсами является одной из главных задач современной инженерии. Использование методов квантования и дистилляции нейронных сетей позволяет запускать сложные модели распознавания образов и детекции аномалий на компактных микропроцессорах. Это дает возможность внедрять интеллектуальные функции непосредственно в камеры видеонаблюдения, датчики вибрации или системы управления электроприводами. Интеллектуальные периферийные устройства способны самостоятельно

обучаться на локальных данных, адаптируясь к уникальным особенностям конкретного оборудования. Такая «умная» периферия значительно снижает требования к серверным мощностям и сокращает операционные расходы предприятия.

В энергетическом секторе периферийные вычисления играют ключевую роль в управлении микросетями (Microgrids) и возобновляемыми источниками энергии. Интеллектуальные контроллеры на местах способны мгновенно балансировать нагрузку и генерацию, предотвращая перегрузки в сети без участия центрального диспетчера. Это особенно важно при интеграции солнечных панелей и ветрогенераторов, выработка энергии которыми сильно зависит от переменчивых погодных условий. Edge-узлы обеспечивают предиктивную диагностику трансформаторного оборудования, выявляя предаварийные состояния на ранних стадиях. Децентрализованное управление делает энергетическую систему более гибкой, надежной и эффективной в условиях динамично меняющегося спроса.

Применение периферийных вычислений в концепции «умного города» позволяет эффективно управлять трафиком и общественной безопасностью в режиме реального времени. Светофорные объекты, оснащенные Edge-контроллерами, могут анализировать плотность транспортных потоков и корректировать фазы движения для минимизации заторов. Видеоаналитика на борту камер позволяет мгновенно обнаруживать дорожно-транспортные происшествия или оставленные предметы, передавая сигнал экстренным службам без задержек на передачу видеопотока в ЦОД. Локальная обработка данных в городских системах освещения и управления отходами помогает рационально использовать ресурсы и снижать нагрузку на экологию. Городская среда становится более предсказуемой и комфортной для граждан за счет распределенного интеллекта.

В области телемедицины периферийные вычисления обеспечивают надежную работу носимых устройств мониторинга состояния пациентов и хирургических роботов. Для проведения удаленных операций требуется сверхнизкая задержка передачи тактильной и визуальной информации, что достижимо только при размещении вычислительных мощностей в непосредственной близости от операционной. Персональные гаджеты могут самостоятельно анализировать показатели ЭКГ или уровень сахара в крови, немедленно оповещая врача при критических отклонениях. Это позволяет спасать жизни в ситуациях, когда каждая секунда имеет значение, и связь с облаком может быть нестабильной. Использование Edge Computing в медицине делает высокотехнологичную помощь более доступной и оперативной.

Аппаратная база для периферийных вычислений активно развивается в сторону создания, специализированных ИИ-ускорителей и нейроморфных процессоров. Новые чипы обладают высокой производительностью на ватт, что позволяет встраивать их в мобильные платформы и устройства с батарейным питанием. Развитие стандартов связи 5G и 6G дополняет архитектуру Edge Computing, обеспечивая высокоскоростные каналы взаимодействия между периферийными узлами. Программные платформы для управления Edge-инфраструктурой позволяют централизованно обновлять модели и конфигурации на тысячах удаленных устройств.

Заключение

В заключении следует отметить, что периферийные вычисления являются не альтернативой, а необходимым дополнением к облачным технологиям, формируя континуум вычислений. Будущее систем реального времени связано с бесшовной интеграцией Edge-устройств в глобальные цифровые платформы для создания гибридных моделей управления. Развитие технологий федеративного обучения позволит устройствам обмениваться опытом, не передавая

при этом сами данные, что выведет безопасность на новый уровень.

Список литературы

1. *Васильев П.А.* Архитектура и алгоритмы периферийных вычислений. М.: Горячая линия — Телеком, 2024.
2. *Кузнецов С.И.* Системы реального времени: от централизованных к распределенным моделям. СПб.: БХВ-Петербург, 2023.
3. *Николаев Д.В., Семенов К.А.* Оптимизация задержек в Edge-инфраструктурах промышленного назначения // Информационные технологии. 2024. № 6. С. 22–35.
4. *Степанов М.А.* Сетевые технологии для интернета вещей и периферийной обработки. Екатеринбург: УрФУ, 2022.
5. *Buyya R., Srirama S.N.* Fog and Edge Computing: Principles and Paradigms. Hoboken: Wiley, 2019.

ИЗУЧЕНИЕ АРХИТЕКТУРЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ОБЕСПЕЧИВАЮЩЕГО ГАРАНТИРОВАННОЕ ВРЕМЯ ОТКЛИКА В СИСТЕМАХ УПРАВЛЕНИЯ

Ремезанов И.[1], Аннагулыева Г.М.[2], Аннаджанова Я.Б.[3]

[1]Ремезанов Иляс – преподаватель;
[2]Аннагулыева Гулзада Мекан гызы – студент,
[3]Аннаджанова Язджемал Балмырадовна – студент,
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *данное исследование направлено на комплексный анализ архитектурных паттернов и программных механизмов, обеспечивающих детерминированное поведение и гарантированное время отклика в автоматизированных системах управления. В работе рассматриваются структурные компоненты программного обеспечения, ответственные за соблюдение*

жестких временных ограничений, включая специализированные ядра операционных систем и драйверы устройств с малым временем латентности. Особое внимание уделяется методам формального анализа временных параметров (WCET — Worst-Case Execution Time) и стратегиям планирования потоков, минимизирующим дрожание фазы (jitter) при выполнении циклических задач управления. Автор исследует влияние различных топологий межпроцессного взаимодействия на общую реактивность системы и предлагает подходы к проектированию отказоустойчивых программных слоев. В заключении обосновывается необходимость интеграции методов верификации временных характеристик на всех этапах жизненного цикла разработки ПО для критически важных промышленных объектов.
Ключевые слова: *архитектура программного обеспечения, системы управления, время отклика, детерминированность, реальное время, планирование задач, время выполнения в худшем случае, латентность, встраиваемое ПО, верификация систем.*

Проектирование программной архитектуры для систем с гарантированным временем отклика требует коренного пересмотра подходов, используемых в классической разработке. В таких системах архитектура должна быть подчинена принципу предсказуемости: каждый слой — от аппаратных абстракций до прикладных алгоритмов — обязан работать за фиксированное число тактов процессора. Это исключает использование механизмов, вносящих неопределенность, таких как динамическое выделение памяти в критических секциях или неконтролируемая сборка мусора. Основная задача архитектора заключается в создании структуры, которая сохраняет устойчивость и предсказуемость даже при пиковых нагрузках на вычислительный узел.

Центральным элементом архитектуры является уровень управления прерываниями и системный планировщик, которые определяют логику переключения контекста. Для

обеспечения гарантий отклика применяются алгоритмы планирования с фиксированными приоритетами или динамическим назначением сроков завершения (Earliest Deadline First). Архитектура строится таким образом, чтобы минимизировать время нахождения системы в критических секциях, где прерывания запрещены. Это позволяет достичь «жесткого» реального времени, когда пропуск установленного дедлайна эквивалентен полному отказу системы.

Разделение программных компонентов на критические и некритические уровни позволяет изолировать процессы управления от фоновых задач, таких как логирование или передача данных по сети. Использование архитектурного паттерна «песочницы» или виртуализации на базе гипервизоров реального времени гарантирует, что сбой в модуле визуализации не повлияет на работу контура регулирования. Межпроцессное взаимодействие (IPC) в таких системах должно быть синхронным и обладать предсказуемыми задержками. Это достигается за счет использования разделяемой памяти с механизмами безблокировочной синхронизации (lock-free), что исключает возможность взаимных блокировок.

Оценка времени выполнения в худшем случае (WCET) является неотъемлемой частью процесса проектирования архитектуры. Анализируется каждый путь исполнения кода, учитывая влияние кэш-памяти, конвейеров процессора и задержек при доступе к шине данных. Архитектурные решения часто включают в себя запрет на использование сложных ветвлений и рекурсий, которые затрудняют статический анализ времени выполнения. Программное обеспечение проектируется как набор периодических задач с жестко заданными временными окнами (time slots), что позволяет математически доказать отсутствие конфликтов ресурсов на этапе разработки.

На уровне драйверов и аппаратных абстракций (HAL) архитектура должна обеспечивать прямой и быстрый доступ к периферийным устройствам. Использование механизмов

прямого доступа к памяти (DMA) позволяет разгрузить центральный процессор и минимизировать задержки при вводе-выводе данных. Программная модель взаимодействия с оборудованием строится на событийной основе, где каждое прерывание обрабатывается минимально необходимым кодом, делегируя сложную обработку задачам с соответствующим приоритетом. Это предотвращает «голодание» менее приоритетных, но все еще важных системных процессов.

Сетевая архитектура систем управления реального времени требует использования специализированных протоколов, таких как EtherCAT или PROFINET IRT, которые гарантируют доставку пакетов в заданные микросекунды. Программный стек сетевого взаимодействия должен быть полностью интегрирован с планировщиком операционной системы для синхронизации времени выполнения задач на разных узлах распределенной системы. Это позволяет реализовывать распределенные контуры управления, где задержка передачи данных по сети становится частью общего расчетного бюджета времени. Синхронизация времени по стандарту IEEE 1588 обеспечивает единую временную шкалу для всех компонентов архитектуры.

Обеспечение отказоустойчивости на архитектурном уровне предполагает внедрение механизмов временной и избыточной надежности. Примером может служить архитектура «основной-резервный», где резервный вычислитель постоянно синхронизирует свое состояние с основным и готов перехватить управление в течение одного цикла регулирования. Программное обеспечение должно содержать встроенные средства контроля времени выполнения (watchdog timers), которые переводят систему в безопасное состояние при обнаружении зависания или недопустимой задержки. Такая «защита от дурака» на уровне кода является обязательным требованием для систем, управляющих потенциально опасными объектами.

Психология проектирования систем реального времени требует от разработчика перехода от событийного мышления к циклическому. Архитектура часто строится вокруг «большого цикла» управления, внутри которого распределяются кванты времени для различных подсистем. Это делает поведение системы полностью прозрачным и легким для тестирования, так как состояние программы в любой момент времени можно точно спрогнозировать. Использование модельно-ориентированного проектирования (MBSE) позволяет генерировать программный код из проверенных архитектурных схем, что снижает вероятность внесения человеческих ошибок в критически важные модули.

Экономическая составляющая разработки специализированной архитектуры связана с высокими затратами на этап верификации и валидации. Однако отсутствие гарантированного времени отклика в промышленных системах может привести к браку продукции или поломке оборудования, чья стоимость кратно превышает затраты на качественное проектирование. Архитектура с четкими временными гарантиями упрощает модернизацию системы в будущем, так как границы применимости каждого модуля четко определены и задокументированы. Инвестиции в надежное программное ядро окупаются за счет стабильности технологического процесса и предсказуемости поведения системы в нештатных ситуациях.

Заключение

В заключении следует отметить, что изучение архитектуры ПО для систем реального времени является фундаментом для развития современной робототехники и беспилотного транспорта. Будущее отрасли связано с созданием адаптивных архитектур, способных динамически перераспределять гарантии отклика в зависимости от контекста задачи без потери детерминированности. Дальнейшие исследования будут направлены на автоматизацию доказательства временной корректности сложных многоядерных систем. Программная архитектура перестает быть просто структурой кода, превращаясь в

математически выверенную среду обитания интеллектуальных алгоритмов управления.

Список литературы

1. *Иванов Р.Д.* Оптимизация вычислительных процессов в распределенных системах автоматики. Москва: Техносфера, 2024.
2. *Карпов С.В.* Гибридные облачные технологии для промышленного интернета вещей. Санкт-Петербург: Лань, 2023.
3. *Лебедев А.Н., Попов М.Ю.* Анализ задержек в иерархических структурах управления реального времени // Прикладная информатика. 2024. № 3. С. 40–55.
4. *Федоров В.А.* Архитектуры Edge-Cloud систем для автоматизации производства. Екатеринбург: УрФУ, 2022.
5. *Shi W., Cao J., Zhang Q.* Edge Computing: A Survey // IEEE Internet of Things Journal. 2016. Vol. 3. No. 5. P. 637–646.

ИСПОЛЬЗОВАНИЕ АЛГОРИТМОВ ИИ ДЛЯ АВТОМАТИЧЕСКОГО СОЗДАНИЯ ТЫСЯЧ ВАРИАНТОВ ПЛАНИРОВОК ЗДАНИЙ НА ОСНОВЕ ЗАДАННЫХ ПАРАМЕТРОВ: ОСВЕЩЕННОСТИ, ЭНЕРГОЭФФЕКТИВНОСТИ И СТОИМОСТИ МАТЕРИАЛОВ

Сарыев М.Б.

Сарыев Медет Бабаевич – преподаватель;
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *данное исследование рассматривает применение алгоритмов искусственного интеллекта и генеративного дизайна для автоматизации процесса архитектурного проектирования и создания тысяч вариативных планировок зданий на основе заданных многокритериальных параметров. В работе анализируются*

методы многообъектной оптимизации, позволяющие одновременно учитывать требования к естественной освещенности помещений, показатели энергоэффективности и общую стоимость строительных материалов. Особое внимание уделяется интеграции нейронных сетей с системами информационного моделирования зданий (BIM) для быстрого перебора и оценки жизнеспособности проектных решений в режиме реального времени. Автор исследует влияние автоматизированного поиска форм на сокращение сроков предпроектной подготовки и повышение качества итоговой архитектурной среды. В заключении обосновывается преимущество использования ИИ в качестве мощного инструмента поддержки принятия решений, способного находить нетривиальные и высокоэффективные пространственные конфигурации, недоступные при традиционном проектировании.
Ключевые слова: *искусственный интеллект, генеративный дизайн, планировка зданий, архитектурное проектирование, энергоэффективность, освещенность, оптимизация стоимости, BIM-технологии, машинное обучение, многокритериальный анализ.*

Генеративное проектирование на основе искусственного интеллекта представляет собой радикальный сдвиг в архитектурной практике от ручного черчения к алгоритмическому поиску оптимальных форм. Вместо создания единственного варианта планировки архитектор задает систему ограничений и целей, которые компьютер использует для генерации бесконечного множества решений. Этот подход позволяет исследовать обширное пространство проектных возможностей, которое невозможно охватить традиционными методами за разумное время. Машины не заменяют творческое видение, а расширяют его, предлагая варианты, которые могут быть неочевидны для человеческого восприятия. В результате процесс проектирования превращается в итеративный отбор лучших образцов из тысяч сгенерированных моделей.

Ключевым параметром оптимизации при автоматическом создании планировок является инсоляция, или уровень естественной освещенности внутренних пространств. Алгоритмы ИИ проводят детальный расчет траектории солнца и теней от окружающих строений для каждого сгенерированного варианта. Система стремится максимизировать проникновение дневного света в жилые зоны, что напрямую влияет на комфорт жителей и здоровье человека. Автоматическая корректировка расположения окон и глубины комнат позволяет достичь идеального баланса освещенности без нарушения конструктивной целостности здания. Такой подход делает каждое проектное решение научно обоснованным и экологически ориентированным.

Энергоэффективность зданий становится важнейшим критерием в условиях глобального стремления к устойчивому развитию и снижению углеродного следа. ИИ анализирует теплопотери через внешние ограждающие конструкции и эффективность естественной вентиляции для каждой итерации планировки. Путем изменения компактности формы здания и ориентации по сторонам света алгоритм находит конфигурации с минимальным энергопотреблением. Это позволяет значительно снизить затраты на отопление и кондиционирование в процессе дальнейшей эксплуатации объекта. Генеративный дизайн превращает энергоэффективность из дополнительной опции в базовую характеристику архитектурного решения.

Стоимость строительных материалов интегрируется в алгоритм как жесткое экономическое ограничение, влияющее на выбор итоговой формы. ИИ производит мгновенный расчет объема бетона, стали и фасадных систем для каждого из тысяч сгенерированных вариантов планировок. Система отсеивает избыточно сложные геометрические формы, которые привели бы к неоправданному удорожанию строительства. Это обеспечивает прозрачность бюджета проекта уже на стадии эскизного проектирования и позволяет заказчику видеть финансовые последствия архитектурных решений. Оптимизация материалоемкости способствует

рациональному использованию ресурсов и повышению инвестиционной привлекательности объекта.

Использование генетических алгоритмов позволяет имитировать процесс естественного отбора в архитектурной среде для поиска «сильнейших» проектных решений. Каждое поколение планировок оценивается по заданному фитнес-функциями набору критериев, после чего лучшие варианты скрещиваются и мутируют. С каждой новой итерацией ИИ приближается к идеальному балансу между функциональностью, эстетикой и техническими требованиями. Этот процесс происходит со скоростью миллионов операций в секунду, что позволяет обработать колоссальные массивы данных за считанные минуты. Архитектор выступает в роли куратора этого эволюционного процесса, задавая правила игры и выбирая финальное направление.

Интеграция с технологиями информационного моделирования зданий (BIM) обеспечивает бесшовный переход от сгенерированных алгоритмом концепций к рабочей документации. Каждая созданная ИИ планировка содержит в себе не только геометрию, но и полные данные о свойствах материалов и инженерных систем. Это исключает ошибки при переносе проектных данных между различными этапами проектирования и смежными специалистами. Автоматизация позволяет мгновенно обновлять всю спецификацию материалов при изменении одного из параметров планировки. Синхронизация генеративного дизайна и BIM-среды создает единый цифровой поток информации от идеи до реализации.

Машинное обучение на основе больших данных позволяет ИИ учитывать исторический опыт проектирования и предпочтения пользователей. Алгоритмы анализируют тысячи существующих планировок и отзывы жильцов, чтобы понять, какие пространственные конфигурации наиболее востребованы. Система учится распознавать паттерны удачного зонирования и эргономики, перенося этот опыт на новые уникальные участки застройки. Это помогает избегать

типичных ошибок проектирования и создавать пространства, максимально адаптированные под современные сценарии жизни. Искусственный интеллект становится носителем коллективного архитектурного опыта, доступного для каждого нового проекта.

Автоматический расчет планировок позволяет эффективно решать задачи проектирования в условиях сложной городской застройки и ограниченного пространства. ИИ учитывает градостроительные нормы, отступы от границ участка и требования по пожарной безопасности в автоматическом режиме. Алгоритм может вписать сложную многофункциональную программу в участок неправильной формы, обеспечивая при этом соблюдение всех нормативов. Это освобождает архитектора от рутинной проверки соответствия нормам и позволяет сосредоточиться на эстетической ценности проекта. Машина берет на себя роль неутомимого контролера, гарантируя легитимность каждого предложенного варианта.

Генеративный дизайн также способствует созданию более инклюзивной городской среды за счет учета потребностей различных групп населения. Алгоритмы могут быть настроены на оптимизацию путей движения маломобильных групп граждан и создание безбарьерного пространства. ИИ анализирует пешеходные потоки и доступность ключевых зон внутри здания, предлагая наиболее удобные планировочные решения.

Заключение

В будущем ожидается еще более глубокая интеграция ИИ с процессами робототехники на строительных площадках для прямой реализации сгенерированных моделей. Планировки будут создаваться с учетом возможностей строительных 3D-принтеров и автономных монтажных кранов. Это позволит строить здания сложнейших форм с точностью до миллиметра при минимальном участии человека. Развитие облачных сервисов для генеративного дизайна сделает эти мощные инструменты доступными для архитекторов по всему миру. Искусственный интеллект станет надежным

партнером в создании городов будущего, которые будут умными, красивыми и экологичными.

