DOI: 10.25728/avtprom.2020.12.01

Передача информации с эталонной диагностикой данных

А.А. Калашников (НИУ "МЭИ")

Представлена концепция эталонной диагностики цифровых и аналоговых линий передачи информации. Описаны принципы и методы ее реализации. Внедрение эталонной диагностики в промышленной измерительной и вычислительной технике позволяет повысить надежность работы линий передачи информации в целом и измерительных каналов в частности за счет повышения достоверности информации и мониторинга целого ряда их технических и метрологических характеристик. Освоение таких технологий способствует развитию отечественной цифровой и измерительной техники и позволяет автоматизировать и развить метрологическое и техническое обслуживание производств.

Ключевые слова: эталонная диагностика, аналоговая и цифровая передача информации, повышение достоверности информации.

Введение

Современное развитие цифровых технологий приводит к повышению уровня цифровизации промышленности, появлению "умных" городов, "умного" здравоохранения и других социальных сфер жизни. В промышленной измерительной технике, метрологии и передаче информации такие изменения привели к новым вызовам времени, в числе которых можно отметить две научно-технические проблемы.

Первая проблема обусловлена многократным ростом числа контрольно-измерительных приборов (КИП) на предприятиях. Так, например, на отраслевом научно-техническом совете ГК «Росатом» в феврале 2020 г. отмечалось, что число КИП на новых энергоблоках АЭС по отношению к проектам 2010 г. увеличилось более чем в 2,5 раза. На современном типовом энергоблоке АЭС с реактором ВВЭР-1200 число измерительных каналов стало достигать свыше 14 тыс. ед.. Трудозатраты на их метрологическое обслуживание по приблизительным оценкам составляют свыше 42 тыс. человеко-часов, то есть для 10 человек требуется 525 рабочих дней для однократного выполнения поверки измерительных каналов. Такие тенденции не отвечают современным потребностям промышленности и требуют пересмотра самих подходов и методов метрологического обслуживания.

Вторая проблема обусловлена тем, что во многих сферах промышленности происходит постепенный переход от аналоговой передачи информации к цифровой, затем от проводной передачи к беспроводной. Наглядный тому пример — это цифровизация нефтехимических предприятий холдинга «СИБУР», в рамках которой происходит установка датчиков Internet вещей в объеме около 5000 ед. на каждом основном предприятии. Внедрение таких технологий, с одной стороны, повышает уровень автоматизации, а с другой — приводит к повышенным рискам кибер-угроз. Отсюда возникает потребность

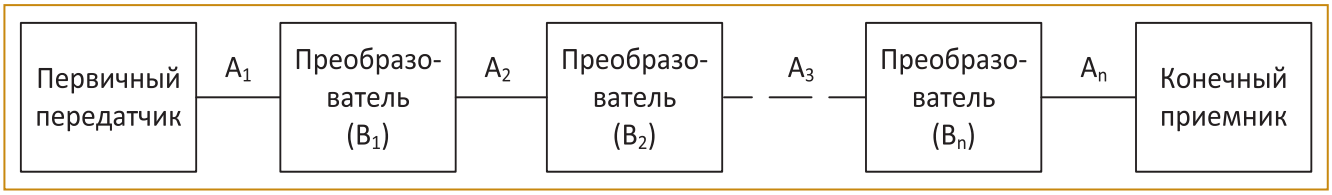

Рис. 1. Упрощенная структурная схема линии передачи информации с проводными связями

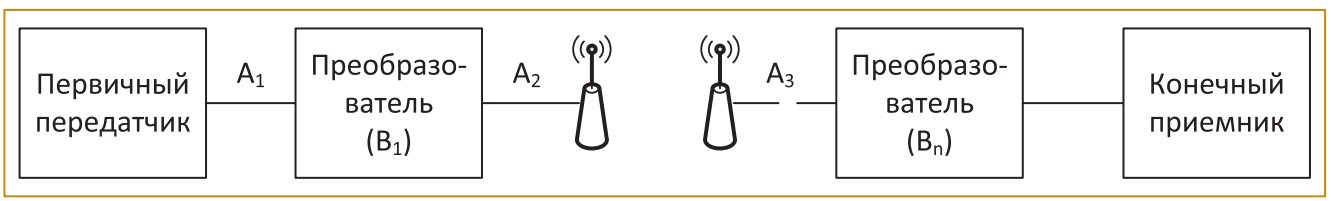

Рис. 2. Упрощенная структурная схема линии передачи информации с беспроводными связями

в освоении технологий передачи информации повышенной надежности.

