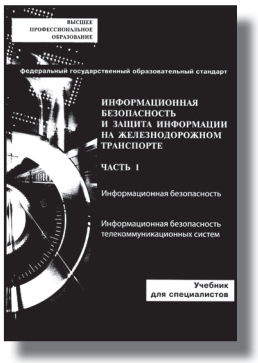
УДК 004.05

Как защитить транспортное киберпространство



Информационная безопасность и защита информации на железнодорожном транспорте: Учебник в 2 ч. / Под ред. А. А. Корниенко. – М.: ФГБОУ «Учебно-методический центр по образованию на железнодорожном транспорте», 2014. Ч. 1. Методология и система обеспечения информационной безопасности на железнодорожном транспорте. – 440 с. Ч. 2. Программно-аппаратные средства обеспечения информационной безопасности на железнодорожном транспорте. – 448 с.

В первой части учебника последовательно изложены основные сведения о методологии обеспечения информационной безопасности. Во второй части предлагается системный обзор программно-аппаратных методов и средств обеспечения информационной безопасности корпоративных информационных, автоматизированных и информационно-управляющих систем и сетей на железнодорожном транспорте.

Рассмотрены базовые средства защиты информации от несанкционированного доступа, методы и механизмы обеспечения информационной безопасности в системах управления базами данных, архитектура и средства защиты информации в корпоративных вычислительных системах на основе мэйнфреймов zSeries, принципы построения и функционирования корпоративных систем обеспечения информационной безопасности и защиты информации (систем управления доступом и антивирусной защиты, защищенного сегмента электронной почтовой системы, инфраструктуры открытых ключей), типовые программно-аппаратные средства защиты информации региона ведения железной дороги, методы и инструментальные средства подтверждения соответствия и сертификации программного обеспечения по требованиям безопасности информации.

Ключевые слова: компьютерная безопасность, кибербезопасность, киберпространство, защита информации, киберугроза, кибератака.

Что такое кибербезопасность в нашей стране знают немногие. Чаще всего используется термин «компьютерная безопасность», но и он у нас не так популярен, как за рубежом. Между тем, практически 20% киберпреступлений в мире в 2012 году пришлось именно на Россию. С целью обеспечения кибербезопасности личности, организаций и государства временная комиссия Совета Федерации по развитию информационного общества приступила к разработке стратегии национальной кибербезопасности Российской Федерации. Согласно проекту стратегии, под кибербезопасностью понимается совокупность условий, при которых все составляющие киберпространства защищены от любой угрозы и нежелательного воздействия [1]. В киберпространство входят программное обеспечение, которое работает в компьютерных устройствах, информация, которая сохраняется (и передается) в этих устройствах, или информация, которая создается этими устройствами. Оборудование и здания, их содержащие, также являются частью киберпространства. Такие элементы должны приниматься в расчет при разработке систем кибербезопасности.

Кибербезопасность ставит своей целью организацию безопасности киберсреды, она призвана быть всесторонней во всех уровнях сетей. Киберугроза – это незаконное проникновение или угроза вредоносного проникновения в виртуальное пространство для достижения политических, социальных или иных целей. Киберугроза может воздействовать на информационное пространство компьютера, в котором находятся сведения, хранятся материалы закрытого характера.

В настоящее время сравнительно легко можно получать информацию, общаться, наблюдать и управлять системами IT на значительных расстояниях. По существу, современные сети играют ключевую роль во многих инфраструктурах государственной важности: транспорта и обороны, электронной торговли, передаче данных и голоса, коммунальных услуг, финансовой сферы, здравоохранения. Угрозы для кибербезопасности быстро возрастают. Вирусы, черви, троянские кони, попытки нарушения защиты типа имитации соединения, кража идентичности, спам и кибератаки находятся на подъеме.

С появлением сложных автоматизированных систем управления, связанных с автоматизированным вводом, хранением, обработкой и выводом информации, проблемы ее защиты приобретают еще большее значение. Координатор Белого дома по вопросам кибербезопасности Майкл Даниил считает, что проблема кибербезопасности больше не является задачей исключительно директоров служб информационной безопасности или директоров по информационным технологиям. Она смещается в сферу деятельности руководящих политиков.

О важности проблемы говорит и тот факт, что в 2014 году вышел первый номер научно-практического журнала «Вопросы кибербезопасности». Этот новый журнал учрежден коллективом НПО «Эшелон» совместно с Научным центром правовой информации при Министерстве юстиции РФ. На страницах журнала будут печататься научные и методические статьи в области информационной безопасности и информационного противоборства, в первую очередь статьи по кибербезопасности, технической защите информации и оценке соответствия требованиям безопасности информации.

