Оригинальная статья
https://doi.org/10.21683/1729-2646-2024-24-4-48-57

Комплексная безопасность АСУ ТП объектов КИИ железнодорожного транспорта

Integrated Safety of ACS of Railway CII Facilities

Попов П.А.[1], Розенберг Е.Н.[1], Сабанов А.Г.[1*], Шубинский И.Б.[1]
Popov P.A.[1], Rozenberg E.N.[1], Sabanov A.G.[1*], Shubinsky I.B.[1]
[1]АО «НИИАС», Москва, Россия
[1]JSC NIIAS, Moscow, Russian Federation
[*]a.sabanov@vniias.ru


Попов П.А.


Розенберг Е.Н.


Сабанов А.Г.


Шубинский И.Б.

Резюме. *Приводится анализ системы стандартов по безопасности автоматизированных систем управления технологическими процессами железнодорожного транспорта, включающий основные тенденции развития стандартизации на ближайшую перспективу. Рассматриваются теоретические вопросы обеспечения функциональной безопасности, в том числе концепция безопасности зоны управления перевозочным процессом низового уровня и основные принципы обеспечения безопасности.*
Abstract. *The paper analyses the system of standards related to the safety of railway automated process control systems, including the key trends of standardisation for the near future. The authors examine theoretical matters of functional safety, including the safety concept of the bottom-layer transportation management process and the basic safety principles.*

Ключевые слова: *комплексная безопасность, функциональная безопасность, стандарты, автоматизированные системы управления технологическими процессами железнодорожного транспорта, информационная безопасность.*
Keywords: *integrated safety, functional safety, standards, automated railway transportation processes management systems, information security.*

Для цитирования: *Попов П.А., Розенберг Е.Н., Сабанов А.Г., Шубинский И.Б. Комплексная безопасность АСУ ТП объектов КИИ железнодорожного транспорта // Надежность. 2024. №4. С. 48-57. https://doi.org/10.21683/1729-2646-2024-24-4-48-57*
For citation: *Popov P.A., Rozenberg E.N., Sabanov A.G., Shubinsky I.B. Integrated Safety of ACS of Railway CII Facilities. Dependability 2024;4:48-57. https://doi.org/10.21683/1729-2646-2024-24-4-48-57*

Поступила: *11.07.2024* / **После доработки:** *27.08.2024* / **К печати:** *18.11.2024*
Received on: *11.07.2024* / **Revised on:** *27.08.2024* / **For printing:** *18.11.2024*

Введение

АСУ ТП железнодорожного транспорта обеспечивают контроль и автоматизированное управление технологическим оборудованием и средствами (исполнительными устройствами), а также технологическими процессами по управлению, контролю и обеспечению безопасности движения поездов. Такие системы выделяют в отдельный объект защиты – автоматизированные системы управления технологическими процессами железнодорожного транспорта (далее – АСУ ТП ЖТ), поскольку кроме требований транспортной безопасности к ним предъявляются требования Федерального закона № 187 как к объектам критической информационной инфраструктуры (КИИ). По уровню управления перевозочным процессом эти системы целесообразно разделить на следующие три зоны управления:

- низового уровня;
- среднего (промежуточного) уровня;
- верхнего уровня.

За последние 25 лет опубликовано свыше 50 стандартов [1–55], включающих требования к системам управления, системам обеспечения безопасности и их элементам, а также принципы обеспечения их безопасности. Тем не менее, процесс разработки стандартов продолжается в настоящее время, в качестве примера можно привести стандарт [55], в котором разработаны требования функциональной безопасности (ФБ) и информационной безопасности (ИБ) к программному обеспечению (ПО) АСУ ТП ЖТ. Одновременный учет требований ФБ и ИБ в конкретной АСУ ТП ЖТ зачастую вызывает столкновение интересов специалистов обоих направлений обеспечения безопасности, хотя приоритет выполнения требований ФБ не оспаривается. В данной работе соотношению требований ФБ на основе действующих стандартов и требований ИБ как объектов КИИ уделяется повышенное внимание.

В настоящее время в ОАО «РЖД» планируется разработка как минимум, еще одного корпоративного стандарта, включающего в себя одновременно требования ФБ и ИБ к ПО АСУ ТП ЖТ. За прошедшие 10 лет с момента публикации стандарта [28], существенно изменилась нормативно-правовая база в части ИБ, что

обусловило необходимость разработки ряда стандартов, согласованных с современным состоянием технологий и нормативных актов регуляторов. В связи с вышеизложенным, задачи данной работы по рассмотрению и анализу проблем обеспечения безопасности систем различного уровня управления и связанных с обеспечением комплексной безопасности стандартов [1–55] представляются актуальными. Данная статья концентрируется на рассмотрении проблем обеспечения ФБ и ИБ для систем низового уровня управления перевозочным процессом.

1. Краткий анализ системы стандартов по ФБ

В рассмотрении истории развития стандартов по ФБ ограничимся периодом примерно в четверть века, поскольку предметом исследования являются действующие стандарты и их взаимное влияние, а стандарты, как правило, пересматриваются каждые 5 лет в международной организации по стандартизации (ИСО) и не более, чем каждые 10 лет, в других организациях.

Сначала кратко рассмотрим стандарты, созданные к началу XXI века. Как отмечено в работе [56], существенное влияние на развитие действующих специализированных систем стандартов по ФБ для систем управления движением железнодорожного транспорта (ЖТ) оказал выход в середине 1990-х годов серии стандартов [2–5]. Разработанные CENELEC (аббревиатура французского наименования Европейского комитета электротехнической стандартизации, отвечающего за европейские стандарты в области электротехники – Comité Européen de Normalisation Électrotechnique) стандарты [2–5] стали обязательными после выхода директив Европейского Союза № 93/38/EEC и № 2001/95/EC.

Появление указанных стандартов по времени почти совпало с появлением международного стандарта МЭК 61508 в семи частях. Первый выпуск этого стандарта публиковался в 1998 и 2000 годах, второй выпуск был опубликован в 2010 г. [18–23, 46]. Этот стандарт носит общий характер и может применяться для задач ФБ в любых отраслях.

