АВТОМАТИКА, ТЕЛЕМЕХАНИКА И СВЯЗЬ

УДК 656.2.08

К. А. БОЧКОВ, доктор технических наук, П. М. БУЙ, кандидат технических наук, Белорусский государственный университет транспорта, г. Гомель; О. А. ЧЕКАНОВА, инженер ГФ РУП «БЕЛТЕЛЕКОМ», г. Гомель

КРИТИЧЕСКИ ВАЖНЫЕ ОБЪЕКТЫ ИНФОРМАТИЗАЦИИ НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ

Рассмотрен особый подход к микропроцессорным системам обеспечения безопасности движения поездов как систем управления нижнего уровня. Дано понятие критически важного объекта информатизации. Проанализированы критерии отнесения объектов информатизации к критически важным на примере микропроцессорных систем обеспечения безопасности движения поездов. Указаны возможные последствия нарушения информационной и функциональной безопасности микропроцессорных систем управления на транспорте на примере известных фактов крушений подвижного состава.

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, а также является самым доступным транспортом для граждан республики. Следовательно, Белорусская железная дорога должна обеспечить потребности государства, юридических и физических лиц в железнодорожных перевозках, работах и услугах, оказываемых железнодорожным транспортом, а также извлечь из этого прибыль.

Анализ инцидентов в сфере информационной безопасности за последние годы, публикуемый в открытом доступе [1], наглядно показывает динамику увеличения их количества. Кроме того, всё больший интерес в качестве объектов кибератак вызывают у нарушителей ранее труднодоступные автоматизированные системы управления технологическими процессами (АСУ ТП), к которым относятся микропроцессорные системы обеспечения безопасности движения поездов и, в особенности, использующие современные информационные технологии и программное обеспечение (ПО). Для обеспечения большей эффективности функционирования Белорусской железной дороги в его информационное пространство как раз и внедряются передовые информационные технологии.

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, легко переходящие в кибератаки при недостаточной защищенности АСУ ТП. Одной из самых опасных и при этом достаточно просто реализуемой кибератак является распределенная атака против доступности системы управления, при которой она перестает обрабатывать управляющие воздействия из-за перегрузки (DDoS-атака). В настоящее время существуют риски реализации угроз кибербезопасности, последствиями которых могут стать нарушение функционирования АСУ ТП в целом и микропроцессорных систем обеспечения безопасности движения поездов в частности.

Высокая степень ответственности функций, выполняемых микропроцессорными системами обеспечения безопасности движения поездов, требует особого подхода к выполнению требований по безопасности функционирования железнодорожного подвижного состава и объектов инфраструктуры железнодорожного транспорта. В соответствии с техническими регламентами Таможенного союза [2–4] 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 микропроцессорных систем обеспечения безопасности движения поездов и связанные с этим риски определяют необходимость расширения и комплексного подхода к оценке их соответствия требованиям не только информационной, но и обязательно функциональной безопасности.

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. Информационная безопасность, безусловно, тоже важна, но при отсутствии у объекта информатизации информации, предоставление которой должно быть ограничено, мероприятия по обеспечению информационной безопасности фактически сводятся к функциям разграничения доступа к объекту информатизации и контроля выполняемых пользователем операций на этом объекте. Все эти мero-

приятия важны при обеспечении функциональной безопасности.

Ошибки и не декларированные возможности ПО микропроцессорных систем обеспечения безопасности движения поездов, нарушают в первую очередь как раз функциональную безопасность. Однако существующие нормативные документы касаются защиты информации с точки зрения целостности, доступности, конфиденциальности, но полностью понятия функциональной безопасности не раскрывают. Поэтому необходимы такие нормативные документы, которые будут оперировать понятием «функциональная безопасность» применительно к объектам информатизации железнодорожного транспорта для обеспечения их полноценной защиты. Для работы в данном направлении необходимо создать специализированную лабораторию, объединяющую специалистов в областях микропроцессорных систем обеспечения безопасности движения поездов и защиты информации.

Объект информатизации согласно [5] – это средства электронной вычислительной техники (автоматизированные системы различного уровня и назначения, вычислительные сети и центры, автономные стационарные и персональные электронные вычислительные машины, а также копировально-множительные средства, в которых для обработки информации применяются цифровые методы) вместе с ПО, используемые для обработки информации.

Влиянию кибератак в настоящее время подвержены все объекты информатизации и, к сожалению, интенсивность, а также практическое разнообразие таких атак растет и развивается из года в год. В связи с этим в Республике Беларусь была выделена особая категория объектов информатизации – критически важные объекты информатизации (КВОИ).

В соответствии с Указом Президента Республики Беларусь от 25.10.2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации» [6] критически важный объект информатизации – это объект информатизации, который:

– обеспечивает функционирование экологически опасных и (или) социально значимых производств и (или) технологических процессов, нарушение штатного режима которых может привести к чрезвычайной ситуации техногенного характера;

– осуществляет функции информационной системы, нарушение (прекращение) функционирования которой может привести к значительным негативным последствиям для национальной безопасности в политической, экономической, социальной, информационной, экологической, иных сферах;

– обеспечивает предоставление значительного объема информационных услуг, частичное или полное прекращение оказания которых может привести к значительным негативным последствиям для национальной безопасности в политической, экономической, социальной, информационной, экологической, иных сферах.

