Шаблон MVVM делится на три части:

Модель (англ. model) (так же, как в классической MVC) представляет собой логику работы с данными и описание фундаментальных данных, необходимых для работы приложения.

Представление (англ. view) – графический интерфейс (окна, списки, кнопки и т. п.). Выступает подписчиком на событие изменения значений свойств или команд, предоставляемых Моделью Представления. В случае, если в Модели Представления изменилось какое-либо свойство, то она оповещает всех подписчиков об этом, и Представление в свою очередь запрашивает обновленное значение свойства из Модели Представления. В случае, если пользователь воздействует на какой-либо элемент интерфейса, Представление вызывает соответствующую команду, предоставленную Моделью Представления.

Модель Представления (англ. ViewModel) – с одной стороны, абстракция Представления, а с другой – обертка данных из Модели, подлежащие связыванию. То есть она содержит Модель, преобразованную к Представлению, а также команды, которыми может пользоваться Представление, чтобы влиять на Модель.

На данный момент производится выработка технического задания и реализация мобильного приложения в среде разработки Xcode. Также ведется интеграция облачной базы данных Firebase в приложение для имитации серверной части МТКД ввиду закрытого доступа к оригинальным серверам. Таким образом, разработка МТКД под операционную систему iOS расширит круг мобильных устройств, которые могут обеспечить функционирование МТКД, а также предложит новые решения, которые в последующем можно применить в версии под Android.

**Список литературы**

1 **Neuburg, M.** iOS 12 Programming Fundamentals with Swift / M. Neuburg. – O'REILLY, 2019.

2 Apple Developer Documentation [Электронный ресурс]. – Режим доступа : https://developer.apple.com/documentation. – Дата доступа : 17.09.2019.

УДК 621.38

## ВЛИЯНИЕ ФУНКЦИОНАЛЬНОЙ, ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПРЕДНАМЕРЕННОГО ЭЛЕКТРОМАГНИТНОГО ВОЗДЕЙСТВИЯ НА МИКРОЭЛЕКТРОННЫЕ СИСТЕМЫ ЖЕЛЕЗНОДОРОЖНОЙ АВТОМАТИКИ И ТЕЛЕМЕХАНИКИ

*К. А. БОЧКОВ, Н. В. РЯЗАНЦЕВА, Д. В. КОМНАТНЫЙ*

*Белорусский государственный университет транспорта, г. Гомель*

На железнодорожном транспорте системы железнодорожной автоматики и телемеханики (СЖАТ) призваны в первую очередь обеспечить безопасность движения поездов. Повышенные требования по обеспечению безопасности движения поездов налагали и особые методы построения СЖАТ. Ранее СЖАТ строились на основе аппаратной реализации с использованием специальных реле первого класса надежности с несимметричными отказами. При этом не существовало проблем обеспечения информационной безопасности и доказательства функциональной безопасности и угроз преднамеренного электромагнитного воздействия на СЖАТ.

Современные СЖАТ строятся на основе аппаратно-программных комплексов (АПК) с использованием микроэлектронной элементной базы с симметричными отказами. Для СЖАТ принято различать согласно ГОСТ Р 53431–2009 два вида неработоспособного состояния: защитное и опасное. При этом в защитном состоянии все функции по обеспечению безопасности движения поездов соответствуют требованиям нормативно-технической документации (НТД). В опасном состоянии значение хотя бы одного параметра по обеспечению функций безопасности движения поездов не соответствуют требованиям НТД. В опасное состояние система переходит при наличии опасного отказа. Для возможности оценки наличия опасных отказов для каждой из СЖАТ или ее компонентов формулируются критерии опасных отказов в соответствующих НТД.