Стандарт базируется на двух фундаментальных принципах:

1) инженерный процесс, называемый жизненным циклом безопасности, определяется на основе передовой практики с целью выявления и устранения проектных ошибок и упущений;

2) вероятностный подход к отказам для учета влияния отказов устройств на безопасность.

В целом некоторые положения стандартов CENELEC можно представить в виде адаптации различных частей стандарта МЭК 61508 для железнодорожного транспорта, хотя между ними имеются и существенные отличия. В частности, в отличие от стандартов [2–5], в МЭК 61508 была недостаточно представлена структура доказательства соответствия требованиям безопасности (Safety Case). Вторым отличием является разный подход к формированию набора показателей управления RAMS (надежности, оперативной готовности, пригодности к техническому обслуживанию и безопасности). Более полный набор требований безопасности в стандартах CENELEC может объясниться тем, что у МЭК концепция RAMS развивалась почти одновременно в двух стандартах, состоящих их нескольких частей – 61508 и 60300, а стандарты CENELEC вобрали в себя значительных опыт обеспечения безопасности железнодорожного транспорта Германии и США.

Из стандартов, опубликованных до 2000 года, можно выделить еще работу [49], разработанную рабочей группой IEEE «Проверка жизненно важных функций в процессорных системах, используемых для управления железнодорожным транспортом» (P1483). Это стандарт для верификации жизненно важных функций в процессорных системах, применяемых для управления на железнодорожном транспорте, в котором рассмотрен ряд задач верификации процессорного оборудования, используемого в критически важных с точки зрения безопасности приложениях в железнодорожных и транзитных системах. В стандарте также рассмотрены процессы проверки уровня безопасности, достигнутого при реализации критически важных для безопасности отказоустойчивых функций.

Опубликование стандартов с 2000 года по время написания данной работы, можно условно разделить на три этапа:

- первый этап – с 2000 г. по 2012 г.;
- второй этап – с 2013 г. по 2017 г.;
- третий этап – с 2018 г. по настоящее время.

Первый этап характеризуется появлением базовых международных стандартов и разработки с учетом их анализа основополагающих российских стандартов, на основе которых в последующем строились стандарты по ФБ. Среди базовых международных стандартов следует выделить уже упомянутые стандарты CENELEC [2–5, 14, 17] и семь частей ГОСТ 61508 по функциональной безопасности систем электрических, электронных, программируемых электронных, связанных с безопасностью [18–23, 46]. Кроме этого, именно на первом этапе в системе национальных стандартов появились базовые стандарты системы ГОСТ Р 54хх, в том числе стандарт по управлению рисками на железнодорожном транспорте [15]. Этот стандарт был разработан не только на основе анализа мирового опыта, но и с использованием российских наработок. В это же время на основе Технических регламентов Таможенного союза (в частности, регламента «О безопасности инфраструктуры железнодорожного транспорта») и РД для железнодорожного транспорта были разработаны стандарты, содержащие требования безопасности и методы контроля для систем железнодорожной автоматики и телемеханики на железнодорожных станциях [24] и переездах [25], а также для систем диспетчерской централизации и диспетчерского контроля движения поездов [26] и поездов на перегонах железнодорожных линий [27].

Несмотря на его небольшую продолжительность, **второй** этап условно можно назвать становлением не только отечественной, но и межгосударственной систем стандартов по функциональной безопасности автоматизированных систем технологических процессов железнодорожного транспорта и перевозочного процесса. Главным событием данного этапа стал выход серии межгосударственных стандартов ГОСТ 33хх по функциональной безопасности. В эту серию вошли стандарты по доказательству безопасности объектов железнодорожного транспорта [30], управлению рисками [32], системам железнодорожной автоматики и телемеханики на сортировочных станциях [37], железнодорожных переездах [38], железнодорожных станциях [39], перегонах [41], системах диспетчерской централизации и диспетчерского контроля [42]. Эта серия стандартов была создана на основе разработанной в 2012 году серии ГОСТ Р 54хх. Знаковыми для развития требований и методов оценки функциональной безопасности автоматизированных систем управления технологическими процессами и техническими средствами железнодорожного транспорта явились стандарты ОАО «РЖД» [28, 34], а также национальные стандарты по требованиям к автоматизированным системам в защищенном исполнении [29], требованиям к ПО на тяговом подвижном составе [35].

Третий этап развития стандартов по функциональной безопасности продолжается в настоящее время. Его можно охарактеризовать как этап совершенствования системы стандартов и развития специализированных решений, хотя имеются и не до конца решенные вопросы, одним из которых является соотношение функциональной и информационной безопасности для автоматизированных систем управления технологическими процессами железнодорожного транспорта. Одной из задач совершенствования является апгрейд стандартов в связи с существенным обновлением нормативно-правовой базы и накоплением практического опыта. Примерами публикации специализированных документов являются: стандарт по обеспечению безопасности передачи информации [44], стандарт по системам интервального регулирования движения поездов на высокоскоростных линиях [47], стандарт по требованиям к интерфейсам и протоколам обмена информацией [50], стандарт по безопасности приложений [52]. В качестве одного из подходов к решению задачи разделения ролей и соотношения предметных областей функциональной и информационной безопасности в обеспечении задач безопасности движения можно рекомендовать стандарт [53].

2. Концепция безопасности зоны управления перевозочным процессом низового уровня

Низовой уровень управления перевозочным процессом реализуется с помощью систем железнодорожной автоматики и телемеханики, систем электроснабжения, связи и передачи данных, а также средств управления подвижным составом. Все эти средства управления представляют собой разветвленные программно-аппаратные устройства, в которых большинство функций контроля и управления безопасностью возлагается на программное обеспечение. Безусловным приоритетом обеспечения безопасности средств управления низового уровня являются задачи реализации функциональной безопасности. Они сочетаются с задачами обеспечения безопасности информации, которые входят составной частью в задачи обеспечения функциональной безопасности.