Впервые КВОИ упоминается в Указе Президента Республики Беларусь от 9 ноября 2010 г. № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь» [7]. В Концепции национальной безопасности Республики Беларусь относительно КВОИ сказано следующее:

1) одним из основных национальных интересов в информационной сфере является обеспечение надежности и устойчивости функционирования критически важных объектов информатизации (Глава 2. Национальные интересы);

2) одной из основных потенциальных либо реально существующих угроз национальной безопасности является: нарушение функционирования критически важных объектов информатизации (Глава 4. Основные угрозы национальной безопасности);

3) в информационной сфере одним из внутренних источников угроз национальной безопасности является несовершенство системы обеспечения безопасности критически важных объектов информатизации (Глава 5. Внутренние источники угроз национальной безопасности).

Окончательно порядок отнесения объектов информатизации к КВОИ, вопросы их технической и криптографической защиты, а также контроля определены следующими правовыми документами:

– Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20 декабря 2011 г., № 96 «О некоторых мерах по реализации указа Президента Республики Беларусь от 25 октября 2011 г. № 486» [8];

– Постановление Совета Министров Республики Беларусь от 30 марта 2012 г. № 293 «О некоторых вопросах безопасной эксплуатации и надежного функционирования критически важных объектов информатизации» [9];

– Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 30 апреля 2012 г., № 42 «Об утверждении инструкции о порядке проведения внешнего контроля критически важных объектов информатизации» [10];

– Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 30 августа 2013 г., № 62 «О некоторых вопросах технической и криптографической защиты информации» [11].

В Российской Федерации аналогом КВОИ выступают ключевые системы информационной инфраструктуры (КСИИ), описанные руководящими документами Федеральной службой по техническому и экспортному контролю (ФСТЭК) с грифом ДСП.

КСИИ – это информационно-управляющая или информационно-телекоммуникационная система, которая осуществляет управление критически важным объектом (процессом), или информационное обеспечение управления таким объектом (процессом), или официальное информирование граждан, в результате деструктивных информационных воздействий на которую может сложиться чрезвычайная ситуация либо будут нарушены выполняемые системой функции управления со значительными негативными последствиями.

В ОАО «РЖД» микропроцессорные системы обеспечения безопасности движения поездов отнесены к КСИИ.

Перед руководством любой государственной организации или крупной частной компании актуальным становится вопрос об отнесении своих объектов информатизации к КВОИ и выполнение соответствующих этому статусу мероприятий по защите информации.

При отнесении объекта информатизации к КВОИ, необходимо охарактеризовать его по четырем критериям [9]:

1) критерий экологической опасности производства, функционирование которого обеспечивается объектом информатизации;

2) критерий социальной значимости производства, функционирование которого обеспечивается объектом информатизации;

3) критерий важности объекта информатизации, осуществляющего функции информационной системы;

4) критерий важности объекта информатизации, обеспечивающего предоставление значительного объема информационных услуг.

Соответствие микропроцессорных систем обеспечения безопасности движения поездов отраслевым критериям отнесения объектов информатизации к КВОИ приведено в таблице 1. Так как исследуемые микропроцессорные системы управления являются системами управления нижнего уровня при обеспечении безопасности движения поездов, то говорить об их важности с точки зрения информационной системы или при предоставлении информационных услуг не приходится. Однако первые два из перечисленных критериев нельзя оставить без внимания при анализе возможных последствий при нарушении функционирования микропроцессорной системы обеспечения безопасности движения поездов.

Таблица 1 – **Соответствие микропроцессорных систем обеспечения безопасности движения поездов отраслевым критериям отнесения объектов информатизации к КВОИ**

Отраслевые критерии отнесения объектов информатизации к КВОИ	Соответствие микропроцессорных систем обеспечения безопасности движения поездов отраслевым критериям отнесения объектов информатизации к КВОИ
Критерий экологической опасности производства, функционирование которого обеспечивается объектом информатизации	**Соответствует**
Критерий социальной значимости производства, функционирование которого обеспечивается объектом информатизации	**Соответствует**
Критерий важности объекта информатизации, осуществляющего функции информационной системы	**Не соответствует**
Критерий важности объекта информатизации, обеспечивающего предоставление значительного объема информационных услуг	**Не соответствует**

В качестве грузов, перевозимых железнодорожным транспортом, могут быть как взрывоопасные смеси и жидкости, так и ядовитые вещества, которые при крушении поезда могут привести к существенным негативным экологическим последствиям.

Транспорт в целом имеет большую социальную значимость, а железнодорожный транспорт играет не последнюю роль в процессах грузо- и пассажироперевозок в нашей стране. Существенные задержки в исполнении графика движения поездов могут привести к падению престижа Белорусской железной дороги и неудовлетворенности граждан в качестве предоставляемых ею услуг.

