УДК 528.02; 528.06

Киберпространство транспортной инфраструктуры

Transport infrastructure cyberspace

Цветков В.Я., д.т.н., профессор, начальник научного отдела, АО «НИИАС»,
E-mail: cvj2@mail.ru, Москва, Россия
Tsvetkov V.Ya., Doc.ofSci.(Tech), Professor, Head of Scientific Department, JSC "NIIAS",
E-mail: cvj2@mail.ru, Moscow, Russia

Аннотация

Исследуется киберпространство транспортной инфраструктуры. Объективная необходимость применения киберпространства вытекает с одной стороны из-за широкого использования разных информационных пространств, с другой стороны возникает потребность новых форм управления производством и транспортом. Киберпространство транспортной инфраструктуры рассматривается как новый инструмент управления в сфере транспорта. Описаны системы управления транспортом в киберпространстве. Статья описывает киберпространство как совокупность вложенных информационных и киберпространств. Раскрывается содержание двух основных компонент киберпространства: координатного и коммуникационного. Описаны локальные информационные пространства, входящие в киберпространство: радиорелейное информационное пространство и пространство радиоэлектронных меток.

Ключевые слова: транспорт, транспортная инфраструктура, киберпространство, кибербезопасность, управление.

Abstract

The article explores the cyberspace of transport infrastructure. The objective need for the use of cyberspace arises, on the one hand, from the widespread use of various information spaces, on the other hand, there is a need for new forms of production and transport management. The cyberspace of transport infrastructure is seen as a new management tool in the field of transport. The transport control systems in cyberspace are described. The article describes cyberspace as a set of nested information and cyberspaces. The content of two main components of cyberspace is revealed: coordinate and communication. The local information spaces included in the cyberspace are described: the radio relay information space and the space of electronic labels.

Keywords: transport, transport infrastructure, cyberspace, cybersecurity, management.

»»

Введение

Киберпространство транспортной инфраструктуры возникло естественным путем за счет тенденции развития и интеграции информационных пространств и в первую очередь сетевых типа интернета и Интернета вещей. Современное управление транспортной инфраструктурой требует применения разных информационных пространств [1]. Информационные пространства выполняют две основные функции: информационное обеспечение и управленческую поддержку. Следует подчеркнуть, что они выполняют именно функции поддержки. Управление осуществляют различные центры управления. Взаимодействие между киберпространством и реальным пространством открывает возможность создания новых пространств, которые являются синтетическими пространствами, ранее не существовавшими.

Киберпространство есть новая форма искусственного информационного пространства, построенная на отношении искусственного и реального пространства. Если рассматривать отношение киберпространства и кибернетики, то киберпространство ближе к социальной кибернетике [2], чем к технической кибернетике. В первоначальной концепции кибернетики Винера основная идея была построена на обратной связи и тому, при которой одна часть системы может контролировать другую. Киберпространство опирается в первую очередь на коммуникации и на глобальное информационное пространство, с вложенными в него локальными информационными и киберпространствами.

Киберпространство, в отличие от технической системы управления, является открытым и ориентировано в большей степени на мягкое управление. Киберпространство создает условия для саморазвития и проявления синергетических эффектов. Существует различие между киберпространством и информационным пространством. Информационное пространство большей частью пассивно и выполняет функции информирования. Кибер пространство активно и активно воздействует на объекты транспортной инфраструктуры [3] и может менять их состояние.

Киберпространство в области транспорта выполняет четыре основные функции. Первая функция связана на обеспечением информационной безопасности и кибербезопасности. Вторая функция связна с поддержкой управленческих технологий. Наиболее ярко эта функция проявляется в технологии «цифровых двойников». Третья функция связана с созданием коммуникационного пространства или коммуникационной среды. Наиболее ярко эта функция проявляется в технологии Интернета вещей и цифровой железной дороги. Четвертая функция киберпространства связана с обучением, в том числе в сфере транспорта. В этой части широко применяют виртуальные и иммерсивные технологии. Обучение осуществляют на основе виртуальной реальности, смешанной реальности, дополненной реальности и иммерсивных технологий и систем. Еще одна функция кибер пространства связана с взаимодействием человека с кибер пространством и с осознанием человека в кибер пространстве [4].