От качества решения таких проблем на сегодняшний день зависит уровень готовности потенциально опасных отраслей РФ к растущим темпам цифровизации измерительной техники и систем автоматического управления технологическим процессом. Для совершенствования метрологического обслуживания и повышения кибер-безопасности предприятий предлагается новый подход в организации промышленных линий передачи информации в целом и измерительных каналов в частности на базе эталонной диагностики данных.

Задача диагностики данных

В контексте рассмотренных проблем задачей диагностики данных является повышение надежности линии передачи информации за счет контроля и обеспечения достоверности данных в течение всего срока ее эксплуатации. Рассмотрим данную задачу на примере упрощенной структурной схемы типовой линии передачи информации.

В общем случае в состав линии передачи информации входят передатчики, преобразователи B_1, B_2 ...B_n, приемники, проводные и/или беспроводные связи A_1, A_2 ...A_n (рис. 1, рис. 2). Вероятные искажения и изменения информации могут происходить в каждом из структурных элементов линии. Например, в процессе передачи данных по линиям связи A_1, A_2 ...A_n по причине наличия ошибок кодирования и декодирования информации, деградации технических характеристик линий связи, а также по причине наличия наведенных помех и т. п. Другие причины искажения информации, не связанные с качеством ее передачи, характеризуются умышленными или неумышленными ошибками в самих преобразованиях информации B_1, B_2 ...B_n, обусловленные, например, ошибками вычислений, неточностями поправок и ложной коррекцией данных. Учитывая основную номенклатуру возможных ошибок и искажений информации, проанализируем достаточность современных технологий их обнаружения.

Технологии по обнаружению и исправлению ошибок, возникающих при передаче информации по линиями связи A_1, A_2 ...A_n, на сегодняшний день достаточно сильно развиты, особенно в отношении цифровой передачи данных. На практике широко используются протоколы передачи цифровой информации с контрольными битами, БЧХ-коды, турбо-коды и многие др., способные обнаружить и исправить ошибки в пакетах передаваемых данных [1]. Такие протоколы постоянно совершенствуются, ведутся исследования по оценке и улучшению эффективности их работы в задачах помехоустойчивого кодирования и передачи информации [2, 3]. Однако, исходя из своего назначения, они не диагностируют ошибки и искажения информации в преобразователях B_1, B_2 ...B_n. Если преобразователь ввиду ошибочных вычислений отправит ложные данные, то это не будет диагностировано, так как применяемые цифровые протоколы, по сути, контролируют только качество передачи информации, а не ее достоверность. Из опыта пусконаладочных работ измерительных каналов можно отметить, что именно ошибки в преобразованиях информации чаще всего являются скрытыми, и обнаружить их на практике в ряде случаев крайне затруднительно [4]. Именно такие скрытые дефекты приводят к повышенным производственным рискам.

Таким образом, для полноценного решения поставленной задачи диагностики рассмотренных протоколов передачи данных не достаточно. Для обеспечения качественно нового уровня надежности передачи информации необходимы дополнительные технологии по контролю достоверности самих передаваемых данных и диагностике всех выполняемых преобразований, начиная от формирования информации до ее обработки и отображения на приемных устройствах.

Полноценно решить поставленную задачу предлагается на основе эталонной on-line диагностики данных, позволяющей развить технологии передачи информации в целях повышения безопасности предприятий.