Список литературы

1. *Беляева С.В.* Искусственный интеллект в архитектуре и градостроительстве. Москва: Архитектура-С, 2024.
2. *Лисицын Д.А.* Параметрическое моделирование и генеративный дизайн: учебное пособие. Санкт-Петербург: Лань, 2023.
3. *Марков К.И.* Оптимизация проектных решений на основе алгоритмов машинного обучения // Вестник гражданских инженеров. 2024. № 2. С. 15–28.
4. *Савельев А.П.* Автоматизация оценки энергоэффективности зданий на ранних стадиях проектирования. Казань: КГАСУ, 2022.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ АВТОМАТИЗАЦИИ

Сарыев М.[1], Башимова Г.А.[2], Баглиев Б.А.[3]

[1]Сарыев Медет – преподаватель;
[2]Башимова Гунча Азадовна - студент,
[3]Беглиев Бегли Атамырадович – студент,
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *данное исследование посвящено комплексному анализу проблем и методов обеспечения информационной безопасности критически важных объектов автоматизации (КВОА) в условиях растущих киберугроз. В работе рассматриваются специфические уязвимости промышленных систем управления (АСУ ТП), связанные с интеграцией изолированных ранее сегментов в глобальные сети и использованием стандартных ИТ-протоколов. Особое внимание уделяется разработке многоуровневых*

систем защиты, включающих средства обнаружения вторжений, криптографическую защиту каналов передачи данных и механизмы изоляции критических контуров управления. Автор исследует нормативно-правовую базу в области защиты критической информационной инфраструктуры и предлагает алгоритмы оценки рисков для предотвращения техногенных катастроф, вызванных деструктивными программными воздействиями. В заключении формулируются рекомендации по созданию отказоустойчивых архитектур, способных поддерживать функционирование объекта в условиях активного киберпротивоборства.
Ключевые слова: *критическая информационная инфраструктура, информационная безопасность, АСУ ТП, киберугрозы, сетевая безопасность, защита данных, отказоустойчивость, промышленная автоматизация, обнаружение вторжений, управление рисками.*

Информационная безопасность критически важных объектов автоматизации является приоритетной задачей национального масштаба, так как сбои в их работе могут привести к масштабным техногенным катастрофам. К таким объектам относятся системы управления энергетическими сетями, водоканалы, транспортные узлы и крупные промышленные предприятия. Современные киберугрозы эволюционировали от простых вирусов до сложных целевых атак, направленных на физическое разрушение инфраструктуры. Защита подобных систем требует не только программных решений, но и глубокого понимания специфики технологических процессов. Интеграция информационных и операционных технологий делает границы объектов прозрачными для потенциальных злоумышленников.

Специфика критических систем управления заключается в приоритете доступности и целостности данных над их конфиденциальностью. В отличие от корпоративных сетей, где задержка в несколько секунд допустима, в системах автоматизации реального времени любая пауза может

вызвать аварию. Использование устаревшего оборудования и проприетарных протоколов, созданных без учета требований безопасности, создает дополнительные уязвимости. Злоумышленники могут использовать легитимные команды управления для перевода оборудования в закритические режимы работы. Это требует внедрения специализированных средств защиты, не оказывающих негативного влияния на производительность сети.

Основой защиты критической инфраструктуры является концепция глубокоэшелонированной обороны, предполагающая создание множества независимых барьеров на пути атакующего. Первый эшелон включает в себя физическую изоляцию сегментов сети и использование межсетевых экранов промышленного класса. На втором уровне внедряются системы обнаружения и предотвращения вторжений, настроенные на анализ специфических промышленных протоколов. Третий уровень подразумевает строгий контроль доступа персонала и использование многофакторной аутентификации для критических операций. Такая многоуровневая структура позволяет локализовать угрозу на ранней стадии и не допустить ее распространения к исполнительным механизмам.

Мониторинг безопасности в реальном времени позволяет своевременно выявлять аномалии, характерные для начальных этапов кибератаки. Системы класса SIEM собирают и анализируют логи со всех узлов автоматизации, выявляя подозрительную активность, которую сложно заметить вручную. Важным элементом является использование систем глубокого анализа пакетов (DPI), способных проверять содержимое команд внутри технологического трафика. Любое отклонение от стандартного профиля работы системы должно немедленно вызывать оповещение службы безопасности. Автоматизация процессов реагирования помогает сократить время между обнаружением угрозы и её нейтрализацией.

Человеческий фактор остается одним из самых слабых звеньев в системе безопасности критически важных

объектов. Социальная инженерия и использование зараженных съемных носителей часто становятся вектором первоначального проникновения в изолированную сеть. Обучение персонала правилам кибергигиены и проведение регулярных тренировок по отражению атак являются обязательными элементами защиты. Регламенты должны четко определять порядок действий при обнаружении признаков компрометации системы. Ответственность сотрудников за нарушение политик безопасности должна быть закреплена на уровне руководства предприятия.

Нормативно-правовое регулирование в сфере защиты критической информационной инфраструктуры накладывает на владельцев объектов серьезные обязательства. Требования государственных регуляторов включают обязательное категорирование объектов и внедрение сертифицированных средств защиты. Регулярный аудит безопасности и проведение тестов на проникновение позволяют объективно оценить текущий уровень защищенности. Взаимодействие с государственными центрами мониторинга помогает своевременно получать информацию о новых типах угроз и уязвимостей. Соблюдение стандартов является необходимым условием для легитимного функционирования предприятия в правовом поле.

Криптографическая защита каналов связи обеспечивает целостность команд управления и предотвращает их подмену в процессе передачи. Применение отечественных алгоритмов шифрования гарантирует отсутствие «закладок» и независимость от зарубежных поставщиков технологий. Важно обеспечить надежное управление ключами шифрования, исключая возможность их компрометации через административные интерфейсы. Шифрование должно применяться не только для внешних соединений, но и внутри технологического сегмента для защиты от внутренних нарушителей. Это создает доверенную среду взаимодействия между датчиками, контроллерами и диспетчерскими пунктами.

Обеспечение отказоустойчивости подразумевает способность системы сохранять минимально необходимый функционал даже в условиях успешной кибератаки. Использование механизмов резервирования и дублирования критических узлов управления повышает живучесть объекта. В случае обнаружения деструктивного воздействия система должна автоматически переходить в безопасный режим работы или переключаться на изолированные резервные контуры. Регулярное создание резервных копий конфигураций оборудования позволяет быстро восстановить работоспособность после инцидента. Архитектура системы должна проектироваться с учетом возможности «деградации» функций без полной потери контроля.

Использование технологий искусственного интеллекта в системах защиты помогает выявлять ранее неизвестные угрозы (Zero-day). Нейронные сети обучаются на нормальном поведении технологического процесса и способны фиксировать мельчайшие отклонения, указывающие на скрытое воздействие. Это позволяет обнаруживать атаки, которые маскируются под легитимную деятельность персонала или естественный износ оборудования. Применение машинного обучения снижает количество ложноположительных срабатываний, освобождая ресурсы аналитиков для разбора действительно важных инцидентов.

Заключение

В заключении следует отметить, что информационная безопасность критических объектов — это непрерывный процесс, а не разовое мероприятие. Постоянное развитие технологий и методов ведения кибервойн требует от специалистов по безопасности регулярного обновления своих знаний и инструментов. Сотрудничество между разработчиками систем автоматизации, производителями средств защиты и государственными органами является ключом к созданию надежного цифрового щита. Будущее отрасли связано с переходом к концепции врожденной

безопасности (Security by Design), когда защита закладывается в оборудование на этапе производства.

Список литературы

1. *Баранов А.П.* Защита критически важных объектов в цифровой среде. Москва: Горячая линия — Телеком, 2024.
2. *Васильев С.И.* Обеспечение кибербезопасности промышленных систем автоматизации. Санкт-Петербург: БХВ-Петербург, 2023.
3. Методы оценки защищенности критически важных информационных систем / под ред. Д.В. Козлова. Екатеринбург: УрФУ, 2022.
4. *Романов А.М.* Кибербезопасность АСУ ТП: от теории к практике // Защита информации. Инсайд. 2024. № 2. С. 45–58.
5. *Stouffer K., Pillitteri V., Lightman S.* Guide to Industrial Control Systems (ICS) Security. NIST Special Publication 800-82. 2023.

АВТОМАТИЗАЦИЯ СИСТЕМ ЖИЗНЕОБЕСПЕЧЕНИЯ В КОНЦЕПЦИИ SMART CITY

Сарыев М.[1], Акыев С.Г.[2], Арсланова Г.А.[3]

[1]Сарыев Медет – преподаватель;
[2]Акыев Сахетмырат Гочмурадович - студент,
[3]Арсланова Гозел Арслановна – студент,
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *данное исследование посвящено анализу методов и технологий автоматизации систем жизнеобеспечения в рамках реализации концепции «умного города» (Smart City). В работе рассматриваются архитектурные подходы к интеграции разрозненных муниципальных сетей — водоснабжения,*

электроэнергетики, отопления и управления отходами — в единую интеллектуальную экосистему на базе технологий промышленного интернета вещей (IIoT). Особое внимание уделяется разработке алгоритмов адаптивного управления ресурсопотреблением, позволяющих оптимизировать нагрузку на инфраструктуру города в зависимости от времени суток, погодных условий и текущих потребностей населения. Автор исследует роль облачных платформ и аналитики больших данных в создании систем предиктивного обслуживания, способных предотвращать аварийные ситуации и снижать эксплуатационные издержки. В заключении формулируются рекомендации по внедрению интеллектуальных систем мониторинга для повышения экологической устойчивости и качества жизни в современных мегаполисах.
Ключевые слова: *умный город, Smart City, автоматизация жизнеобеспечения, интернет вещей, IIoT, энергоэффективность, интеллектуальные сети, мониторинг городской среды, устойчивое развитие, городская инфраструктура.*

Автоматизация систем жизнеобеспечения в рамках концепции Smart City представляет собой создание интегрированной цифровой среды управления критически важной городской инфраструктурой. Традиционные системы ЖКХ, работающие изолированно, заменяются единым интеллектуальным контуром, где данные от сетей водоснабжения, тепловых пунктов и электросетей стекаются в общие аналитические центры. Это позволяет городским службам видеть комплексную картину состояния города в режиме реального времени и оперативно реагировать на любые изменения. Внедрение автоматизации направлено не только на повышение комфорта граждан, но и на обеспечение глобальной устойчивости мегаполиса к внешним вызовам и внутренним сбоям. Городская среда превращается в адаптивный механизм, способный к самодиагностике и оптимизации.

Интеллектуальное управление энергоснабжением (Smart Grid) является фундаментом «умного города», обеспечивая рациональное распределение электричества и предотвращая перегрузки сетей. Автоматизированные системы анализируют графики потребления и динамически перераспределяют мощности между жилыми кварталами и промышленными зонами. Внедрение интеллектуальных приборов учета (умных счетчиков) позволяет пользователям контролировать свои расходы, а поставщикам — мгновенно фиксировать попытки несанкционированного подключения или аварийные обрывы линий. Интеграция возобновляемых источников энергии, таких как солнечные панели на крышах зданий, также требует высокого уровня автоматизации для балансировки сети.

Системы автоматизированного водоснабжения и водоотведения позволяют радикально снизить потери ресурса за счет точного обнаружения утечек на ранних стадиях. Датчики давления и расхода, установленные на магистральных трубопроводах, передают данные алгоритмам, которые сравнивают фактические показатели с эталонными моделями. При выявлении расхождений система автоматически локализует поврежденный участок, перекрывая задвижки и уведомляя ремонтные бригады. Это предотвращает подтопление городских территорий и экономит колоссальные объемы очищенной воды. Кроме того, автоматизация насосных станций оптимизирует энергопотребление, подстраивая напор под текущие нужды потребителей в зависимости от этажности и времени суток.

Управление теплоснабжением в концепции Smart City строится на принципе погодной компенсации и предиктивного моделирования тепловых потерь зданий. Автоматизированные индивидуальные тепловые пункты (ИТП) регулируют температуру теплоносителя на основе данных от внешних датчиков температуры и прогнозов погоды. Это исключает проблему «перетопов» в весенне-осенний период и обеспечивает комфортный микроклимат внутри помещений. Дистанционный мониторинг состояния

теплотрасс позволяет выявлять зоны с нарушенной теплоизоляцией и планировать замену труб до наступления отопительного сезона. В масштабах города такая оптимизация приводит к значительному сокращению сжигаемого топлива и снижению углеродного следа.

Автоматизация систем управления отходами (Smart Waste Management) оптимизирует логистику мусороуборочной техники и повышает экологическую чистоту городских кварталов. Контейнеры, оснащенные ультразвуковыми датчиками заполнения, передают информацию в единую диспетчерскую службу. Программное обеспечение на базе искусственного интеллекта строит динамические маршруты для мусоровозов, исключая заезды к пустым бакам и предотвращая переполнение площадок в праздничные дни. Это сокращает пробег спецтехники, снижает выбросы выхлопных газов и уровень шума в жилых зонах. Внедрение систем автоматической сортировки на перерабатывающих заводах завершает цикл рационального обращения с отходами в «умном» мегаполисе.

Интеллектуальное городское освещение является одним из наиболее заметных элементов автоматизации жизнеобеспечения для жителей. Умные фонари, оснащенные датчиками движения и освещенности, регулируют яркость свечения в зависимости от присутствия людей и времени суток. В ночные часы при отсутствии пешеходов освещенность может снижаться до минимально безопасного уровня, что экономит до 60% электроэнергии. Дополнительно опоры освещения могут выступать в роли узлов связи (Wi-Fi хот-спотов), метеостанций или станций мониторинга качества воздуха. Автоматическая диагностика ламп позволяет заменять перегоревшие элементы без необходимости проведения регулярных визуальных осмотров всей сети.

Обеспечение экологической безопасности в «умном городе» опирается на сеть датчиков мониторинга атмосферного воздуха, почвы и уровня шума. Автоматизированные посты наблюдения в режиме реального

времени анализируют концентрацию вредных веществ и передают данные на общедоступные городские порталы. В случае превышения допустимых норм система может автоматически корректировать работу транспортных потоков или ограничивать деятельность промышленных объектов в определенных зонах. Это позволяет жителям выбирать наиболее безопасные маршруты для прогулок, а городским властям — принимать обоснованные решения по озеленению и градостроительному планированию. Прозрачность экологических данных способствует повышению гражданской ответственности и заботе о здоровье населения.

Безопасность систем жизнеобеспечения в цифровой среде требует особого внимания к киберзащите критической инфраструктуры. Поскольку управление всеми сетями сосредоточено в программных комплексах, риск несанкционированного доступа может иметь катастрофические последствия. Автоматизированные системы безопасности используют алгоритмы машинного обучения для выявления аномалий в поведении сети, которые могут указывать на попытку взлома или диверсии. Сегментация сетей и использование отечественных криптографических стандартов обеспечивают защиту от внешних кибератак. Надежность «умного города» определяется не только функциональностью, но и способностью инфраструктуры противостоять цифровым угрозам в условиях активного противоборства.

Заключение

В заключении следует отметить, что автоматизация систем жизнеобеспечения — это непрерывный процесс технологической эволюции городской среды. Будущее Smart City связано с более глубокой интеграцией искусственного интеллекта и созданием полноценных «цифровых двойников» городов для моделирования их развития. Этические вопросы использования больших данных и обеспечения приватности жителей станут центральными темами при проектировании будущих систем управления. Мы движемся к модели города, который не просто

потребляет ресурсы, но и эффективно распределяет их, минимизируя антропогенное воздействие на планету. Только комплексный подход к автоматизации позволит создать города, в которых технологии служат благополучию каждого человека.

Список литературы

1. *Андреев В.К.* Автоматизация инженерных систем современных мегаполисов. М.: Стройиздат, 2024.
2. *Кузнецов Л.А.* Концепции и технологии Smart City: учебное пособие. СПб.: Лань, 2023.
3. *Николаев С.П., Федоров А.И.* Интеллектуальное управление водными и энергетическими ресурсами города // Энергосбережение и водоподготовка. 2024. № 1. С. 15–28.
4. *Соколова М.В.* Системы мониторинга и безопасности умной городской среды. Екатеринбург: УрФУ, 2022.
5. *Townsend A.M.* Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia. New York: W. W. Norton & Company, 2013.

ПЕРЕХОД ОТ КЛАССИЧЕСКИХ ПИД-РЕГУЛЯТОРОВ К АДАПТИВНЫМ СИСТЕМАМ УПРАВЛЕНИЯ НА ОСНОВЕ ГЛУБОКОГО ОБУЧЕНИЯ

Сеитов С.[1], Хасанов А.Т.[2], Хыдыргулыева С.Ч.[3]

[1]Сеитов Сулейман – преподаватель;
[2]Хасанов Алмаз Тахирович - студент,
[3]Хыдыргулыева Сонагул Чарыевна – студент,
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *данное исследование рассматривает методологическую трансформацию систем автоматизации, заключающуюся в переходе от классических пропорционально-интегрально-дифференцирующих регуляторов к адаптивным структурам на базе алгоритмов*

глубокого обучения. В работе анализируются функциональные ограничения традиционных методов управления при работе с высоконелинейными и динамически нестабильными объектами, а также предлагаются способы их преодоления через внедрение нейросетевых архитектур, способных к самообучению в реальном времени. Особое внимание уделяется применению глубокого обучения с подкреплением для синтеза стратегий управления, которые обеспечивают минимальное время переходных процессов и высокую устойчивость к внешним возмущениям без необходимости построения точных математических моделей. Автор оценивает технические аспекты интеграции интеллектуальных агентов в существующую промышленную инфраструктуру и доказывает эффективность такого перехода для повышения общей производительности и точности автономных систем.

Ключевые слова: *адаптивное управление, ПИД-регулятор, глубокое обучение, нейронные сети, обучение с подкреплением, промышленная автоматизация, нелинейные системы, интеллектуальные агенты, цифровая трансформация, оптимизация управления.*

Традиционные ПИД-регуляторы долгое время доминировали в промышленной автоматизации благодаря своей структурной простоте и предсказуемости в линейных режимах работы. Однако современные технологические процессы характеризуются высокой степенью неопределенности и сложными нелинейными взаимосвязями, которые трудно формализовать классическими уравнениями. Переход к адаптивным системам на основе глубокого обучения обусловлен необходимостью повышения динамической точности и устойчивости систем управления. Нейросетевые архитектуры позволяют извлекать признаки непосредственно из потоков данных, не требуя построения точных математических моделей объекта. Это открывает новые возможности для автоматизации процессов, которые ранее считались слишком сложными для классического регулирования.

Методы глубокого обучения позволяют нейросетевым регуляторам выполнять роль универсальных аппроксиматоров функций управления любой сложности. В отличие от жестко заданных коэффициентов ПИД-алгоритма, веса нейронной сети могут динамически подстраиваться под текущее состояние внешней среды. Это критически важно при управлении объектами с изменяющейся массой, переменным трением или нестационарными тепловыми потоками. Адаптивность глубоких моделей обеспечивает сохранение оптимальных характеристик переходного процесса в течение всего жизненного цикла оборудования. Интеллект системы управления минимизирует износ механических узлов за счет более плавного формирования сигналов.