Рисунок 1. **Основные системы управления транспортом в киберпространстве**

Системы киберпространства

Транспортное киберпространство содержит ряд систем, связанных с управлением объектами транспортной инфраструктурой, и в первую очередь с управлением подвижными объектами. На рис.1 приведены основные системы управления, входящие в транспортное киберпространство.

На рис.1 системы управления расположены в порядке усложнения слева направо. Первыми и наиболее простыми в этом типологическом ряду являются автоматизированные системы управления транспортом (АСУТ). К классу АСУТ относят также ситуационные центры управления движением. Их работа строилась на технологиях АСУ и технологиях автоматизации процессов управления в разной степени. Качественно новым этапом стали интеллектуальные транспортные системы (ИТС), которые являлись адаптацией интеллектуальных систем применительно к задачам управления дискретными транспортными потоками и подвижными объектами. В этих системах алгоритмы заменялись на правила и эти системы стали самообучаемыми и само развивающимися.

Следующим этапом, характеризующим распределенное управление, стали технологии Интернета-вещей (IoT). Самыми сложными системами в киберпространстве являются транспортные кибер-физические системы, которые характеризуются распределенной системой датчиков и встроенными вычислителями. Информация от датчиков поступает в локальный и центральный узлы обработки. Встроенные вычислители обладают субсидиарностью. Они позволяют вычислять и оценивать ситуацию на месте и на этой основе принимать решение независимо от центра управления движением.

Вложенные информационные пространства в киберпространстве

Киберпространство в области транспортной инфраструктуры обладает вложенностью. Глобальное пространство включает меньшие по масштабу пространства. На рис.2 показана связь различных информационных пространств, входящих в киберпространство транспортной инфраструктуры (КПТИ).

Киберпространство транспортной инфраструктуры включает два качественно разных, но дополняющих друг друга информационных пространства. Коммуникационное пространство является типичным для мно- »»»

гих видов киберпространства. Например, для сетевого киберпространства или киберпространства Интернет. Координатное пространство [5] транспортной инфраструктуры является специфическим и характеризует именно транспортную инфраструктуру. Это пространство задает пространственное управление. Координатное пространство КПТИ используется: при управлении недвижимостью транспортной инфраструктуры; при управлении подвижными объектами; при решении задач размещения объектов транспортной инфраструктуры, при оптимизации маршрутов движения. Координатное пространство КПТИ используется при проектировании и строительстве объектов транспортной инфраструктуры.

Координатное пространство КПТИ создается двумя путями «снизу и сверху». Традиционно в геодезии координатное пространство создавалось с основания, то есть с использования геодезических сетей на поверхности Земли, на основе которых проводилось разбивочные работы и выносились проекты в натуру. Это технология «снизу».

Развитие спутниковых технологий предоставило новый вариант создания координатного пространства с помощью Глобальных навигационных спутниковых систем (ГНСС). Это технология «сверху». Спутники образуют независимую от земной поверхности пространственную систему координат, привязанную к центру масс Земли. Недостатком этой системы является неточная привязка к земной поверхности. Земля имеет относительно сложную конфигурацию, далекую от правильной геометрической фигуры. Поэтому идеальное геометрическое пространство не всегда точно описывает положение пространственных объектов применительно к поверхности Земли.

Для устранения этого недостатка придумали системы базовых станций как пространственный интерфейс. Эти системы, с одной стороны, привязаны к ГНСС как к глобальной общеземной системе координат, с другой стороны они привязан к конкретной части земной поверхности. Они фактически связан с геодезическими сетями и измеряют координаты на конкретной части земной поверхности с учетом реперных или иных геодезических сетей.

