ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СИСТЕМ УПРАВЛЕНИЯ БЕЛОРУССКОЙ ЖЕЛЕЗНОЙ ДОРОГИ

С. Г. Кульгавик, О. А. Чеканова, П. М. Буй
Кафедра «Системы передачи информации», Белорусский государственный университет транспорта
Минск, Республика Беларусь
E-mail: kalashnikovn27.sk@gmail.com

В статье поднимается вопрос об актуальности обеспечения безопасности микропроцессорных систем управления железнодорожной автоматики, телемеханики и связи Белорусской железной дороги. Ставится вопрос об обеспечении не только информационной, но и функциональной безопасности таких систем. Приводится перечень основных целей кибератак на железнодорожном транспорте, а также основные направления совершенствования их кибербезопасности.

Введение

Учитывая складывающуюся экономическую ситуацию, тенденции развития рынка услуг железнодорожных грузо- и пассажироперевозок, объективные требования инновационного развития реального сектора экономики, а также перспективы модернизации хозяйства грузовой и коммерческой работы, Белорусская железная дорога выполняет амбициозные задачи по внедрению в свою основную производственную деятельность – перевозку грузов и пассажиров, современных проектов, основанных на повсеместном внедрении современных микропроцессорных систем управления движением поездов, интерактивных информационных сервисов, средств и систем электронного документооборота. На рубеже 2015-2016 годов можно с уверенностью сказать, что принятые ориентиры не только достигнуты, но и в значительной мере преодолены. Широкое применение современных микропроцессорных систем управления (МПСУ) на Белорусской железной дороге влечет за собой массовое внедрение цифровых и компьютерных систем и сетей. Использование в таких комбинированных системах стандартного программного обеспечения, сетевых протоколов, удаленного управления, облачных вычислений и реализация интерактивных информационных сервисов приводят к увеличению уязвимостей для реализации кибератак. Это обуславливает необходимость детальной проработки новых требований к инфраструктуре связи на Белорусской железной дороге. Анализ инцидентов в сфере информационной безопасности за последние годы, публикуемый в открытом доступе [1], наглядно показывает динамику увеличения их количества. Кроме того, все больший интерес в качестве объектов кибератак вызывает у нарушителей ранее труднодоступные автоматизированные системы управления технологическими процессами (АСУ ТП), к которым следует отнести системы обеспечения безопасности движения поездов и, в особенности, использующие современные информационные технологии и программное обеспечение, например МПСУ.

I. Информационная и функциональная безопасность

В связи с возрастающей ролью информатизации в перевозочном процессе и интеграции систем и средств управления объектами железнодорожного транспорта в единое информационное пространство – киберпространство, возникают новые угрозы для АСУ ТП. Требования к обеспечению безопасности зачастую построены только на информационной безопасности, т. е. на концепции обеспечения «конфиденциальности», «целостности» и «доступности» информации, но главная задача защиты МПСУ железнодорожной автоматики, телемеханики и связи (ЖАТС) заключается в обеспечении их функциональной безопасности, что напрямую обеспечивает безопасность движения поездов. Системы ЖАТС – это системы решающие задачи регулирования и обеспечения безопасности движения поездов методами и средствами автоматического и телемеханического управления. Функциональная безопасность – это совокупность таких условий функционирования системы управления, при которых предотвращаются или минимизируются последствия от внешних или внутренних деструктивных информационных воздействий, приводящих к нарушению процесса штатного функционирования системы. Именно нарушение функциональной безопасности становится более опасным для микропроцессорных систем обеспечения безопасности движения поездов, как систем управления нижнего уровня. Ответственность функций, выполняемых АСУ ТП, требует особого подхода к выполнению требований по безопасности функционирования МПСУ. В соответствии с техническим регламентом Таможенного союза [2] для объектов инфраструктуры железнодорожного транспорта должны быть предусмотрены программные средства, обеспечивающие безопасность их функционирования. Данные средства должны обеспечивать защищенность от компьютерных вирусов, несанкционированного доступа, последствий отказов, ошибок и сбоев при хранении, вводе, обработке и выводе информации, возможности случайных из-