Применение глубокого обучения с подкреплением позволяет системе управления обучаться на основе собственного опыта через взаимодействие с цифровым двойником объекта. Агент управления получает вознаграждение за каждое действие, приближающее систему к целевому состоянию, и штрафы за нарушение ограничений безопасности. Со временем нейросеть вырабатывает сложную политику управления, которая учитывает долгосрочные последствия текущих решений. Такой подход превосходит реактивный характер ПИД-регулирования, добавляя системе элементы стратегического планирования. Процесс обучения может продолжаться и после ввода системы в эксплуатацию, обеспечивая непрерывное совершенствование алгоритмов.

Интеграция глубоких нейронных сетей в существующую инфраструктуру автоматизации часто начинается с гибридных схем «нейро-ПИД». В такой конфигурации классический регулятор обеспечивает базовую стабилизацию, а нейросеть выступает в роли интеллектуального компенсатора ошибок. Глубокая модель обучается предсказывать и нивелировать влияние внешних возмущений еще до того, как они существенно отклонят регулируемую величину. Это позволяет значительно снизить

время установления и практически полностью исключить перерегулирование. Гибридный подход является наиболее безопасным путем миграции к полностью автономным интеллектуальным системам.

Вычислительная сложность алгоритмов глубокого обучения требует использования специализированных аппаратных ускорителей на периферии производства. Современные тензорные процессоры и ПЛИС позволяют выполнять выводы глубоких нейросетей с миллисекундными задержками, необходимыми для управления реальным временем. Переход от централизованных серверных вычислений к граничным вычислениям (Edge Computing) повышает надежность и кибербезопасность систем. Локальная обработка сигналов исключает риски потери связи и обеспечивает мгновенную реакцию на аварийные ситуации. Технологическая база для такого перехода уже сформирована ведущими мировыми производителями электроники.

Одним из ключевых барьеров для внедрения глубокого обучения является проблема «черного ящика» и отсутствие интерпретируемости решений нейросети. В отличие от ПИД-регулятора, где каждый коэффициент имеет физический смысл, логика работы глубокой сети скрыта за миллионами параметров. Для решения этой проблемы активно развиваются методы объяснимого ИИ, которые позволяют визуализировать логику работы нейросетевого агента. Математическое доказательство устойчивости нейросетевых контуров проводится с использованием расширенных методов теории Ляпунова. Это гарантирует, что интеллектуальный регулятор не приведет систему к критическим автоколебаниям или потере управления.

Экономическая эффективность перехода к глубокому обучению проявляется в значительном снижении процента производственного брака и экономии энергоресурсов. Традиционные системы часто работают с избыточными запасами устойчивости, что замедляет производственные циклы и повышает энергопотребление. Адаптивные системы могут безопасно работать на границе физических

возможностей оборудования, максимизируя производительность. Снижение необходимости в постоянном сервисном обслуживании и ручной подстройке регуляторов также сокращает операционные расходы предприятия. Инвестиции в интеллектуализацию управления окупаются за счет повышения гибкости и прозрачности производства.

Переход к глубокому обучению стимулирует развитие концепции цифровых двойников, которые служат полигоном для тренировки адаптивных систем. Виртуальная среда позволяет моделировать редкие и катастрофические сценарии без риска повреждения реального оборудования. Обученная в симуляции нейросеть переносится на физический объект с минимальными корректировками через методы переноса обучения (Transfer Learning). Это сокращает время пусконаладочных работ с недель до нескольких часов, что критично для современных гибких производств. Цифровой двойник становится неотъемлемой частью жизненного цикла интеллектуальной системы управления.

Интеллектуальные системы управления на базе глубокого обучения обладают способностью к многозадачности и одновременному контролю множества переменных. В классических многосвязных системах настройка перекрестных связей между ПИД-контурами представляет собой сложнейшую инженерную задачу. Глубокие сети естественным образом обрабатывают многомерные векторы данных, оптимизируя работу всей системы в комплексе. Это находит применение в управлении сложными энергетическими установками, климатическими системами центров обработки данных и химическими реакторами.

Заключение

Социальный аспект перехода к адаптивным системам связан с изменением роли инженера по автоматизации. Вместо рутинной настройки коэффициентов специалисты занимаются проектированием архитектур нейросетей и формированием функций вознаграждения. Потребность в глубоких знаниях как в области классической теории управления, так и в сфере Data Science формирует новый

профессиональный стандарт. Обучение персонала работе с интеллектуальными системами становится стратегической задачей для крупных промышленных холдингов.

Список литературы

1. *Иванов С.П.* От ПИД-регуляторов к интеллектуальному управлению: учебное пособие. Москва: Энергоатомиздат, 2024.
2. *Кузнецов А.М.* Адаптивные системы на базе глубоких нейронных сетей. Санкт-Петербург: Наука и техника, 2023.
3. *Павлов В.В., Сидоров И.К.* Глубокое обучение с подкреплением в задачах автоматизации // Робототехника и техническая кибернетика. 2024. Т. 12. № 3. С. 44–58.
4. *Степанов Д.А.* Методы синтеза нейросетевых регуляторов для сложных динамических объектов. Казань: КФУ, 2022.
5. *Sutton R.S., Barto A.G.* Reinforcement Learning: An Introduction. Cambridge: MIT Press, 2018.

РАЗРАБОТКА ПРОТОКОЛОВ ЗАЩИТЫ ДЛЯ ПРОМЫШЛЕННЫХ СЕТЕЙ И ПРЕДОТВРАЩЕНИЕ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К СИСТЕМАМ АСУ ТП

Ханалыев А.[1], Чарыев Ы.Е.[2], Чарыева А.Ч.[3]

[1]Ханалыев Азымберди – преподаватель;
[2]Чарыев Ысмайыл Енишович - студент,
[3]Чарыева Айшат Чарыевна – студент,
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *данное исследование направлено на проектирование и анализ специализированных протоколов защиты, предназначенных для обеспечения целостности и конфиденциальности данных в промышленных сетях. В работе рассматриваются методы предотвращения несанкционированного доступа к системам*

автоматизированного управления технологическими процессами (АСУ ТП) через внедрение механизмов строгой аутентификации устройств и криптографического шифрования трафика. Особое внимание уделяется специфике промышленных протоколов, требующих минимальных задержек при передаче пакетов, и разработке алгоритмов обнаружения аномалий, способных идентифицировать попытки деструктивного воздействия на ранних стадиях. Автор исследует подходы к сегментации сетей и созданию доверенной среды взаимодействия между контроллерами и диспетчерскими пунктами для минимизации рисков техногенных инцидентов.
Ключевые слова: *информационная безопасность, промышленные сети, АСУ ТП, протоколы защиты, кибербезопасность, шифрование данных, несанкционированный доступ, сетевая сегментация, обнаружение вторжений, промышленная автоматизация.*

Проектирование защищенных протоколов для промышленных сетей является критически важной задачей в эпоху цифровой трансформации и роста числа киберугроз. В отличие от офисных сетей, системы АСУ ТП требуют строгого соблюдения временных регламентов и непрерывности передачи управляющих сигналов. Классические методы шифрования часто создают недопустимые задержки, что вынуждает разработчиков искать баланс между криптостойкостью и скоростью обработки пакетов. Разработка специализированных протоколов защиты направлена на создание доверенной среды, где каждое устройство идентифицируется и проверяется перед выполнением команды. Это позволяет минимизировать риски несанкционированного вмешательства в технологический цикл на ранних стадиях атаки.

Основная сложность предотвращения несанкционированного доступа заключается в уязвимости стандартных промышленных протоколов, таких как Modbus или Profibus, которые изначально создавались без встроенных функций безопасности. Злоумышленник,

получивший доступ к сетевому сегменту, может легко перехватить трафик или внедрить ложные команды управления. Внедрение оберток безопасности и туннелирования данных позволяет инкапсулировать незащищенные пакеты в зашифрованные контейнеры. Такой подход обеспечивает целостность информации и защиту от атак типа «человек посередине» (MITM). Современные архитектуры безопасности строятся на принципе «нулевого доверия», где каждое соединение подвергается строгой аутентификации.

Сегментация промышленных сетей является фундаментальным методом ограничения распространения угроз внутри предприятия. Разделение сети на изолированные зоны ответственности позволяет локализовать возможную атаку и предотвратить её переход от корпоративного уровня к исполнительным механизмам. Межсетевые экраны промышленного класса выполняют глубокий анализ пакетов, фильтруя трафик по специфическим параметрам технологического процесса. Это гарантирует, что к контроллеру (ПЛК) поступают только легитимные команды от авторизованных операторских станций. Четкое разграничение прав доступа на физическом и логическом уровнях значительно повышает общую устойчивость системы.

Криптографическая защита в АСУ ТП требует использования легковесных алгоритмов шифрования, оптимизированных для работы на устройствах с ограниченными вычислительными ресурсами. Использование симметричных ключей и механизмов быстрой смены векторов инициализации позволяет достичь высокой степени защиты без критического влияния на время цикла управления. Важно обеспечить надежную доставку ключей к полевым устройствам, исключая возможность их компрометации через административные интерфейсы. Автоматизированные системы управления ключами (KMS) позволяют централизованно контролировать политику безопасности во всей промышленной сети. Это создает

надежный барьер против попыток подмены данных или интеллектуального саботажа.

Системы обнаружения вторжений (IDS), адаптированные для промышленных сред, играют роль интеллектуального фильтра, отслеживающего аномалии в сетевом трафике. В отличие от стандартных ИТ-решений, промышленные IDS анализируют семантику технологических команд и выявляют отклонения от нормального режима работы оборудования. Например, резкое изменение частоты вращения двигателя или попытка одновременного открытия нескольких клапанов может быть признаком кибератаки. Использование методов машинного обучения позволяет системе адаптироваться к специфике конкретного производства и снижать количество ложных срабатываний. Своевременное оповещение персонала дает возможность перевести систему в безопасный режим до наступления аварийной ситуации.

Контроль физического доступа к сетевому оборудованию и интерфейсам контроллеров остается не менее важным аспектом комплексной защиты. Зачастую первичным вектором атаки становится подключение зараженного внешнего носителя напрямую к USB-порту или сервисному разъему на заводе. Опечатывание неиспользуемых портов, установка камер видеонаблюдения и биометрическая аутентификация сотрудников в серверных помещениях являются обязательными мерами. Регулярный аудит физической инфраструктуры помогает выявить попытки установки «закладок» или несанкционированных ретрансляторов. Безопасность системы автоматизации начинается с надежного периметра и дисциплины персонала.

Разработка защищенных протоколов должна учитывать необходимость сохранения работоспособности системы при потере связи с серверами аутентификации. Отказоустойчивые алгоритмы защиты предусматривают возможность автономной работы локальных сегментов сети в режиме «чрезвычайной ситуации». Использование кэшированных учетных записей и децентрализованных списков доступа позволяет операторам сохранять контроль

над процессом в условиях активного подавления связи. Архитектура безопасности должна проектироваться таким образом, чтобы защитные меры не становились причиной полной остановки завода при возникновении технических сбоев. Гибкость настройки политик безопасности позволяет адаптировать систему под конкретные уровни критичности каждого узла.

Нормативно-правовое регулирование в области информационной безопасности АСУ ТП обязывает предприятия использовать сертифицированные средства защиты информации. Применение отечественных разработок в области криптографии и межсетевого экранирования гарантирует отсутствие скрытых уязвимостей и независимость от внешнеполитических факторов. Регулярное проведение тестов на проникновение (пентестов) силами сторонних экспертов позволяет объективно взглянуть на слабые места в обороне. Формирование отчетов об инцидентах и обмен данными с государственными центрами кибербезопасности помогают формировать коллективный иммунитет к новым угрозам. Соблюдение стандартов серии ГОСТ Р ИСО/МЭК и приказов ФСТЭК России является базовым требованием для критических объектов.

Обучение инженерно-технического персонала основам кибербезопасности является залогом успешного функционирования систем защиты. Специалисты, работающие с АСУ ТП, должны понимать не только технологическую схему, но и принципы безопасной эксплуатации сетевых устройств. Проведение регулярных киберучений позволяет отработать координацию действий между ИТ-отделом и операторами цехов при отражении атак.

Заключение

В заключении следует отметить, что защита промышленных сетей — это динамический процесс, требующий постоянного совершенствования методов и инструментов. С появлением индустриального интернета вещей (IIoT) количество точек входа в систему автоматизации кратно возрастает, что требует новых

подходов к безопасности. Будущее отрасли связано с интеграцией функций защиты непосредственно в программно-аппаратную базу контроллеров и сенсоров на этапе их производства.

Список литературы

1. *Белов А.С.* Защита информации в автоматизированных системах управления. Москва: Техносфера, 2024.
2. *Григорьев В.В.* Кибербезопасность промышленных протоколов и сетей. Санкт-Петербург: БХВ-Петербург, 2023.
3. *Егоров Д.А., Морозов С.П.* Методы предотвращения атак на АСУ ТП в критических инфраструктурах // Вопросы кибербезопасности. 2024. № 1. С. 32–45.
4. *Смирнова О.Н.* Проектирование систем защиты для индустриального интернета вещей. Екатеринбург: УрФУ, 2022.

ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ В СИСТЕМАХ АВТОМАТИЧЕСКОГО РЕГУЛИРОВАНИЯ

Хатамов С.[1], Гелдимаммедова М.Т.[2], Ходжабаев А.Б.[3]

[1]Хатамов Селим – преподаватель;
[2]Гелдимаммедова Маягозел Тачмухаммедовна - студент,
[3]Ходжабаев Аймырат Башимович – студент,
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *данное исследование направлено на анализ архитектуры и преимуществ интеграции искусственных нейронных сетей в современные системы автоматического регулирования для повышения точности управления объектами с выраженной нелинейностью. В работе рассматриваются алгоритмы адаптивного управления, способные к обучению в реальном времени и эффективной компенсации внешних возмущений, которые сложно*

формализовать классическими математическими методами. Особое внимание уделяется гибридным структурам, объединяющим надежность традиционных ПИД-регуляторов с аппроксимирующими возможностями нейросетевых моделей, что позволяет значительно снизить ошибку регулирования и время переходных процессов. Автор исследует вопросы устойчивости и сходимости нейросетевых алгоритмов в замкнутых контурах управления, а также оценивает перспективы их применения в высокоточных отраслях промышленности и автономной робототехнике.
Ключевые слова: *нейронные сети, автоматическое регулирование, адаптивное управление, интеллектуальные системы, ПИД-регулятор, нелинейные системы, машинное обучение, идентификация объектов, кибернетика, динамические системы.*

Применение искусственных нейронных сетей в системах автоматического регулирования позволяет решать задачи управления объектами с неопределенной или переменной структурой. В отличие от классических методов, нейросетевые регуляторы не требуют точного аналитического описания динамики процесса, что значительно упрощает этап проектирования. Сеть обучается на основе экспериментальных данных, выявляя сложные нелинейные зависимости между входными сигналами и выходными переменными. Это обеспечивает высокую точность формирования управляющих воздействий в условиях, когда традиционные модели оказываются недостаточно эффективными. Автоматизация процесса настройки параметров регулятора сокращает время ввода систем в эксплуатацию и минимизирует влияние человеческого фактора.

Основным преимуществом нейросетевых систем является их способность к адаптации в режиме реального времени к изменяющимся условиям окружающей среды. В процессе функционирования нейронная сеть может корректировать свои весовые коэффициенты, реагируя на износ

оборудования или изменение характеристик сырья. Это позволяет поддерживать заданное качество регулирования без необходимости повторной ручной калибровки системы управления. Такие алгоритмы особенно востребованы в химической и аэрокосмической промышленности, где параметры процессов могут варьироваться в широком диапазоне. Интеллектуальный подход гарантирует стабильность работы технологического контура даже при возникновении непредвиденных внешних возмущений.

Архитектура нейросетевого регулятора обычно включает в себя несколько слоев, выполняющих нелинейное преобразование сигналов ошибки и состояния объекта. На вход подаются текущие значения регулируемой переменной и их производные, что позволяет сети учитывать предысторию процесса. Внутренние слои формируют абстрактные признаки, описывающие динамику системы, а выходной слой генерирует конкретный сигнал управления. Использование различных функций активации позволяет аппроксимировать функции управления практически любой сложности. Современные микропроцессоры обеспечивают необходимую скорость вычислений для работы таких сетей в жестком реальном времени.

Интеграция нейронных сетей с классическими алгоритмами, такими как ПИД-регулирование, создает мощные гибридные структуры управления. В подобных схемах нейросеть часто используется в качестве блока компенсации нелинейностей или динамической настройки коэффициентов базового регулятора. Классическая часть системы обеспечивает гарантированную устойчивость вблизи рабочей точки, в то время как нейросетевой модуль берет на себя управление в переходных режимах. Это позволяет сочетать надежность проверенных десятилетиями решений с гибкостью искусственного интеллекта. Гибридный подход существенно снижает требования к вычислительным ресурсам по сравнению с полностью нейросетевым управлением.

Использование нейронных сетей в качестве идентификаторов состояния объекта позволяет создавать системы управления с предсказанием. Сеть выступает в роли модели, которая прогнозирует поведение регулируемой величины на несколько шагов вперед. Основываясь на этом прогнозе, регулятор может заранее скорректировать управляющее воздействие, минимизируя динамическую ошибку. Такой подход крайне эффективен для объектов с большим запаздыванием, где традиционные методы управления работают неудовлетворительно. Предсказательная способность нейросетей превращает систему автоматического регулирования в упреждающий инструмент контроля.

Нейросетевые наблюдатели состояния предоставляют возможность оценивать переменные процесса, которые невозможно измерить напрямую из-за отсутствия подходящих датчиков. Это позволяет реализовать алгоритмы управления по полному вектору состояния, что значительно повышает качество переходных процессов. Программная реализация таких «виртуальных сенсоров» снижает общую стоимость системы автоматизации и повышает её надежность. Нейросеть обучается моделировать сложные зависимости между доступными измерениями и ненаблюдаемыми параметрами. Это открывает путь к автоматизации процессов в агрессивных средах, где физические сенсоры быстро выходят из строя.

Обеспечение устойчивости нейросетевых систем управления является критически важной задачей для промышленного применения. Математическое доказательство стабильности замкнутого контура проводится с использованием методов теории Ляпунова или частотных критериев. Разработчики применяют специальные архитектуры сетей с ограниченными весами и функции активации, гарантирующие предсказуемость поведения. Валидация алгоритмов включает в себя длительное тестирование на цифровых моделях с внесением случайных помех и структурных изменений. Только после

подтверждения безопасности алгоритм допускается к управлению реальным технологическим объектом.

Обучение нейронных сетей в системах автоматического регулирования может осуществляться как автономно, так и в контуре управления. Автономное обучение на накопленных исторических данных позволяет сформировать базовую стратегию управления еще до запуска системы. Обучение «на лету» позволяет системе непрерывно совершенствоваться в процессе эксплуатации, учитывая уникальные особенности конкретного экземпляра оборудования. Методы обучения с подкреплением позволяют регулятору самостоятельно находить оптимальные траектории движения без явных указаний инженера. Это делает системы управления по-настоящему автономными и интеллектуальными.

Нейронные сети эффективно справляются с управлением многосвязными системами, где изменение одного параметра влияет на несколько выходных величин. В классической теории управления такие объекты требуют сложных процедур декомпозиции и настройки перекрестных связей. Нейросеть естественным образом учитывает эти зависимости, оптимизируя работу всей системы в целом. Это находит применение в управлении сложными энергетическими установками, климатическими системами зданий и многозвенными манипуляторами. Способность обрабатывать большие массивы взаимосвязанных данных делает ИИ незаменимым в комплексной автоматизации.

