Проведение работ по автоматизации производства: пути развития АСУТП, необходимые для создания цифрового предприятия

Э.Л. Ицкович (ИПУ РАН)

Показано, что при модернизации существующих и проектировании новых АСУТП на предприятиях технологических отраслей необходимо предусматривать определенное расширение автоматически реализуемых функций контроля и управления для соответствия АСУТП требованиям построения и функционирования цифрового предприятия.

Ключевые слова: необходимое развитие АСУТП, АСУТП в рамках цифрового предприятия, последовательность модернизации АСУ отдельных технологических агрегатов.

Введение

В настоящее время, когда наблюдается информационный бум заявлений, реклам, статей, конференций, книг об очередной промышленной революции «Индустрия 4.0», о наступлении неоиндустриального развития промышленности, о распространении промышленного Интернета вещей, о цифровизации производства, важно правильно оценить рациональные линии развития АСУТП, которые бы вписывались в рамки указанных коренных перестроек работы предприятий. Для этого необходимо оценить разницу между текущим состоянием подавляющего большинства АСУТП на предприятиях различных отраслей промышленности с тем состоянием, которое необходимо достичь, чтобы соответствовать прогнозируемой перестройке работы предприятий. При этом следует иметь в виду, что никакие «революционные» сдвиги в автоматизации технологических агрегатов невозможны и не нужны, а эволюция повсеместно существующих АСУТП в определенных направлениях необходима и целесообразна. Этот эволюционный процесс должен проводиться в рамках общего продвижения к построению цифрового предприятия и являться его частью.

Ниже рассматриваются основные пути необходимого развития АСУТП, соответствующие поставленной задаче.

Расширение средств и функций автоматического контроля и учета работы технологического агрегата

На сегодня автоматический контроль и учет работы технологических агрегатов на предприятиях практически достаточно ограничен. Обычно автоматически непрерывно измеряются только режимные величины технологического процесса в агрегате, то есть определяются физические показатели его работы: температуры, давления, уровни, расходы материальных потоков. Кроме того, периодически оценивается качественный состав потребляемых сырьевых компонентов и выпускаемых агрегатом продуктов (полуфабрикатов) дискретными во времени лабораторными анализами. Такой состав автоматического контроля и учета далеко не охватывает всех исходных данных, необходимых для полноценного автоматического текущего и прогнозного анализа работы технологических агрегатов, что требуется при формировании цифрового предприятия.

Ниже дано краткое перечисление тех классов контрольных и учетных исходных данных о текущей работе агрегатов, автоматическое получение которых полностью или в большей части отсутствует на предприятиях, но которые необходимы для полной и качественной автоматизации работы агрегатов в рамках цифрового предприятия.

1.Текущий контроль и учет материальных потерь в агрегате и в окружающих его линиях материальных потоков.

2.Текущий контроль и учет различных видов энергоресурсов, потребляемых агрегатом, и учет удельного расхода каждого энергоресурса на выпускаемую агрегатом продукцию/полуфабрикат.

3.Текущий контроль и учет энергетических потерь в агрегате и в окружающих его линиях энергоподачи.

4.Мониторинг текущего состояния каждой единицы оборудования, от нормальной работы которой зависит заданное функционирование агрегата, и прогноз развития выявляемых дефектов оборудования.

5.Текущий контроль работы датчиков: смещение нуля, увеличение погрешности сверх паспортных данных, выход из строя.

6.Текущий контроль работы регулирующих органов (клапанов): их текущее положение, залипание, гистерезис, замедление хода, недостижение конечных положений, учет процента времени нахождения в конечных положениях, учет диапазона изменения положения регулирующих органов за заданный интервал времени.

7.Текущий контроль работы исполнительных механизмов: точность и реактивность выполнения ими управляющих команд.

8.Текущий контроль работы сетей АСУТП: наличие искажения передаваемой ими информации, обрывы линий связи, неисправности технических средств сетей.

9.Текущий контроль работы контуров управления: автоматический или ручной режим текущего управления (в последнем случае, причина управления в ручном режиме), качество работы автоматически управляемых контуров регулирования: точность поддержания заданного значения регулируемой величины, время переходного процесса после изменения задания регулятору контура управления, учет процента времени работы контура на ручном режиме.

10.Текущий экологический контроль окружающей агрегат среды и среды, которую может загрязнить функционирование агрегата.