В основу функциональной безопасности автоматизированных систем управления перевозочным процессом низового уровня должны быть положены следующие физические и технические принципы.

Физические принципы проектирования функционально безопасных систем управления базируются на законе сохранения энергии (первый закон термодинамики) и на законе роста энтропии (второй закон термодинамики). Закон сохранения энергии гласит, что энергия не исчезает, а может лишь менять свою форму. Ущерб людям, материальным ценностям или окружающей среде всегда сопровождается преобразованием энергии из одной формы в другую, т.е. работой. Когда энергия преобразуется из одной формы в другую, ее часть может превратиться в такую форму, которая нанесет вред. Чтобы предотвратить в системе управления преобразование энергии в нежелательную форму, рекомендуются следующие базовые правила:

1) отказ системы должен приводить ее в состояние с минимальным энергетическим потенциалом. Такое состояние должно быть защитным (безопасным);

2) проектировать относящиеся к безопасности функции системы следует таким образом, чтобы система использовала минимально возможное количество энергии.

Второй закон термодинамики гласит, что в замкнутой системе энтропия никогда не убывает. Поэтому желательно удерживать энтропию на низком уровне с тем, чтобы число состояний системы было невелико. Рекомендованы следующие правила обеспечения безопасности:

• система должна быть простой. Только в таком случае будет небольшое число состояний и минимальная энтропия. Также понятно, что простая система проще в проектировании, разработке и управлении;

• инструкции должны быть ясными и понятными;

• не допускать потерю информации.

Технические принципы функциональной безопасности. К ним относятся:

• принцип избыточности;

• принцип отказоустойчивости;

• принцип отказобезопасности.

Принцип избыточности предполагает, что для обеспечения функциональной безопасности систем железнодорожного транспорта предусматривается введение в создаваемые элементы, узлы, устройства и системы

дополнительные средства сверх минимально необходимых. Этот комплексный принцип включает в себя ряд составляющих принципов:

• применение резервирования и избыточных средств;

• безопасный ресурс;

• применение разнообразных способов обеспечения безопасности;

• применение средств, локализующих развитие неблагоприятных событий.

Разнообразие характеризует ситуацию, где несколько подсистем выполняют одну и ту же функцию различным способом. Разнообразие может быть относительно процесса разработки, алгоритма, программного обеспечения, аппаратных средств и т.д. Основное назначение принципа разнообразия состоит в том, чтобы исключить отказы по общим причинам в максимально возможной степени, так как они приводят к опасному отказу системы.

Обеспечение безопасности возможно за счет применения средств, локализующих развитие неблагоприятных процессов. Эти средства защищают систему от выдачи неправильных воздействий, предупреждают о возможном наступлении экстремальных ситуаций и управляют функционированием объекта в критических случаях (парируют развитие отказа и переводят объекты управления в защитное состояние).

Принцип отказоустойчивости предназначен для сохранения возможности системы управления сохранять свою работоспособность после отказа одного или нескольких составных компонентов. Здесь речь идет об аппаратной отказоустойчивости. Программная отказоустойчивость имеет место тогда, когда система имеет возможность сохранять работоспособность после появления при определенном наборе входных данных одной или нескольких скрытых программных ошибок. Этот принцип основывается на избыточности средств системы.

Отказобезопасность – способность системы управления сохранять безопасное состояние и (или) обеспечивать безопасность управления подчиненными объектами в случае отказов самой системы или ее составных частей, а также в случае негативного внешнего информационного воздействия. Этот принцип предназначен для управления опасными отказами. Он определяет способность системы управления совместно с объектом управления оставаться в безопасном состоянии или переходить в безопасное состояние в случае возникновения отказа.

Согласно стандартам [30–34, 37–42] и др., в которых сосредоточены принципы и практические способы обеспечения функциональной безопасности систем управления, принцип отказобезопасности определяется как «выйти из работы безопасным образом или выйти из работы без опасных последствий». Заметим, что в этих стандартах установлено требование обеспечения допустимой (заданной) интенсивности опасных отказов даже при наличии в системе управления совместно с объектом управления одного случайного отказа.

Этот принцип может быть реализован тремя различными способами:

• свойственная системе отказобезопасность;

• реактивная отказобезопасность;

• составная или комбинированная отказобезопасность.

Система разрабатывается согласно *свойственному системе принципу отказобезопасности,* если все возможные режимы ее работы при возникновении отказа не приводят к опасным последствиям. Отсюда следует, что никакой отказобезопасности не может быть без существования защитного состояния (безопасного состояния останова).

Реактивная отказобезопасность характеризуется быстрым обнаружением любой отказавшей функции системы управления и активной реакцией по переводу системы в безопасное состояние.

Системы, спроектированные согласно *принципу комбинированной (составной) отказобезопасности,* должны отвечать следующим условиям:

• в составе системы должно содержаться несколько подсистем (по крайней мере, две), которые обеспечивают ту же самую функцию безопасности;

• эти подсистемы должны быть независимыми друг от друга;

• результаты работы всех этих подсистем должны быть идентичными (комбинированная отказобезопасность со сравнением), или большинство подсистем должно иметь одинаковый результат (решение голосованием большинства);

• обнаружение отказа одной подсистемы и последующая реакция должно быть достаточно быстрыми, чтобы вероятность отказа второй подсистемы была незначительна;

• должно существовать защитное состояние;

• процедуры сравнения или решение, принятое большинством голосов, должны быть выполнены в отказобезопасном режиме и достаточно быстро.

Безопасность информации автоматизированных систем низового уровня управления перевозочным процессом состоит в обеспечении *целостности и доступности информации.* Задача обеспечения *конфиденциальности информации* в этих системах имеет второстепенное значение и сводится к защите от внутренних нарушителей, поскольку эти системы в большинстве своем не решают задачи обмена информацией. Требования в отношении целостности и доступности информации реализуются, главным образом, на основе указанных выше принципов функциональной безопасности. Требования к безопасности информации систем управления на железнодорожном транспорте в основном сосредоточены на требованиях к безопасности ПО. Эти требования задают для обеспечения такого состояния ПО, при котором оно не содержит недекларированных возможностей (НДВ) и уязвимостей, создающих угрозу безопасному и безотказному функционированию системы.