Заключение

В заключение следует отметить, что внедрение нейронных сетей в системы автоматического регулирования является необратимым трендом цифровой трансформации. Синергия классической теории управления и современных методов машинного обучения создает фундамент для появления полностью автономных заводов. Будущее отрасли связано с созданием когнитивных систем, способных не только регулировать параметры, но и планировать действия в сложных условиях.

Список литературы

1. *Андреев В.П.* Нейросетевые системы управления техническими объектами. Москва: Физматлит, 2024.
2. *Макаров И.М.* Интеллектуальные системы автоматического управления. Санкт-Петербург: Лань, 2023.
3. *Николаев Д.А.* Применение нейронных сетей в адаптивных регуляторах // Автоматика и телемеханика. 2024. № 1. С. 12–25.
4. *Терехов В.А.* Нейросетевые системы управления: учебное пособие. Екатеринбург: УрФУ, 2022.
5. *Narendra K.S., Parthasarathy K.* Identification and control of dynamical systems using neural networks // IEEE Transactions on Neural Networks. 1990. Vol. 1. No. 1. P. 4–27.

РАЗРАБОТКА АДАПТИВНЫХ СИСТЕМ УПРАВЛЕНИЯ НА ОСНОВЕ НЕЧЕТКОЙ ЛОГИКИ И ГЕНЕТИЧЕСКИХ АЛГОРИТМОВ

Ходжаев С.[1], Аннагелдиев М.Г.[2], Ашыров М.Г.[3]

[1]Ходжаев Седа – преподаватель;
[2]Аннагелдиев Мердан Гелдимырат оглы – студент,
[3]Ашыров Мухаммет Гурбанмырадович – студент,
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *данное исследование посвящено разработке и анализу эффективности адаптивных систем автоматического управления, функционирующих на стыке методов нечеткой логики (Fuzzy Logic) и генетических алгоритмов (GA). В работе рассматриваются архитектурные решения для гибридных интеллектуальных контроллеров, способных эффективно работать в условиях высокой неопределенности параметров объекта и нестабильности внешней среды. Особое внимание уделяется*

процедуре автоматической настройки параметров функций принадлежности и оптимизации базы правил нечеткого вывода с использованием эволюционных стратегий поиска. Автор исследует механизмы адаптации системы в режиме реального времени, позволяющие минимизировать динамическую ошибку и время переходного процесса по сравнению с классическими ПИД-регуляторами. В заключении обосновывается применимость предложенных гибридных подходов для управления сложными нелинейными техническими объектами, такими как беспилотные летательные аппараты и робототехнические комплексы.
Ключевые слова: *адаптивное управление, нечеткая логика, генетические алгоритмы, интеллектуальные системы, функции принадлежности, оптимизация, мягкие вычисления, база правил, переходный процесс, гибридные контроллеры.*

Разработка адаптивных систем управления на базе нечеткой логики позволяет эффективно формализовать экспертные знания и управлять объектами, математическое описание которых затруднено или невозможно. В отличие от традиционных методов, нечеткие контроллеры оперируют лингвистическими переменными, что делает логику управления более гибкой и устойчивой к шумам в измерениях. Однако эффективность такой системы напрямую зависит от точности настройки функций принадлежности и полноты базы правил, что при ручном проектировании требует значительных временных затрат и высокой квалификации инженера. Использование адаптивных механизмов позволяет системе самостоятельно корректировать свои параметры, подстраиваясь под изменяющиеся характеристики объекта управления.

Генетические алгоритмы выступают в качестве мощного инструмента глобальной оптимизации, позволяющего автоматизировать процесс синтеза нечетких систем. В рамках данного подхода параметры контроллера кодируются в виде «хромосом», а качество управления оценивается с помощью целевой функции (фитнес-функции), отражающей точность и быстродействие системы. Эволюционный поиск позволяет

находить оптимальные конфигурации функций принадлежности даже в многомерных пространствах параметров, где классические градиентные методы могут оказаться неэффективными из-за наличия локальных экстремумов. Это обеспечивает высокую сходимость процесса настройки и гарантирует получение устойчивого решения для широкого класса динамических задач.

Гибридизация нечеткой логики и генетических алгоритмов порождает синергетический эффект, при котором недостатки одного метода компенсируются преимуществами другого. Генетический алгоритм берет на себя наиболее трудоемкую часть работы по поиску структуры и параметров, в то время как нечеткая логика обеспечивает интерпретируемость полученных правил и стабильность управления. Такая архитектура позволяет создавать «самообучающиеся» контроллеры, которые начинают работу с базовыми настройками и постепенно совершенствуют свою стратегию управления на основе накопленного опыта. Адаптация может происходить как на этапе проектирования (офлайн), так и непосредственно в процессе эксплуатации системы (онлайн).

Особое значение в проектировании адаптивных нечетких систем имеет выбор формы и расположения функций принадлежности, которые определяют чувствительность контроллера к входным сигналам. Генетический алгоритм может оптимизировать не только координаты вершин треугольных или гауссовых функций, но и их количество для каждого входа. Это позволяет создать разреженную или, наоборот, детализированную сетку управления там, где это необходимо для компенсации нелинейностей объекта. Оптимизированная таким образом система демонстрирует более плавные переходные процессы и отсутствие автоколебаний вблизи установившегося состояния, что критично для прецизионных систем позиционирования.

База правил нечеткого вывода определяет логическую связь между входными ошибками и управляющим воздействием. Генетические алгоритмы позволяют не только настраивать веса существующих правил, но и исключать

избыточные или противоречивые зависимости, упрощая вычислительную сложность контроллера. Это особенно важно для встраиваемых систем реального времени с ограниченными вычислительными ресурсами, где время выполнения одного цикла управления жестко лимитировано. В результате оптимизации база правил становится компактной и логически стройной, что облегчает её верификацию и дальнейшую модификацию человеком при необходимости.

Применение адаптивных контроллеров в управлении беспилотными летательными аппаратами (БПЛА) позволяет эффективно компенсировать изменения массы аппарата, порывы ветра и изменения плотности воздуха. Нечеткая логика обеспечивает устойчивость к резким возмущениям, а генетическая оптимизация позволяет настроить регулятор на достижение максимальной энергоэффективности полета. Адаптивная система способна перестраивать свои параметры в случае отказа одного из двигателей или повреждения управляющих поверхностей, обеспечивая живучесть аппарата в критических условиях. Такой уровень автономности недостижим для систем с жестко заданными коэффициентами усиления.

В промышленной робототехнике использование нечетко-генетических систем позволяет роботам-манипуляторам эффективно взаимодействовать с объектами неопределенной массы и жесткости. Адаптивный контроллер подстраивает усилия в захвате и траекторию движения в зависимости от тактильной обратной связи, предотвращая повреждение хрупких деталей. Эволюционный подход позволяет быстро перенастраивать робота на выполнение новых операций без необходимости привлечения специалистов по теории управления. Робототехнические комплексы становятся более гибкими и способными к работе в недетерминированной среде, что является ключевым требованием современной концепции Индустрии 5.0.

Экономическая эффективность внедрения адаптивных систем управления связана со снижением затрат на

пусконаладочные работы и сокращением времени простоев оборудования. Автоматическая настройка контроллера исключает человеческий фактор и ошибки, связанные с неточной идентификацией параметров объекта. Повышение качества переходных процессов напрямую ведет к снижению износа исполнительных механизмов и экономии энергоресурсов. Возможность системы адаптироваться к естественному старению компонентов оборудования продлевает его межремонтный интервал и общую долговечность производственных активов.

Заключение

В заключении следует отметить, что разработка адаптивных систем на базе нечеткой логики и генетических алгоритмов открывает новые горизонты в создании по-настоящему автономных и интеллектуальных машин. Дальнейшее развитие технологий будет связано с интеграцией методов глубокого обучения и подкрепляемого обучения для расширения адаптивных возможностей систем. Будущее отрасли принадлежит гибридным решениям, способным сочетать строгость математических моделей с гибкостью биологически вдохновленных алгоритмов. Такие системы станут основой для нового поколения умных производств и транспортных средств, обеспечивая беспрецедентный уровень эффективности и надежности в меняющемся мире.

Список литературы

1. *Игнатов А.П.* Коллаборативные роботы в современном производстве. Москва: Машиностроение, 2024.
2. *Михайлов В.С., Петров Д.А.* Психология взаимодействия человека и робота на сборочных линиях. Санкт-Петербург: Наука, 2023.
3. *Сидоров К.М.* Технологии технического зрения для систем безопасной коллаборации // Робототехника и техническая кибернетика. 2024. № 2. С. 45–58.

4. *Уваров Е.Н.* Проектирование интерфейсов «человек-машина» в робототехнических комплексах. Екатеринбург: УрФУ, 2022.
5. *Peshkin M., Colgate J.E.* Cobots: Robots for Collaboration with Human Operators // IEEE Transactions on Robotics and Automation. 1999. Vol. 15. No. 4. P. 711–723.

РАЗРАБОТКА СПЕЦИАЛИЗИРОВАННЫХ ОПЕРАЦИОННЫХ СИСТЕМ РЕАЛЬНОГО ВРЕМЕНИ

Ялкапова М.[1], Ашыров Э.С.[2], Атабаева А.А.[3]

[1]Ялкапова Мая – преподаватель;
[2]Ашыров Эшретмырат Сахетмырадович – студент,
[3]Атабаева Арзыгул Айдогдыевна– студент,
Туркменский государственный архитектурно-строительный институт
г. Ашхабад, Туркменистан

Аннотация: *данное исследование посвящено методологии и технологическим аспектам разработки специализированных операционных систем реального времени (ОСРВ), предназначенных для управления критически важными объектами. В работе рассматриваются архитектурные особенности ядер ОСРВ, обеспечивающие жесткую детерминированность временных интервалов и минимизацию латентности при обработке прерываний. Особое внимание уделяется механизмам планирования задач, предотвращению инверсии приоритетов и обеспечению отказоустойчивости систем в условиях высокой вычислительной нагрузки. Автор исследует подходы к созданию микроядерных архитектур, позволяющих изолировать критические компоненты и повысить общую информационную безопасность программных комплексов. В заключении формулируются принципы верификации и сертификации специализированных ОС для применения в авиационной, космической и промышленной отраслях, где*

надежность программного обеспечения является определяющим фактором безопасности.
Ключевые слова: *операционные системы реального времени, ОСРВ, детерминированность, планировщик задач, микроядерная архитектура, системы реального времени, встраиваемые системы, обработка прерываний, отказоустойчивость, верификация ПО.*

Разработка специализированных операционных систем реального времени (ОСРВ) является фундаментом для создания высоконадежных встраиваемых систем, где корректность работы определяется не только логическим результатом, но и временем его получения. В отличие от систем общего назначения, ОСРВ должны гарантировать жесткую детерминированность — способность системы реагировать на внешние события в течение строго заданного временного интервала. Это критически важно для управления авиационными двигателями, медицинским оборудованием и атомными реакторами, где любая задержка может привести к катастрофическим последствиям. Проектирование таких систем требует глубокого понимания взаимодействия программного обеспечения с аппаратными ресурсами процессора на самом низком уровне.

Основным компонентом ядра ОСРВ является планировщик задач, работающий на основе приоритетов и обеспечивающий вытесняющую многозадачность. В отличие от обычных ОС, планировщик реального времени не стремится к справедливому распределению ресурсов между всеми процессами, а отдает абсолютное предпочтение задачам с высшим приоритетом. Это позволяет гарантировать, что критически важный поток управления получит доступ к процессору немедленно после наступления прерывания. Для предотвращения конфликтов доступа к общим ресурсам в ядро внедряются механизмы протокола наследования приоритетов, исключающие возникновение классической проблемы инверсии приоритетов, способной парализовать работу системы.

Архитектура микроядра считается наиболее перспективной для разработки специализированных ОСРВ благодаря своей высокой отказоустойчивости и безопасности. В такой модели в привилегированном режиме работает только минимальный набор функций: управление памятью, планирование и межпроцессное взаимодействие (IPC). Все остальные службы, включая драйверы устройств и файловые системы, выносятся в пространство пользователя. Это означает, что сбой в драйвере сетевой карты не приведет к краху всей операционной системы, так как ядро останется изолированным от ошибок прикладных компонентов. Подобная модульность существенно упрощает процесс формальной верификации кода и сертификации системы по строгим отраслевым стандартам безопасности.

Минимизация латентности обработки прерываний является одной из ключевых метрик при проектировании ОСРВ. Время от момента физического сигнала на ножке процессора до начала выполнения соответствующего кода обработчика должно быть не только минимальным, но и постоянным. Разработчики специализированных систем стремятся исключить ситуации, когда ядро запрещает прерывания на длительный срок для выполнения собственных внутренних процедур. Использование быстрых контекстных переключений и оптимизированных векторов прерываний позволяет современным ОСРВ достигать времени реакции в доли микросекунд, что открывает возможности для управления сверхбыстрыми физическими процессами в силовой электронике и лазерной технике.

Управление памятью в операционных системах реального времени существенно отличается от подходов, принятых в настольных ОС. Использование виртуальной памяти с подкачкой страниц на диск недопустимо из-за непредсказуемых задержек, возникающих при операциях ввода-вывода. В специализированных ОСРВ часто применяется статическое выделение памяти или использование пулов памяти фиксированного размера с детерминированным временем выделения. Это

предотвращает фрагментацию кучи и гарантирует, что система не столкнется с нехваткой ресурсов в критический момент работы. Жесткое разделение адресных пространств между задачами с помощью модулей защиты памяти (MPU) или управления памятью (MMU) обеспечивает надежную изоляцию процессов.

Информационная безопасность специализированных ОСРВ становится критическим фактором в эпоху промышленного интернета вещей (IIoT). Традиционные ОС содержат миллионы строк кода, что неизбежно ведет к наличию уязвимостей, тогда как компактные ядра реального времени позволяют провести аудит безопасности каждого модуля. Внедрение механизмов контроля целостности и доверенной загрузки гарантирует, что на устройстве выполняется только авторизованное программное обеспечение. Разработчики интегрируют средства мониторинга выполнения в реальном времени, которые способны обнаружить аномальное поведение системы и перевести её в безопасное состояние до того, как злоумышленник сможет нанести ущерб физическому объекту.

Процесс верификации и сертификации специализированных ОСРВ является наиболее трудоемким этапом разработки, зачастую превышающим по затратам само написание кода. Системы, предназначенные для авиации или космоса, должны соответствовать стандартам типа DO-178C или ISO 26262. Это подразумевает полное покрытие кода тестами, доказательство отсутствия взаимоблокировок и математическое подтверждение временных характеристик всех критических путей выполнения. Использование инструментов статического анализа и формальных методов верификации позволяет выявить ошибки проектирования на ранних стадиях. Сертифицированная ОСРВ становится проверенным фундаментом, на котором разработчики прикладного ПО могут строить свои решения с высокой степенью уверенности.

Поддержка многоядерных архитектур в реальном времени ставит перед разработчиками ОСРВ новые вызовы, связанные с конкуренцией за общую шину данных и кэш-память. В многоядерных системах реального времени часто применяется подход разделения ядер (partitioning), где за каждой критической задачей закрепляется конкретное вычислительное ядро. Это исключает влияние низкоприоритетных процессов, работающих на соседних ядрах, на время выполнения важных функций. Межъядерное взаимодействие должно быть строго синхронизировано, чтобы избежать неопределенности временных задержек. Современные ОСРВ поддерживают как симметричную (SMP), так и асимметричную (AMP) многопроцессорность, предоставляя гибкие инструменты для оптимизации производительности сложных систем.

Заключение

В заключении следует отметить, что разработка специализированных ОСРВ — это область, требующая высочайшей квалификации и соблюдения строгих инженерных дисциплин. Будущее отрасли связано с автоматизацией процессов генерации кода ядер и развитием адаптивных планировщиков на базе технологий машинного обучения, способных оптимизировать нагрузку в динамических средах. Рост сложности встраиваемых систем и ужесточение требований к безопасности будут способствовать дальнейшему вытеснению универсальных решений специализированными микроядерными ОС.

Список литературы

1. *Васильев П.С.* Разработка и оптимизация ядер операционных систем реального времени. Москва: Техносфера, 2024.
2. *Кузнецов И.А.* Архитектура встраиваемых систем: от железа до ОСРВ. Санкт-Петербург: БХВ-Петербург, 2023.

3. *Николаев Д.В., Семенов К.А.* Сравнительный анализ алгоритмов планирования в ОСРВ жесткого реального времени // Программные продукты и системы. 2024. № 2. С. 12–25.
4. *Степанов М.А.* Надежность и безопасность системного программного обеспечения. Екатеринбург: УрФУ, 2022.
5. *Tanenbaum A.S., Woodhull A.S.* Operating Systems Design and Implementation. Upper Saddle River: Pearson, 2023.

РОЛЬ КОРРУПЦИОННЫХ СВЯЗЕЙ В УСТОЙЧИВОСТИ ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТИ

Мальгин И.В.[1], Алейникова В.А.[2]

[1]Мальгин Илья Владимирович – студент,
[2]Алейникова Валерия Андреевна – ассистент
кафедры уголовного права и процесса,
Белгородский государственный национальный
исследовательский университет,
г. Белгород

Аннотация: *в статье рассматривается роль коррупционных связей как ключевого фактора устойчивости организованной преступности в современных обществах. Коррупция анализируется не как совокупность отдельных правонарушений, а как системный социоэкономический и институциональный феномен, формирующий устойчивые неформальные сети взаимодействия между представителями государственной власти и криминальных структур. Теоретическую основу исследования составляют экономическая модель «принципал–агент» и институциональный подход, позволяющие объяснить механизмы возникновения, воспроизводства и долговременного функционирования коррупционных связей. Особое внимание уделяется анализу функций коррупции для организованной преступности, включая защитную, оперативную и стратегическую (политико-институциональную) функции.*

Ключевые слова: *коррупция, коррупционные связи, организованная преступность, институциональная теория, теневая экономика.*

Коррупционные связи представляют собой сложный социоэкономический феномен, который невозможно объяснить одной лишь личной жадностью. Для всестороннего понимания их возникновения,

функционирования и устойчивости необходимо обратиться к синтезу различных теоретических подходов.

В своей основе коррупционная связь – это неформальное, часто скрытое взаимодействие между двумя или более акторами, направленное на получение личной выгоды за счет злоупотребления публичной властью и нарушения формальных норм.

Коррупция начала зарождаться с появлением государства, чиновничества и централизованной власти. Чиновники, пользуясь своим высоким статусом и положением, старались получить личную выгоду и увеличить размер своих доходов. Если обратиться к временам античности, то можно сказать, что люди неоднозначно относились к коррупции. Так, в римском праве говорится, что коррумпировать (от лат. «corrumpere») обозначает портить желудок вредной пищей, портить воду, расточать состояние, уничтожать имущество, позорить достоинство [6].

Джон Локк, политический философ, рассматривает коррупцию как нарушение самых фундаментальных принципов правительства. Он считает, что если поведение правителя опирается на удовлетворение их собственной выгоды, желаний вместо законов, защиты собственности и интересов людей, то независимо от того, являются ли причины их действий оправданными или нет, все они называются коррумпированным поведением [5].

Ключевые положения для теоретического осмысления коррупционных процессов опираются на разработки модели «принципал–агент» в экономической теории. Данная модель интерпретирует взаимодействие между обществом как носителем суверенной власти (принципалом), передающим полномочия по управлению, и государственным служащим (агентом), обязанным использовать предоставленные ресурсы в интересах принципала. Коррупционное поведение объясняется возникающей между ними информационной асимметрией: агент располагает знаниями о фактических мотивах и характере своих действий, которые остаются скрытыми от принципала.