В целом следует отметить, что в общем информационном пространстве АСУТП каждого агрегата должны находиться контрольные и учетные данные режимных величин, качественных показателей, энергопотребления, материальных и энергетических потерь, экологии окружающей среды, состояния основного оборудования, качества работы всех технических и программных средств АСУТП.

Углубление и конкретизация автоматического анализа функционирования технологического агрегата

Необходимо перестроить (или скорее достроить) имеющийся автоматический контроль и учет работы агрегата так называемым «глубоким» (продвинутым) анализом получаемых текущих исходных данных, целями которого являются:

— автоматическое, своевременное выявление любых имеющихся и прогнозируемых ситуаций типа отклонений от нормального, заданного режима функционирования агрегата, требующих определенных управляющих воздействий;

— оценки степени критичности выявленных ситуаций для дальнейшей нормальной работы агрегата;

— выявление возможных или наиболее вероятных, или определенных причин возникновения этих ситуаций;

— автоматическая реализация управляющих воздействий, компенсирующих выявленные ситуации, либо выдача оперативному персоналу агрегата подробного анализа выявленных ситуаций и рекомендаций по их компенсации.

Глубина и точность текущего анализа получаемых исходных данных определяется использованием в нем перечисленных ниже классов алгоритмов:

— верификацией всех получаемых исходных данных, то есть проверкой их точности, правильности и полноты;

— структурированием исходных данных, то есть их привязкой и сопоставлением с заданными нормами, показателями, характеристиками контролируемого технологического агрегата;

— статистическим (корреляционным, регрессионным) анализом получаемых исходных данных, позволяющим обнаруживать возникновение определенных ситуаций и их взаимосвязи с возможными причинами возникновения;

— кластерным анализом (автоматической классификацией) ситуаций, упорядочивающим все принципиально возможные ситуации сопоставлением их признаков и характеристик и подразделяющим ситуации на отдельные классы однородных, имеющих близкие причины возникновения и однотипные целесообразные реакции на них, что позволяет отнести текущую, наблюдаемую ситуацию к определенному классу и указать ее рекомендуемую компенсацию;

— дискриминантным анализом ситуаций, разделяющим возможные ситуации на однородные группы путем использования обучающих выборок, когда на основе измерения различных характеристик наблюдаемой ситуации ее относят к одной из групп, зафиксированных в историческом архиве наблюдаемых ранее ситуаций, где приведены и необходимые реакции на ситуации этой группы;

— факторным анализом, классифицирующим признаки (факторы) возможных ситуаций и определяющим взаимосвязи между ними, что позволяет анализировать и классифицировать наблюдаемую ситуацию по выделенным факторам, число которых значительно меньше исходного числа взаимосвязанных признаков и характеристик ситуации;

— предикативным (прогнозным) анализом наблюдаемой ситуации, строящим математическую модель прогноза развития этой ситуации на основе как текущих наблюдений за ее развитием, так и на базе исторических данных по развитию близких ситуаций;

— ассоциативным (ретроспективным) анализом возникшей ситуации, основанном на построении прогноза наблюдаемой ситуации и ее рациональной компенсации путем ассоциативного поиска и выявления уже наблюдаемых ранее подобных (близких) ситуаций, зафиксированных в исторической базе данных.

Следует отметить важные способы расширения и углубления анализа определенных, возникающих ситуаций, основанных на следующих принципах:

— дополненная реальность, заключающаяся при наблюдении определенной ситуации во введении в рассмотрение еще ряда добавочных измеряемых текущих данных, которые прямо или косвенно могут быть взаимосвязаны с данной ситуацией, и в проведении их совместного анализа;

— машинное обучение, под которым понимается автоматическое самообучение системы автоматизации в классификации ситуаций путем анализа и сопоставления наблюдаемых ситуаций с имеющимися претендентами или путем использования экспертных рекомендаций выделения однотипных задач, базиру-

ющихся на различных математических методах: статистики, нейросетей, теории графов и т. п.

Возможна взаимосвязь АСУТП с облаком и проведение в нем глубокого анализа всех или части исходных данных. В нем могут быть реализованы указанные выше классы алгоритмов и сопоставлены полученные значения исходных данных с необходимыми значениями при заданной нормальной работе агрегата.