Следует отметить, что наличие опасного отказа еще не означает нарушения условий безопасности движения поездов, поскольку оно может возникнуть только при условии

$$Q_{дп} = Q_{оо} Q_{пс} Q_{чо},$$

где $Q_{дп}$ – вероятность нарушения условий безопасности движения поездов (авария, крушение, гибель людей, огромные материальные потери и т. д.); $Q_{оо}$ – вероятность опасного отказа; $Q_{пс}$ – веро-

ятность наличия опасной поездной ситуации; $Q_{чо}$ – вероятность ошибки человека-оператора (непарирование опасной ситуации), дежурного по станции, машиниста.

Исходя из этого безопасность АПК микроэлектронных СЖАТ существует как самостоятельное понятие вне связи с человеком-оператором, наличием опасной поездной ситуации и определяется величиной вероятности опасного отказа. Поэтому для АПК микроэлектронных СЖАТ следует проводить анализ (оценивать степень) влияния функциональной, информационной безопасности и преднамеренного электромагнитного воздействия на безопасность движения поездов.

Следует четко определить обьекты защиты с позиций информационной, функциональной безопасности и угроз преднамеренного воздействия микроэлектронных СЖАТ. Все дело в том, что объектом защиты предмета информационной безопасности является информация. Но АПК микроэлектронных СЖАТ строятся таким образом, чтобы одиночные, маскируемые и двойные отказы аппаратных средств, ошибки программного обеспечения и недекларируемые возможности (закладки) не приводили систему в опасное состояние. Циркулирующая в АПК СЖАТ информация не является конфиденциальной с позиции ее раскрытия, хищения и доступности сторонним лицам. АПК СЖАТ построены таким образом, что лицо, принимающее решения (ЛПР) (ДСП, ДНЦ, машинист и др.) использует эту информацию только по прямому назначению организации движения поездов на станциях и участках железной дороги. И даже если по ошибке или злому умыслу ЛПР попытается создать своими действиями на автоматизированном рабочем месте (АРМ) условия, ведущие к нарушению безопасности движению поездов, то АПК СЖАТ при их исправном состоянии не допустят этого исходя из заложенных в них принципов недопущения опасного отказа на уровне SIL4 по ГОСТ Р МЭК 61508–2012.

Вопросы же нарушения целостности информации должны решаться известными методами кодировки, квитирования, криптографии и др. и являются основным предметом обеспечения информационной безопасности в соответствии с требованиями НТД.

Комплексный подход к оценке соответствия программного обеспечения (ПО) СЖАТ, учитывающий требования к функциональной и информационной безопасности, отражен в СТО РЖД 02.049–2014 г., в котором введено понятие киберзащищенности. Это совокупность политик и действий, которые должны быть предприняты для защиты критически важных объектов от деструктивных информационных воздействий (несанкционированный доступ, компьютерная атака, программно-аппаратные закладки, недекларированные возможности, искажение, уничтожение информации), направленные на нарушение штатного функционирования микропроцессорных СЖАТ.

Микропроцессорные СЖАТ имеют следующие дополнительные особенности с позиций обеспечения киберзащищенности по сравнению с 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 нарушение функциональной безопасности, а следовательно, и нарушение безопасности движения поездов;

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

Наиболее реальной и опасной по последствиям является возможная DDOS кибератака (отказ в обслуживании) путем перехвата злоумышленником управления и задания секущего маршрута в горловине станции, являющегося враждебным всем маршрутам приема и отправки и тем самым блокирующим движение поездов (без нарушения условий безопасности движения) и приносящим большой материальный ущерб. Но такая атака может быть парирована специальными техническими и организационными мероприятиями, один из возможных вариантов которых разработан в БелГУТе.

Одним из новых видов угроз микропроцессорным СЖАТ является «электромагнитный терроризм», суть которого заключается в преднамеренном воздействии сверхширокополосным импульсом высокой энергии.