Это порождает два фундаментальных риска. Первый связан с проблемой неблагоприятного отбора, когда принципал не в состоянии заранее определить, кто из потенциальных исполнителей склонен к добросовестному исполнению обязанностей, а кто — к злоупотреблениям. Второй – риск морального ущерба, проявляющийся после передачи полномочий: обладая широкими дискретными полномочиями и ограниченной подконтрольностью, агент может использовать служебное положение для извлечения личной выгоды.

В рамках данной логики коррупционная связь рассматривается как координация действий между агентом и внешним участником (например, частным предпринимателем), направленная на перераспределение рент в их пользу. Такая кооперация обеспечивает максимизацию частной выгоды участников взаимодействия, но подрывает интересы принципала и общественное благосостояние. Долговременность и устойчивость подобных связей определяются соотношением ожидаемой выгоды от коррупционного поведения и ожидаемых издержек, связанных с вероятностью выявления и тяжестью потенциальных санкций.

Однако чисто экономический подход недостаточен для объяснения структурной устойчивости коррупции. Здесь на помощь приходит институциональная теория. Она утверждает, что коррупция процветает не столько из-за моральных слабостей, сколько из-за слабости формальных институтов. К таким слабостям относятся: чрезмерная бюрократическая сложность процедур; низкий уровень прозрачности и подотчетности государственных органов; широкие дискреционные полномочия должностных лиц при отсутствии эффективного контроля.

Коррупционные связи формируются как неформальные институты или «правила игры», которые возникают в ответ на неэффективность или дороговизну формальных правил. Эти неформальные правила обеспечивают предсказуемость в

среде формальной неопределенности и становятся самоподдерживающимися.

Организованная преступность наряду с коррупцией являются антисоциальными явлениями. Эти явления имеют свои специфические особенности для каждой страны. Устойчивость организованной преступности в современном мире не может быть объяснена исключительно ее финансовой мощью или жесткой внутренней иерархией. Ключевым элементом, который трансформирует криминальную группу из временного явления в долговечную, институционализированную структуру, является ее способность устанавливать и поддерживать обширные коррупционные связи [2].

Само слово «организованный» происходит от греческого organon («орудие, инструмент»), от латинского organizo («сообщать стройный вид», «устраивать») и от французского organiser («устроить, соединить в одно целое, упорядочить что-либо, придать чему-либо планомерность»). В этих толкованиях слово «организованный» относится скорее к деятельности, чем к субъекту [3].

Организованная преступность должна быть определена как разновидность негативной социальной деятельности тех членов общества (как организованных, так и не организованных), которые сознательно и систематически используют преступные средства и методы для достижения своих целей [1].

Коррупция для организованной преступности — это не просто инструмент для разовых сделок; это жизненно важная инфраструктура, выполняющая функции защиты, оперативного обеспечения и стратегической легитимации в «теневом государстве». Связь между организованной преступностью и коррупцией позволяет криминальным сетям функционировать с низким уровнем риска и высокой степенью предсказуемости, что является признаком любой успешной организации.

Наиболее очевидной и одновременно стратегически значимой для функционирования организованных

преступных структур выступает их защитная функция, обеспечиваемая коррупционными связями. Вовлечение представителей правоохранительных органов, прокуратуры и судебной системы формирует для таких групп своеобразный «буфер безопасности», который снижает вероятность привлечения к ответственности или делает его вовсе невозможным.

Подобные связи предоставляют преступным организациям доступ к информации, относящейся к оперативно-розыскным мероприятиям: планируемым задержаниям, проверкам, прослушиванию и иным действиям компетентных органов. Обладая такими сведениями, структуры организованной преступности получают возможность заранее предпринять меры по минимизации рисков — укрыть доказательства, изменить место пребывания членов группировки или временно приостановить деятельность.

В случае задержания коррупция работает как гарантия манипулирования доказательствами, оказания давления на свидетелей, фальсификации судебных решений или обеспечения чрезмерно мягких приговоров. Эта система "купленной юстиции" лишает государство его монополии на принуждение и создает у криминальных лидеров уверенность в их неуязвимости. Более того, эти связи используются для внутренних целей организованной преступности, например, для устранения конкурентов на криминальном рынке путем "заказа" уголовного преследования через подконтрольные органы.

Вторая важнейшая роль коррупции заключается в оперативном обеспечении и расширении криминальной деятельности. Организованная преступность оперирует на нелегальных рынках, которые по определению требуют пересечения формальных государственных границ и контроля. Чаще всего организованные преступные формирования подкупают должностных лиц, которые занимают посты в системе государственной власти [4]. Коррумпированные чиновники в таможенных службах, пограничном контроле, а также в органах, выдающих

лицензии и разрешения, выступают в роли неформальных «брокеров». Они превращают административные барьеры в платные услуги, обеспечивая организованной преступности бесперебойную контрабанду наркотиков, оружия, нелегальную миграцию или отмывание денег.

Например, получение доступа к государственным контрактам через подкуп чиновников позволяет организованной преступности легализовать свои доходы и даже получать финансирование из бюджета, что размывает границу между криминальным и легальным бизнесом. Эта функция позволяет организованной преступности масштабировать операции, превращая локальные криминальные группы в транснациональные сети.

Наконец, высшей стадией использования коррупционных связей является институционализация и политическое проникновение. На этом уровне организованная преступность стремится не просто нейтрализовать отдельные угрозы, а встраивать свои интересы непосредственно в механизм государственного управления. Это достигается через финансирование политических кампаний, подкуп высокопоставленных чиновников и депутатов. Целью становится не столько уклонение от законов, сколько их формирование или изменение в пользу криминальных структур (например, лоббирование законов, упрощающих отмывание денег или ослабляющих контроль за определенными секторами экономики).

Коррупция представляет собой одно из наиболее разрушительных явлений, способных подрывать устойчивость политических институтов, экономическую эффективность и социальное доверие. Ее последствия выходят далеко за рамки конкретных правонарушений — коррупционные связи становятся системным фактором деградации государственного управления, деформации общественных ценностей и торможения развития. Для государства и общества это явление несет комплекс долгосрочных последствий, которые проявляются в

политической, правовой, экономической и социальной сферах.

Коррупционные практики прежде всего подрывают основы легитимности публичной власти. Когда значимые управленческие решения принимаются не в соответствии с законом и общественными интересами у населения формируется ощущение несправедливости и неравного доступа к государственным ресурсам. Восприятие власти постепенно трансформируется.

Подобная динамика неизбежно приводит к снижению уровня общественного доверия, ослаблению политической включённости граждан и нарастанию отчуждения между государством и обществом. В условиях устойчиво высокого уровня коррупции наблюдается последовательная эрозия доверия к ключевым институтам — судебной системе, правоохранительным органам, административным структурам. Это, в свою очередь, ставит под сомнение сам принцип верховенства права и препятствует формированию эффективной и стабильной системы государственного управления.

С коррупционными связями тесно связана и деградация правовой системы. В условиях, когда решения можно «купить», закон перестает быть универсальным регулятором общественных отношений. Появляется «двойной стандарт» правоприменения: для одних — строгие нормы закона, для других — возможности избежать ответственности. Это ведет к криминализации государственного аппарата: коррупционные связи проникают в суды, полицию, органы контроля. Нарушение принципа неизбежности наказания ослабляет профилактическую функцию права и стимулирует рост преступности. Возникает порочный круг: чем выше уровень коррупции, тем слабее государство.

Таким образом, коррупционные связи являются тем самым социальным капиталом, который придает организованной преступности ее устойчивость. Они создают неформальную систему взаимных обязательств, основанную на доверии и страхе, которая оказывается более надежной, чем любой

формальный правовой механизм. Разрушение этого щита и его инфраструктуры требует не просто разовых арестов, а комплексного удара по коррупционным сетям на всех уровнях: от тактического (защита от правосудия) до стратегического (политическая инфильтрация). Только лишив ОП этого системного коррупционного обеспечения, можно подорвать ее способность к самовоспроизводству и долгосрочному существованию.

Список литературы

1. *Барис В.В., Яковлев С.В.* Сущность организованной преступности в ее взаимосвязи с коррупцией и внутриполитическими процессами // Вестник Московского университета. Серия 18. Социология и политология. 2009. №4. URL: https://cyberleninka.ru/article/n/suschnost-organizovannoy-prestupnosti-v-ee-vzaimosvyazi-s-korruptsiey-i-vnutripoliticheskimi-protsessami (дата обращения: 04.12.2025).
2. *Морозков К.Д.* Взаимосвязи организованной и коррупционной преступности // ВЭПС. 2020. №3. URL: https://cyberleninka.ru/article/n/vzaimosvyazi-organizovannoy-i-korruptsionnoy-prestupnosti (дата обращения: 04.12.2025).
3. Новейший словарь иностранных слов и выражений. М., Аст. 2002. – 975 с.
4. *Номоконов В.А.* Особенности политики борьбы с организованно преступностью и коррупцией в России // Организованная преступность, терроризм, коррупция и в их проявления, и борьба с ними. – М.: Российская криминологическая ассоциация, 2005. – С. 25-34.
5. *Пимкина Д.О.* Коррупция: понятие и виды // Россия в глобальном мире. 2021. №19 (42). URL: https://cyberleninka.ru/article/n/korruptsiya-ponyatie-i-vidy (дата обращения: 04.12.2025).
6. Римское право: Понятия, термины, определения: [Пер. с чеш.] / Милан Бартошек; [Спец. науч. ред., авт. предисл. и коммент. З.М. Черниловский]. М.: Юрид. лит., 1989. 447 с.

СУЩЕСТВУЕТ ЛИ «ГЕН УБИЙЦЫ»? ДЕКОНСТРУКЦИЯ ПОПУЛЯРНОГО МИФА

Попкова А.И.[1], Алейникова В.А.[2]

[1]Попкова Анастасия Ивановна - студент
[2]Алейникова Валерия Андреевна – ассистент кафедры уголовного права и процесса,
Белгородский государственный национальный исследовательский университет,
г. Белгород

Аннотация: *в статье рассматривается комплексный характер этиологии агрессивного и криминального поведения. На примере ключевых исследований опровергается редукционистский миф о существовании «гена убийцы». Доказывается, что поведенческие фенотипы, включая склонность к насилию, формируются в результате динамического взаимодействия (G×E) генетических предиспозиций, эпигенетических модификаций, вызванных средой, и социально-психологических факторов, прежде всего детского травматического опыта. Анализ данных близнецовых исследований, лонгитюдных проектов и молекулярно-генетических работ подтверждает, что генетический риск реализуется преимущественно в условиях неблагоприятной среды.*

Ключевые слова: *антисоциальное поведение, гено-средовое взаимодействие, эпигенетика, полиморфизм MAOA, детская травма, психопатия, близнецовые исследования.*

«На Западе сейчас в связи с расцветом науки о генетике пытаются найти маркеры, определяющие поведение человека. Активно выдвигается гипотеза о том, что многие преступления – всего лишь следствие наличия определенных генов», – Петр Меньшанов, старший научный сотрудник Института цитологии и генетики СО РАН [2].

Речь идет о дофаминовом рецепторе D4. Вариация гена этого рецептора определят тип поведения человека: низкая внимательность, гиперреактивность, неумение

сконцентрироваться, желание быстро что-то получить. По распространенной гипотезе, носители этого гена часто начинают с мягких асоциальных действий, а потом переходят к более жестоким преступлениям: становятся маньяками, убийцам, грабителями. Новосибирские учёные решили проверить, насколько данный тезис корректен. Изучали, есть ли этот ген у тихих и спокойных людей. Оказалось, что эти гены вполне могут встречаться и без реальной гиперактивности у человека. Следовательно, теория о том, что гиперактивность сама по себе приводит людей на путь агрессивности и жестокости – не доказывается. В ходе исследования, были собраны данные о двух группах людей: первая группа состояла из 161 человека, куда вошли преступники со всей страны, совершившие спланированные убийства, побои, и т.д.; во второй группе – 400 обычных людей, за которыми уголовных статей не числится. Их биологические данные были изучены, и как результат, никаких определенных закономерностей, позволяющих сказать – у преступников есть «ген убийцы», а у людей, находящихся на свободе его нет, – не получилось. Законы генетики и уголовного кодекса оказались не совместимы.

Особый научный интерес в рамках данной проблематики представляют исследования, сфокусированные на гене моноаминоксидазы-А (МАОА). Данный ген кодирует фермент, критически важный для метаболизма ключевых нейромедиаторов — серотонина, дофамина и норадреналина. Согласно ряду исследований, определенные аллельные варианты, ассоциированные со сниженной активностью этого гена, могут обусловливать нарушения в регуляции нейромедиаторных систем. Подобные дисфункции, в свою очередь, рассматриваются в качестве одного из потенциальных нейробиологических факторов, повышающих предрасположенность к импульсивным формам поведения, включая агрессию. Важно отметить, что несмотря на распространение в массовой культуре упрощенческого термина «ген убийцы», его использование не соответствует академической точности.

На основании анализа данных доказательной медицины и психологии установлено, что формирование устойчивой склонности к агрессивному и противоправному поведению является следствием комплексного взаимодействия биологических и социальных факторов.

Классическое исследование, проведенное под руководством Каспи и Моффитт в 2002 году, стало важной вехой в изучении гено-средового взаимодействия. Они изучили связь между генетическими факторами (полиморфизмом MAOA) и детскими травмами. Было обнаружено, что носители низкоактивной версии гена MAOA, которые в детстве подвергались физическому и эмоциональному насилию, более склонны к агрессивному поведению. Однако те, кто не имел негативного опыта в детстве, несмотря на ту же генетическую предрасположенность, не демонстрировали повышенной склонности к насилию.

Проект "Dunedin" (Новая Зеландия): В этом лонгитюдном исследовании была отмечена сочетанная модель действия генетических и экологических факторов — генетическая предрасположенность не реализуется без воздействия внешних факторов (стресс, жестокое воспитание, социальные трудности). Современные исследования в области поведенческой генетики выходят за рамки изучения гена MAOA, охватывая и другие ключевые генетические вариации, влияющие на нейромедиаторный обмен.

-Ген COMT, кодирующий фермент катехол-О-метилтрансферазу, подвержен полиморфизмам, которые оказывают существенное влияние на индивидуальные различия в реактивности нервной системы и способности противостоять стрессовым воздействиям.

-Гены DAT1 и SLC6A4, отвечающие за функционирование дофаминовой и серотониновой систем соответственно, также находятся в фокусе научного интереса. Анализ их полиморфных вариантов проводится для выявления молекулярно-генетических основ нарушения импульсного контроля.

Серийное насилие не может быть адекватно интерпретировано в рамках какой-либо одной дисциплины, включая генетику. Данная поведенческая аномалия возникает на пересечении трех ключевых осей: биологической (как потенциальная уязвимость нервной системы), психологической (как сформированные личностные паттерны и расстройства) и социальной (как триггерная или способствующая среда). Таким образом, генетика является не ответом, а лишь одним из компонентов сложной объяснительной модели.

В основном, всё идёт из детства, когда психика ребёнка ещё не до конца окрепла, и он наиболее подвержен всем негативным факторам, возникающих из окружающего мира [6, 287- 292]

Сравнительный анализ монозиготных и дизиготных близнецов служит надежным методом оценки наследуемости поведенческих черт. Согласно данным масштабного мета-анализа, объединившего результаты пятидесяти лет исследований, наследственный компонент антисоциального поведения составляет около 50%. При этом, как подчеркивается в научной литературе, данный показатель не является статичным: оценки наследуемости варьируются в зависимости от социоэкономического контекста, методов воспитания и других средовых переменных, что указывает на сложный характер генно-средового взаимодействия [4, 702-709].

Эпигенетические исследования предоставляют молекулярное объяснение принципу G×E, демонстрируя, как опыт изменяет экспрессию генов без изменения самой ДНК. Ключевым примером является гипометилирование промотора гена глюкокортикоидного рецептора (*NR3C1*) у лиц, переживших в детстве жестокое обращение [3, 342-348]. Показано, что негативные средовые воздействия, такие как детская травма или жестокое обращение, могут индуцировать химические модификации ДНК (например, метилирование), тем самым повышая риск проявления агрессивного поведения даже при отсутствии патогенных генетических мутаций.

Роль внешних факторов невозможно переоценить. Хронический стресс, физическое и эмоциональное насилие, пренебрежение и формирование небезопасной привязанности (по Дж. Боулби) приводят к структурным и функциональным изменениям в мозге. Нейровизуализационные исследования фиксируют снижение объема и активности префронтальной коры (ответственной за самоконтроль и принятие решений) и миндалевидного тела (связанного с обработкой эмоций, особенно страха и агрессии) у лиц с историей детской травмы [5, 652-666]. Эти изменения создают нейробиологическую основу для дефицита эмпатии, импульсивности и неспособности к эмоциональной регуляции — черт, характерных как для антисоциального поведения в целом, так и для психопатии в частности. Феномен серийного насилия представляет собой крайнее проявление комплекса рассмотренных факторов. Для серийных преступников часто характерна психопатия, черты которой (глубокая эмпатическая дисфункция, манипулятивность, отсутствие вины) имеют как генетическую составляющую (умеренную наследуемость), так и отчетливую связь с тяжелым детским опытом и специфическими нейробиологическими аномалиями [1, 786-799].

Таким образом, серийный убийца — не «носитель гена убийцы», а продукт редкой и фатальной констелляции генетической уязвимости, эпигенетических изменений, сформированных средой, тяжелой психологической травмы и специфических личностных расстройств.

Современная наука отвергает линейные модели «ген → преступление». Агрессивное и антисоциальное поведение является продуктом многомерного взаимодействия биологической предиспозиции (часто в виде полигенного риска), эпигенетических модификаций, индуцированных средой, и мощного влияния социально-психологических факторов, прежде всего травматического детского опыта. Упрощенная интерпретация данных о генетических ассоциациях, порождающая миф о «гене убийцы», не только

научно несостоятельна, но и этически опасна, так как ведет к стигматизации и биологическому детерминизму. Понимание комплексной природы такого поведения должно служить основой для разработки профилактических мер, направленных на смягчение средовых рисков (поддержка семей, предотвращение насилия над детьми, психологическая помощь), а не на спекулятивные генетические скрининги.