Практическое использование на предприятиях всех приведенных методов глубокого анализа позволяет автоматически, без участия персонала реагировать на большинство ситуаций типа отклонений работы технологических агрегатов от нормального, заданного режима, но (следует подчеркнуть) их применение не исключает необходимости управления работой технологических агрегатов оперативным персоналом; то есть они не меняют расшифровку АСУТП как «Автоматизированной системы управления ТП» и не делают ее «Автоматической системой управления ТП». Более того, они сопровождаются возможностью расширения доступа оператора к системе управления через различные мобильные устройства.

Основные причины этого принципиального положения:

— интерпретация возникающей ситуации, даже при наличии ее автоматического, глубокого анализа, далеко не всегда может быть правильна и тем более однозначно проведена без участия опытного оператора;

— возможны причины возникновения ситуаций, не контролируемые автоматически, но известные оператору;

— существуют не формализованные в настоящее время способы компенсации отдельных ситуаций, которые может использовать только оператор.

Расширение информационного взаимодействия АСУТП с другими системами и средствами автоматизации предприятия

Создание цифрового предприятия, подразумевающего реализацию в нем промышленного Интернета вещей, требует существенного расширения информационного взаимодействия каждой АСУТП с цеховым руководством, с соседними по ходу производства технологическими агрегатами и другими производственными объектами, с основными производственными службами (производственной, диспетчерской, технологической, экономической, энергетической, ремонтной, КИП-овской и т. д.), с бизнес-отделами (плановым, снабжения, сбыта и т. д.), с руководством предприятия. Причем это должно быть не только информационное взаимодействие персонала с системами автоматизации технологических агрегатов, но и самих систем автоматизации между собой и зачастую систем автоматизации с объектами вне предприятия (например, с облаком). Практически следует открыть доступ к информационному обеспечению АСУТП в реальном времени различным службам и отделам предприятия, различным его системам автоматизации, которые смогут запрашивать отдельные данные для решения своих задач.

В первую очередь, это требование касается стандартизации протоколов для упрощения взаимодействия различных систем автоматизации и физических объектов предприятия между собой. Конкретно это требование обычно реализуется повсеместным использованием стандартного протокола OPC UA, связывающим технические средства разных производителей. Он обеспечивает взаимодействия между устройствами внутри предприятия и между любым устройством и облаком при любых операционных системах и размерах передаваемых данных.

Важно отметить, что при указанном выше существенном расширении объема исходных данных контроля и учета, а также при их многократно увеличенной и осложненной обработке при глубоком анализе в АСУТП возникает новая проблема — так называемая «Big Data» (большие данные), решение которой требует мощного прикладного программного обеспечения и соответствующей технической вычислительной среды для реализации необходимых аналитических функций. В ряде публикаций предлагается не устраивать глубокий анализ исходных данных в каждом отдельном АСУТП, а вывести его на верхний уровень в информационную платформу MES, которая при этом будет объединять все исходные контрольные и учетные данные всех производственных объектов. Это предложение представляется ошибочным, поскольку золотое правило любых иерархических систем управления заключается в том, что решения должны приниматься на наиболее низком уровне иерархии, на котором обеспечена необходимая для них информационная база. Это правило однозначно формулирует необходимость проводить глубокий анализ всех исходных данных работы конкретного агрегата в его АСУТП и здесь же принимать все решения по его текущему функционированию, а наверх выдавать только те исходные данные и вычисленные показатели работы агрегата, которые необходимы для формирования решений различных служб производства. Кстати, при этом не засоряется база данных каждой службы лишней информацией.

Усиление внимания к кибербезопасности АСУТП

Поскольку необходимые в цифровом предприятии непрерывные информационные взаимосвязи по Internet между подразделениями предприятия различных иерархических уровней управления, включая взаимосвязи различных подразделений с АСУТП, создают гораздо большую ее открытость, то возникает гораздо большая уязвимость АСУТП для внешних информационных угроз и опасность несанкционированного доступа к его информации. При этом следует иметь в виду, что в последние годы информационные угрозы АСУТП непрерывно возрастают численно и становятся все более изощренными. В связи с этим необходимо значительно усилить внимание к ин-

формационной безопасности АСУТП, то есть к защите его программных и технических компонентов от несанкционированного доступа.

