4 Таможенный кодекс Евразийского экономического союза (приложение № 1 к Договору о Таможенном кодексе Евразийского экономического союза) от 01.01.2018 // КонсультантПлюс [Электронный ресурс]. – Режим доступа : http://www.consultant.ru. – Дата доступа : 24.02.2019.

A. PIATROU-RUDAKOUSKI, PhD, Associate Professor
V. BAZAKA
Belarusian State University of Transport

CUSTOMS INFRASTRUCTURE EFFICIENCY AS A FACTOR OF TRANSIT POTENTIAL DEVELOPMENT

The specific of concept customs infrastructures is considerated here and main elements of customs infrastructures of Brest customs office are also researched. The efficiency of measures for its development are estimated and next steps in this direction are proposed.

Получено 10.10.2019

ISSN 2225-6741. Рынок транспортных услуг (проблемы повышения эффективности). Вып. 12. Гомель, 2019

УДК 004.9 : 656.2

Б. Б. РЯБЦЕВ
Белорусский государственный университет транспорта

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ

Рассматриваются системы, обеспечивающие контроль и автоматизированное управление технологическим оборудованием на железнодорожном транспорте. Описываются особенности применения данных систем. Даются рекомендации по повышению уровня информационной безопасности автоматизированных систем управления технологическими процессами.

Железнодорожный комплекс имеет особое стратегическое значение для Республики Беларусь. Он является связующим звеном единой экономической системы, обеспечивает стабильную деятельность промышленных предприятий, своевременный подвоз жизненно важных грузов в самые отдаленные уголки страны, а также является самым доступным транспортом для миллионов граждан.

Миссия Белорусской железной дороги состоит в эффективном удовлетворении рыночного спроса на перевозки, повышении конкурентоспособности, достижении финансовой стабильности, реализации принципов социальной ответственности бизнеса и глубокой интеграции в Евроазиатскую транспортную систему.

На железнодорожном транспорте автоматизированные системы управления технологического назначения, обеспечивающие контроль и автоматизированное управление технологическим оборудованием и средствами (исполнительными устройствами) и реализованными на нем технологическими процессами по управлению, контролю и обеспечению безопасности движения поездов выделяют в отдельный объект защиты – автоматизированные системы управления технологическими процессами (далее – АСУ ТП).

Высокая степень ответственности функций, выполняемых программным обеспечением (далее – ПО) АСУ ТП, требует особого подхода к выполнению требований по безопасности функционирования железнодорожного подвижного состава и объектов инфраструктуры железнодорожного транспорта. В соответствии с техническими регламентами Таможенного союза для железнодорожного подвижного состава и объектов инфраструктуры железнодорожного транспорта должны быть предусмотрены программные средства, обеспечивающие безопасность их функционирования. Программные средства железнодорожного подвижного состава, как встраиваемые, так и поставляемые на материальных носителях, должны обеспечивать защищенность от компьютерных вирусов, несанкционированного доступа, последствий отказов, ошибок и сбоев при хранении, вводе, обработке и выводе информации, возможности случайных изменений информации.

Особенности применения ПО АСУ ТП и связанные с этим риски определяют необходимость расширения комплексного подхода к оценке соответствия требованиям функциональной и информационной безопасности.

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.

В целях обеспечения максимальной эффективности деятельности Белорусской железной дороги в её информационной инфраструктуре применяются или планируются к применению самые современные информационные технологии, включая технологии виртуализации и «облачных вычислений».

Вместе с неоспоримыми преимуществами применения современных информационных технологий, существуют риски реализации угроз кибербезопасности, последствиями которых могут стать нарушение безопасного функционирования железнодорожного транспорта.

Всё это можно показать на примере процессорно-релейной централизации (далее – ПРЦ) «Іпуть», установленной на станции Ипуть Гомельского отделе-

ния Белорусской железной дороги. Данная система предназначена для управления оконечными устройствами железнодорожной автоматики на станции.

Система ПРЦ функционирует в реальном времени, осуществляя сбор, обработку и хранение технологической информации о текущем состоянии устройств железнодорожной автоматики и обеспечения безопасного управления движения подвижного состава на железнодорожной станции. Реализованные в системе ПРЦ технологические алгоритмы на основании информации о текущем состоянии поездной обстановки и диспетчерских команд формируют сигналы управления релейно-контактными устройствами станционных объектах низовой и локальной автоматики. Объектами управления и контроля в системе ПРЦ являются элементы систем железнодорожной автоматики и телемеханики (объекты централизации): стрелочные электроприводы одиночных и спаренных стрелок станции; светофоры; рельсовые цепи; шлагбаумы; устройства специальных видов сигнализации.

Система процессорно-релейной централизации стрелок и сигналов предназначена для реализации современных принципов управления движением поездов и маневровой работой на железнодорожных станциях с помощью средств микропроцессорной вычислительной техники с сохранением существующих правил управления устройствами сигнализации, централизации и блокировки и действий дежурного по станции (далее – ДСП) при обеспечении требуемой степени безопасности и безотказности.