Воздействие широкополосных импульсных помех на микроэлектронные СЖАТ может вызвать:

– сбои в работе объектных контроллеров, как наиболее ответственных узлов, влияющих на возможное нарушение условий безопасности движения поездов;

– отказ объектных контроллеров, вызванный физическим повреждением и разрушением микроэлектронной элементной базы;

– сбои и отказы в работе приемопередающих устройств каналов связи, что приведет к нарушению передачи информации в системе ЖАТ;

– сбои и отказы в работе узлов самопроверки и аппаратуры защиты информации микропроцессорных многоканальных СЖАТ;

– повреждение и разрушение устройств хранения долговременной информации в центральных компьютерах и АРМ СЖАТ.

Отсюда следует, что воздействие СШИП может привести к нарушению как информационной, так и функциональной безопасности одновременно. Это обстоятельство делает указанное воздействие более опасным, чем кибератака или искажение алгоритмов работы СЖАТ.

Следует также учитывать, что СЖАТ являются распределенными системами. Их аппаратура территориально разнесена на большие расстояния: посты ЭЦ, ДЦ, путевые парки железнодорожных станций, переезды, перегоны и др. Поэтому защита таких систем путем оперативно-охранных мероприятий по периметру территории объекта затруднительна.

Сверхширокополосные импульсы, в отличие от традиционных источников помех, обладают распределением спектральной плотности в диапазоне от сотен МГц до единиц ГГц, что позволяет им легко проникать в АПК микроэлектронных устройств через паразитные емкостные каналы. Отличительной особенностью СШИП является также соизмеримость длительности воздействия импульсов с длительностью рабочих и тактовых импульсов АПК СЖАТ, что делает их значительно опаснее, чем уже изученное воздействие электромагнитного импульса высотного ядерного взрыва микросекундной длительности с шириной спектра от единиц кГц до сотен МГц.

Приведенный краткий анализ заставляет сделать вывод об обязательности обеспечения устойчивости микроэлектронных СЖАТ к СШИП в рамках решения проблемы киберзащищенности систем обеспечения безопасности движения поездов.

В докладе приводятся результаты проведенных в НИЛ БЭМС ТС БелГУТа исследований, позволяющих прогнозировать поведение ЛПК микропроцессорных СЖАТ при преднамеренном электромагнитном воздействии и определить направление работ по повышению их устойчивости к этим воздействиям.

Таким образом, в докладе показано, что для микроэлектронных АПК СЖАТ определяющим является выполнение требований по функциональной безопасности на уровне SIL4 по ГОСТ Р МЭК 61508–2012 и выполнение исследований, направленных на повышение устойчивости к преднамеренным электромагнитным воздействиям.

УДК 004.021

## АВТОМАТИЗАЦИЯ МЕТОДОВ ВЕРИФИКАЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ МИКРОПРОЦЕССОРНЫХ СИСТЕМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДВИЖЕНИЯ ПОЕЗДОВ

*К. А. БОЧКОВ, С. Н. ХАРЛАП, Б. В. СИВКО*
*Белорусский государственный университет транспорта, г. Гомель*

Системы железнодорожной автоматики и телемеханики (СЖАТ) необходимы для обеспечения безопасного управления транспортными процессами на железных дорогах, и главным в них является аспект безопасности. При этом СЖАТ регулируют процессы перевозок и предупреждают аварии и крушения. Соответственно, к ним предъявляются повышенные требования функциональной безопасности, что относится в том числе и к современным системам, построенным на микропроцессорной элементной базе.

Микропроцессорные СЖАТ представляют собой аппаратно-программные комплексы (АПК), использующие различные методы и средства передачи и обработки информации. Их неотъемлемой частью является программное обеспечение (ПО), для которого характерна высокая сложность. В связи с этим разработка и верификация микропроцессорных АПК, относящихся к системам обеспечения безопасности движения поездов (СОБД), сопровождается дополнительными мероприятиями, позволяющими получить необходимый уровень безопасности и отказоустойчивости. В то же время для подобных задач отсутствует единый подход решения, что формирует потребность в создании