Хакерские атаки на АСУТП возможны разными путями:

— через их связи с другими системами/средствами автоматизации предприятия;

— через их связи с пользователями любых служб;

— через внешние подключения к АСУТП электронной почты, USB, компьютеров;

— через проводимые обновления программного обеспечения АСУТП.

Все эти варианты атак должны учитываться при разработке средств киберзащиты АСУТП.

Общие меры защиты информации в АСУТП конкретного производственного объекта от несанкционированного доступа формируются путем проведения следующих работ [1–4]:

— анализ уязвимостей системы/средств и рисков отдельных видов информационных атак, а также их ранжирование по степени тяжести последствий (потерь);

— сегментация АСУТП на отдельные зоны, требующие разные уровни защиты информации, и разделение их сетевых связей специальными межсетевыми экранами (то есть программно-аппаратными компонентами сети, осуществляющими контроль и фильтрацию проходящего через них трафика в соответствии с заданными правилами);

— составление плана действий по уменьшению рисков, связанных с классом возможных угроз, имеющихся уязвимостей к ним, последствий от проникновения информационных вторжений в систему/средства;

— приобретение программных и технических компонентов АСУТП, уже оснащенных элементами защиты от информационных атак;

— внедрение антивирусной защиты от удаленного доступа к АСУТП через Internet;

— включение жесткого контроля подключаемых к АСУТП различных посторонних средств вычислительной техники: персональных компьютеров, ноутбуков, USB-накопителей и т. п.;

— авторизация всех пользователей АСУТП и управлением полномочиями их доступа: определение и разграничение прав пользователей, их активация, изменение, пересмотр, деактивация и удаление; цифровые криптографические подписи пользователей;

— строгогое ограничение реализуемых в АСУТП функций контроля, учета и управления;

— мониторинг компьютерных адресных атак и построения системы обнаружения вторжений посторонней информации в АСУТП;

— разработка алгоритмов реакции на проникновение посторонней информации в АСУТП и на восстановление нормальной работы производства с минимизацией потерь от инцидента;

— обучение работающего и обслуживающего АСУТП персонала обнаружению киберугроз и их компенсации;

— документирование всех изменений в прикладном программном обеспечении АСУТП и записи в них кто, когда и почему их провел;

— создание резервных копий прикладного программного обеспечения АСУТП и их периодического сопоставления;

— периодический аудит эксплуатируемой системы автоматизации на предмет соответствия безопасности системы/средств вероятным классам текущих угроз.

Защита информации в АСУТП по месту расположения защитных средств и их функций должна подразделяться на два уровня, что в целом создает двухуровневую защиту:

— внутренний уровень защиты состоит из включения в программные и технические средства АСУТП (контроллеры, исполнительные механизмы, SCADA-программы), специальных компонентов защиты от информационных угроз;

— внешний уровень защиты формируется из отдельных устройств, процедур и мероприятий по информационным границам АСУТП.

Защита информации должна реализовываться как машинной, так и человеческой частями АСУ:

— пассивная защита, реализуемая машинной частью АСУТП, состоит из антивирусных программ, межсетевых экранов, систем обнаружения информационных атак, авторизации пользователей, аутентификации (то есть проверки подлинности удаленных узлов) и т. п.

— активная защита, реализуемая человеческой частью АСУТП, заключается в мониторинге безопасности на информационной границе АСУТП и в программных и технических средствах АСУТП, в обнаружении и оценке текущих угроз по нарушению информации в системе, в возможно более быстром формировании управляющих воздействий, реагирующих на возникающие угрозы и устраняющих их последствия.

Важно подчеркнуть разницу между созданием системы защиты информации от несанкционированного доступа в уже имеющихся, эксплуатируемых АСУТП и во вновь разрабатываемых АСУТП. В уже существующих на предприятии АСУТП невозможно изменить их программные и технические средства и обычно последние не могут быть дополнены компонентами защиты, поэтому повышение их уровня информационной безопасности целиком ложится на внешний уровень защиты, который формируется по информационным границам АСУТП. Вновь разрабатываемые АСУТП должны быть обеспечены защитой информации как на внутреннем, так и на внешнем уровне. Для этого еще в технических требованиях на АСУТП должны быть предусмотрены конкретные пункты по необходимой защите информации в программных и технических средствах планируемого АСУТП; а при ее приемке должна быть проверена степень защиты информации в ней

путем применения специальных тестов — типа кибератак.