В отличие от существующих зарубежных аналогов отечественная ПРЦ «Іпуть» имеет более высокие показатели по безопасности и эксплуатационной готовности за счет более глубокого резервирования, что подтверждено как комиссией НАН Беларуси, так и данными опытной эксплуатации.

Концепция обеспечения безопасности: двухканальная система с умеренными связями, параллельной и независимой обработкой данных, взаимным сравнением логики функционирования и переходом в защитное состояние при рассогласовании логики управления в каналах.

Цикл управления системой ПРЦ, реализуемый средствами ПО ядра (опрос состояния объектов станционной автоматики и их отображение, обработка команд ДСП, принятие решений с учётом состояния объектом станционной автоматики и поездной обстановки, выдача сигналов управления на блоки управления) составляет порядка 280–320 мс.

Говоря о безопасности АСУ ТП, нельзя не упомянуть системы железнодорожной автоматики и телемеханики (далее – СЖАТ). Микропроцессорные СЖАТ имеют следующие дополнительные особенности с позиций обеспечения кибербезопасности по отношению к массовым промышленным АСУ ТП:

– главной целью кибератаки на микропроцессорные СЖАТ является не информация сама по себе, а возможность воздействия на исполнительные объекты;

– возможная атака будет направлена на вывод из строя микропроцессорной СЖАТ (в том числе и методами электромагнитного терроризма) или

нарушения функциональной безопасности, а следовательно, и нарушения безопасности движения поездов;

– атака может быть направлена на конкретные (наиболее опасные по последствиям), объекты СЖАТ с помощью специально разработанных средств, поэтому традиционные (шаблонные) средства защиты могут быть неэффективными;

– микропроцессорные СЖАТ, объединенные в АСУ процессом перевозок, территориально разобщены и работают в реальном масштабе времени, и применение средств защиты, основанных, например, на методах криптографии, шифрования, потребует дополнительных вычислительных ресурсов и, естественно, к увеличению времени на реализацию команд и получении информации о состоянии объектов, что может явиться ограничивающим фактором в обеспечении функциональности систем.

Отличительной особенностью АСУ ТП, связанных с безопасностью движения поездов, является широкое применение современных информационных систем в важных для жизнеобеспечения государства отраслях. Нарушение процессов их нормального функционирования может привести к срыву выполнения функций государственного управления, управления войсками, оружием, экологически опасными и экономически важными производствами и, как следствие, к недопустимому ущербу национальным интересам. Исходя из этого, такие информационные системы рассматриваются как критически важные в силу того, что от их безопасности ключевым образом зависит безопасность важнейших секторов жизнедеятельности государства.

Вопросы сохранения способности нормального функционирования информационных систем в условиях деструктивных воздействий традиционно решаются с использованием понятий информационной безопасности и надёжности и соответствующего им методологического базиса.

Конфиденциальность, целостность и доступность отражают разные аспекты информационной безопасности систем, вследствие чего и задачи, решаемые для их обеспечения, различны. Так, при обеспечении конфиденциальности и целостности, как правило, решаются задачи защиты информации от несанкционированного доступа. Для их эффективного решения широко используются организационные, технологические и правовые методы, классификация и описание которых приведены в обширной литературе.

Они ориентированы в основном на защиту собственно информационных систем, в силу чего вне поля их применения остаётся решение такой важной для АСУ ТП проблемы, как предотвращение или минимизация ущерба внешней среде. Этот ущерб может быть вызван негативным воздействием на внешнюю среду вследствие нарушения нормального процесса функционирования таких систем. Поэтому должны решаться вопросы обеспечения гарантированных уровней безопасности различных АСУ ТП, включая формирование количественных требований к безопасности; доказательство безопасности (выпол-

нения требований) на основе совместного применения результатов ускоренных натурных испытаний, аналитических методов, стендовых испытаний, экспертных оценок и разработки «паспорта» безопасности критически важной системы на всех этапах жизненного цикла; анализа рисков возникновения состояний опасных функциональных отказов, соответствующих недопустимому ущербу внешней среде, и создания механизмов блокирования перехода в такие состояния.

Таким образом, безопасность АСУ ТП, как и безопасность критически важных систем информационной инфраструктуры, определяется безопасностью информации, циркулирующей в системах, гарантированной реализацией процессов их нормального функционирования, а также безопасностью влияния систем на внешнюю среду, то есть, соответственно, их информационной безопасностью, надёжностью и функциональной безопасностью.

Мониторинг безопасности АСУ ТП является неотъемлемой частью процесса обеспечения безопасных условий их функционирования при деструктивных воздействиях. Основной целью данных мероприятий является получение информации о реальном состоянии систем для организации противодействия таким воздействиям. В связи с этим на мониторинг безопасности возлагаются функции обнаружения деструктивных воздействий на системы, анализа их состояния и оценки уровня безопасности после осуществления таких воздействий. Реализация этих функций связана с решением задач формирования множества деструктивных воздействий и их признаков, разработки методов обнаружения и идентификации деструктивных воздействий, выбора (разработки) методов контроля состояний систем, формирования системы показателей и разработки методов оценки уровня безопасности систем. Таким образом, безопасность АСУ ТП информационной инфраструктуры определяется их способностью нормально функционировать в условиях деструктивных воздействий, а также противодействовать опасным функциональным отказам, вызывающим недопустимый ущерб внешней среде.