Список литературы

1. *Блэр Р.Дж.Р.* (2013). Нейробиология психопатических черт у молодежи. Nature Reviews Neuroscience, 14 (11), 786-799.
2. *Комякова Е.* «Существует ли ген убийцы? Исследование новосибирских ученых включили в американский учебник по криминалистике» // «Комсомольская правда» https://www.nsk.kp.ru/daily/26997/4059067/
3. *Макгоуэн П., Сасаки А., Д'Алессио А. и др.* Эпигенетическая регуляция глюкокортикоидного рецептора в мозге человека связана с жестоким обращением в детстве // Nat Neurosci 12, 342-348 (2009). https://doi.org/10.1038/nn.2270
4. *Полдерман Т., Беньямин Б., де Леу С. и др.* Метаанализ наследуемости черт человека на основе пятидесяти лет исследований близнецов // Nat Genet 47, 702-709 (2015). https://doi.org/10.1038/ng.3285
5. *Тейчер М.Х., Самсон Дж.А., Андерсон К.М. и Охаши К.* (2016). Влияние жестокого обращения в детстве на структуру, функции и взаимосвязи мозга // Nature Reviews Neuroscience, 17 (10), 652-666.
6. *Чубарова А.В.* Влияние социальной среды на формирование преступности несовершеннолетних // Бюллетень науки и практики. – 2021. – №3. – С. 287- 292

КРИМИНОЛОГИЧЕСКАЯ ОБОСНОВАННОСТЬ КРИМИНАЛИЗАЦИИ НОВЫХ ВИДОВ ДЕЯНИЙ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ (НА ПРИМЕРЕ КИБЕРБУЛИНГА И ДОКСИНГА)

Солодовникова В.Д.[1], Алейникова В.А.[2]

[1]Солодовникова Валерия Дмитриевна - студент,
[2]Алейникова Валерия Андреевна – ассистент
кафедры уголовного права и процесса,
Белгородский государственный национальный
исследовательский университет,
г. Белгород

Аннотация: *статья посвящена криминологическому обоснованию необходимости криминализации новых общественно опасных деяний в цифровой среде на примере кибербуллинга и доксинга. Цель исследования – проанализировать данные явления через призму критериев общественной опасности, недостаточности существующих правовых мер, а также выявить проблемы и перспективы введения уголовно-правовых запретов. В результате установлено, что, несмотря на высокую общественную опасность и массовость данных деяний, их криминализация сопряжена с рисками избыточного ограничения свобод, сложностями правоприменения и необходимостью международного сотрудничества. Основной вывод заключается в том, что криминализация должна быть субсидиарной, основанной на четко определенных составах и интегрированной в систему профилактических и восстановительных мер.*

Ключевые слова: *криминализация, кибербуллинг, доксинг, общественная опасность, уголовная политика, цифровая среда, восстановительное правосудие.*

Современный этап технологического развития, характеризуемый всеобщей цифровизацией социальных коммуникаций, закономерно порождает не только новые возможности, но и принципиально новые формы

противоправного поведения. Среди них наиболее социально-резонансными и широко распространенными стали кибербуллинг (систематическая травля, преследование, унижение или шантаж с использованием цифровых технологий) и доксинг (злонамеренное собирание и публичное раскрытие персональной или приватной информации о лице без его согласия с целью причинения вреда). Общественный запрос на защиту от подобных деяний закономерно приводит к дискуссиям о необходимости их криминализации, то есть введения уголовно-правового запрета. Однако данный процесс не должен быть реактивным ответом на публичную тревогу; он требует глубокой криминологической проработки, основанной на анализе объективных признаков деяния, оценке его общественной опасности и прогнозе эффективности уголовного закона. Криминологическая обоснованность выступает ключевым фильтром, отсекающим популистские решения и направляющим уголовную политику в русло взвешенного, целесообразного и эффективного правового регулирования.

Основным критерием, с позиции криминологической науки, для признания деяния преступным является высокая степень общественной опасности. И кибербуллинг, и доксинг в своих агрессивных, системных проявлениях полностью соответствуют этому критерию, причем их опасность носит специфический, усиленный цифровой средой характер. Кибербуллинг трансформирует традиционную травлю, придавая ей свойства тотальности и перманентности: анонимность или псевдонимность агрессора снижает уровень социального контроля и чувство ответственности; потенциально бесконечная аудитория интернета умножает унижение жертвы; постоянная доступность травмирующего контента создает эффект «вечного присутствия» угрозы, не оставляя жертве безопасного пространства [1, с. 45]. Это приводит к тяжелейшим психологическим последствиям — от хронических тревожных расстройств и глубоких депрессий до суицидальных исходов, что документально подтверждается рядом психологических и социологических

исследований. Доксинг, в свою очередь, прямо посягает на фундаментальные права личности на неприкосновенность частной жизни и личную безопасность. Превращая приватную информацию (адрес, данные о родственниках, финансовые сведения) в орудие мести, шантажа или подстрекательства к оффлайн-насилию, он создает непосредственную угрозу не только психологическому, но и физическому благополучию человека, что особенно опасно в контексте организованного троллинга или преследования активистов [2, с. 112]. Эмпирические данные свидетельствуют о массовости и устойчивой тенденции к росту данных явлений, особенно среди подростков и молодых взрослых, что подчеркивает их характер как масштабной социальной проблемы [3, с. 200-201]. При этом латентность киберпреступлений против личности крайне высока: многие пострадавшие не обращаются в правоохранительные органы из-за неверия в эффективность, страха эскалации травли или отсутствия знаний о механизмах правовой защиты, что искажает официальную статистику и усложняет оценку реальных масштабов явления [4, с. 33].

Важнейшим криминологическим аргументом в пользу рассмотрения вопроса о криминализации является недостаточность существующих правовых механизмов. Действующие составы о клевете или оскорблении часто не охватывают систематический, многоаспектный характер кибербуллинга, а норма о нарушении неприкосновенности частной жизни (ст. 137 УК РФ) может не учитывать специфику доксинга как целенаправленной кампании по запугиванию и причинению вреда через раскрытие данных, особенно когда информация формально является общедоступной, но используется в агрессивном контексте. Гражданско-правовые иски и административные меры оказываются неадекватными тому масштабу морального и психического ущерба, который причиняется жертвам, и не выполняют в полной мере превентивную функцию, поскольку не несут в себе достаточно мощного карательного

и воспитательного потенциала [5, с. 67]. Таким образом, с точки зрения классической криминологической теории, кибербуллинг и доксинг в их наиболее опасных формах демонстрируют признаки «пробела» в системе уголовно-правовой защиты личности, что является формальным основанием для рассмотрения возможности криминализации.

Однако процесс криминализации сопряжен с комплексом серьезных проблем, игнорирование которых может привести к негативным социальным и правовым последствиям, сводящим на нет потенциальную пользу нового закона. Первой и ключевой является проблема точного юридического определения диспозиции состава преступления. Сложно сформулировать юридически безупречные формулировки, которые четко отделяли бы уголовно наказуемый кибербуллинг от грубых, но единичных оскорбительных высказываний в ходе жаркой дискуссии, а криминальный доксинг — от легитимной публикации общедоступных данных в рамках журналистского расследования или общественного обсуждения деятельности публичных лиц. Вторая проблема лежит в сфере доказывания: установление прямой причинно-следственной связи между актом кибербуллинга или доксинга и наступившими тяжкими последствиями (например, попыткой самоубийства или тяжелым психическим расстройством) представляет значительную процессуальную сложность. Это может привести к высокой доле оправдательных приговоров и, как следствие, к дискредитации новой нормы права и разочарованию потерпевших. Третья проблема связана с субъектом преступления — значительную долю агрессоров в киберпространстве составляют несовершеннолетние, что ставит сложные вопросы о целесообразности и этической допустимости применения к ним уголовной репрессии, а также актуализирует необходимость развития восстановительных и воспитательных практик, которые могут быть более эффективны, чем судимость. Наконец, трансграничная природа интернета означает, что преступник

и жертва могут находиться в разных странах, что требует сложной международно-правовой кооперации для расследования и может сделать национальный уголовный закон трудноисполнимым на практике, сводя его действие к случаям, когда все участники находятся в одной юрисдикции.

Перспективы криминологически обоснованной криминализации лежат в плоскости поиска сбалансированной, дифференцированной модели уголовной ответственности, которая бы минимизировала риски и максимизировала защитный потенциал закона. Прежде всего, уголовный закон должен играть субсидиарную роль, вступая в действие лишь при причинении тяжкого вреда психическому или физическому здоровью либо при доказанной систематичности и интенсивности преследования, когда все иные меры (административные, гражданско-правовые, медиационные) исчерпаны. Во-вторых, необходима «ювелирная» проработка составов, ориентированная на криминализацию не самого факта распространения информации, а конкретного способа и цели ее использования для причинения вреда. Например, криминализации может подлежать не любое раскрытие данных, а только доксинг, совершенный с конкретной умышленной целью — побудить третьих лиц к совершению насильственных или иных противоправных действий в отношении жертвы, что соответствует опыту некоторых зарубежных правопорядков, где акцент делается на «намерении запугать» [6, с. 95]. В-третьих, криминализация должна быть неразрывно связана с развитием системы профилактических и восстановительных мер, включая образовательные программы по цифровой гигиене и кибербезопасности в школах, создание низкопороговых служб психологической помощи жертвам и внедрение технологий восстановительного правосудия для работы с агрессорами-подростками. Без этого уголовный закон рискует стать лишь карательным инструментом, не решающим корни проблемы. В-четвертых, эффективность

любой новой нормы напрямую зависит от процессуального и кадрового обеспечения: необходима специальная подготовка следователей и судей в сфере работы с цифровыми доказательствами, криминалистического анализа интернет-трафика, а также гармонизация международного сотрудничества по быстрому сбору доказательств.

Таким образом, кибербуллинг и доксинг обладают значительным криминогенным потенциалом и объективно высокой общественной опасностью, что в принципе обосновывает постановку вопроса об их уголовно-правовом запрете. Однако решение о криминализации должно быть результатом тщательного криминологического анализа, а не сиюминутной реакции на общественный резонанс. Такой подход требует тщательного взвешивания баланса между необходимостью защиты личности от новых цифровых угроз и защитой фундаментальных прав и свобод, таких как свобода слова и информационная открытость. Только сбалансированный и научно обоснованный путь позволит эффективно защитить достоинство и права личности в цифровую эпоху, не поступившись при этом принципами правового государства.

Список литературы

1. *Бочавер А.А., Хломов К.Д.* Кибербуллинг: травля в пространстве современных технологий // Психология. Журнал Высшей школы экономики. 2014. Т. 11, № 3. С. 32–57.
2. *Головань А.В., Смирнова Е.О.* Распространенность кибербуллинга среди подростков в России: социологический анализ // Мониторинг общественного мнения: Экономические и социальные перемены. 2021. № 3. С. 108–125.
3. Информационная безопасность и правовые основы защиты персональных данных [Электронное издание]: учебное пособие / А.В. Терехов, В.Н. Чернышов, А.В. Платенкин, А.В. Селезнев. – Тамбов: Издательский центр ФГБОУ ВО «ТГТУ», 2023.

4. *Бочавер А.А., Хломов К.Д.* (2013). Буллинг (травля) как объект исследований и культурный феномен. Психология. Журнал Высшей школы экономики, 10(3), 149–159.
5. *Бобровникова Н.С.* Кибербуллинг: виды и особенности проявления / Н.С. Бобровникова // Международный научно-исследовательский журнал. — 2022. — №11 (125). — URL: https://research-journal.org/archive/11-125-2022-november/10.23670/IRJ.2022.125.86 (дата обращения: 15.12.2025).
6. *Романовская Е.А.* Публично-правовые основы противодействия доксингу // Наука. Общество. Государство. 2023. №2 (42). URL: https://cyberleninka.ru/article/n/publichno-pravovye-osnovy-protivodeystviya-doksingu (дата обращения: 16.12.2025).

КРИМИНОЛОГИЧЕСКИЕ РИСКИ НА РЫНКЕ КРИПТОАКТИВОВ: ОТ МОШЕННИЧЕСТВА ДО ОТМЫВАНИЯ ДЕНЕГ

Савин В.Д.[1], Алейникова В.А.[2]

[1]Савин Владимир Дмитриевич - студент,
[2]Алейникова Валерия Андреевна – ассистент
кафедры уголовного права и процесса,
Белгородский государственный национальный исследовательский университет,
г. Белгород

Аннотация: *в статье проводится криминологический анализ ключевых рисков на рынке криптоактивов, основными из которых являются мошенничество и отмывание денег. Исследование раскрывает специфику противоправной деятельности через призму классических криминологических теорий.*

Ключевые слова: *криптоактивы, криминологические риски, мошенничество, отмывание денег, теория рационального выбора, теория рутинной деятельности, беловоротничковая преступность, киберпреступность, виктимология, фишинг.*

Криптоактивы, представляя собой инновационный финансовый инструмент на основе распределённых реестров, с момента своего появления сформировали обширное и динамично развивающееся рыночное пространство. Кочергин Д.А., определил криптоактивы как частные активы, которые воплощают ценности или права, записываемые в электронной форме в распределённом реестре, защищённом криптографически. Такие активы не выпускаются и не гарантируются государственными органами [1]. Однако их децентрализованная природа, анонимность или псевдоанонимность транзакций, а также изначально трансграничный характер создали уникальную среду для возникновения и эволюции новых криминологических рисков, которые требуют глубокого осмысления. Ключевые риски концентрируются вокруг двух основных видов противоправной деятельности: мошенничества, направленного на незаконное изъятие активов у владельцев, и отмывания денег, нацеленного на легализацию доходов, полученных преступным путём.

Мошенничество на рынке криптоактивов отличается значительным разнообразием и технологической изощрённостью. Одной из наиболее распространённых и опасных форм являются мошеннические схемы при первичном размещении монет и токенов (фальшивое ICO). Токен – это цифровой актив, который может использоваться в различных целях: как средство оплаты, подтверждение права собственности, участие в проекте или голосование в децентрализованной системе. Токены не имеют собственного блокчейна, их использование основано на функционале других платформ.

Первичное размещение монет (ICO) – это способ привлечь финансирование для рискованных проектов, не оформляя никаких бумаг и не давая ничего взамен. В ходе ICO команда проекта распродаёт цифровые токены среди инвесторов за криптовалюты или фиатные деньги [2].

Другой массовой формой являются финансовые пирамиды, которые маскируются под высокодоходные

инвестиционные программы. Деньги все так же выплачивают за привлечение новых инвесторов, а не за счёт реальной прибыли. Когда приток вкладчиков прекращается, схема рушится. К примеру, новая инвестиционная платформа обещает высокую доходность и агитирует участников вкладывать деньги и приглашать друзей и членов семьи. Чем больше – тем выше выплаты. Ранним инвесторам действительно выплачивают деньги за счёт средств новых участников. Но как только вкладчики и инвесторы перестают приходить, пирамида рушится – и большинство теряет свои вложения [2].

Второй масштабный блок криминологических рисков связан с использованием криптоактивов для отмывания денег. Процесс легализации преступных доходов в этой сфере, как правило, состоит из трёх классических стадий, которые, однако, приобретают специфические черты. На этапе размещения криминальные фиаты конвертируются в криптовалюту через онлайн-обменники или криптобанкоматы, которые могут иметь слабые системы контроля. Далее следует стадия расслоения, направленная на разрыв связи между источником средств и их конечным получателем [3].

С точки зрения криминологии, мошенничество на рынке криптоактивов представляет собой комплексную и многогранную проблему, корни которой лежат в уникальном стечении криминогенных факторов. Преступная деятельность в этой сфере является классическим примером теории рационального выбора, представителями которой являются Дж. Корнуиш и Р. Кларк. Теория предполагает, что правонарушители делают рациональный выбор и поэтому выбирают цели, которые сулят высокую награду при минимальных усилиях и риске. Совершение преступления зависит от двух факторов: наличия по крайней мере одного мотивированного правонарушителя, который готов совершить преступление, и условий окружающей среды, в которой находится этот правонарушитель, а именно возможностей для совершения преступления [4].

Криминогенность этой среды идеально описывается теорией рутинной деятельности, где для совершения преступления необходимы три элемента: мотивированный преступник, подходящая жертва и отсутствие способного опекуна. На крипторынке все три элемента присутствуют в избытке: мотивированные преступники привлекаются лёгкими деньгами; в роли подходящих жертв выступают как недостаточно информированные, так и движимые жадностью инвесторы, охваченные ажиотажем; а в качестве «опекуна» выступают запаздывающие с реакцией регуляторы и правоохранительные органы, чьи полномочия ограничены национальными юрисдикциями [5].

Криптомошенничество как массовое явление стало возможным благодаря уникальному сочетанию технологических особенностей блокчейна, социально-экономических условий и психологии человека. Ключевой причиной является псевдоанонимность и необратимость криптовалютных транзакций, что создаёт для мошенников ощущение безнаказанности и серьёзно затрудняет работу правоохранительных органов [6]. Эти технологические условия совпали с растущим, но поверхностным интересом широких масс к цифровым активам, который часто подогревается «страхом упустить выгоду». Многие новые инвесторы, по данным «Chainalysis», приходят на рынок в периоды роста, движимые желанием быстро обогатиться, но при этом не обладают достаточной цифровой и финансовой грамотностью, чтобы распознать обман. Именно этот разрыв между высокими ожиданиями и низкой осведомлённостью активно эксплуатируют преступники. Мошенники используют изощрённые методы социальной инженерии, такие как схемы «свиного убоя», когда долго и методично формируют доверительные, даже романтические отношения с жертвой в сети, прежде чем предложить «гарантированную» инвестиционную возможность. В 2024 году фишинг, особенно с использованием поддельных адресов, стал главным методом кражи, позволив увести более $1 миллиарда. Параллельно развиваются технически

сложные атаки на смарт-контракты, такие как «ковровое выдёргивание», когда создатели токена внезапно изымают всю ликвидность, или создание токенов-«ловушек», которые нельзя продать [7].

Личность современного криптомошенника эволюционировала от одиночных хакеров к высокоорганизованным, часто транснациональным группам, которые действуют как профессиональные бизнес-структуры.

Ещё в 2012 году в статье «Общая характеристика психологии киберпреступника» [8] и других подобных публикациях киберпреступников называли крэкерами или кракерами, но в современных работах терминология в целом соответствует общепринятой в IT-среде.

Отдельные авторы предпринимают попытки ввести более подробную классификацию. Например, Дворянкин О. А. (кандидат юридических наук Московского университета МВД России) выделяет в своей работе 11 групп хакеров с разной мотивацией, включая Script Kiddie, чей основной мотив причинить ущерб, Blue Hat, которые «нанимаются организациями для проверки своих программ или сетей на наличие ошибок до их выпуска или внедрения», нанятых правительством Red Hat и даже игровых хакеров, которые «обычно проводят свои атаки в попытке украсть кредитные кэши конкурентов или вызвать распределенные атаки типа «отказ в обслуживании», чтобы вывести их из игры» [9], [10].

При попытке описать типичного киберпреступника среди исследователей нет единого мнения. Существующие данные и подходы формируют противоречивую картину. Одна группа авторов указывает на широкий демографический и психологический диапазон: преступниками в цифровом пространстве могут быть как мужчины, так и женщины в возрасте от 12 до 30 лет, с различным уровнем интеллекта - от невысокого до исключительного. В этом портрете часто фигурируют психические расстройства, такие как аутизм (в частности, синдром Аспергера), или наличие детских психологических травм.

По мнению Полякова В.В., Попова Л.А., другая, более распространённая точка зрения, напротив, сужает профиль до более конкретного образа: чаще всего это молодые мужчины, проживающие в городах, с доходом выше среднего. Они часто являются студентами технических специальностей или уже работающими IT-специалистами (например, программистами) и, как правило, не имеют судимостей [11]. В литературе можно встретить достаточно широкий спектр психологических особенностей, которые приписываются киберпреступникам: тревожные расстройства (социальная фобия, обсессивно-компульсивное расстройство, генерализованное тревожное расстройство, посттравматическое стрессовое расстройство); депрессия; аутизм и такой его подвид, как синдром Аспергера с «ограниченным, стереотипным, повторяющимся набором интересов и занятий»; диссоциальное расстройство (социопатия); парциальное диссоциативное расстройство идентичности; другие диссоциативные расстройства личности. Шизоидная акцентуация личности - характерная для компьютерных гениев-одиночек, выполняющих заказы террористических группировок. Преобладание негативных черт NET-мышления у «чёрных» хакеров: поверхностность, синдром рассеянного внимания, расщепление сознания, отрывистость мышления; трудности анализа и синтеза, сравнения и обобщения. Эти данные, в основном полученные в результате опросов пойманных киберпреступников, представляют их не в лучшем свете. Однако есть исследователи, которые рисуют хотя бы отчасти более привлекательный портрет [10].

