сформулированными в документе «Требования к программному обеспечению», что позволит в дальнейшем выполнить проверки на корректность реализации. Оно должно контролировать целостность исполняемого кода и данных, а в многоканальном исполнении – целостность и адекватность данных во всех вычислительных каналах.

**Технологическое ПО** предназначено для корректной реализации всех технологических алгоритмов системы ЖАТ в соответствии с предъявляемыми к нему требованиями. Оно должно минимально зависеть от операционной системы или компилятора, что обеспечивает переносимость на другие платформы. Его следует разрабатывать с учетом возможности проведения испытаний, в том числе отдельно от аппаратных средств системы ЖАТ (с применением имитаторов). Для технологического ПО должна быть выбрана, использована и задокументирована стратегия управления ресурсами, в том числе оперативной памятью, а также предусмотрен механизм самопроверки с целью выявления возможных некорректных состояний данных. Нужно строго соблюдать временные характеристики функционирования технологического ПО. В частности, в худшем случае длительность выполнения одного цикла вычислений не должна превышать допустимых для данной системы ЖАТ значений. Использование сторонних программных компонентов в технологическом ПО следует свести к минимуму и документально обосновать.

В заключение нужно сказать, что в статье рассмотрена лишь часть мероприятий, направленных на решение вопросов обеспечения безопасности и качества ПО систем ЖАТ. В совокупности с решением других вопросов, таких как документирование и порядок разработки ПО, они весьма актуальны при проектировании и создании ПО систем ЖАТ.

Практика работы в области экспертной оценки ПО систем ЖАТ показывает, что зачастую не соблюдаются даже элементарные правила разработки качественного и безопасного ПО. Это обусловлено рядом причин, к которым можно отнести недостаточную развитость – как государственной, так и отраслевой нормативных баз.

УДК 004.056:656.25

# КИБЕРБЕЗОПАСНОСТЬ МИКРОПРОЦЕССОРНЫХ УСТРОЙСТВ ЖАТ

**С.В. ГОРДЕЙЧИК,**
технический директор,
ЗАО «Позитив Текнолоджиз»

***Ключевые слова:*** *кибербезопасность, функциональная безопасность, информационная безопасность, надежность, анализ рисков, МПСУ ЖАТ, уязвимость*

**Внедрение микропроцессорных систем управления (МПСУ) и, в первую очередь, технических средств железнодорожной автоматики и телемеханики (ЖАТ) способствует повышению интенсивности и скорости движения поездов, оптимизации процесса организации перевозок пассажиров и грузов. При этом на первый план выходят вопросы кибербезопасности таких устройств. Так что же такое кибербезопасность МПСУ ЖАТ и как она влияет на обеспечение безопасности движения поездов и экономическую эффективность перевозок?**

■ Применение микропроцессорных систем влечет за собой массовое внедрение цифровых систем проводной и радиосвязи, поддерживающих протокол TCP/IP. Однако использование в таких системах стандартного системного и прикладного программного обеспечения и сетевых протоколов, а также широкое применение механизмов удаленного управления, беспроводных сетей и интернет-технологий приводит к наследованию проблем обеспечения безопасности типовых компонентов. Это предопределяет необходимость выдвижения новых требований к инфраструктуре связи.

Исследования [1] в области информационной безопасности автоматизированных систем управления технологическими процессами (АСУ ТП) с описанием ряда уязвимостей продемонстрировали возможность использования традиционных методов и подходов, применяющихся для нарушения информационной и компьютерной безопасности в целях негативного влияния на функциональную безопасность, надежность и безопасность технологического процесса.

Сложная геополитическая обстановка и развитие средств проведения компьютерных атак заставляют пересмотреть модели

угроз, которые использовались для анализа защищенности и построения средств защиты. Предпринятая в прошлом году комплексная кибератака Havex, описанная в ряде исследований [2], позволила злоумышленникам скомпрометировать сайты компаний-производителей компонентов АСУ ТП, подменив оригинальные дистрибутивы программного обеспечения, загружаемые пользователем. В результате специализированное вредоносное ПО загружалось с официальных репозиториев производителя и устанавливалось в сегментах автоматизированных систем управления технологическими процессами самим оператором системы.

Детальный анализ защищенности ряда широко распространенных систем АСУ ТП, в том числе и МПСУ ЖАТ, выявил дефекты и уязвимости, используя которые злоумышленники не только снижают ключевые показатели надежности и обходят механизмы функциональной безопасности, но и реализуют атаки, напрямую влияющие на безопасность движения поездов. Примечательно, что с точки зрения информационной и функциональной безопасности эти системы соответствуют всем выдвигаемым требованиям, имеют все необходимые международные, отраслевые и государственные сертификаты.