Информационное пространство базовых станций (рис.2) связывает глобальную систему спутниковых координат с геодезическими сетями на участке земной поверхности. ГНСС обеспечивает сопоставимость и координацию в масштабе Земли. Навигационное пространство ГНСС есть глобальное информационное пространство для всей Земли. Базовые станции обеспечивают привязку и точность измерений на конкретных участках поверхности Земли. Они создают локальное информационное пространство для части земной поверхности, на которой решаются задачи управления ОТИ.

Координатное пространство КПТИ за рубежом дополняется системой реперных сетей (информационное координатное пространство сетей), расположенных вдоль железнодорожных трасс. Это пространство решает задачи геометрического контроля состояния трасс и объектов транспортной инфраструктуры независимо

Рисунок 2. **Вложенные информационные пространства**

от спутниковых технологий. Оно представляет собой автономную геодезическую сеть, предназначенную только для решения задач транспорта. В России из-за большой протяженности дорог и, соответственно, высокой стоимости эти сети не создают полностью, но кое где создают фрагментарно.

Коммуникационное пространство КПТИ решает задачи не только связи, но и координирования. Как известно, системы космической телефонной связи обладают принципиально теми же возможностями по навигации, что и ГНСС, но с меньшей точностью.

Как альтернатива ГНСС возможно создание радиорелейного координатного пространства, которое решает задачи координирования и управления подвижными объектами. Эта идея запатентована в НИИАС [6] в виде создания радиорелейного информационного пространства, которое обладает возможностью оперативного управления объектами при наличии цифровой модели железнодорожного полотна. С одной стороны это ограничение, но с другой стороны эта информация независимо собирается, существует и ее можно использовать для управления.

Локальным информационным пространством является информационное пространство электронных меток [7]. Электронные метки обычно используют индивидуально для контроля вагонов или грузов. В работе предложена идея создания такого пространства путем массовой установки системы меток координирования их с помощью дополнительных геодезических методов. В результате возникает система электронного контроля движения, которая может работать селективно по видам грузов. Обычная электронная метка отвечает на вопрос «да/нет». Есть вагон или нет, есть груз или нет. Вопросы координации отходят на второй план. Система электронных меток дает возможность: отслеживать наличие объекта, определять его координаты с геодезической точностью, определять скорость движения, а также дополнительно интенсивность потока грузов. »»

Угрозы в киберпространстве

Киберпространство является более открытым, чем техническая система управления. такая открытость создает дополнительные угрозы и ставит дополнительные проблемы. С областью угроз в киберпространстве связаны понятия управления рисками и кибербезопасность. Кибербезопасность — это «способность защищать или защищать использование киберпространства от кибератак [8].

Существуют различные типы кибератак, такие как вредоносное ПО, фишинг, атака «человек посередине», межсайтовый скриптинг, внедрение SQL, ботнеты, социальные ботнеты, атаки на основе шпионажа, которые крадут данные и информацию, перехват последней мили, ошибки/перехват передачи, критическая инфраструктура, кибер-похищение, кибер-вымогательство, хактивизм [9]. Поэтому для повышения кибербезопасности большинство стран разработали законы о защите данных.

Растущая тенденция к аутсорсингу данных третьим сторонам создает неизбежные риски для информационной безопасности и защиты данных.

Современное киберпространство включает облачные технологии. Применение облачных технологий приводит к тому, что системы управления и системы данных будут мигрировать на облачную платформу.

Традиционные инструменты безопасности не предназначены для решения проблем при внедрении облака. Это мотивирует разработку специальных решений по управлению безопасностью облачных технологий. Предлагаются различные решения типа CSA [10].

Кроме того, при решении проблемы больших данных за счет облачных вычислений [11, 12] также возникает несколько проблем с точки зрения облачного хранения данных с учетом конфиденциальности, безопасного и масштабируемого контроля доступа.

Кибербезопасность является самой большой проблемой для клиентов, которые передают свои личные и личные данные в облачное хранилище, поскольку это связано со многими киберрисками. Существует множество кибер-рисков, связанных с облаком, таких как захват учетной записи, сложные постоянные угрозы (APT), утечка данных, потеря данных, отказ в обслуживании, небезопасный API, злонамеренные инсайдеры, неправомерное и нечестное использование облачных сервисов, недостаточная осторожность, проблемы с общими технологиями, уязвимости систем и приложений и слабая идентификация.