Эти требования на низовом уровне управления перевозочным процессом задаются для обеспечения защи-

щенности системы (включая составное ПО, обрабатываемые и хранимые данные) от следующих воздействий:

• случайного и преднамеренного характера воздействий, главным образом, внутренних нарушителей;

• от последствий ошибок при хранении, вводе, выводе и обработке информации;

• от нарушений целостности и доступности ПО системы управления при собственных сбоях и после перезагрузок, вызванных сбоями и отказами аппаратных средств системы.

При задании требований по безопасности информации на систему управления разработчик приводит в соответствие уровень доверия к безопасности ПО и функциональные требования по информационной безопасности ПО системы.

Функциональные требования по безопасности ПО также задают на основе модели угроз безопасности информации на систему управления с использованием нормативных документов национального регулятора и заказчика системы.

Уровень доверия к безопасности информации системы задают в зависимости от установленной или предполагаемой категории значимости системы управления как объекта критической информационной инфраструктуры и/или в зависимости от установленного или предполагаемого класса защищенности системы управления как автоматизированной системы управления (составной части автоматизированной системы управления) технологическими процессами критически важных объектов, определяемых в соответствии с нормативными правовыми актами в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации [57–59].

Для ПО систем управления перевозочным процессом на железнодорожном транспорте задают один из двух уровней доверия к безопасности информации (по мере возрастания требований: низкий уровень – 6, средний уровень – 5).

При этом:

• ПО, соответствующее 6 уровню доверия, может использоваться в системах третьей категории значимости и (или) третьего класса защищенности;

• ПО, соответствующее 5 уровню доверия, может использоваться в системах второй и третьей категории значимости и (или) второго и третьего класса защищенности;

В случае, если для систем управления на железнодорожном транспорте не была установлена категория значимости и класс защищенности, то рекомендуется задавать уровень доверия к безопасности информации в системе не ниже 6 уровня.

Функции информационной безопасности не должны отрицательно влиять на требуемую производительность (включая время отклика), эффективность, надежность и выполнение функций, важных для обеспечения ФБ [60, п. 5.2, перечисление c)].

Любые меры информационной безопасности, которые рассматриваются для включения в проект системы, следует оценивать в части возможности их влияния на возникновение неисправностей, приводящих к отказам по общей причине, между системами, которые диверсифицированы по соображениям безопасности. При обнаружении таких рисков следует по мере необходимости внедрять альтернативные средства обеспечения надлежащей безопасности информации.

Программно-аппаратные средства обеспечения безопасности информации, включенные в составные системы зоны управления перевозочным процессом низового уровня, не должны снижать эффективности функций безопасности систем управления.

Для категорированных значимых объектов КИИ (а также для объектов без категории) согласно требованиям приказа ФСТЭК России [58] базовые требования к системам АСУ ТП ЖТ независимо от категории (в том числе объектов КИИ без категории) состоят из минимального набора, базового набора и уточненного набора требований.

Минимальный набор состоит из следующих требований:

• защита от несанкционированного доступа;

• обеспечение целостности программ и данных;

• обеспечение доступности информации для легальных пользователей в пределах их полномочий;

• отсутствие недекларированных возможностей;

• отсутствие уязвимостей.

Указанный минимальный набор требований к АСУ ТП ЖТ установлен как из требований стандартов функциональной безопасности, так и из требований действующей нормативно-правовой базы защиты информации объектов КИИ.

Заключение

Рассмотрены проблемы обеспечения безопасности в АСУ ТП ЖТ низового уровня управления. Проведен анализ стандартов по функциональной безопасности, включающий основные тенденции развития стандартизации на ближайшую перспективу. Представлена концепция безопасности зоны управления перевозочным процессом низового уровня, в которой впервые сформулированы основные принципы обеспечения безопасности. Определены требования безопасности информации к АСУ ТП ЖТ.

Данная работа рассматривается в качестве подготовки материала для научно обоснованной разработки стандартов, объединяющих требования функциональной и информационной безопасности к АСУ ТП ЖТ.

Библиографический список

1. IEC 60300:1997 Dependability Management. (Управление обобщенной надежностью) [Электронный ресурс]. URL: https://www.en-standard.eu/bs-iec-60300-3-6-1997-dependability-management-application-guide-software-aspects-of-dependability/ (дата обращения: 14.10.2024).

2. CENELEC EN 50126-1:2017 (MAIN) Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Generic RAMS process (Применения на ж/д транспорте. Общий процесс RAMS) [Электронный ресурс]. URL: https://standards.iteh.ai/catalog/standards/clc/e5456892-eb2c-437e-8c4b-91c08007f0b4/en-50126-1-2017 (дата обращения: 14.10.2024).

3. EN 50128:2011/AC:2014 – Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems (Применения на ж/д транспорте. ПО для СУ и систем обеспечения безопасности на ж/д транспорте) [Электронный ресурс]. URL: https://standards.iteh.ai/catalog/standards/clc/6b4df0cf-4054-4bff-9207-9d1b0d0473ed/en-50128-2011 (дата обращения: 14.10.2024).

4. CENELEC EN 50159:2001 Railway applications – Communication, signalling and processing systems – Safety-related communication in transmission systems (Применения на ж/д транспорте. Передача инф, связанной с безопасностью, в откр./закр. системах связи) [Электронный ресурс]. URL: https://standards.globalspec.com/std/14256321/EN%2050159 (дата обращения: 14.10.2024).

5. CENELEC EN 50129:2003 Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling (Применения на ж/д транспорте. Системы коммуникаций, сигнализации и обработки данных. Электронные системы сигнализации, связанные с безопасностью) [Электронный ресурс]. URL: https://standards.globalspec.com/std/1266373/en-50129 (дата обращения: 14.10.2024).

6. ГОСТ Р 52980-2008. Системы промышленной автоматизации и их интеграция. системы программируемые электронные железнодорожного применения. Требования к программному обеспечению. М.: Стандартинформ, 2009. III, 20 с.