Основным отличием таких воздействий от привычной «дачи ложного контроля» является возможность проведения атак удаленно, без непосредственного физического доступа, а также простота сокрытия доказательств, что не позволяет выявить причину инцидента (так называемая безуликовость).

Очевидно, что при проектировании, разработке и внедрении МПСУ ЖАТ нужно учитывать возможности целенаправленного антропогенного воздействия, негативно влияющего на обеспечение безопасности движения, заданный уровень пропускной и провозной способности участков дорог.

Основной задачей кибербезопасности применительно к железнодорожному транспорту является обеспечение безопасности движения поездов. Анализ тематических научных публикаций показывает, что до недавнего времени основным направлением исследований и разработок было обеспечение достаточного уровня надежности и функциональной безопасности микропроцессорных систем управления. В большинстве работ антропогенные угрозы сводились к ошибкам оператора и обслуживающего персонала, что вполне обосновано при исключении широкомасштабных удаленных воздействий. Но такое ограничение не позволяет учитывать актуальные угрозы, связанные с возможностью удаленного воздействия на микропроцессорные устройства, при внедрении которых используются распределенные системы связи и беспроводные технологии. А без этого невозможно сформировать объективную картину обеспечения безопасности движения поездов.

Базовые требования по информационной безопасности МПСУ на железнодорожном транспорте, изложенные в технических регламентах Таможенного Союза [3], [4], достаточно поверхностны и сводятся к обеспечению «защищенности от компьютерных вирусов, несанкционированного доступа, последствий отказов, ошибок и сбоев при хранении, вводе, обработке и выводе информации, возможности случайных изменений информации». Как видим, речь опять идет, в основном, о «случайных воздействиях», не учитывающих целенаправленную атаку. Тем не менее в этих документах упоминается «несанкционированный доступ», что косвенно подтверждает необходимость учета антропогенного фактора при анализе защищенности.

Ряд требований к обеспечению безопасности функционирования АСУ ТП в целом изложен в документе ФСТЭК России [5]. Однако он построен на привычной концепции обеспечения «целостности», «доступности» и «конфиденциальности» информации, тогда как целью защиты МПСУ ЖАТ является безопасность движения.

Таким образом, нормативные, организационные и технические вопросы кибербезопасности современных систем МПСУ на железнодорожном транспорте проработаны недостаточно полно. Это говорит о разрыве между подходами и методами обеспечения информационной безопасности и практикой решения задач обеспечения безопасности движения поездов.

Для устранения обозначенного разрыва предлагается определять кибербезопасность как процесс обеспечения функционирования МПСУ ЖАТ, при котором исключаются опасные отказы и недопустимый ущерб, обеспечивается заданный уровень экономической эффективности, функциональной безопасности и надежности в случае целенаправленного негативного антропогенного информационного воздействия на их компоненты.

При развитии этой концепции в рамках решения вопроса о кибербезопасности МПСУ ЖАТ предлагается использовать методический аппарат трех дисциплин: безопасности движения, функциональной и информационной безопасности.

Такой подход позволит использовать существующие научные и методические инструменты, исключая при этом ограничения, не позволяющие применять для решения задач каждую из дисциплин самостоятельно. Так, например, функциональная безопасность связана со случайными отказами системы и не учитывает целенаправленных угроз, а информационная безопасность направлена на обеспечение целостности, доступности и конфиденциальности информации, что напрямую не связано с задачами обеспечения безопасности движения.

Основными преимуществами данного подхода является возможность интеграции предмета кибербезопасности в существующие процессы проектирования, разработки и внедрения систем МПСУ ЖАТ с использованием зарекомендовавших себя наработок. В таблице приведены некоторые методики различных дисциплин и возможность их использования в обеспечении кибербезопасности этих технических средств.

Основой обеспечения безопасности является корректное определение угроз. С точки зрения кибербезопасности можно выделить три основных класса угроз МПСУ ЖАТ:

| Дисциплина | Используемые методики |
|---|---|
| Безопасность движения | Требования к уровню безопасности<br>Функциональные требования к МПСУ |
| Функциональная безопасность и теория надежности | Методический аппарат анализа рисков<br>Методы доказательства безопасности<br>Оценка эффективности средств защиты |
| Информационная безопасность | Методический аппарат моделирования угроз<br>Методики анализа защищенности<br>Процессы, средства и механизмы защиты<br>Оценка эффективности средств защиты |

нарушение безопасности движения поездов;

снижение эффективности процесса перевозок путем влияния на пропускную и провозную способности, а также другие экономические показатели;

другие нарушения функциональной безопасности и надежности, которые косвенно влияют на безопасность движения и эффективность процесса перевозок.