Железные дороги являются важной критической инфраструктурой. Железнодорожная отрасль оказывает существенное влияние на общество как в пассажирских, так и в грузовых перевозках. Это облегчает массовый транспорт людей из одного места в другое и огромное количество товаров для торговли и бизнеса с более быстрой досягаемостью и экономической ценностью. Кибер-инциденты могут привести к целому ряду возможных последствий, от нарушения статуса до прерывания работы и даже травм и гибели людей из-за взлома систем.

В настоящее время разработаны несколько архитектур, для обеспечения безопасности на железных дорогах [8]. Одно из предложений включает архитектуру многоуровневой интеллектуальной системы защиты информации. Предлагают меры по смягчению последствий с учетом жесткой политики безопасности, сотрудничества между юридическими, государственными, технологическими и социальными аспектами. Комплексный подход к безопасности, конфиденциальности и надежности (SPD) во встроенных системах был разработан платформой SHIELD, которая может применяться к железнодорожному наблюдению [13].

Поскольку эксплуатация и техническое обслуживание железных дорог имеют первостепенное значение, в LTU разработана платформа eMaintenance для реализации систем поддержки принятия решений, отвечающих требованиям железнодорожной отрасли [14]. Она действует как стратегия обслуживания, при которой различные задачи управляются в электронном виде с использованием данных об элементах в режиме реального времени, таких как мобильные устройства, дистанционное беспроводное зондирование, мониторинг состояния, инженерия знаний, телекоммуникации и интернет-технологии.

В рамках стандарта ISO 27000 (информационная безопасность) модель PDCA применяют для структурирования всех процессов системы управления информационной безопасностью (Information Security Management System, ISMS), где требования информационной безопасности и ожидания заинтересованных сторон выступают в качестве входных данных, а необходимые действия и процессы обеспечивают результаты информационной безопасности, которые соответствуют этим требованиям. и ожидания [15]. Основными задачами данного исследовательского проекта являются:

1. Выявить потенциальный риск и последствия сбоев в защите данных/информации в железнодорожной инфраструктуре.
2. Изучить современные методы исследования в области безопасности данных/информации и рекомендовать наиболее подходящие методы для железнодорожной инфраструктуры.
3. Провести исследование потенциала защищенных данных и его стоимостную оценку.

Железнодорожные системы переходят на более интеллектуальные и связанные системы, что открывает новые возможности для злоумышленников и киберпреступников. Безопасность должна учитываться в транспортной сфере для защиты операторов, экономических аспектов и безопасности граждан.

Транспортная сфера сталкивается со многими проблемами. Во-первых, в Европе нет закона о кибербезопасности на транспорте. Поэтому в этой области системы управления сталкиваются с низким уровнем осведомленности. Заинтересованным сторонам железных дорог трудно выделить бюджет на эту конкретную тему из-за отсутствия законодательных нормативных документов. Использование разнородных технологий и программных решений приводит к очень разнообразным и несопоставимым наборам данных. Существует также множество проблем, связанных с большими данными для железных дорог. »»»

С точки зрения информационной безопасности, основной задачей железнодорожного сектора является снижение риска потенциальной потери данных и обеспечение стабильной и стабильной работы железных дорог. В случае возникновения проблемы могут возникнуть важные последствия, такие как остановка поезда, негативные экономические последствия, потеря доверия и несчастные случаи. Меры защиты от кибератак в железнодорожном секторе еще не полностью разработаны. Недостаточно осведомлены о новых рисках, и риски не учитываются в полной мере из-за невысокого уровня безопасности на железнодорожном транспорте [16].