Концепция эталонной диагностики цифровой передачи данных

С целью оценки достоверности информации, выявления ошибок преобразований, контроля быстродействия и ряда других метрологических и технических характеристик всей линии передачи информации в целом и каждого технического средства, входящего в ее структуру, предлагается использовать эталонную диагностику данных. Такая диагностика предполагает введение заранее известных или рассчитываемых по известному алгоритму эталонных данных на первичном передатчике информации. Последующая передача таких данных позволяет выполнить диагностику работоспособности всей линии в целом и каждого из входящих в нее компонентов за счет сравнения полученной информации с эталонными данными или с их преобразованиями.

В случае цифровой передачи данных эталонную диагностику можно осуществлять в режиме on-line или в определенные временные срезы без прерывания передачи основного потока рабочих данных, которые используются в управлении технологическим процессом. Такую диагностику можно осуществить, передавая эталонные и рабочие данные отдельными пакетами или объединяя и комбинируя их в общих пакетах данных. При этом для повышенной устойчивости к кибер-угрозам запись и хранение эталонных данных на самом первичном передатчике информации рекомендуется выполнять на базе жесткой логики.

Эталонная диагностика цифровых линий передачи информации в своей перспективе имеет широкие возможности и обеспечивает мониторинг ее метрологических и технических характеристик. Например, передавая метку времени отправки эталонных

данных можно контролировать временные характеристики передачи информации, быстродействие работы линии и производительность работы входящих в нее компонентов, так как время обработки эталонных данных можно определить заранее. Если производительность линии обычно оценивается по объему отправленных или полученных данных в единицу времени, то здесь несколько другой подход — определяется фактическое время передачи и обработки данных, что обеспечивает дополнительные возможности диагностики и выявления причин задержек в передаче информации. В целом эталонная диагностика позволяет выявлять погрешности и ошибки в передаче данных и их преобразованиях, в том числе обеспечивается возможность диагностики ошибок в самих протоколах передачи данных. Архивирование результатов эталонной диагностики обеспечивает возможность оценки эксплуатационного ресурса линии передачи информации и контроля деградации ее метрологических и технических характеристик.

По результатам диагностики возможна перенастройка технических средств и автоматическая коррекция данных с целью минимизации погрешностей и исключения ошибок преобразования информации, что повышает надежность работы цифровой линии передачи информации и увеличивает ее эксплуатационный ресурс.

Освоение и внедрение такой эталонной диагностики в измерительной и вычислительной технике стратегических отраслей РФ требует разработки новых стандартов в организации цифровой передачи данных, подобных стандартам МЭК на зарубежные цифровые интерфейсы связи[1]. Принципиальные отличия от известных стандартов МЭК будут обусловлены тем, что необходимо предусмотреть не только новый протокол цифровой передачи данных или обозначить способы реализации диагностики на базе существующих зарубежных протоколов и интерфейсах связи, но и главное – сформировать правила и рекомендации к проектированию, наладке и эксплуатации таких линий передачи информации и измерительных каналов, регламентировать требования к изготовлению соответствующей измерительной и вычислительной техники.

Разработка такого стандарта и необходимых технологий предполагает выполнение целого комплекса НИОКР. В частности, необходимо определить алгоритмы поиска, признаки и однозначные идентификаторы диагностируемых ошибок в работе линии передачи информации. Например, ошибку в преобразованиях можно диагностировать по пороговому превышению отклонений полученной информации от эталонных данных. Для этого необходимо разработать однозначный показывающий индикатор, который позволит распознавать и различать потоки с эталонными и рабочими данными и запускать алгоритмы диагностики. Другой более трудный путь отличать потоки эталонных данных от рабочих основан на четкой синхронизации времени передачи информации, он может применяться в качестве крайней меры в тех случаях, когда отсутствуют любые другие технические возможности по идентификации данных. Одновременно с этим необходимо разработать алгоритмы поиска и идентификации конкретного технического устройства, на котором происходит искажение или задержка передачи информации.