В последние годы международные организации по разработке стандартов в области промышленной автоматизации выпускают семейство стандартов ISA/IEC 62443 «Industrial automation and control systems security», которые переводятся и становятся российскими стандартами. В частности, в ГОСТе Р МЭК 62443-3-3-2016, часть 3–3 для формирования требований к информационной безопасности проектируемой АСУТП рекомендуется выявление и анализ рисков вторжений в ее программное обеспечение. Для этого описывают поэтапное моделирование работы АСУ: создание укрупненной (референтской) модели; более детальной модели ее компонентов и связи с сетями (модель активов) и подробной модели ее работы (модель архитектуры), обосновывающей подразделение АСУ на зоны различных уровней риска, требующие разные уровни защиты информации.

Важным прописанным в этом ГОСТе решением является классификация средств и систем автоматизации по их уровню защиты от несанкционированного доступа, который должен проверяться и подтверждаться органами сертификации. Требуемое снижение риска нарушения информационного обеспечения АСУТП определяется ее уровнем требуемой информационной безопасности или (что то же) уровнем надежности ее защиты от киберугроз — Safety Integrity Level, который обозначается аббревиатурой — SIL.

Типы информационных угроз, от которых зависит категория SIL, подразделяются на случайные, непредумышленные, простые, изощренные и обширные. В соответствии с этим подразделением принимаются следующие категории SIL, задаваемые особенностями возможных типов информационных угроз к конкретному автоматизируемому объекту:

— SIL 0: информационная защита не требуется (к этой категории SIL могут относиться некоторые функции АСУТП; например: электронная почта, IP-телефония, совместный доступ к файлам);

— SIL 1: информационная защита от случайного или непредумышленного нарушения безопасности;

— SIL 2: информационная защита от умышленного нарушения безопасности с использованием простых средств и при низкой мотивации;

— SIL 3: информационная защита от умышленного нарушения безопасности с использованием изощренных средств, при умеренных ресурсах и умеренной мотивации;

— SIL 4: информационная защита от умышленного нарушения безопасности с использованием изощренных средств при обширных ресурсах и высокой мотивации (информационная защита от угроз организованной преступной группировки).

Реализация отмеченных уровней информационной безопасности SIL различается числом и глубиной реализуемых (встраиваемых) элементов (процедур) в программные и технические средства АСУТП, специально нацеленных на повышение их информационной защиты.

Благодаря истинному знанию ты будешь гораздо смелее и совершеннее в каждой работе, нежели без него.
А. Дюрер

В соответствие с этим стандартом сертификационные фирмы в США и в Европе (Exida Certification, ISA Security) проводят сертификацию средств автоматизации (контроллеров, SCADA программ и т.д.) различных производителей по информационной защите, оценивая их функциональную безопасность, программную безопасность, коммуникационную безопасность и выдавая этим средствам сертификаты, определяющие их уровень информационной безопасности (имеющуюся категорию SIL).

Особенности практической реализации рассмотренного развития АСУТП

Все выше приведенные работы по развитию существующих на предприятиях АСУТП и по пересмотру проектов планируемых АСУТП, естественно, не являются одноразовой работой, а требуют длительного, целенаправленного, последовательного совершенствования АСУТП по выделенным направлениям. Поскольку объем выше перечисленных работ по совершенствованию АСУТП всех агрегатов производства достаточно велик, важно предварительно распланировать целесообразную последовательность обследования существующих и проектируемых АСУТП и их необходимого совершенствования и развития. Основным критерием рациональности разработанного плана является выполнение следующего условия: каждый этап плана должен давать ощутимый технический и/или экономический эффект и одновременно быть фундаментом для дальнейших работ по развитию АСУТП.

В большинстве случаев целесообразно начать работы по необходимому развитию АСУТП с модернизации и дополнения системы автоматического контроля на одном/двух технологических агрегатах, на которых затем последовательно, поэтапно отработать все выше приведенные линии развития АСУТП.

Важно подчеркнуть, что еще на начальном этапе работ необходимо проанализировать текущее состояние с автоматизацией на предприятии следующих производственных служб:

— службы главного энергетика: наличия автоматических систем контроля и учета всех энергоресурсов;

— службы главного механика: наличия системы текущего мониторинга основного оборудования производства;

— заводской лаборатории: наличия системы автоматизированного выполнения анализов качественных показателей материальных производственных потоков.

