



Центр научно-технической информации и библиотек
– филиал ОАО «РЖД»

Дифференцированное Обеспечение Руководства

87/2025

Готовность к будущему – три распространенных ошибки при модернизации железнодорожного транспорта и как их избежать

По всей Европе железнодорожный сектор испытывает потребность в модернизации. Число пассажиров неуклонно растет, как и их ожидания в отношении надежного, долговечного и современного железнодорожного транспорта. Кроме того, многие существующие поезда больше не соответствуют необходимому уровню техники, хотя их жизненный цикл ещё далек от завершения. Железнодорожные операторы сталкиваются с серьезными проблемами, поскольку они не могут просто полностью заменить и расширить свой существующий парк новыми поколениями поездов из-за затрат, сроков поставки и производственных мощностей. Оптимальным является дооснащение: модернизация существующих поездов и приведение их в соответствие с требованиями в течение следующих 10-20 лет.

Deutsche Bahn (DB) в 2024 г. запустили многолетнюю программу реформ S3¹, в рамках которой не только инвестирует в инфраструктуру, но и уделяет особое внимание цифровым улучшениям существующих поездов и повышению уровня комфорта пассажиров. Железнодорожные операторы во всем мире используют модернизацию как решение по внедрению современных возможностей, таких как цифровое подключение, кибербезопасность и диагностика, без необходимости создания с нуля. Но модернизация сопряжена с рисками, которые могут сделать такие проекты более дорогими, чем планировалось. Можно выделить три наиболее распространенные типовые ошибки, а также возможности их не совершать.

¹ Программа DB S3 по реструктуризации начата в середине 2024 г. с акцентом на инфраструктуру, операционную деятельность и прибыльность.

Монолитная ИТ-архитектура

Означает ли модернизация полную замену старой системы путем её полного разрушения и замены её чем-то совершенно новым? Нет, но многие железнодорожные операторы оказываются в таком положении, потому что на готовых современных платформах отсутствуют интерфейсы, необходимые для сохранения работоспособности устаревших подсистем, например, MVB², последовательными соединениями или сетями CAN. MVB ещё функционируют во многих транспортных средствах, но часто вынуждены от неё отказываться, потому что новые системы её не поддерживают.

Создается ложный выбор: либо сохранить устаревшую систему и отказаться от современных функций, таких как Wi-Fi для пассажиров, мониторинг состояния с помощью ИИ и расширенная диагностика, либо заменить всё, включая то, что в замене не нуждается. Ещё более неприятным является тот факт, что большинство решений по модернизации по-прежнему являются жесткими – фиксированные по форме, их трудно расширять, а адаптация в дальнейшем обходится дорого. В результате проекты откладываются, затраты растут, а операторы получают системы, которые либо чрезмерно сложны, либо недостаточно функциональны.

Решение заключается в модульной модернизации. Все начинается с выбора совместимых компонентов, предназначенных для поэтапного обновления с учетом рисков. Это может быть реализовано в виде использования стандартизированных платформ, таких как CompactPCI Serial³, которые предлагают масштабируемую вычислительную архитектуру на базе стандартных серверных стоек. Это позволяет подключать только необходимую функциональность, будь то современный процессор, модуль Wi-Fi, компонент кибербезопасности или устаревший интерфейсный адаптер. Другой возможный подход заключается в разделении заменяемой системы на отдельные, более управляемые компоненты, например, системы граничных вычислений в сочетании с внешним сотовым модемом или универсальным шлюзом. Вместо замены целых систем это позволяет повысить функциональность, а не сложность. Ещё преимуществом является то, что производители поездов и операторы могут более эффективно управлять сертификациями, поскольку каждый элемент конструкции независимо тестируется и сертифицируется для использования на железных дорогах. Они могут поддерживать соответствие требованиям, не повторяя дорогостоящие

² Многофункциональная шина (MVB) – стандартизированный сетевой протокол связи, определенный стандартом IEC 61375, используемый в железнодорожном транспорте для передачи данных между различными системами, такими как управление поездом, информация о пассажирах, двери и кондиционирование воздуха

³ CompactPCI Serial – промышленный стандарт для встраиваемых компьютерных систем, который является дальнейшим развитием стандарта PICMG 2.0 CompactPCI на основе использования интерфейса PCI Express.

процессы переквалификации при каждой модернизации компонента.

Кибербезопасность

Устаревший подвижной состав не был спроектирован для современных подключений. Существующие возможности подключения, как правило, основаны на устаревших шинах с низкой скоростью передачи данных и ограниченной функциональностью. Обмен данными осуществлялся исключительно в оперативных целях. Но сегодня появились новые цифровые сервисы, такие как Wi-Fi, удаленный доступ, облачная телеметрия, оперативная диагностика – все это подвергает систему киберугрозам, противостоять которым она никогда не была способна. В результате модернизации появляются новые возможности для атак даже в изолированных или сертифицированных по безопасности системах. Появляются такие нормативные акты, как Закон о киберустойчивости (CRA⁴). Однако, когда речь заходит о кибербезопасности, многие проекты приостанавливаются. Это считается слишком сложным, дорогостоящим или трудным для применения в сложных условиях. Поэтому кибербезопасность либо внедряется поздно, либо полностью игнорируется.