Второй этап такого комплекса исследовательских и конструкторских работ рекомендуется направить на техническую реализацию разработанных алгоритмов диагностики. Это предполагает НИОКР по разработке новой или совершенствованию существующей измерительной и вычислительной техники, которая обеспечит возможность выполнения эталонной диагностики цифровых линий передачи информации в промышленности. При этом до промышленного внедрения рекомендуется выполнить стендовые, приемочные и аттестационные испытания разработанных технологий.

В довершение ко всему отметим, что полноценное решение проблемы повышения кибербезопасности стратегических отраслей РФ по определению базируется на разработке отечественных технологий. Выполнение перечисленного комплекса НИОКР и разработка соответствующего стандарта решает эту проблему в части диагностики цифровой передачи информации. В случае разработки протокола передачи данных и эталонной диагностики обеспечивается развитие цифровой техники с достижением синергии этих разработок. Эталонная диагностика в части цифровой передачи данных обладает новизной по отношению к зарубежным и отечественным технологиям, что можно учесть при разработке протокола передачи данных, специализированного для отечественной промышленности.

Другие перспективы эталонной диагностики раскрываются в области аналоговой передачи данных.

Концепция эталонной диагностики аналоговой передачи данных

В случае аналоговой передачи данных никакие турбо-коды, БЧХ-коды и код Рида-Соломона не применить в связи с их специализацией для цифровой техники. Вновь предлагаемая эталонная диагностика в аналоговой технике не просто применима, но и позволяет пересмотреть подходы в организации метрологического и технического обслуживания производств[2]. Поэтому в отличие от известных технологий

[1] Речь идет о стандартах: МЭК-61850. Сети и системы связи на подстанциях; МЭК-61158. Сети связи промышленные. Спецификации на полевые шины; МЭК-870. Устройства и системы телемеханики.

[2] Заявка на изобретение № 2020119014. Способ определения метрологических характеристик измерительного канала (варианты) / А.А. Калашников.

эталонная диагностика может применяться на аналоговых, цифровых и линиях передачи информации сложной структуры с аналоговой и цифровой передачей данных, причем как проводной, так и беспроводной. Итак, рассмотрим эталонную диагностику данных применительно к аналоговой передаче.

В случае аналоговой передачи информации, например, с использованием унифицированных токовых сигналов 4...20 мА, эталонная диагностика принципиально имеет два варианта реализации с прерыванием и без прерывания передачи рабочих данных. В осуществление диагностики по первому варианту первичный передатчик кратковременно прерывает передачу рабочих данных (используемых в управлении технологическим процессом) и передает заранее установленные на нем эталонные данные. Длительность такого прерывания для выполнения диагностики оценивается в несколько секунд. Поэтому при наличии на предприятии резервной линии передачи информации (измерительного канала) такую диагностику можно осуществлять в условиях непрерывного технологического процесса. Это позволяет существенно улучшить метрологическое обслуживание предприятий, повысить точность результатов калибровки и поверки измерительных каналов (ИК) и оптимизировать трудозатраты, что на сегодняшний день особенно актуально для атомной отрасли.

Дело в том, что современная нормативная база по метрологии главным образом базируется на подходах 70-х гг. XX века, разработка и применение которых были актуальны для того уровня развития измерительной техники и систем автоматического управления предприятий. Так, на сегодняшний день наиболее распространенным в промышленности остается покомпонентный метод поверки ИК (ГОСТ Р 8.596–2002 ГСИ. Метрологическое обеспечение измерительных систем. Основные положения). Он предполагает подключение токовых и/или других калибраторов к каждому измерительному компоненту в составе ИК, что требует высоких трудозатрат на метрологическое обслуживание.