Потенциальными системами, которые могут быть подвержены кибербезопасности на железной дороге, являются электронные системы блокировки, системы защиты железнодорожных переездов, автоматическая система блокировки, системы трансмиссии гусеничного транспорта, дополнительные системы (например, связь, обнаружение отказов)

Существует и применяется вредоносное ПО для атак на Центр управления операциями или блокировками, существуют беспроводные атаки на беспроводную связь (GSM-R), существуют парольные атаки на *Radio Block Center* и т. Контекстно общим методом поддержки безопасности являются разные виды мониторинга. В том числе и радио электронный мониторинг.

Заключение

Современное киберпространство рассматривают как «глобальный домен в информационной среде, состоящий из взаимозависимой сети инфраструктур информационных систем, включая Интернет, телекоммуникационные сети, компьютерные системы и встроенные процессоры и контроллеры» [9].

Киберпространство транспортной инфраструктуры формируется на основе интеграции глобальных и локальных информационных пространств, и локальных киберпространств. Оно является новым инструментом управления в сфере транспорта. Киберпространства транспортной инфраструктуры обеспечивает преемственность между разными системами управления транспортом: АСУТ, ИТС, ТКФС. Киберпространства транспортной инфраструктуры создает условия для функционирования цифровой железной дороги. Основная проблема киберпространства – проблема кибербезопасности. Киберпространство является открытой системой. Поэтому по мере его развития возрастают разнообразные кибер угрозы. Нейтрализация этих угроз вторая задача после задачи управления. ■

Список литературы

1. Ознамец В.В. Информационное управляющее транспортное пространство // Наука и технологии железных дорог. 2020. Т.4.– 4(16). – С.43-50.
2. Розенберг И.Н., Цветков В.Я. Социальная кибернетика в цифровизации транспортной инфраструктуры // Наука и технологии железных дорог. 2020. Т.4.– 3(15). – С.3-14.
3. Андреева О.А. Кибернетическое зеркалирование для управления предприятиями транспортной инфраструктуры // Наука и технологии железных дорог. 2021. Т. 5. №4 (20). – С.19-27.
4. Gálik S. On human identity in cyberspace of digital media //European Journal of Tranformation Studies. – 2019. – Т. 7. – №. 2. – С. 33-44.
5. Розенберг И.Н., Цветков В. Я. Координатные системы в геоинформатике – МГУПС, 2009. -67 с.
6. Розенберг Е.И., Розенберг И. Н., Цветков В. Я., Шевцов Б.В. Устройство контроля подвижного объекта. Патент на полезную модель. № RU 95851 U1. Зарегистр. 10.07.2010
7. Цветков В.Я., Ознамец В.В. Геодезические сети электронных меток // Науки о Земле. – 2018. – №4. – С.17-27.
8. Kour R. et al. A review on cybersecurity in railways //Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit. – 2023. – Т. 237. – №. 1. – С. 3-20.
9. Thaduri A. et al. Cybersecurity for eMaintenance in railway infrastructure: risks and consequences //International Journal of System Assurance Engineering and Management. – 2019. – Т. 10. – С. 149-159.
10. CSA Top Threats Working Group (2016) The treacherous 12: cloud computing top threats in 2016. Cloud Security Alliance (CSA), Feb.
11. Буравцев А.В., Цветков В.Я. Облачные вычисления для больших геопространственных данных // Информация и космос. 2019. – №3. – С.110-115.
12. Лёвин Б.А., Цветков В.Я. Информационные процессы в пространстве «больших данных» // Мир транспорта. 2017. – Т.15, №6(73). – С.20-30.
13. Priscoli FD, Giorgio AD, Esposito M, Fiaschetti A, Flammini F, Mignanti S, Pragliola C (2017) Ensuring cyber-security in smart railway surveillance with SHIELD. Int J Crit Comput Based Syst 7(2):138–170.
14. Karim R (2008) A service-oriented approach to e-maintenance of complex technical systems (Doctoral dissertation, Luleå tekniska universitet).
15. ISO/IEC (2007) 27001:2005, Information technology—security techniques—information security management systems—requirements.
16. Masson É, Gransart C (2017) Cyber security for railways–a huge challenge–Shift2Rail perspective. In: International workshop on communication technologies for vehicles. Springer, Cham, pp 97–104.