Однако существует и альтернативный взгляд, который рисует несколько иную, отчасти более привлекательную картину. Согласно этой точке зрения, личности профессиональных киберпреступников отличаются устойчивостью и сформированностью. Это амбициозные люди, хорошо осознающие собственную ценность и последствия своих действий. Формирование их противоправного поведения происходит, как правило, на ранних этапах погружения в IT-

сферу, где изначальной мотивацией служит не столько материальная выгода, сколько демонстрация интеллектуального превосходства и мастерства.

Общая статистика и динамика этого явления противоречивы, что требует взвешенной интерпретации. Согласно отчёту TRM Labs за 2025 год, общий объем незаконных операций с криптовалютой в 2024 году оценивается в $44.7 млрд, что составляет около 0.4% от общего транзакционного объёма (более $10.6 трлн) [12]. Этот показатель снизился с 0.9% в 2023 году. Однако авторы отчёта сразу предупреждают, что эти цифры будут существенно пересмотрены в сторону увеличения по мере поступления новых данных - как это произошло с оценкой за 2023 год, которая выросла с $34.8 до $58.7 млрд. То есть, видимое снижение доли может быть статистическим артефактом.

Профилактика криптомошенничества в современных условиях должна быть многоуровневой, сочетающей технические меры, регуляторное давление и, что важнее всего, просвещение пользователей. На институциональном уровне эффективность демонстрируют инициативы вроде подразделения T3 по борьбе с финансовыми преступлениями, созданного TRON, Tether и TRM Labs, которое за несколько месяцев работы по запросам правоохранителей заблокировало активы на $130 млн. Криптобиржи внедряют сложные алгоритмы для проверки смарт-контрактов и анализа поведения токенов до их листинга. Однако основная нагрузка ложится на самого пользователя. Специалисты по безопасности, в том числе из компании Malwarebytes, Gate.io и авторы криптоаналитики, сходятся в базовых правилах [6].

Основываясь на анализе, рынок криптоактивов представляет собой высококриминогенную среду, где ключевыми угрозами являются мошенничество и отмывание денег. Эти риски порождены технологической псевдоанонимностью блокчейна, отставанием регуляторов и эксплуатацией жадности и неосведомлённости жертв, что идеально соответствует криминологической модели, где есть

мотивированный преступник, уязвимая цель и отсутствующий защитник. Личность преступника эволюционировала от хакера-одиночки до участника транснациональных групп, а методы стали сложнее, сместившись к социальной инженерии и техническим атакам. Хотя статистика может показывать колебания, общий ущерб остаётся значительным, а преступность становится более организованной. Поэтому эффективная профилактика требует комплексного подхода: ускоренного развития международного регулирования, внедрения строгих мер контроля на биржах и, что важнее всего, постоянного повышения финансовой и цифровой грамотности пользователей, которые являются последним и ключевым барьером на пути мошенников.

Список литературы

1. *Кочергин Д.А.* Криптоактивы: экономическая природа, классификация и регулирование оборота // Журнал Вестник международных организаций: образование, наука, новая экономика. - 2022. - №3. - С. 75-77.
2. Что такое скам в криптовалюте: шесть популярных видов мошенничества // СОВКОМБЛОГ URL: https://journal.sovcombank.ru/investitsii/chto-takoe-skam-v-kriptovalyute-shest-populyarnih-vidov-moshennichestva (дата обращения: 04.11.2025).
3. Что такое криптографическая фишинговая атака и как ее избежать // Quickex URL: https://quickex.io/ru/blog/guide/what-is-a-phishing-attack-in-crypto (дата обращения: 07.11.2025).
4. *Плешаков В.А.* Зарубежный опыт ситуационного подхода в криминологии // Гуманитарные, социально-экономические и общественные науки. - 2021. - С. 109-111.
5. Теория рутинной деятельности // Бетши URL: https://betshy.com/ru/2024/03/08/теория-рутинной-деятельности (дата обращения: 07.11.2025).
6. Распространенные криптовалютные мошенничества - как защитить свои инвестиции и не стать жертвой //

Alwarebytes URL: https://www.malwarebytes.com/ru/cybersecurity/basics/cryptocurrency-scams (дата обращения: 26.10.2025).
7. Тенденции криптопреступности в 2024 году: Незаконная деятельность снижается по мере снижения уровня мошенничества и кражи средств, но рынки программ-вымогателей и Даркнета растут // Chainalysis URL: https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/ (дата обращения: 26.10.2025).
8. *Косенков А.Н., Черный Г.А.* Общая характеристика психологии киберпреступника // Всероссийский криминологический журнал, 2012.
9. *Оганов А.А.* Оперативно-розыскные особенности киберпреступлений в отношении детей и подростков с использованием киберпространства // Журнал «Вестник Московского университета МВД России», 2019.
10. Киберпреступник глазами российских психологов: черты, мотивы, ценности, отклонения // Хабр URL: https://habr.com/ru/companies/bastion/articles/765490/ (дата обращения: 30.10.2025).
11. *Поляков В.В., Попов Л.А.* Особенности личности компьютерных преступников // Журнал «Известия Алтайского государственного университета», 2018.
12. Отчет о криптопреступности за 2025 год Основные тенденции, которые сформировали нелегальный рынок криптовалют в 2024 году // TRM URL: https://www.trmlabs.com/reports-and-whitepapers/2025-crypto-crime-report (дата обращения: 30.10.2025).

СЕМЕЙНОЕ НЕБЛАГОПОЛУЧИЕ КАК ФАКТОР ФОРМИРОВАНИЯ КРИМИНОГЕННОГО ПОВЕДЕНИЯ У НЕСОВЕРШЕННОЛЕТНИХ

Семикопенко Д.С.[1], Алейникова В.А.[2]

[1]Семикопенко Дарья Сергеевна - студент,
[2]Алейникова Валерия Андреевна – ассистент кафедры уголовного права и процесса,

Белгородский государственный национальный исследовательский университет,
г. Белгород

Аннотация: *статья посвящена анализу влияния семейного неблагополучия на формирование криминогенного поведения у несовершеннолетних. Рассматриваются две условные категории неблагополучных семей: явные и скрытые. Автор доказывает, что независимо от формы, дисфункциональная семья выступает первичной и ключевой криминогенной средой. В работе раскрываются основные механизмы этого влияния: усвоение асоциальных поведенческих моделей через подражание, деформация системы ценностей и нравственных ориентиров, психологическая депривация, провоцирующая противоправное поведение, а также прямое или косвенное вовлечение подростка в антиобщественную деятельность. Делается вывод о том, что профилактика должна быть в первую очередь нацелена на раннее выявление семейного неблагополучия и комплексную работу по восстановлению воспитательного потенциала семьи как основного института социализации.*
Ключевые слова: *преступность несовершеннолетних, криминогенное поведение, семья, семейное неблагополучие, девиантное поведение, первичная социализация.*

Криминогенное поведение несовершеннолетних представляет собой сложный социально-правовой феномен, обусловленный биологическими, психологическими и социальными факторами. Среди них особое значение принадлежит семейному неблагополучию, которое выступает одним из основных определяющих отклонений в подростковой среде. Семья - это первичный социальный институт, в рамках которого строятся базовые поведенческие модели, ценностные установки и механизмы взаимодействия, определяющие траекторию социальной адаптации ребенка. Неблагополучная семейная атмосфера, ухудшение эмоциональных связей, асоциальное поведение родителей, жестокое обращение или, наоборот, гиперопека - могут

создать предпосылки для возникновения девиантного поведения ребенка.

В законодательстве Российской Федерации, в частности в Федеральном законе «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних» от 24.06.1999 N 120-ФЗ не дано определение «неблагополучной семьи», акцент ставится лишь на «семье, находящийся в социально опасном положении» [1]. В криминологической науке также отсутствует единый подход к понятию «неблагополучной семьи», каждый исследователь вкладывает в него свои особенности.

Так, В.М. Целуйко по этому поводу считает, что «под неблагополучной мы склонны понимать такую семью, в которой нарушена структура, обесцениваются или игнорируются основные семейные функции, имеются явные или скрытые дефекты воспитания, в результате чего появляются «трудные» дети» [2].

Однако стоит отметить, что не всегда «неблагополучной» можно назвать семью, где родители употребляют спиртные напитки и наркотические вещества, ведут антисоциальный образ жизни. Очень часто это внешне благополучные семьи с достаточно высоким уровнем дохода, с хорошими возможностями для воспитания и обучения детей, благоприятными жилищными условиями.

По этому поводу нельзя не согласиться с мнением врача-психиатра, писателя М.И. Буянова, который в своих научных трудах отмечает: «Неблагополучная для ребенка семья - это не синоним антисоциальной или асоциальной семьи. Существует великое множество семей, о которых ничего плохого с формальной точки зрения сказать нельзя, но, тем не менее, для данного конкретного ребенка эта семья будет неблагополучной. Конечно, семья пьяницы или хулигана для любого ребенка будет неблагополучной, однако в большинстве случаев, которые мы обсуждаем, понятие неблагополучной семьи может возникать лишь в соотношении с конкретным ребенком, на кого это неблагополучие действует. Для одного ребенка семья может

быть подходящей, а для другого эта же семья станет причиной тягостных душевных переживаний и даже психического заболевания. Разные бывают семьи, разные встречаются дети, так что только система отношений «семья - ребенок» имеет право рассматриваться как благополучная или неблагополучная» [3].

Точка зрения М.И. Буянова безусловно верна в своей гуманистической и психологической ориентации, подчеркивающей уникальность детско-родительских отношений. Однако в контексте криминологического исследования и социальной политики она должна применяться в совокупности с объективными критериями.

Критериями благополучия семьи для полноценного развития ребенка может являться:

- материальная обеспеченность и безопасные условия жизни. Наличие стабильного источника дохода, удовлетворяющего базовые потребности ребенка.

- физическое и психическое здоровье родителей. Способность выполнять родительские функции, отсутствие зависимостей, которые приводят к пренебрежению в воспитании ребенка.

- безусловное эмоциональное принятие и любовь, чтобы ребенок чувствовал себя любимым, ценным и защищенным вне зависимости от его успехов или поведения.

- стабильная и безопасная привязанность, то есть наличие у ребенка надежной эмоциональной связи хотя бы с одним значимым взрослым, к которому он может обратиться за поддержкой и утешением.

- согласованность действий и единство взглядов родителей.

Совпадение семьи со всеми критериями идеала встречается редко. Благополучная семья - это не семья без проблем, а семья, которая обладает достаточными ресурсами (материальными, психологическими, социальными) и функциональными паттернами для удовлетворения базовых потребностей ребенка и преодоления трудностей, минимизируя ущерб для

его развития. Ключевым является именно способность системы «семья-ребенок» обеспечивать безопасность, стабильность и поддержку.

Несмотря на очевидную важность чуткости и оперативной реакции родителей на нужды ребёнка для создания комфортной среды, во многих семьях, к сожалению, этого не происходит. Чтобы разобраться в истоках проблемы, необходимо обратиться к типологии семей, которые могут иметь тенденцию стать неблагополучными.

Исследователи отмечают несколько типов неблагополучных семей, влияющих на формирование криминогенного поведения подростков. Так, В.М. Целуйко разделяет неблагополучные семьи на две большие группы: «Первую группу составляют семьи с явной (открытой) формой неблагополучия: это так называемые конфликтные, проблемные семьи, асоциальные, аморально-криминальные и семьи с недостатком воспитательных ресурсов (в частности, неполные). Второю группу представляют внешне респектабельные семьи, образ жизни которых не вызывает беспокойства и нареканий со стороны общественности, однако ценностные установки и поведение родителей в них резко расходятся с общечеловеческими моральными ценностями, что не может не сказаться на нравственном облике воспитывающихся в таких семьях детей» [2].

Б.Н. Алмазов классифицирует неблагополучные семьи на семьи с недостатком воспитательных ресурсов, конфликтные семьи, нравственно неблагополучные семьи, и педагогически некомпетентные семьи [4].

В свою очередь, Ю.В. Корчагина предлагает более расширенную классификацию.

- «Проблемные семьи - это семьи, функционирование которых нарушено из-за педагогической несостоятельности родителей. Как правило, это конфликтные семьи с дисгармоничным стилем семейного воспитания (авторитарные, гипо- или гиперопекающие)».

- «Кризисные семьи - это семьи, переживающие внешний или внутренний кризис (изменение состава семьи,

взросление детей, развод, болезнь, смерть кого-либо из членов семьи, утрата работы, жилья, документов, средств к существованию и т.д.)»

- «Асоциальные семьи - признаком этих семей является наличие таких проблем, как алкоголизм, пренебрежение нуждами детей. При этом детско-родительские отношения полностью не разорваны (например, дети пытаются скрывать пьянство родителей, берут на себя ответственность за обеспечение семьи, уход за младшими детьми, продолжают учиться в школе).

- Аморальные семьи - это семьи, полностью утратившие семейные ценности, характеризующиеся алкоголизмом, наркоманией, жестоким обращением с детьми, не занимающиеся воспитанием и обучением детей, не обеспечивающие необходимых безопасных условий жизни. Дети в такой семье, как правило, не учатся, являются жертвами насилия, уходят из дома.

- Антисоциальные семьи - в этих семьях наблюдается крайняя степень семейной дисфункции. Они характеризуются противоправным, антиобщественным поведением, несоблюдением моральных, нравственных норм в отношении наименее защищенных членов семьи, нарушением экономических прав ближних. Это семьи, ведущие паразитический образ жизни, зачастую за счет принуждения детей к воровству, попрошайничеству и проституции» [5].

По нашему мнению, среди неблагополучных семей условно можно выделить два типа: явные и скрытые. К явно неблагополучным относятся аморальные, асоциальные, криминальные семьи, семьи алкоголиков или наркоманов, а также открыто конфликтные и неполные. Скрыто неблагополучные семьи внешне выглядят вполне благополучно: их члены ведут нормальный образ жизни и социально активны. Однако внутри таких семей отношения часто лишены моральных ценностей, сопровождаются антисоциальными установками и неблагоприятным поведением родителей [6].

Неблагополучная семья, как явная, так и скрытая, является одним из ключевых факторов формирования криминогенного поведения у несовершеннолетних. Это влияние проявляется через несколько взаимосвязанных механизмов:

- копирование моделей поведения. Ребенок, наблюдая за асоциальными, аморальными или противоправными поступками родителей, воспринимает их как допустимую или даже единственно возможную норму жизни. В скрыто неблагополучных семьях это может быть не прямое нарушение закона, а демонстрация цинизма, пренебрежение моралью, манипуляций или скрытой жестокости.

- деформация системы ценностей и нравственных ориентиров. В условиях отсутствия позитивных моральных установок, любви, поддержки и четких границ у ребенка не формируется внутренний запрет на противоправные действия. Ценности силы, обмана или потребления заменяют собой ценности сотрудничества, уважения и ответственности.

- психологическое неблагополучие. Хронические конфликты, эмоциональная холодность, отвержение, или наоборот, гиперопека порождают у подростка глубокие психологические проблемы: низкую самооценку, тревожность, агрессию, чувство ненужности. Криминальное поведение может становиться способом компенсации - получения ложного уважения в группе сверстников, материальных благ для самоутверждения или выплеска накопленной злости.

- непосредственное вовлечение в антиобщественную деятельность. В явно неблагополучных семьях дети могут быть прямо вовлечены в противоправные действия: попрошайничество, воровство, хранение или сбыт запрещенных веществ. Семья становится первичной «криминальной группой».

- ослабление или разрыв социальных связей. Неблагополучная семья, как правило, плохо выполняет свою посредническую функцию между ребенком и обществом (школой, государством). Это приводит к социальной

изоляции подростка, его бегству из дома и поиску замены в криминальных уличных группах, где он находит понимание и статус.

Таким образом, неблагополучная семья создает для несовершеннолетнего криминогенную среду, где деформируются личность, ценности и поведенческие навыки. Это значительно повышает риск того, что подросток изберет противоправный путь как способ адаптации к жизни, решения внутренних конфликтов или следования усвоенным в семье моделям.

В связи с этим, предложим комплекс рекомендаций для позитивного развития несовершеннолетнего и профилактики противоправного поведения.

Основой для гармоничного развития личности подростка и формирования у него устойчивого иммунитета к противоправным действиям является создание целостной и поддерживающей среды. Эта среда строится, прежде всего, на прочном фундаменте безусловного принятия и открытых, уважительных отношений внутри семьи. Подросток должен знать и чувствовать, что его любят и ценят не за достижения, а просто так, и что он может прийти к взрослому с любой, даже самой сложной проблемой, не боясь осуждения или наказания. Эмоциональная безопасность - первая и главная альтернатива поиску понимания в асоциальных группах. Одновременно с принятием важны разумные правила, обсужденные заранее, и логичные, предсказуемые последствия за их нарушение учат подростка ответственности и дают ему ощущение структуры и справедливости мира.

Параллельно необходимо целенаправленно работать над развитием внутреннего мира подростка. Ключевым становится воспитание эмпатии - способности понимать и чувствовать переживания других людей, что является прямой противоположностью эгоцентризму и жестокости. Не менее важно формировать здоровую, адекватную самооценку, хваля за приложенные усилия и найденные решения, а не за

врожденные качества, и помогая подростку находить и развивать свои сильные стороны через увлечения и хобби.

Нельзя оставлять вакуум в жизни подростка, который может заполниться деструктивным влиянием. Крайне важно помочь ему найти «свое дело» - будь то спорт, искусство, техническое творчество или научный кружок, где он сможет переживать успех, видеть свой прогресс и получать конструктивное признание. Это создает мощную положительную альтернативу скуке и псевдосамоутверждению в противоправных поступках.

Тесно с этим связана задача формирования здорового социального круга. Стоит поощрять общение в позитивных коллективах и создавать дома доброжелательную атмосферу для друзей. В современном мире отдельное внимание требует воспитание цифровой культуры - обучение не просто безопасности, а критическому восприятию информации, осознанию рисков в сети и развитию цифровой гигиены.

Фундаментом же всего этого процесса неизменно остается личный пример взрослых. Их поступки, манера общения, отношение к закону, словам и обещаниям являются самым мощным и наглядным учебником жизни. Невозможно требовать уважения, проявляя неуважение, или учить честности, будучи нечестным.

Эти рекомендации работают не по отдельности, а как система. Их цель - не тотальный контроль, а воспитание внутреннего стержня, системы ценностей и социальных связей, которые сделают для подростка совершение противоправного поступка внутренне неприемлемым, эмоционально невыгодным и социально неоправданным.

Таким образом, путь, уводящий подростка от пропасти противоправного мира, лежит не через запреты и контроль, а через любовь, понимание и созидание. Это кропотливая работа по строительству мостов - от одинокого острова детской неуверенности к материку взрослой ответственности, от тишины невысказанных обид - к диалогу, от внутренней пустоты - к наполненности смыслом и делом.