Для определения новых подходов метрологического обслуживания проанализируем работу современных ИК. На сегодняшний день преобладающее большинство промышленных датчиков в своем составе имеют контроллеры, и работа современного ИК по существу выглядит следующим образом. Датчик преобразует измеряемый параметр, например, давление, в цифровую информацию, затем осуществляется цифро-аналоговое преобразование, и во вторичную часть ИК передается аналоговый сигнал. Все последующие его преобразования и изменения в тракте ИК, по сути, сводятся к измерению той самой величины, которая изначально была получена на контроллере датчика в цифровом виде. Исходя из этого, чтобы поверить ИК в границах от выходного преобразования датчика до конечного показывающего устройства достаточно задать заранее известную эталонную информацию в самом контроллере датчика. При этом в отличие от рабочих эталонов, вторичных и даже первичных эталонов такой «цифровой эталон» абсолютно известен. Это позволяет повысить точность результатов поверки ИК по отношению к применяемым калибраторам и всем другим поверочным средствам, которые априори имеют свою погрешность. При этом стоимость и доступность такого «цифрового эталона» несоизмерима с получением и обслуживанием первичных, вторичных и рабочих эталонов.

Таким образом, предлагаемый метод эталонной диагностики позволяет в автоматическом режиме выполнять поверку ИК в целом и каждого из входящих в него измерительных компонентов за исключением первично-измерительного преобразователя. При этом для ее реализации не требуется подключать поверочное оборудование и осуществлять монтаж/демонтаж датчиков и кабельных линий, что повышает эксплуатационный ресурс ИК.

Детально особенности и возможности вновь предлагаемого принципа и метода поверки ИК на базе эталонной диагностики рассмотрены в описании изобретения № 2020119014. В действительности такой способ поверки можно было внедрять с момента распространения процессорной измерительной техники в промышленности.

Резюмируя вышесказанное, еще раз отметим, что для выполнения такой поверки необходимо прерывание передачи рабочих данных, но оно несоизмеримо меньше по отношению к поверкам с подключением токовых калибраторов. Поэтому при наличии резервированных ИК такую поверку можно выполнять в условиях непрерывного технологического процесса.

В тех условиях, когда прерывание процесса измерений и передачи информации не допустимо, можно осуществлять диагностику в режиме on-line или в определенные моменты времени, дублируя передачу рабочих данных по дополнительной цифровой линии связи, используемой в целях диагностики. Такая диагностическая линия трассируется от первичного передатчика до конечного приемного устройства, что исключает промежуточные преобразования информации (рис. 3). Если передача данных по цифровой диагностической линии осуществляется без каких-либо пренебрежений и сокращений, то такие передаваемые данные допустимо считать эталонными по отношению к аналоговой передаче данных, используемой в самом ИК. Последующий анализ рабочих и эталонных данных на приемном устройстве обеспечивает выполнение диагностики и калибровки всего ИК в целом. Такое решение менее устойчиво к кибер-угрозам и является более дорогостоящим по отношению к предыдущему варианту реализации эталонной диагностики, но и возможности его значительно шире. Так как диагностика выполняется непрерывно, можно контролировать быстродействие работы ИК, выявлять непроходимость импульс-

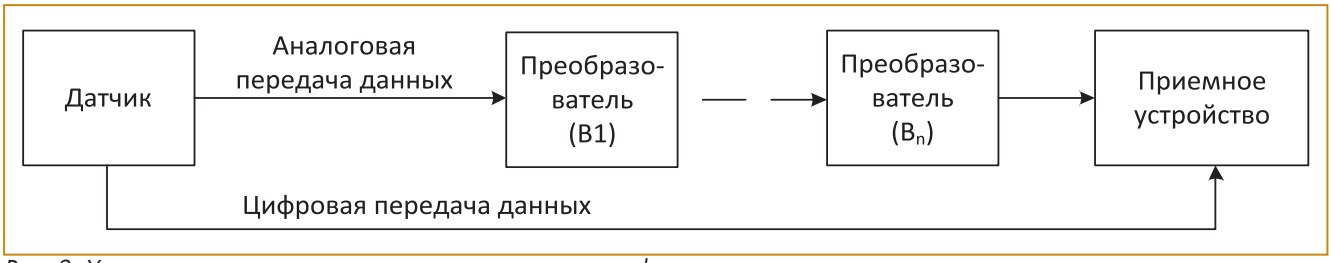

Рис. 3. Упрощенная структурная схема линии передачи информации с проводными связями

ных линий (трубных проводок) датчиков давления на основе частотного анализа работы ИК, определять оптимальное значение настроенного на ИК демпфирования сигнала и дистанционно выполнять настройку датчиков, не прерывая процесс измерений. Такой способ диагностики с возможностью удаленной настройки и технического обслуживания датчиков имеет особую актуальность в тех условиях, когда необходимо минимизировать непосредственный контакт эксплуатационного персонала с оборудованием с целью уменьшения воздействия вредных факторов.

