

МИХАИЛ ФИЛИППОВ

НАСТРОЙКА АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ МОЖЕТ ПРОИСХОДИТЬ В ДИСТАНЦИОННОМ РЕЖИМЕ

→ Созданием собственной цифровой экосистемы занимаются предприятия группы «УЗТМ-КАРТЭКС» (объединяет Уралмашзавод и ИЗ-КАРТЭКС имени П.Г. Коробкова). В частности, они планируют увеличить количество оборудования, подключенного к системе мониторинга производства АИС «Диспетчер», установленной в 2017 году. Она предназначена для контроля состояния станков и получения фактических данных времени выполнения операции, фактических режимов работы оборудования, которые необходимы для мероприятий по повышению эффективности производства. Комплекс предоставляет достоверную информацию о простоях, загрузке, наработках на отказ по каждой единице оборудования, где установлено ПО. За время тестирования АИС «Диспетчер» на ИЗ-КАРТЭКС удалось сократить простои оборудования в целом на 3%, улучшить состояние станков и повысить уровень их обслуживания.

«Главной тенденцией 2020 года стал перевод части бизнес-процессов в дистанционный формат и усиление контроля за соблюдением правил безопасности. Как следствие, заметно вырос спрос на системы мониторинга рабочей активности — решения, которые позволяют удаленно отслеживать действия сотрудников, вести учет реально отработанного времени, отмечать активные вкладки и бизнес-приложения»,— отмечает эксперт по продажам инфраструктурных решений компании Softline в Уральском федеральном округе Денис Дерюгин. По его словам, использование таких решений позволяет эффективнее использовать рабочее время на «удаленке», избегая как нерационального его использования, так и переработок.



ВЛАДИСЛАВ ЛОНШАКОВ

Во время пандемии многие промышленные компании Урала, имеющие непрерывное производство, внедряли тепловизоры, СКУД и системы видеонаблюдения для контроля температуры тела и использования индивидуальных средств защиты сотрудниками и посетителями. «Вырос спрос на интеллектуальные средства защиты, в числе которых программно-аппаратный комплекс “Умная каска”. Каски оснащены модулем позиционирования на базе GPS/Глонасс-трекеров, которые способны определять и контролировать местонахождение работника как внутри помещений, так и на открытом пространстве, а также фиксировать наличие средства индивидуальной защиты на голове и производить измерения целого ряда внешних и внутренних параметров, в том числе касающихся самочувствия человека»,— говорит Денис Дерюгин.

По данным Softline, внедрение средств удаленного мониторинга рабочей активности позволяет повысить производительность труда в среднем на 20%. Применение «умных» средств защиты обеспечивает более высокую эффективность работы сотрудников, снижает количество случаев производственного травматизма, как следствие, сокращает расходы предприятия на страховые выплаты и оплату больничных листов.

Из-за закрытия границ в этом году крупным промышленным холдингам пришлось в дистанционном режиме получать консультации по настройке иностранного оборудования. Например, «Евраз Нижнетагильский металлургический комбинат» занимался настройкой автоматизированных систем управления на доменной печи №6 в режиме видео- и аудиоконференций со специалистами австрийской фирмы Primetals Technologies (на печи была установлена ее автоматика). Запуск домны благополучно произошел в июле. В дистанционном режиме оказывали консультации «НЛМК-Метиз» по монтажу новой колпаковой печи и представители компании-поставщика Danieli, которые не могли прилететь из Италии.

Эксперты отмечают важность обеспечения информационной безопасности при использовании цифровых технологий. «Об информационной безопасности не стоит забывать, так как все больше интеллектуальной собственности будет оцифровываться. Поэтому важно обеспечить надежную защиту IT-ландшафта. Распространенный риск — “черви”, которые заточены на атаку предприятий, от них надо уметь защищаться»,— подчеркнул руководитель направления прикладных решений для промышленности IT-компании КРОК Иван Попков.

Денис Дерюгин подтверждает: «Чем больше цифровых решений используется в работе предприятия, тем выше риск инцидентов информационной безопасности». Он добавил, что даже при наличии всех необходимых технических средств самым уязвимым звеном остается человек: часто сотрудники ненамеренно способствуют взломам и утечкам данных, например, переходя по непроверенным ссылкам. «Поэтому важно сочетать технические и организационные меры для противодействия киберугрозам, регулярно проводить обучение сотрудников, повышая уровень их цифровой грамотности»,— отметил он. ■