менений информации. Особенности применения программного обеспечения АСУ ТП и связанные с этим риски определяют необходимость расширения и комплексного подхода к оценке их соответствия требованиям как информационной, так и функциональной безопасности. С этой точки зрения нормативные, организационные и технические вопросы защиты информации современных систем управления ЖАТС проработаны в не достаточно полном объеме. Кибератаки на железнодорожном транспорте предпринимаются, как правило, с одной из пяти целей:

- кибершпионаж – несанкционированная передача данных, программ или географических координат железнодорожных объектов;
- кибераудит – поиск уязвимостей;
- кибермошенничество – взломы автоматов продажи билетов и квитанций оплаты багажа, счетчиков учета энергоносителей, автоматических расходомеров и заправщиков;
- киберсаботаж – снижение пропускной способности железнодорожных участков вплоть до полной парализации движения;
- кибердиверсии – создание враждебных и опасных маршрутов движения, нарушение технологий транспортировки и скоростного режима, в первую очередь при перевозке особо опасных и социально значимых грузов, пассажирских и воинских перевозках.

Краткий анализ систем управления ЖАТС позволяет сделать вывод о ее высокой уязвимости при кибератаках. Оценка комплекса мероприятий по защите информации и использования как специализированного, так и типового программного обеспечения показывает, что зачастую не соблюдаются даже элементарные правила кибербезопастности. Полностью решить эту проблему практически невозможно, поскольку технологии организации кибератак всегда имеет преимущество перед способами защиты. К ряду причин можно отнести недостаточную развитость как государственной, так и отраслевой нормативной базы, что подталкивает к созданию новой и актуализацию существующей нормативно-технической и методической базы кибербезопасности железнодорожного транспорта, которое учитывает его особенности и специфику. Внедрение и совершенствование принципов защиты информации, как и разработка новых альтернативных вариантов управления движением поездов при сохранении существующих ручных режимов управления, которые будут незаменимы в случае широкого проведения кибератак дадут положительный эффект по обеспечению защиты. Обязательная проверка микропроцессорных технических средств управления процессами движения на стойкость к электромагнитному излучению позволит повысить их надежность. При этом одним из основных факторов достижения положительных результатов будет являться то, что все информационные системы разработаны, эксплуатируются и сопровождаются собственными силами (представителями отрасли железнодорожного транспорта).

II. Безопасность микропроцессорных систем управления Белорусской железной дороги

Анализ международного опыта по обеспечению кибербезопасности систем управления железнодорожного транспорта показал, что основными направлениями совершенствования кибербезопасности МПСУ являются:

- совершенствование законодательной базы;
- развертывание соответствующей организационной структуры;
- создание системы обнаружения нападений и несанкционированных вторжений;
- определение критически важных объектов железнодорожного транспорта, их взаимосвязей и стоящих перед ними угроз;
- создание средств реагирования, реконфигурации и восстановления критически важных объектов управления после кибератак;
- развитие кооперации между различными ведомствами и компаниями, а также международной кооперации в сфере обеспечения кибербезопасности;
- обеспечение подготовки специалистов в сфере кибербезопасности;
- создание системы эшелонированной обороны критически важных объектов железнодорожного транспорта от кибератак;
- создание имитационных моделей критически важных объектов железнодорожного транспорта для отработки методов их защиты и оценки возможного ущерба;
- ведение национальных баз данных уязвимостей программного обеспечения.

Вышеперечисленные направления кибербезопасности необходимо обеспечить для систем управления движением поездов, альтернативных вариантов управления движения, компьютерных систем, интерактивных информационных сервисов, программного обеспечения отрасли, средств и систем электронного документооборота, защиты сетей и порталов Белорусской железной дороги.

1. Kaspersky security bulletin 2015. Основная статистика за 2015 год. [Электронный ресурс] – Дата доступа: 29.06.2016;
2. Технический регламент Таможенного союза ТР ТС 003/2011 «О безопасности инфраструктуры железнодорожного транспорта».