Такой способ диагностики отчасти уже реализован в промышленности, так как многие современные датчики поддерживают одновременную передачу данных по аналоговому и цифровому интерфейсам связи. Более того, зарубежные диагностические комплексы FieldMate Yokogawa (http://www.yokogawa.ru) и Plantweb™ Emerson (https://www.emerson.ru) позволяют выполнять подобную калибровку ИК с тем отличием, что сам процесс сравнения эталонных данных с рабочими не реализован в потенциально возможном объеме. Недостаток таких комплексов заключается в том, что их работа в полной функциональности своих возможностей, как правило, обеспечивается при подключении к датчикам одного и того же завода-изготовителя, что повышает стоимость их применения на производствах. Сведений об аналогичных отечественных диагностических комплексах не обнаружено.

Для повышения кибербезопасности и проверки работы таких диагностических комплексов можно применять ранее рассмотренную эталонную диагностику цифровой линии передачи информации. В этом случае один метод эталонной диагностики будет дополнять другой.

Рассмотренные до этого методы эталонной диагностики можно назвать базовыми, так как они не требуют установки дополнительного диагностического оборудования и могут применяться на любых аналоговых и цифровых линиях передачи информации, в том числе на линиях сложной структуры на примере рис. 3. Это позволяет по необходимости применять и сочетать разные методы эталонной диагностики одновременно на одной линии передачи информации. На практике можно выбрать наиболее подходящий метод эталонной диагностики или их сочетания для оптимального мониторинга метрологических и технических характеристик линии передачи информации с учетом конкретных условий производственной задачи.

В целом все рассмотренные методы позволяют пересмотреть подходы в диагностике линий передачи информации и организации их метрологического и технического обслуживания.

С целью развития промышленного метрологического обслуживания на базе предлагаемых методов эталонной диагностики необходима разработка соответствующего государственного стандарта. Предпосылки для его разработки обусловлены международным «переводом» метрологии на цифровые эталоны с целью освоения технологий, обеспечивающих новый уровень точности измерений [5]. Поэтому разработка такого государственного стандарта способствует следующему шагу прикладного развития метрологии на международном уровне.

Выводы

Рассмотренные в статье методы эталонной диагностики цифровых и аналоговых линий передач информации способствуют становлению и освоению новых отечественных технологий в части измерительной и вычислительной техники стратегических отраслей РФ.

Если применяемые в цифровой технике турбо-коды, БЧХ-коды и код Рида-Соломона и многие другие диагностируют по существу только ошибки кодирования/декодирования и качество передачи информации, то предлагаемая эталонная диагностика позволяет осуществлять мониторинг всех происходящих преобразований информации и качества ее передачи, в том числе позволяет контролировать работу протоколов передачи данных. Самое главное, эталонная диагностика позволяет выполнять оценку достоверности передаваемой информации, что способствует качественному повышению уровня безопасной эксплуатации производств.

В отношении аналоговой передачи информации эталонная диагностика позволяет пересмотреть подходы в организации метрологического обслуживания производств, автоматизировать и существенно улучшить процедуры поверки ИК, обеспечивая современное развитие метрологии на международном уровне.

Разработка и освоение таких технологий в передаче информации требует целого комплекса НИОКР

в сотрудничестве с предприятиями и институтами различных отраслей промышленности РФ.