Такой подход при анализе кибербезопасности МПСУ позволит строить частную модель угроз исходя из требований безопасности движения и функциональной безопасности, выдвигаемых к данному классу систем. Рассмотрим в качестве примера укрупненную модель угроз для микропроцессорной системы централизации стрелок и сигналов (МПЦ), воспользовавшись при этом требованиями ПТЭ. С учетом особенностей других систем ЖАТ список угроз, несомненно, следует расширить.

Угрозы, приводящие к нарушению безопасности движения поездов, как правило, наиболее сложны в реализации и требуют от нарушителя максимальных усилий. Для того чтобы добиться результата, ему потребуется обойти механизмы функциональной безопасности МПЦ. В случае невозможности прямого влияния на объектные контроллеры, например, через уязвимости радиоканала, подобные атаки требуют изменения логики работы основных модулей МПЦ в части контроля взаимозависимости стрелок и сигналов, выполнения требований безопасности движения, что является нетривиальной задачей. Однако если такая возможность существует, нарушитель может:

установить более разрешающее показание светофора (например, зеленый входной сигнал при движении с отклонением по стрелкам);

открыть сигнал светофора при незаданном маршруте (занятых по маршруту следования участках или ненадлежащем положении стрелок);

перевести стрелку под подвижным составом;

задать враждебные маршруты и др.

Угрозы, направленные на снижение эффективности процесса перевозок, как правило, не требуют высокого уровня квалификации злоумышленника и могут быть реализованы с помощью стандартного вредоносного ПО. Поскольку не нужно разрабатывать специальные инструменты для проведения атаки, добиться результата гораздо проще. Это может быть, например, вывод из строя недублированных компонентов, таких как ЦП/ЦПУ, подделка или блокирование сетевого взаимодействия между АРМ ДСП и ЦП/ЦПУ, приводящие к блокировке возможности подачи команд. Все это потребует перехода на ручное управление, а следовательно, вызовет снижение эффективности управления процессом перевозок.

Примером угроз, косвенно влияющих на безопасность движения и эффективность процесса перевозок, могут служить вывод из строя АРМа ШН и принудительная перезагрузка ЦП/ЦПУ или АРМа ДСП. Эти воздействия снижают среднее время наработки на отказ, определяющееся для программных продуктов как срок до полного перезапуска программы или полной перезагрузки операционной системы. С этой же целью могут использоваться атаки, направленные на исчерпание сетевых и вычислительных ресурсов компонентов МПЦ (Deny of Service, DoS). Также возможны атаки на сетевое оборудование, приводящие к изменению конфигурации и параметров протоколов TCP/IP и Ethernet, удалению/замене ПО сетевого оборудования (firmware).

Очевидно, что при проектировании, разработке и внедрении микропроцессорных систем железнодорожной автоматики и телемеханики необходимо учитывать возможности целенаправленного антропогенного воздействия, негативно влияющего на обеспечение безопасности движения поездов, заданный уровень пропускной и провозной способности участков дорог. Определение предмета кибербезопасности через дисциплины безопасности движения, функциональной и информационной безопасности позволит учитывать отраслевую специфику и оценить влияние негативных воздействий в терминах опасных отказов и теории надежности. Это даст возможность встроить процессы кибербезопасности в существующие процессы обеспечения безопасности движения поездов и экономической эффективности перевозок.

### ИСТОЧНИКИ ИНФОРМАЦИИ

1. Sergey Gordeychik, «WinCC Under X-Rays», S4 Conference, Miami, USA.

2. «FireEye обнаружила новый вариант Havex, сканирующий OPC-серверы» http://www.securitylab.ru/news/455022.php.

3. «О безопасности железнодорожного подвижного состава» (ТР ТС 001/2011), http://www.tsouz.ru/db/techreglam/Documents/TR%20Podvignoisostev%20PID.pdf.

4. «О безопасности высокоскоростного железнодорожного транспорта» (ТР ТС 002/2011) http://www.eurasiancommission.org/ru/act/texnreg/deptexreg/tr/Documents/TR%20HighSpeed%20PID.pdf.

5. «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды». Приказ ФСТЭК России от 14 марта 2014 г. N 31, http://www.rg.ru/2014/08/06/fstek-dok.html.