Хорошей новостью является то, что кибербезопасность, даже в случае модернизации, не должна быть чрезмерной. Главное – начать с правильного мышления: кибербезопасность – это не что-то само собой разумеющееся, это часть архитектуры. Особенно при первом подключении старых систем необходимо позаботиться о безопасности на ранней стадии, а не откладывать на потом. Это начинается с основных средств защиты, таких как безопасная загрузка, подписанное встроенное ПО и контроль доступа – функций, которые необходимы.

Не менее важной является возможность отделить критически важные области безопасности от некритичных. В обычном поезде системы безопасности работают параллельно с системами Wi-Fi для пассажиров, видеонаблюдения или диагностики. Это возможно, но только в том случае, если система поддерживает надлежащую изоляцию, например, с помощью виртуальных сетей, брандмауэров или физического разделения, в зависимости от степени безопасности. И, наконец, существует управление жизненным циклом. Только системы, которые поддаются техобслуживанию и обновлению, могут быть безопасными на протяжении всего срока службы продукта. Поэтому для железнодорожных операторов, осуществляющих проекты по модернизации и имеющих смешанные парки поездов, важно

⁴ Закон о киберустойчивости (CRA) – нормативный акт ЕС, направленный на повышение кибербезопасности и киберустойчивости в ЕС с помощью общих стандартов кибербезопасности для продуктов с цифровыми элементами в ЕС, таких как обязательные отчеты об инцидентах и автоматические обновления системы безопасности.

выбирать технологии и партнеров, знакомых со строгими стандартами, границами безопасности и длительными циклами внедрения в железнодорожном секторе. При соблюдении этих требований модернизация и безопасность могут идти рука об руку.

Несоответствие жизненного цикла

В железнодорожной отрасли операторы ожидают, что срок службы активов составит от 15 до 20 лет, а в некоторых случаях даже 30 лет. Это справедливо для механических компонентов, и исторически это было справедливо и для многих электронных платформ. Сейчас типичный период поддержки операционной системы составляет 5-7 лет. Промежуточное программное обеспечение, библиотеки безопасности и цепочки инструментов развиваются ещё быстрее, особенно если они основаны на технологиях общего назначения, которые быстро развиваются, чтобы не отставать от ИТ-инноваций и облачных технологий. Этот пробел создает реальные проблемы: хотя аппаратное обеспечение по-прежнему функционирует безупречно, обновления для операционной системы больше недоступны, набор инструментов больше не поддерживается или кибербезопасность больше не гарантируется из-за отсутствия обновлений для системы безопасности. Поэтому несоответствие жизненного цикла является не просто ИТ-помехой, но и становится стратегическим препятствием для безопасного и устойчивого развития системы, что в равной степени влияет на новые поколения поездов, существующий парк и проекты модернизации. Это несоответствие становится всё более распространенным по мере того, как системы становятся более взаимосвязанными, безопасность требует более частых обновлений, программное обеспечение с открытым исходным кодом становится всё более популярным, а темпы изменений ускоряются. Из-за такого ускоренного развития зависимость от аппаратного обеспечения оказывает влияние гораздо быстрее, чем предполагали традиционные сроки и формы использования (рис 1).

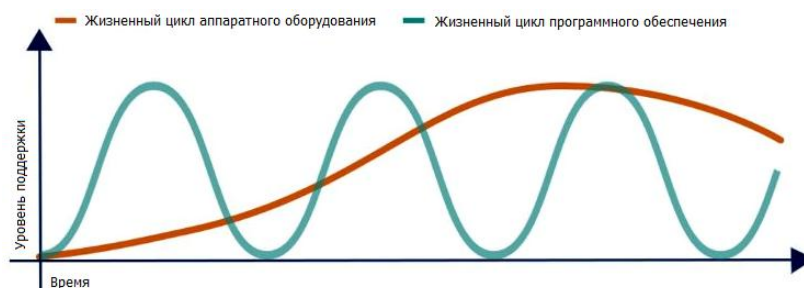


Рис.1. Несоответствие жизненных циклов аппаратного оборудования и ПО

Несоответствия в жизненном цикле можно избежать, если модернизировать не только производительность, но и надежность как аппаратного, так и программного обеспечения. Первым шагом является

выбор платформ, рассчитанных на долгосрочную поддержку. Это означает, что пакеты программного обеспечения были проверены в железнодорожной среде, а не просто заимствованы из быстро меняющихся потребительских или облачных экосистем. Это также стабильные и поддерживаемые операционные системы с известным планом поддержки. Вторым шагом является разделение системных уровней, чтобы они могли развиваться независимо, что включает в себя аппаратное обеспечение, операционную систему, бизнес-логику и платформу. Разделение позволяет обновлять одну часть, не нарушая работу всего остального. В этом контексте это также помогает работать с семействами продуктов, которые механически и электрически совместимы между поколениями – возможна настройка и масштабирование без необходимости перепроектирования с нуля.

И, наконец, планирование жизненного цикла не ограничивается уровнем компонентов. Это также означает наличие процессов мониторинга устаревания, путей модернизации и стратегий использования вторичных источников, особенно для систем, которые должны оставаться в эксплуатации в течение 15 и более лет.

Если объединить все эти аспекты, то в результате получится платформа, которая подходит не только на данный момент, но и на будущее.

*Источники: railwaypro.com, 01.09.2025 (англ. яз.);
сайт duagon.com (англ. яз.)*