Список литературы

1. *Одинец А.И.* Цифровые устройства: учебное пособие. Минобрнауки РФ, ОмГТУ. – Омск: Изд-во ОмГТУ, 2016. – 90 с.
2. *Дружинин В.И., Кузьмин О.В.* Коды Рида – Соломона в системах обнаружения и исправления ошибок при передаче данных // Современные технологии. Системный анализ. Моделирование. – 2015. – № 1. – С. 116 - 124.
3. *Сидоркина Ю.А., Шахтарин Б.И., Балахонов К.А.* Анализ эффективности современных помехоустойчивых кодов // Вестник МГТУ им. Н.Э. Баумана. Серия «Приборостроение». – 2014. – № 6. – С. 108 - 116.
4. *Калашников А.А.* Справочник по настройке промышленных гидростатических уровнемеров. – М.: Инфра-Инженерия, 2017. – 194 с.
5. *Бронников К.А., Иващук В.Д. и др.* Эволюция системы единиц измерений. К будущей ревизии международной системы единиц (СИ) // Законодательная и прикладная метрология. – 2018. – № 1. – С. 11 - 16.

Калашников Александр Александрович *– канд. техн. наук, доцент Национального исследовательского университета «Московский энергетический институт», главный эксперт АО «Русатом автоматизированные системы». E-mail: aakalashnikov@list.ru*

DOI: 10.25728/avtprom.2020.12.02

Исследование оценок защищенности промышленных систем

И.И. Лившиц (Университет ИТМО)

В настоящее время при организации защиты промышленных систем различного назначения наблюдаются две крайности – внедрение несовместимых средств защиты информации, не затрагивая базовую ИТ-инфраструктуру, или реализация различных режимов тотальной изоляции (например, архитектуры Zero Trust). Как следует из ежегодных аналитических отчетов мировых экспертов (IBM, MS, Group-IB, Positive Technology и др.), наблюдается постоянный рост сообщений о закрытии очередных критических уязвимостей, но проблема обеспечения безопасности промышленных систем все еще не решена. Известно, что данная проблема признана многими экспертами актуальной и важной.

Существенным негативным фактом является сохранение практики текущего раздельного оценивания двух сущностей – ИТ и ИБ, что не в полной мере обеспечивает оптимальное решение поставленной выше проблемы. В представленной работе дается краткий обзор существующих подходов оценки защищенности промышленных систем. Сформулированные рекомендации могут быть применены для совершенствования существующих и создания перспективных решений для обеспечения безопасности промышленных систем, в том числе и при обеспечении национального цифрового суверенитета.

Ключевые слова: информационная безопасность, промышленная система, менеджмент рисков, меры защиты, оценка соответствия.

Введение

Обеспечение безопасности в широком толковании (*Safety*) для промышленных систем различного назначения (*Industrial Control System, ICS*) имеет давние традиции, сопоставимые по времени зарождения с первыми проектами в области систем управления вооружением и атомных реакторов. Отметим, что ранее в работах зарубежных и отечественных центров экспертиз в данной области не существовало раздельного определения сущностей информационных технологий (ИТ) и информационной безопасности (ИБ), соответственно системы проектировались, создавались, проходили испытания, эксплуатировались как единое целое [1, 2]. Начиная с XX века основным требованием было обеспечение реализации заложенной функциональности, устойчивая работоспособность программных (программно-аппаратных) комплексов [3]. Новации в этой области в определенной мере вызваны принятием ФЗ «О безопасности критической информационной инфраструктуры РФ» от 26.07.2017 N 187-ФЗ, в котором явно указано отдельное определение систем ИБ. А в ряде подзаконных актов (постановление Правительства № 127, приказы ФСТЭК № 235, № 239 и пр.) определены фиксированные списки угроз и мер защиты для обеспечения защищенности объектов критической информационной инфраструктуры (КИИ).

В СТО Газпром серии 4.2 (Система обеспечения ИБ) представлены требования к функционированию ИТ-компонентов, но требования функциональной безопасности (ФБ), равно как и порядок проектирования, испытаний и управления рисками не опреде-