7. СТО РЖД 1.19.007-2009. Системы и устройства железнодорожной автоматики и телемеханики. Требования к программам обеспечения безопасности. Утв. распоряжением ОАО «РЖД» от 4 декабря 2009 г. № 2473/р. II, 9 с.

8. СТО РЖД 1.19.008-2009. Системы и устройства железнодорожной автоматики и телемеханики. Выбор и общие правила задания требований по безопасности. Утв. распоряжением ОАО «РЖД» от 31 июля 2009 г. № 1623/р. III, 36 с.

9. СТО РЖД 1.19.009-2009. Системы и устройства железнодорожной автоматики и телемеханики. Доказательство безопасности. Утв. распоряжением ОАО «РЖД» от 4 декабря 2009 г. № 2471/р. III, 6 с.

10. СТО РЖД 1.02.030-2010. Управление ресурсами на этапах жизненного цикла, рисками и анализом надежности (УРРАН). Политика обеспечения безотказности, готовности, ремонтопригодности и безопасности объектов железнодорожного транспорта. Утв. распоряжением ОАО «РЖД» от 12 декабря 2011 г. № 2666/р. III, 44 с.

11. СТО РЖД 1.02.034-2010. Управление ресурсами на этапах жизненного цикла, рисками и анализом надежности (УРРАН). Общие правила оценки и управления рисками. Утв. распоряжением ОАО «РЖД» от 13 декабря 2010 г. № 2570/р. III, 45 с.

12. СТО РЖД 1.02.035-2010. Управление ресурсами на этапах жизненного цикла, рисками и анализом надежности (УРРАН). Порядок определения допустимого уровня риска. Утв. Распоряжением ОАО «РЖД» от 13.12.2010 г. № 2570/р. III, 18 с.

13. ГОСТ Р ИСО/МЭК 12207-2010. Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств. М.: Стандартинформ, 2011. V, 100 с.

14. EN 50128:2011 (MAIN) Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems (Применение для железнодорожного транспорта. Системы связи, сигнализации и обработки данных. Программное обеспечение для железнодорожных систем управления и безопасности).

15. ГОСТ Р 54505-2011. Безопасность функциональная. Управление рисками на железнодорожном транспорте. М.: Стандартинформ, 2012. III, 35 с.

16. ГОСТ Р 54833-2011. Системы железнодорожной автоматики и телемеханики на сортировочных станциях. Требования безопасности и методы контроля. М.: Стандартинформ, 2012. III, 12 с.

17. EN 50126-5-2012 (MAIN) Railway applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 5: Functional Safety – Software (Железнодорожные приложения. RAMS. Функциональная безопасность. Программное обеспечение).

18. ГОСТ 61508-1-2012. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования. М.: Стандартинформ, 2014. V, 53 с.

19. ГОСТ 61508-2-2012. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам. М.: Стандартинформ, 2014. V, 81 с.

20. ГОСТ 61508-4-2012. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения. М.: Стандартинформ, 2014. V, 30 с.

21. ГОСТ 61508-5-2012. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5 Рекомендации по применению методов определения уровней полноты безопасности. М.: Стандартинформ, 2014. V, 34 с.

22. ГОСТ 61508-6-2012. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководство по применению ГОСТ Р МЭК 61508-2 и ГОСТ Р МЭК 61508-3. М.: Стандартинформ, 2014. VII, 156 с.

23. ГОСТ 61508-7-2012. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Методы и средства. М.: Стандартинформ, 2014. V, 95 с.

24. ГОСТ Р 54897-2012. Системы железнодорожной автоматики и телемеханики на железнодорожных станциях. Требования безопасности и методы контроля. М.: Стандартинформ, 2012. III, 28 с.

25. ГОСТ Р 54898-2012. Системы железнодорожной автоматики и телемеханики на железнодорожных переездах. Требования безопасности и методы контроля. М.: Стандартинформ, 2012. III, 12 с.

26. ГОСТ Р 54899-2012. Системы диспетчерской централизации и диспетчерского контроля движения поездов. Требования безопасности и методы контроля. М.: Стандартинформ, 2012. III, 12 с.

27. ГОСТ Р 54900-2012. Системы железнодорожной автоматики и телемеханики на перегонах железнодорожных линий. Требования безопасности и методы контроля. М.: Стандартинформ, 2012. III, 11 с.

28. СТО РЖД 02.049-2014. Автоматизированные системы управления технологическими процессами и техническими средствами железнодорожного транспорта. Требования функциональной и информационной безопасности программного обеспечения. Порядок оценки соответствия. Утв. распоряжением ОАО «РЖД» от 30 декабря 2014 г. № 3192/р. III, 21 с.

29. ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. М.: Стандартинформ, 2015. III, 15 с.

30. ГОСТ Р 33432-2015. Безопасность функциональная. Политика, программа обеспечения безопасности. Доказательство безопасности объектов железнодорожного транспорта. М.: Стандартинформ, 2016. II, 22 с.

31. ГОСТ 33358-2015. Безопасность функциональная. Системы управления и обеспечения безопасности движения поездов. Термины и определения. М.: Стандартинформ, 2018. III, 16 с.

32. ГОСТ Р 33433-2015 Безопасность функциональная. Управление рисками на железнодорожном транспорте. М.: Стандартинформ, 2016. IV, 35 с.

33. ГОСТ 33435-2015. Устройства управления, контроля и безопасности железнодорожного подвижного состава. Требования безопасности и методы контроля. М.: Стандартинформ, 2016. IV, 46 с.

34. СТО РЖД 02.051-2015. Микропроцессорные устройства железнодорожной автоматики и телемеханики. Программное обеспечение. Требования функциональной безопасности. Утв. распоряжением ОАО «РЖД» от 11 февраля 2016 г. № 241/р. III, 28 с.

35. ГОСТ 34009-2016. Средства и системы управления железнодорожным тяговым подвижным составом. Требования к программному обеспечению. М.: Стандартинформ, 2018. III, 16 с.