Для иллюстрации значимости качественного функционирования систем обеспечения безопасности движения поездов рассмотрим несколько техногенных катастроф, непосредственно связанных с железнодорожным транспортом. Во всех приведенных ниже примерах причиной крушений были отказы или нештатная работа (по вине человека) систем, обеспечивающих безопасность движения поездов.

1 Крушение пассажирского поезда «Аврора» на перегоне Березайка – Поплавенец 16 августа 1988 г. В результате схода с рельсов всех вагонов поезда 31 человек погиб, более 100 пострадали, движение на участке было остановлено более чем на 15 ч.

2 Крушение пассажирского поезда «Юрмала» 3 марта 1992 г. на разъезде Подсосенка участка Великие Луки – Ржев Октябрьской железной дороги. Пассажирский поезд столкнулся со встречным грузовым составом. В результате столкновения поездов 43 человека погибли, 108 получили травмы. Допущен перерыв движения поездов на участке 15 ч 30 мин.

3 25 апреля 2005 г. в Японии скоростной поезд отставал от графика, поэтому машинист решил рискнуть и превысил скорость до 116 км/ч на опасном повороте, где максимально разрешенной скоростью было 70 км/ч. В результате поезд сошел с рельс и врезался в здание паркинга недалеко от станции Амагасаки. Два первых вагона от удара были буквально расплющены, остальные тоже оказались сильно поврежденными. В поезде находилось около 700 человек, из них 107 погибли, 562 получили ранения.

4 Крушение поезда в Сантьяго-де-Компостела 24 июля 2013 г. Высокоскоростной поезд Alvia подъезжал к станции Сантьяго-де-Компостела, когда все 8 вагонов поезда сошли с рельсов и перевернулись. Причиной катастрофы стало более чем двукратное превышение скорости состава при прохождении кривого участка пути. 79 человек погибли и около 140 получили ранения.

Подобные техногенные катастрофы следует рассматривать с учетом примерного перечня показателей уровня ущерба национальным интересам Республики Беларусь в политической, экономической, социальной, информационной, экологической и иных сферах в случае возникновения угроз различного характера в отношении объекта информатизации (его составляющих элементов), который представлен в источнике [9]. Хотя достаточно сложно предсказать возможное количество жертв или величину материального ущерба, нанесенного отрасли и государству в целом, при крушении вследствие нарушения функциональной и (или) информационной безопасности микропроцессорной системы обеспечения безопасности движения поездов в результате успешной реализации кибератаки, однако уровень ущерба будет по классификации [9] катастрофическим. К системам, которые могут стать объектами кибератак, относятся такие микропроцессорные системы, как микропроцессорная централизация (МПЦ), автоблокировка (АБ), полуавтоматическая блокировка (ПАБ), переездная сигнализация, комплексное локомотивное устройство безопасности (КЛУБ), безопасный локомотивный объединенный комплекс (БЛОК) и т. п. Все они связанны с обеспечением безопасности движения поездов. Необходимо однозначно поднимать вопрос об отнесении таких систем к критически важным объектам информатизации.

Список литературы

1 Kaspersky security bulletin 2015 [Электронный ресурс] – Режим доступа: https://securelist.ru/files/2015/12/Kaspersky-Security-Bulletin-2015_FINAL_RUS.pdf. – Дата доступа: 29.06.2016.

2 Технический регламент Таможенного союза ТР ТС 001/2011 «О безопасности железнодорожного подвижного состава».

3 Технический регламент Таможенного союза ТР ТС 002/2011 «О безопасности высокоскоростного железнодорожного транспорта».

4 Технический регламент Таможенного союза ТР ТС 003/2011 «О безопасности инфраструктуры железнодорожного транспорта».

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

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

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

8 Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20 декабря 2011 г. № 96 «О некоторых мерах по реализации указа Президента Республики Беларусь от 25 октября 2011 г. № 486».

9 Постановление Совета Министров Республики Беларусь от 30 марта 2012 г. № 293 «О некоторых вопросах безопасной эксплуатации и надежного функционирования критически важных объектов информатизации».

10 Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 30 апреля 2012 г. № 42 «Об утверждении инструкции о порядке проведения внешнего контроля критически важных объектов информатизации».

11 Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 30 августа 2013 г. № 62 «О некоторых вопросах технической и криптографической защиты информации».

Получено 31.10.2016

K. A. Bochkov, P. M. Bui, O. A. Chekanova. Critical facilities informatization of the railways.

Considered a special approach to the security of the microprocessor systems of ensuring of the trains' safety as a low-level control systems. The notion of critical informatization object are given. The criteria for assignment of information objects to critical on the example of microprocessor systems of ensuring of the trains' safety are analyzed. The possible consequences of a breach of information's and functional safety of microprocessor systems of management on transport are given with the example of the known facts derailments of rolling stock.