Только наличие на предприятии этих систем позволит на любом технологическом агрегате полно-

ценно выполнить работы по расширению средств и функций автоматического контроля и учета без модернизации посторонних систем автоматизации, внешних по отношению к данной АСУТП.

В противном случае разработка и внедрение указанных систем должны быть включены в планирование первоначальных этапов развития АСУТП, поскольку без их наличия необходимые расширения систем автоматического контроля любого технологического агрегата будут существенно затруднены.

Заключение

Полное достижение выполнения системами автоматизации технологического производства основных требований цифрового предприятия является достаточно медленным эволюционным процессом.

Основными линиями постепенного развития АСУТП, приближающих их к необходимому уровню цифрового предприятия, являются:

— развитие значительно более полного и точного автоматического контроля и учета работы технологического агрегата, охватывающего все стороны его функционирования;

— разработка с помощью современных математических приемов алгоритмов своевременного выявления различных ситуаций, нарушающих заданный ход производства, а также углубленного автоматического анализа этих ситуаций, причин их возникновения и прогноза их развития, что позволяет эффективно, качественно и оперативно управлять технологическим агрегатом;

— существенное расширение без участия персонала информационного взаимодействия АСУТП с различными системами и средствами автоматизации разных служб и отделов предприятия и (при необходимости) с облачным сервисом;

— оснащение систем и средств автоматизации внутренними, встраиваемыми в них элементами (процедурами) киберзащиты, а также организация киберзащиты внешнего слоя каждого выделенного сегмента системы автоматизации.

Организация всех работ требует тщательного анализа текущего состояния автоматизации производства и формирования обоснованного технически и экономически плана развития всех АСУТП производства в требуемых направлениях.

Список литературы

1. *Семеновская Е.* Интернет вещей. Перспективы российского рынка. http://www.rostelecom.ru/projects/IIoT/study_IDC.pdf.
2. *Шолохов А.В.* Мифы и реальность Индустрии 4.0 // Автоматизация в промышленности. 2016. № 8.
3. *Никишин А.В.* Internet вещей в промышленности: как получить преимущества и избежать рисков // Автоматизация в промышленности. 2016. № 8.
4. *Фортин Т., Хокинсон Б.* OPC UA и роль стандартов связи в развитии промышленного Internet вещей // Автоматизация в промышленности. 2016. № 8.

Ицкович Эммануил Львович *– д-р техн. наук, главный научный сотрудник ИПУ им. В.А Трапезникова РАН. Контактный телефон (495) 334-90-21.*

Обзор инновационных платформ IoT

Н.И. Аристова, В.М. Чадеев (ИПУ РАН)

Кратко рассмотрены платформы, реализующие принципы IoT, от компаний IBM, Intel, Microsoft, Oracle, SAP, Hitachi. Отмечается важность объединения потенциала разработчиков и потребителей для совместного развития инновационных технологий Industry 4.0 и поиска новых областей применения разрабатываемых платформ.

Ключевые слова: Industry 4.0, Internet of Things, экосистема, трансформация бизнес-процессов, цифровая трансформация, облачные технологии, аналитика данных, коммуникационные возможности.

Четвертая промышленная революция (Industry 4.0) — переход на полностью автоматизированное цифровое производство, управляемое интеллектуальными системами в режиме реального времени в постоянном взаимодействии с внешней средой, выходящее за границы одного предприятия[1], с перспективой объединения в глобальную промышленную сеть вещей и услуг (www.tadviser.ru). По данным The Economist Intelligence Unit, 63% зарубежных производственных компаний либо уже претерпели существенные цифровые преобразования своих бизнес-процессов, либо находятся в процессе трансформации части организации, а 19% разрабатывают стратегию цифровой трансформации. Такие стремительные действия со стороны предприятий обусловлены их желанием не только сохранять конкурентоспособность в современных условиях, но и достичь принципиально нового уровня производительности и совершенствования различных специфических аспектов производства. А для этого предприятиям необходимо использовать новые технологии и данные для модернизации цепочек поставок и повышения прозрачности производственных процессов.

[1] Уточним, что полностью автоматизированное производство не предполагает устранения человека из контура управления. Оператор по-прежнему следит за технологическими процессами и принимает решение в отдельных, предусмотренных производственным регламентом ситуациях.