36. ГОСТ Р МЭК 62279-2016. Железные дороги. Системы связи, сигнализации и обработки данных. Программное обеспечение систем управления и защиты на железных дорогах. М.: Стандартинформ, 2017. VI, 96 с.

37. ГОСТ 33892-2016. Системы железнодорожной автоматики и телемеханики на сортировочных станциях. Требования безопасности и методы контроля. М.: Стандартинформ, 2019. III, 12 с.

38. ГОСТ 33893-2016. Системы железнодорожной автоматики и телемеханики на железнодорожных переездах. Требования безопасности и методы контроля. М.: Стандартинформ, 2019. IV, 12 с.

39. ГОСТ 33894-2016. Системы железнодорожной автоматики и телемеханики на железнодорожных станциях. Требования безопасности и методы контроля. М.: Стандартинформ, 2019. IV, 27 с.

40. ГОСТ Р 58489-2019/IEC/TS 61508-3-1:2016. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3-1. Требования к программному обеспечению. Повторное использование части программного обеспечения для реализации всей или части функции безопасности. М.: Стандартинформ, 2019. IV, 8 с.

41. ГОСТ 33895-2016. Системы железнодорожной автоматики и телемеханики на перегонах железнодорожных линий. Требования безопасности и методы контроля. М.: Стандартинформ, 2019. IV, 11 с.

42. ГОСТ 33896-2016. Системы диспетчерской централизации и диспетчерского контроля движения поездов. Требования безопасности и методы контроля. М.: Стандартинформ, 2019. III, 12 с.

43. ГОСТ Р МЭК 62443-3-3-2016. Сети промышленной коммуникации. Безопасность сетей и систем. Часть 3-3. Требования к системной безопасности и уровни безопасности. М.: Стандартинформ, 2016. VII, 62 с.

44. ГОСТ Р МЭК 62280-2017. Железные дороги. Системы связи, сигнализации и обработки данных. Требования к обеспечению безопасной передачи информации. М.: Стандартинформ, 2017. IV, 50 с.

45. СТО РЖД 02.052-2017. Требования функциональной и информационной безопасности к системам управления тяговым подвижным составом. Утв. распоряжением ОАО «РЖД» от 10 октября 2017 г. № 2057/р. III, 14 с.

46. ГОСТ 61508-3-2018. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению. М.: Стандартинформ, 2018. V, 108 с.

47. ГОСТ Р 58285-2018. Системы железнодорожной автоматики и телемеханики на высокоскоростных железнодорожных линиях. Системы интервального регулирования движения поездов. Требования безопасности и методы контроля. М.: Стандартинформ, 2018. III, 8 с.

48. ГОСТ Р 58412-2019. Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения. М.: Стандартинформ, 2019. IV, 23 с.

49. IEEE 1483-2000 Standard for the Verification of Vital Functions in Processor-Based Systems Used in Rail Transit Control. March 30, 2000.

50. ГОСТ Р 59263-2020. Системы и устройства железнодорожной автоматики и телемеханики микропроцессорные. Требования к интерфейсам и протоколам обмена информацией. М.: Стандартинформ, 2020. IV, 12 с.

51. ГОСТ Р 59505-2021/IEC TR 63069:2019. Измерение, управление и автоматизация промышленного процесса. Основные принципы обеспечения функциональной безопасности и защиты информации. М.: Стандартинформ, 2021. IV, 28 с.

52. ГОСТ Р ИСО/МЭК 27034-1-2014. Информационная технология. Методы и средства обеспечения безопасности. Безопасность приложений. М.: Стандартинформ, 2015. IX, 64 с.

53. ГОСТ 34673.3-2022. Тяговый подвижной состав железнодорожный. Часть 3. Методы контроля выполнения функций устройствами, обеспечивающими безопасность движения. М.: Российский институт стандартизации, 2022. IV, 16 с.

54. ГОСТ Р 33435-2023. Устройства управления, контроля и безопасности железнодорожного подвижного состава. Требования безопасности и методы контроля. М.: Российский институт стандартизации, 2023. IV, 46 с.

55. ГОСТ Р 70732-2023. Автоматизированные системы управления технологическими процессами и техническими средствами железнодорожного транспорта. Требования к функциональной и информационной безопасности программного обеспечения и методы контроля. М.: Российский институт стандартизации, 2023. IV, 19 с.

56. Брабанд Й., Хирао Ю., Людеке Д.Ф. Взаимосвязь между стандартами CENELEC в области железнодорожной сигнализации и другими стандартами по безопасности [Электронный ресурс]. URL: http://www.ibtrans.ru/upload/iblock/b02/b025373096194a4b9c9a7cebb4a43352.pdf (дата обращения: 14.10.2024).

57. 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 окружающей природной среды. Утв. приказом ФСТЭК России от 14.03.2014 г. № 31.

58. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации. Утв. приказом ФСТЭК России от 25.12.2017 г. № 239.

59. Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий. Утв. приказом ФСТЭК России от 02.06.2020 г. № 76.

60. IEC 62859:2016 Nuclear power plants – Instrumentation and control systems – Requirements for coordinating safety and cybersecurity.

References

1. IEC 60300:1997 Dependability management. (accessed 14.10.2024). Available at: https://www.en-standard.eu/bs-iec-60300-3-6-1997-dependability-management-application-guide-software-aspects-of-dependability/.

2. CENELEC EN 50126-1:2017 Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Generic RAMS process. (accessed 14.10.2024). Available at: https://standards.iteh.ai/catalog/standards/clc/e5456892-eb2c-437e-8c4b-91c08007f0b4/en-50126-1-2017.

3. EN 50128:2011/AC:2014 – Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems. (accessed 14.10.2024). Available at: https://standards.iteh.ai/catalog/standards/clc/6b4df0cf-4054-4bff-9207-9d1b0d0473ed/en-50128-2011.

4. CENELEC EN 50159:2001 Railway applications – Communication, signalling and processing systems – Safety-related communication in transmission systems. (accessed 14.10.2024). Available at: https://standards.globalspec.com/std/14256321/EN%2050159.