Существующая система создания новых технических средств безопасности движения ориентирована на выполнение стандартного технологического процесса разработки, постановки продукции на производство и допуска в эксплуатацию.

Эта система, регламентируемая ранее ГОСТами и ОСТами по поставке аппаратуры систем безопасности, показала свою жизненность, однако она не учитывает появление новых факторов:

– введение технических регламентов, осуществляющих нормирование процесса разработки и приемки изделий;

– необходимость соответствия международным стандартам в части контроля требований безопасности на всем жизненном цикле изделий;

– появление специальных требований по надежности и безопасности программных средств;

– необходимость задания и обеспечения требований по информационной безопасности;

– необходимость создания соответствующих организационных структур, проводящих экспертизу технических решений, а также обучение специалистов, эксплуатирующих и обслуживающих системы безопасности.

– необходимость создания нормативных технических документов стандартов организации (СТО), гарантирующих выполнение требований безопасности и надежности систем управления, гармонизированных с международными стандартами и нормативными документами Республики Беларусь.

С введением технических регламентов возможно упрощение ряда требований по безопасности и надежности для производителей. Это связано с тем, что комплексные показатели зависят от целого ряда отдельных нормативов, каждый из которых определялся ими в технических условиях на изделие.

Мировой опыт подсказывает переход к стандартам, фиксирующим весь жизненный цикл изделий. В качестве такого стандарта для систем безопасности подходит EN 50126 «Определение и подтверждение надежности и безопасности (RAMS) на железных дорогах».

Таким образом, целесообразно организовать выявление во встраиваемых компьютерных системах для автоматизации процессов управления железнодорожным транспортом уязвимых мест закладок и возможных ошибок, действие которых может привести к наихудшим последствиям. Такое выявление может производиться с помощью группы экспертов, пытающихся встать на место злоумышленников, внедряющих закладки.

Для повышения уровня информационной безопасности рекомендуется использовать набор средств защиты информации, состоящий из сервера антивирусной защиты, системы проверки целостности ПО, системы IDS.

СПИСОК ЛИТЕРАТУРЫ

1 **Завгородний, В. И.** Комплексная защита информации в компьютерных системах : учеб. пособие / В. И. Завгородний. – М. : Логос, 2001. – 264 с: ил.

2 СТБ 34.101.30-2007 Информационные технологии. Методы и средства безопасности. Объекты информатизации. Классификация.

3 СТО РЖД 02.049–2014 Автоматизированные системы управления технологическими процессами и техническими средствами железнодорожного транспорта. Требования к функциональной и информационной безопасности программного обеспечения. Порядок оценки соответствия.

4 Указ Президента Республики Беларусь № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации» от 25 октября 2011 г.

5 Указ Президента Республики Беларусь № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь» от 9 ноября 2010 г.

6 **Теренин, А. А.** Как построить модель типового нарушителя информационной безопасности / А. А. Теренин // Защита информации. INSIDE-2005. – № 5. – С. 18–24.

7 **Шатров, С. Л.** Учетные технологии цифровой экономики / С. Л. Шатров // Рынок транспортных услуг (проблемы повышения эффективности): Междунар. сб. науч.тр. – Вып. 11. – Гомель : БелГУТ, 2018. – С. 64–73.

8 **Шатров, С. Л.** Процессный подход в системе управления железнодорожного транспорта: учетно-контрольные аспекты / С. Л. Шатров, Е. О. Фроленкова // Устойчивое развитие экономики: международные и национальные аспекты / Полоцкий государственный университет. – Новополоцк, 2018. – С. 471–475.

B. RABTSAU
Belarusian State University of Transport

MAKING INFORMATION SECURITY OF AUTOMATED MANAGEMENT SYSTEMS FOR TECHNOLOGICAL PROCESSES ON RAILWAY TRANSPORT

Systems that provide control and automated management of technological equipment in railway transport are considered. The features of the application of these systems are described. Recommendations on improving the information security of automated process control systems are given.

Получено 23.09.2019

ISSN 2225-6741. Рынок транспортных услуг (проблемы повышения эффективности). Вып. 12. Гомель, 2019

УДК 004.9 : 629.4

Н. А. РЯБЦЕВА
А. А. НИКИТЕНКО
Белорусский государственный университет транспорта

АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ В ЛОКОМОТИВНОМ ХОЗЯЙСТВЕ

Рассматривается роль локомотивного хозяйства в структуре железной дороги. Приводятся примеры автоматизированных систем управления для совершенствования работы локомотивных депо, их цели и задачи, выполнение которых улучшит количественные и качественные показатели работы железной дороги.

В условиях экономических преобразований к транспортному обеспечению предъявляются новые, более повышенные требования. Надежность, бесперебойность, высокая скорость доставки продукции из пунктов производства в пункты потребления в строго обусловленные сроки и без потерь, порчи и по-