Список литературы

1. Федеральный закон «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних» от 24.06.1999 № 120 // Российская газета. - 1999 г. - № 121. - с изм. и допол. в ред. от 01.04.2025.
2. Психология неблагополучной семьи [Текст]: книга для педагогов и родителей / В.М. Целуйко. - Москва: Владос-Пресс, 2006. - 270.
3. *Буянов М.И.* Ребенок из неблагополучной семьи: записки детского психиатра: книга для учителей и родителей. - Москва: Просвещение, 1988. - 207 с.
4. *Алмазов Б.Н.* Психическая средовая дезадаптация несовершеннолетних- Свердловск: Уральский университет, 2006. -180 с.
5. *Корчагина Ю.В.* Неблагополучные семьи: факторы риска и методы работы. Методическое пособие по профилактике и преодолению жестокого обращения, девиантного поведения и алкогольной зависимости в семье. - Москва, 2008. - 159 с.
6. *Соловьева Т.В., Долотказина Н.Ю.* К ВОПРОСУ ОБ ОПРЕДЕЛЕНИИ ПОНЯТИЯ «СЕМЕЙНОЕ НЕБЛАГОПОЛУЧИЕ» // E-Scio. 2022. №5 (68). URL: https://cyberleninka.ru/article/n/k-voprosu-ob-opredelenii-ponyatiya-semeynoe-neblagopoluchie (дата обращения: 23.12.2025).

ВЛИЯНИЕ РЕЧИ РОДИТЕЛЯ НА РЕЧЕВОЕ РАЗВИТИЕ РЕБЕНКА

Кудусова Э.И.[1], Якубова Ф.Р.[2]

[1]Кудусова Эмине Илимдаровна – студент,
[2]Якубова Фериде Рустемовна - кандидат педагогических наук, старший преподаватель,
кафедра специального (дефектологического) образования,
ГБОУВО РК «Крымский инженерно-педагогический университет имени Февзи Якубова»,
г. Крым

Аннотация: *в данной статье рассматривается важность речи родителей в процессе речевого развития детей. Подчеркивается, что качество и количество речевых взаимодействий между родителями и детьми напрямую влияют на формирование языковых навыков, словарного запаса и коммуникативных умений. Исследуются различные подходы к общению с детьми, а также рекомендации для родителей по созданию благоприятной речевой среды.*
Ключевые слова: *речевое развитие, дошкольный возраст, влияние речи родителя.*

Постановка проблемы. В современном обществе родители часто недооценивают влияние своей речи на развитие языковых навыков у детей. Это вызывает необходимость изучения стилей общения и речевых практик родителей. Факторы, влияющие на речевое взаимодействие, включают уровень образования родителей, их речевые навыки, культурные особенности и наличие времени для общения. В условиях роста использования технологий важно исследовать их влияние на качество семейных речевых взаимодействий.

Цель статьи – рассмотреть важность речи родителей в процессе речевого развития детей.

Изложение основного материала. Влияние речевого поведения родителей на когнитивное и лингвистическое

развитие ребенка представляет собой ключевой аспект формирования его коммуникативных компетенций. Семья, как первичная социальная инстанция, является основополагающим институтом, в рамках которого закладываются фундаментальные основы языкового развития детей дошкольного возраста. Именно в семейном контексте происходит первичная социализация языка, формирование базовых моделей речевого поведения, которые впоследствии подвергаются дальнейшему развитию и усложнению в образовательных и социальных средах [3].

Семья представляет собой основополагающий базис для формирования речевых компетенций дошкольника. Создание благоприятной лингвистической среды и активное участие родителей в коммуникативных процессах способствуют развитию у ребенка необходимых навыков, обеспечивающих успешную учебную и социальную адаптацию[2].

Роль семьи в этом процессе заключается в создании насыщенной, поддерживающей и стимулирующей лингвистической среды. Родители, выступая в качестве первых носителей языкового кода для ребенка, служат важным образцом для подражания. Их речевые паттерны, эмоциональная окраска, интонационные характеристики, а также разнообразие лексических единиц и синтаксических конструкций оказывают непосредственное влияние на формирование лексико-грамматического строя и коммуникативных навыков ребенка [1].

Кроме того, семья оказывает значительное воздействие на речевое развитие через организацию совместных игровых практик, чтение литературы, ведение диалогов и рассказывание историй. Эти виды деятельности способствуют расширению активного и пассивного словарного запаса ребенка, а также улучшению его способности к пониманию и интерпретации языковых структур. Эмоциональное взаимодействие, включающее поддержку, поощрение и активное слушание, играет ключевую роль в формировании у ребенка уверенности в использовании речевых средств [2].

В контексте психолингвистических исследований, речевое развитие ребёнка рассматривается как многогранный процесс, на который существенное влияние оказывает языковая среда, формируемая родителями. Этот процесс можно охарактеризовать как основополагающий фактор, определяющий успешность овладения речью и коммуникативными навыками у детей раннего возраста. Создание насыщенной и благоприятной языковой среды предполагает активное участие родителей в речевом взаимодействии с ребёнком. Это включает в себя не только вербальное общение, но и невербальные компоненты, такие как интонация, жесты и мимика. В результате такого взаимодействия у ребёнка формируются когнитивные структуры, необходимые для понимания и продуцирования речи [4].

Развитие речи у детей является ключевым аспектом их когнитивного и социального развития. Эффективное речевое взаимодействие способствует формированию у ребёнка способности к осмысленному общению, что, в свою очередь, подготавливает его к успешному обучению в школе. Таким образом, родители играют критически важную роль в процессе формирования языковой компетенции у своих детей, что подтверждается многочисленными исследованиями в области психологии и педагогики [3].

Влияние речевой деятельности родителей на онтогенез речи ребенка представляет собой один из фундаментальных факторов, определяющих формирование коммуникативных компетенций, лексико-грамматического строя и общей языковой компетентности. В данном контексте можно выделить несколько ключевых аспектов этого влияния:

1. Качество и разнообразие речевого окружения: Родители, являясь основными информаторами и модели для подражания, оказывают существенное влияние на лексическое обогащение и грамматическую правильность речи ребенка. Исследования показывают, что дети, воспитывающиеся в среде с богатым и разнообразным

лексическим репертуаром, демонстрируют более высокий уровень языковой компетенции.

2. Частота и интенсивность речевой стимуляции: Регулярное взаимодействие с родителями, включающее в себя активное использование речи в различных контекстах, способствует развитию у ребенка способности к пониманию и воспроизведению языковых конструкций. Это, в свою очередь, положительно сказывается на формировании его синтаксических и морфологических навыков.

3. Эмоциональная окраска и интонационные модели: Интонационные особенности речи родителей, такие как мелодичность, ритм и эмоциональная окраска, играют важную роль в восприятии и интерпретации речевых сигналов ребенком. Эти параметры способствуют развитию у детей способности к эмоциональной выразительности и адекватной интерпретации эмоциональных состояний других людей.

4. Коррекционная функция: Родители часто выступают в роли первых корректоров речевых ошибок ребенка, что способствует формированию у него правильного произношения и грамматической корректности. Этот процесс является важным элементом первичной языковой социализации и влияет на дальнейшее развитие речевых навыков.

5. Контекстуальная обусловленность: Речевое взаимодействие с родителями происходит в конкретных социальных и культурных контекстах, что способствует усвоению ребенком социальных норм и правил речевого поведения. Это, в свою очередь, влияет на формирование у него коммуникативной компетентности и способности к адекватному взаимодействию с окружающими [1].

Если родители стремятся к всестороннему развитию своего ребенка, включая его коммуникативные способности, они должны уделять особое внимание формированию правильной речи. Исследования в области психолингвистики и логопедии подтверждают, что качество речевого взаимодействия между родителями и ребенком на ранних этапах его жизни играет ключевую роль в развитии речевых навыков.

Для достижения оптимального речевого развития ребенка необходимо соблюдать ряд основополагающих принципов [5]:

1. Ясность и четкость речи взрослых. С момента начала речевого общения с ребенком, взрослые должны стремиться к использованию ясной и четкой артикуляции. Это способствует более эффективному восприятию речи ребенком и стимулирует его к активному речевому подражанию.

2. Контекстуальное общение с ребенком. С первых месяцев жизни ребенка следует обращаться к нему как к мыслящему субъекту, способному понимать и реагировать на речь взрослых. Важно учитывать тон, темп и лексику разговоров, избегая сложных и малопонятных конструкций.

3. Эмоциональная и ритмическая составляющая речи. Спокойная, плавная и неторопливая речь способствует созданию благоприятной речевой среды, в которой ребенок может комфортно осваивать новые речевые паттерны. Ритмическая структура речи также играет важную роль в формировании мелодической составляющей речи ребенка.

4. Своевременное обращение к специалистам. При выявлении отклонений в речевом развитии ребенка, необходимо незамедлительно обратиться за консультацией к логопеду или дефектологу. Раннее вмешательство специалистов позволяет предотвратить развитие серьезных речевых нарушений и способствует более эффективному коррекционному воздействию.

В заключение можно отметить, что речь родителей играет решающую роль в речевом развитии ребенка. Именно от качества, богатства и эмоциональной насыщенности речевого взаимодействия зависит формирование у малыша лексико-грамматической базы, навыков коммуникации и умения выражать свои мысли. Создавая благоприятную языковую среду, родители не только способствуют развитию речи, но и закладывают основу для успешного обучения и полноценного социализации ребенка. Поэтому важным аспектом воспитания является осознанное и активное

использование речи в повседневной жизни, что существенно влияет на будущее речевое и личностное развитие малыша.

Список литературы

1. *Русанова Л.С.* Влияние семейных взаимоотношений на речевое развитие ребенка / Л.С. Русанова // Вестник Костромского государственного университета. Серия: Педагогика. Психология. Социокинетика. − 2016. − №4. – С. 45-52.
2. *Чигинцева Е.Г.* Доверительное общение в семье, имеющей ребенка с речевыми нарушениями / Е.Г. Чингинцева // Теория и практика современной науки. − 2015. − №6 (6). – С. 78-93.
3. *Смелова А.В., Бондаренко Т.А.* Взаимодействие логопеда с семьей по проблеме профилактики речевых нарушений у детей / А.В. Смелова, Т.А. Бондаренко // The Scientific Heritage. − 2019. − №32-3 (32). – С. 12-18.
4. *Костюк А.В., Малышева О.С., Брызгалова С.О., Тенкачева Т.Р.* Создание и использование информационных веб-ресурсов в работе с родителями дошкольников с нарушениями речи / А.В. Костюкова // Педагогическое образование в России. − 2020. − №6. – С. 52-56.
5. *Аванесян Р.Д., Белоусова С.В.* О работе с родителями в специализированном (речевом) детском саду / Р.Д. Аванесян, С.В. Белоусова // Специальное образование. − 2017. − №3. – С. 39-44.

РОЛЬ СЕМЬИ В КОРРЕКЦИИ ОТКЛОНЕНИЙ В РЕЧЕВОМ РАЗВИТИИ В ДОШКОЛЬНОМ ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ ДЛЯ ДЕТЕЙ С НАРУШЕНИЯМИ РЕЧИ

Аджемирова А.С.[1], Завьялова А.А.[2]

[1]Аджемирова Алина Серверовна - студент
[2]Завьялова Анастасия Александровна - преподаватель
кафедра специального (дефектологического) образования,
ГБОУВО РК «Крымский инженерно-педагогический университет имени Февзи Якубова»
г. Крым

Аннотация: *в данной статье рассматривается значение семьи в процессе коррекции отклонений в речевом развитии детей в дошкольном образовательном учреждении. Роль семьи оценивается с точки зрения сотрудничества с педагогами, обеспечения дополнительной практики и стимулирования речи дома, а также поддержки психологического благополучия ребенка. Статья предлагает рекомендации для улучшения сотрудничества между дошкольным учреждением и семьей для достижения успеха в речевом развитии детей с нарушениями.*
Ключевые слова: *семья, нарушение речи, дошкольный возраст, дошкольное образовательное учреждение (ДОУ).*

Постановка проблемы. В современном обществе растет число детей с нарушениями речи. Эти нарушения негативно влияют на коммуникацию, социализацию и обучение ребенка. Ранняя и комплексная коррекция речевых отклонений является важным условием успешного развития ребенка. Дошкольные образовательные учреждения для детей с нарушениями речи играют ключевую роль в этом процессе. Однако эффективность коррекционно-логопедической работы зависит от активного участия семьи. Данную тему освещали следующие авторы: Максименко О.П., Плотникова А.А., Семенова Т.Г., Фирсова И.Б. и другие.

Цель статьи – определить роль семьи в коррекции отклонений в речевом развитии детей, посещающих дошкольные образовательные учреждения для детей с нарушениями речи.

Изложение основного материала. Семья играет важную роль в коррекции речевых отклонений у детей, посещающих ДОУ. Ее значение обусловлено следующим:

1. Семья является первичной социальной средой, где ребенок формирует речевые навыки. Качество речевой среды, любовь и забота родителей способствуют развитию речи.

2. Семья может влиять на возникновение и развитие речевых нарушений через генетические, социальные и психологические факторы.

3. Семья закрепляет результаты коррекционной работы, создает речевую среду, проводит домашние занятия и сотрудничает со специалистами ДОУ.

4. Семья повышает свою компетентность через консультации логопеда и психолога, родительские собрания и индивидуальные беседы.

Активное участие родителей, сотрудничество со специалистами ДОУ и создание благоприятной речевой среды дома способствуют успешной коррекции речевых отклонений и полноценному развитию ребенка [2].

Роль семьи в процессе коррекции речевых нарушений у детей дошкольного возраста многогранна и может быть рассмотрена с различных точек зрения, каждая из которых вносит свой вклад в успешность коррекционной работы.

Сотрудничество с педагогами:

1. Обмен информацией. Родители и педагоги должны поддерживать постоянную связь, обмениваясь информацией о прогресс ребенка, его достижениях и трудностях.

2. Совместное планирование. Родители могут участвовать в планировании индивидуальных занятий с ребенком, предлагая свои идеи и учитывая особенности его развития.

3. Выполнение рекомендаций. Важно, чтобы родители выполняли рекомендации логопеда и воспитателей,

проводили с ребенком домашние занятия и создавали дома благоприятную речевую среду.

4. Участие в мероприятиях. Родители могут принимать участие в мероприятиях, организуемых ДОУ, таких как открытые занятия, родительские собрания, семинары и мастер-классы [4].

Обеспечение дополнительной практики:

– Закрепление навыков. Родители могут помогать ребенку закреплять навыки, полученные на занятиях с логопедом, проводя с ним специальные упражнения и игры.

– Речевые игры и упражнения. Существует множество речевых игр и упражнений, которые родители могут использовать для развития речи ребенка в домашних условиях.

– Чтение книг. Чтение книг – это один из самых эффективных способов развития речи ребенка. Родители должны читать ребенку книги ежедневно, обсуждая прочитанное и задавая вопросы.

– Расширение словарного запаса. Родители могут помогать ребенку расширять словарный запас, называя предметы окружающего мира, обсуждая их свойства и качества[1].

Стимулирование речи дома:

1. Создание речевой среды, где ребенок будет слышать грамотную речь и общаться с близкими.

2. Поощрение речевой активности: слушать ребенка, задавать вопросы и поддерживать разговор.

3. Использование различных ситуаций: совместные игры, прогулки, походы в магазин, приготовление еды.

Поддержка психологического благополучия ребенка:

– Любовь и поддержка. Родительская любовь и поддержка помогают ребенку чувствовать себя уверенно и справляться с трудностями.

– Позитивная атмосфера. Важно создавать дома позитивную атмосферу, где ребенок будет чувствовать себя комфортно и безопасно.

– Поощрение успехов. Родители должны поощрять успехи ребенка, поддерживать его мотивацию и веру в свои силы [3].

Чтобы улучшить сотрудничество между дошкольными учреждениями и семьями, рекомендуется применять следующие рекомендации:

1. Установите открытую коммуникацию между семьями и педагогами, чтобы обсуждать прогресс в речевом развитии.
2. Организуйте совместные мероприятия, где родители и педагоги могут обмениваться опытом.
3. Создайте индивидуальные планы речевого развития для каждого ребенка, учитывая его особенности.
4. Предоставляйте родителям подробные рекомендации и материалы для домашних заданий.
5. Проводите семинары и тренинги для родителей.
6. Учитывайте особые потребности ребенка в дошкольном учреждении.
7. Регулярно оценивайте успехи детей в речевом развитии и адаптируйте подход в соответствии с их потребностями [5].

Выводы: семья играет основополагающую роль в коррекции отклонений в речевом развитии детей дошкольного возраста. Родители и близкие должны осознавать свою ответственность за своевременную диагностику и начало коррекционной работы. Совместная деятельность педагогов и родителей, основанная на принципах сотрудничества, уважения и взаимного доверия, позволяет добиться значительных успехов в преодолении речевых нарушений. Семейные занятия по развитию речи, выполнение домашних заданий, регулярные посещения логопедических занятий и других форм коррекционной помощи способствуют формированию правильной речи у детей. Эффективная коррекция речевых отклонений возможна только при активном участии и тесном взаимодействии семьи и специалистов образовательного учреждения.

Список литературы

1. *Максименко О.П.* Формирование педагогической компетенции родителей в развитии речевых навыков ребенка в семье. / О.П. Максименко // Сборник материалов Ежегодной международной научно-практической конференции «Воспитание и обучение детей младшего возраста». – 2016. – №5. – С. 33-38.
2. *Плотникова А.А.* Развитие родительской компетентности в условиях дошкольного логопедического пункта / А.А. Плотникова // Вестник Таганрогского института имени А.П. Чехова. – 2008. – №1. – С. 74-80.
3. *Семенова Т.Г.* Формирование готовности родителей к коррекционно-логопедической работе с детьми с речевыми нарушениями / Т.Г. Семенова // Вестник СВФУ. – 2008. – №3. – С. 60-65.
4. *Фирсова И.Б.* Развитие представлений родителей о специфике речевого развития дошкольника / И.Б. Фирсова // Ярославский педагогический вестник. – 2014. – №1. – С. 88-91.
5. *Фирсова И.Б.* Особенности взаимодействия дошкольного образовательного учреждения с семьей по вопросу развития речи ребенка / И.Б. Фирсова // Специальное образование. – 2012. – №3 (27). – С.202-205.

НАУЧНОЕ ИЗДАНИЕ

ИЗДАТЕЛЬСТВО
«НАУЧНЫЕ ПУБЛИКАЦИИ»

АДРЕС РЕДАКЦИИ:
153000, РФ, ИВАНОВСКАЯ ОБЛ., Г. ИВАНОВО,
УЛ. КРАСНОЙ АРМИИ, Д. 20, 3 ЭТАЖ, КАБ. 3-3,
ТЕЛ.: +7 (915) 814-09-51.

HTTPS://SCIENTIFICPUBLICATION.RU
EMAIL: TEL9203579334@YANDEX.RU

ИЗДАТЕЛЬ:
ООО «ОЛИМП»
153002, РФ, ИВАНОВСКАЯ ОБЛ., Г. ИВАНОВО, УЛ. ЖИДЕЛЕВА, Д. 19
ГЛАВНЫЙ РЕДАКТОР, УЧРЕДИТЕЛЬ: ВАЛЬЦЕВ СЕРГЕЙ ВИТАЛЬЕВИЧ

ИЗДАТЕЛЬСТВО «НАУЧНЫЕ ПУБЛИКАЦИИ»
HTTPS://SCIENTIFICPUBLICATIONS.RU
EMAIL: INFO@SCIENTIFICPUBLICATIONS.RU

РОСКОМНАДЗОР
СВИДЕТЕЛЬСТВО ЭЛ № ФС 77–65699

INTERNATIONAL STANDARD
SERIAL NUMBER 2542-081X

ЦЕНА СВОБОДНАЯ