Безопасность трудно проверить, предсказать и реализовать. Она не может заготовить рецепты «на все случаи жизни». Требования к безопасности и рекомендуемая стратегия в каждой организации будут всегда различны.

Обеспечение доступности киберпространства, а также целостности, достоверности и конфиденциальности информации в киберпространстве стало одной из важнейших проблем XXI столетия. Именно поэтому защита киберпространства свсе чаще называется главной задачей экономики и общества как на государственном, так и на международном уровне, рассматривается как стратегическая цель государственной важности, затрагивающая интересы всех слоев мирового сообщества.

Практически во всех видах деятельности ОАО «РЖД» информационные и телекоммуникационные технологии и информационная безопасность играют решающую роль. Их широкое внедрение в автоматизированные и информационно-управляющие системы, корпоративные и вычислительные сети различного назначения значительно повышает эффективность холдинга и создает ощутимые конкурентные преимущества. При этом существует риск, что нарушение таких характеристик информации, как конфиденциальность, целостность, доступность, достоверность, может привести к неприемлемому ущербу или катастрофическим последствиям.

Решению проблемы защиты информации и информационной безопасности ОАО «РЖД», корпоративных информационных систем и сетей компании уделяется немалое внимание. В начале 2000-х годов была создана и развивается система обеспечения информационной безопасности (СОИБ), одним из функциональных направлений которой является совершенствование системы опережающей подготовки и переподготовки специалистов в области информационной безопасности, кибербезопасности и защиты информации, в том числе в вузах железнодорожного транспорта.

В этой связи актуальным и своевременным признано издание в 2014 году фундаментального двухчастевого учебника по данной тематике – «Информационная безопасность и защита информации на железнодорожном транспорте» под редакцией А. А. Корниенко.

Авторскому коллективу, сочетающему в своем составе известных специалистов – профессоров и доцентов Петербургского государственного университе-

та путей сообщения и руководителей различного уровня ОАО «РЖД», удалось продуманно и глубоко изложить как теоретические основы, методологию обеспечения и управления информационной безопасностью корпорации, так и содержательно раскрыть основные принципы и методы и описать подсистемы и средства защиты конкретных автоматизированных и телекоммуникационных систем, используемых на железнодорожном транспорте.

Сейчас подготовка специалистов в области информационной безопасности в вузах железнодорожного транспорта осуществляется по специальностям 090302 (Информационная безопасность телекоммуникационных систем), 090303 (Информационная безопасность автоматизированных систем), 090905 (Организация и технология защиты информации), а также в рамках ряда дисциплин учебных планов направлений подготовки 230100 (Информатика и вычислительная техника), 230400 (Информационные системы и технологии) и других. Рецензируемый учебник покрывает содержание значительного числа дисциплин по данным специальностям и направлениям подготовки.

В первой его части последовательно изложены основные понятия, концептуальные аспекты, дается характеристика мер и систем информационной безопасности и защиты информации, комментируются организационное и правовое их обеспечение на территории Российской Федерации.Показаны методология управления информационной безопасностью, базирующаяся на управлении рисками и инцидентами, аудите информационной безопасности, принципы построения систем безопасности на железнодорожном транспорте, тенденции развития технологий управления информационной безопасностью, организационные, нормативно-методические и технические особенности связанных с этим процеесов.

Рассмотрены как объекты информационной безопасности корпоративные и телекоммуникационные сети, информационно-управляющие и автоматизированные системы железнодорожного транспорта, примеры разработки профилей защиты, построения систем обеспечения информационной безопасности и защиты информации единой магистральной цифровой сети связи, сети передачи данных ОАО «РЖД», сети цифровой технологической радиосвязи и беспроводных сетей доступа, единой корпоративной автоматизированной системы управления финансами и ресурсами (ЕК АСУФР), АСУ «Экспресс-3», автоматизированной системы «ЭТРАН». Изложены также вопросы подтверждения соответствия и сертификации программных и программно-аппаратных средств по требованиям безопасности информации и качества, методы криптографической защиты и предотвращения перехвата информации.

Во второй части книги описаны программно-аппаратные методы и средства обеспечения информационной безопасности корпоративных информационных, автоматизированных и информационно-управляющих систем и сетей на железнодорожном транспорте.