5. CENELEC EN 50129:2003 Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling. (accessed 14.10.2024). Available at: https://standards.globalspec.com/std/1266373/en-50129.

6. [GOST R 52980:2008 Functional safety of electrical, electronic, programmable electronic safety-related systems applications for railways. Software requirements]. Moscow: Standartinform; 2009. (in Russ.)

7. [STO RZD 1.19.007-2009. Railway signalling systems and devices. Requirements for safety programs. Approved by the Order of JSC RZD dated December 4, 2009 No. 2473/r. II]. (in Russ.)

8. [STO RZD 1.19.008-2009. Railway signalling systems and devices. Selection and general rules for defining safety requirements. Approved by the Order of JSC RZD dated July 31, 2009 No. 1623/r. III]. (in Russ.)

9. [STO RZD 1.19.009-2009. Railway signalling systems and devices. Safety case. Approved by the Order of JSC RZD dated December 4, 2009 No. 2471/r. III]. (in Russ.)

10. [STO RZD 1.02.030-2010. Managing asset lifecycle, risks, and dependability analysis (URRAN). Policy of reliability, availability, maintainability, and safety of railway assets. Approved by the order of JSC RZD dated December 12, 2011 No. 2666/r. III]. (in Russ.)

11. [STO RZD 1.02.034-2010. Managing asset lifecycle, risks, and dependability analysis (URRAN). General rules of risk assessment and management. Approved by the order of JSC RZD dated December 13, 2010 No. 2570/r. III]. (in Russ.)

12. [STO RZD 1.02.035-2010. Managing asset lifecycle, risks, and dependability analysis (URRAN). General rules of risk assessment and management. Procedure for defining the allowable level of risk. Approved by the order of JSC RZD dated 13.12.2010 No. 2570/r. III]. (in Russ.)

13. GOST R ISO/IEC 12207-2010. Information technology. System and software engineering. Software life cycle processes. Moscow: Standartinform; 2011. (in Russ.)

14. EN 50128:2011 Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems.

15. GOST R 54505-2011. Functional safety. Risk management on railway transport. Moscow: Standartinform; 2012. (in Russ.)

16. GOST R 548332011. Automatics and telemechanics railway systems on rail classification yards. Safety requirements and methods of checking. Moscow: Standartinform; 2012. (in Russ.)

17. EN 50126 5 2012 Railway applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 5: Functional Safety – Software.

18. GOST 27.0022012. Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 1. General requirements. Moscow: Standartinform; 2014. (in Russ.)

19. GOST 61508 2 2012. Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 2. Requirements for systems. Moscow: Standartinform; 2014. (in Russ.)

20. GOST 61508 4 2012. Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 4. Terms and definitions. Moscow: Standartinform; 2014. (in Russ.)

21. GOST 61508 5 2012. Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 5. Guidelines for methods of the determination of safety integrity levels. Moscow: Standartinform; 2014. (in Russ.)

22. GOST 61508 6 2012. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 6. Guidelines on the application of GOST R IEC 61508-2 and GOST R IEC 61508-3. Moscow: Standartinform; 2014. (in Russ.)

23. GOST 61508 7 2012. Functional safety of electrical electronic programmable electronic safety-related systems. Part 7. Techniques and measures. Moscow: Standartinform; 2014. (in Russ.)

24. GOST R 54897-2012. Automatics and telemechanics railway systems on railway stations. Safety requirements and methods of checking. Moscow: Standartinform; 2012. (in Russ.)

25. GOST R 54898-2012. Automatics and telemechanics railway systems on railway stations. Safety requirements and methods of checking. Moscow: Standartinform; 2012. (in Russ.)

26. GOST R 54899-2012. Automatics and telemechanics railway systems on railway stations. Safety requirements and methods of checking. Moscow: Standartinform; 2012. (in Russ.)

27. GOST R 54900-2012. Automatics and telemechanics railway systems on railway stations. Safety requirements and methods of checking. Moscow: Standartinform; 2012. (in Russ.)

28. [STO RZD 02.049-2014. Automated process and equipment management systems in railway transportation. Software functional safety and information security requirements. Conformity confirmation procedure. Approved by the Order of JSC RZD dated December 30, 2014 No. 3192/r. III]. (in Russ.)

29. GOST R 51583-2014. Information protection. Sequence of protected operational system formation. General provisions. Moscow: Standartinform; 2015. (in Russ.)

30. GOST R 33432-2015. Functional safety. Policy and programm of safety provision. Safety proof of the railway objects. Moscow: Standartinform; 2016. (in Russ.)

31. GOST 33358-2015. Functional safety. Control and safety systems for train operation. Terms and definitions. Moscow: Standartinform; 2018. (in Russ.)

32. GOST R 33433-2015. Functional safety. Risk management on railway transport. Moscow: Standartinform; 2016. (in Russ.)

33. GOST 33435-2015. Control, monitoring and safety means of railway rolling stock. Safety requirements and control methods. Moscow: Standartinform; 2016. (in Russ.)

34. [STO RZD 02.051-2015. Computer-based railway signalling devices. Software. Functional safety requirements. Approved by the Order of JSC RZD dated February 11, 2016 No. 241/r. III]. (in Russ.)

35. GOST 34009-2016. Control devices and systems for railway traction rolling stock. Software requirements. Moscow: Standartinform; 2018. (in Russ.)

36. GOST R IEC 62279-2016. Railway applications. Communication, signalling and processing systems. Software for railway control and protection systems. Moscow: Standartinform; 2017. (in Russ.)

37. GOST 33892-2016. Railway automatics and telemechanics systems on rail classification yards. Safety requirements and methods of checking. Moscow: Standartinform; 2019. (in Russ.)

38. GOST R 33893-2016. Railway automatics and telemechanics systems on railway crossings. Safety requirements and methods of checking. Moscow: Standartinform; 2019. (in Russ.)

39. GOST 33894-2016. Railway automatics and telemechanics systems on railway stations. Safety requirements and methods of checking. Moscow: Standartinform; 2019. (in Russ.).

40. GOST R 58489-2019/IEC/TS 61508-3-1:2016. Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 3-1. Software requirements. Reuse of pre-existing software elements to implement all or part of a safety function. Moscow: Standartinform; 2019. (in Russ.)

41. GOST 33895-2016. Railway automatics and telemechanics systems on stages of railroad lines. Safety requirements and methods of checking. Moscow: Standartinform; 2019. (in Russ.).

42. GOST R 33896-2016. Centralized traffic and dispatching control systems of trains movement. Safety requirements and methods of checking. Moscow: Standartinform; 2019. (in Russ.)

43. GOST R IEC 62443-3-3-2016. Industrial communication networks. Network and system security. Part 3-3. System security requirements and security levels. Moscow: Standartinform; 2016. (in Russ.)

44. GOST R IEC 62280-2017. Railway applications. Communication, signalling and processing systems. Safety communication requirements. Moscow: Standartinform; 2017. (in Russ.)

45. [STO RZD 02.052-2017. Functional safety and information security requirements for traction rolling stock control systems. Approved by the Order of JSC RZD dated October 10, 2017 No. 2057/r. III]. (in Russ.)

46. GOST 61508 3 2018. Functional safety of electrical, electronic, programmable electronic safety-related systems. Part 3. Software requirements. Moscow: Standartinform; 2018. (in Russ.)

47. GOST R 58285-2018. Railway automatics and telemechanics systems at high-speed railways. Interval train traffic systems. Safety requirements and methods of checking. Moscow: Standartinform; 2018. (in Russ.)

48. GOST R 584122019. Information protection. Secure software development. Software development life cycle threats. Moscow: Standartinform; 2019. (in Russ.)

49. IEEE 1483-2000 Standard for the Verification of Vital Functions in Processor-Based Systems Used in Rail Transit Control. March 30; 2000.

50. GOST R 59263-2020. Microprocessor systems and devices of railway automatics and telemechanics. Requirements for interfaces and information exchange protocols. Moscow: Standartinform; 2020. (in Russ.)

51. GOST R 59505-2021/IEC TR 63069:2019. Industrial-process measurement, control and automation. Framework for functional safety and security. Moscow: Standartinform; 2021. (in Russ.)

52. GOST R ISO/IEC 27034-1-2014. Information technology. Security techniques. Application security. Part 1. Overview and concepts. Moscow: Standartinform; 2015. (in Russ.)

53. GOST 34673.3-2022. Railway tractive rolling stock. Part 3. Inspection methods for devices ensuring traffic safety. Moscow: Standartinform; 2022. (in Russ.)

54. GOST 33435-2023. Control, monitoring and safety means of railway rolling stock. Safety requirements and control methods. Moscow: Standartinform; 2023. (in Russ.)

55. GOST R 70732-2023. Automated control systems of technological processes and technical facilities for railway transport. Software functional and information safety requirements and control methods. Moscow: Russian Standardization Institute; 2023. (in Russ.)

56. Braband J., Hirao Y., Lüdecke D.F. Interrelation between CENELEC standards in the field of railway signalling and other safety standards. (accessed 14.10.2024). Available at: http://www.ibtrans.ru/upload/iblock/b02/b025373096194a4b9c9a7cebb4a43352.pdf.

57. [Information security requirements for automated process management systems at critical facilities, potentially hazardous facilities, as well as facilities that pose an increased danger to human life and health and the environment. Approved by the order of the FSTEC of Russia dated 03.14.2014 No. 31.] (in Russ.)

58. [Safety requirements for significant facilities of critical information infrastructure of the Russian Federation. Approved by the order of the FSTEC of Russia dated December 25, 2017 No. 239]. (in Russ.)

59. [Information security requirements that define the levels of trust to the information security and information technology protection tools. Approved by the order of the FSTEC of Russia dated 06.02.2020 No. 76]. (in Russ.)

60. IEC 62859:2016. Nuclear power plants – Instrumentation and control systems – Requirements for coordinating safety and cybersecurity.

Сведения об авторах

Попов Павел Александрович – кандидат технических наук, заместитель Генерального директора – директор Санкт-Петербургского филиала АО «НИИАС» Москва Российская Федерация, e-mail: P.Popov@vniias.ru

Розенберг Ефим Наумович – профессор, доктор технических наук, первый заместитель Генерального директора АО «НИИАС», Москва, Российская Федерация, e-mail: info@vniias.ru

Сабанов Алексей Геннадьевич – доцент, доктор технических наук, главный эксперт научно-технического комплекса «Технологии информационного общества» АО «НИИАС» Москва Российская Федерация, e-mail: asabanov@mail.ru

Шубинский Игорь Борисович – профессор, доктор технических наук, эксперт Научного совета при Совете Безопасности РФ, главный эксперт АО «НИИАС», Москва, Российская Федерация, e-mail: igor-shubinsky@yandex.ru

About the authors

Pavel A. Popov, Candidate of Engineering, Deputy Director General, Director of the St. Petersburg Branch, JSC NIIAS, Moscow, Russian Federation, e-mail: P.Popov@vniias.ru

Efim N. Rozenberg, Professor, Doctor of Engineering, First Deputy Director General, JSC NIIAS, Moscow, Russian Federation, e-mail: info@vniias.ru

Alexey G. Sabanov, Associate Professor, Doctor of Engineering, Chief Expert, Integrated Research and Development Unit for Information Society Technologies, JSC NIIAS, Moscow, Russian Federation, e-mail: asabanov@mail.ru

Igor B. Shubinsky, Professor, Doctor of Engineering, Expert, Scientific Council under the Security Council of the Russian Federation, Chief Expert, JSC NIIAS, Moscow, Russian Federation, e-mail: igor-shubinsky@yandex.ru.

Вклад авторов

Попов П.А. – функционирование АСУ ТП железнодорожного транспорта.

Розенберг Е.Н. – постановка задачи.

Сабанов А.Г. – анализ стандартов.

Шубинский И.Б. – теория функциональной безопасности (концепция и основные принципы) АСУ ТП ЖТ.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.