Представлены базовые средства защиты информации от несанкционированного доступа, методы и механизмы обеспечения информационной безопасности в системах управления базами данных, архитектура и средства защиты информации в корпоративных вычислительных системах на основе мэйнфреймов zSeries, принципы построения и функционирования корпоративных систем обеспечения информационной безопасности и защиты информации (систем управления доступом и антивирусной защиты, защищенного сегмента электронной почтовой системы, инфраструктуры открытых ключей), типовые программно-аппаратные средства защиты информации региона ведения железной дороги, методы и инструментальные средства подтверждения соответствия и сертификации программного обеспечения по требованиям безопасности информации.

В учебнике впервые, пожалуй, авторы столь комплексно оперируют:

– методологией, принципами построения и тенденциями развития системы обеспечения информационной безопасности на железнодорожном транспорте и ее важнейшей компоненты – системы управления информационной безопасностью;

– политикой корпоративной информатизации, обеспечения информационной безопасности структурных подразделений ОАО «РЖД» и корпоративных информационных систем и сетей железнодорожного транспорта;

– риск-ориентированным подходом и методологией управления информационной безопасностью, детальным представлением вопросов оценки и управления рисками, инцидентами, аудита состояния подведомственной сферы;

– данными корпоративных информационных систем и сетей железнодорожного транспорта как объектов информационной безопасности;

– аналитическим материалом систем обеспечения информационной безопасности корпоративного уровня и программно-аппаратных средств защиты информации региона ведения железной дороги.

Однако при возможном переиздании учебника необходимо учесть последние тенденции в сфере информационной безопасности, рост числа прицельных компьютерных атак (кибератак) на АСУ производственными и технологическими процессами и внимания к реализации мер по обеспечению кибербезопасности российских железных дорог, прежде всего – защите систем управления движением поездов, в частности, микропроцессорных систем управления.

Владимир ГОРЕЛИК,
доктор технических наук, профессор, заведующий кафедрой «Вычислительная техника» Московского государственного университета путей сообщения (МИИТ), Москва, Россия

ЛИТЕРАТУРА

1. Михайлова, Алина. Проблемы кибербезопасности в России и пути их решения. Опубликовано 20.01.2014. ИА «Гарант»: http://www.garant.ru/article/520694/#ixzz31ADZNrl. Доступ: 29.04.2014. ●

HOW TO PROTECT TRANSPORT CYBERSPACE

Gorelik, Vladimir Yu. *– D. Sc. (Tech), professor, head of the department of computer engineering of Russian open transport academy of Moscow State University of Railway Engineering (MIIT), Moscow, Russia.*

The review of the book:
Railway Information Security and Data Protection [Informatsionnaya bezopasnost' i zaschita informatsii na zheleznodorozhnom transporte]. Textbook. In 2 parts. Part 1: Methodology and the system of providing of railway information security, 440 p. Part 2: Firmware of providing of railway information security, 448 p. Edited by Kornienko, A.A. (Adadurov, S.E. et alt). Moscow, Uchebno-metodicheskiy tsentr po obrazovaniyu na zheleznodorozhnom transporte [Training and methodological center of railway education], 2014.

ABSTRACT

The first part of the textbook under review is dedicated to systematic description of basic data concerning methodology of information security.

The second part refers to system review of firmware and instruments of information security of railway corporate information, automatic and control.

The textbook describes basic tools of data protection against unauthorized access, instruments of protection of databases, architecture and protective measures within corporate computing systems based on mainframes of zSeries, principles of information security and data protection (control of access, anti-virus tools, protected segment of e-mail, infrastructure of open keys), firmware of data protection within the zone of a railway, instruments of confirming conformity and certification of software.

The reviewer notes that the textbook concerns almost all autonomous courses that are included in relevant study courses and syllabus.

The reviewed book gives possibility to reviewer to differentiate the notions of cybersecurity, computer security, information security, data security, cyberspace, cyberthreat, and to offer his proper system vision of the related problems, to underline the need to search of solutions which will be well adapted to each given organization.

Key words: computer security, cybersecurity, cyberspace, data protection, cyberthreat, cyber attack.

REFERENCES

1. Mikhailova, Alina. Problems of cybersecurity in Russia and solutions [*Problemy kiberbezopasnosti v Rossii I puti ih resheniya*]. Published on 20.01.2014 in information system Garant at http://www.garant.ru/article/520694/#ixzz31ADZNrl. Last accessed 29.04.2014.

Координаты автора (contact information): Горелик В. Ю. (Gorelik V. Yu.) – V. Gorelik@rgotups.ru.