Крючков А.В.

Возникновение опасных ситуаций при внедрении цифровых двойников на объектах ТЭК и использование для снижения данных рисков новых методов синтеза специального программного обеспечения

Аннотация: Автоматизированные системы управления предприятиями (АСУП) стали создаваться задолго до появления цифровых двойников. Большинство систем обеспечения безопасности объектов топливно-энергетического комплекса (ТЭК) интегрировано в АСУП, программное обеспечение которых разрабатывалось с помощью платформ предыдущих поколений. Поэтому применение новых технологий связано с их адаптацией к уже используемым, что всегда влечёт риски возникновения опасных ситуаций на этапе их внедрения в непрерывный процесс, которым является обеспечение безопасности. Для купирования таких проявлений разработан новый набор методов синтеза программного обеспечения.

Ключевые слова: автоматизированные системы управления предприятиями, объекты топливно-энергетического комплекса, комплексная безопасность, цифровые двойники, синтез программного обеспечения, программное обеспечение

Новые технологии требуют развития новых идей. Применение каждой из них в современном мире связано прежде всего с использованием информационных технологий (ИТ). Особенно заметным применение таких технологий становится в нефтегазовой отрасли и на объектах топливно-энергетического комплекса (ТЭК).

Применение на объектах ТЭК новых ИТ связано с построением цифровых двойников как для отдельных предприятий, так и для их групп или отдельных технологических процессов. В сопровождающей данный процесс описательной литературе его принято называть также и термином «Индустрия 4.0». Положительными сторонами данного процесса, безусловно, является сокращение издержек объектов ТЭК, которые являются в большинстве своём коммерческими предприятиями, а также

ускорение проведения разведки и подготовки месторождений, последующих добычи, хранения и транспортировки добытого сырья. «Интеллектуальные месторождения и заводы, роботы и беспилотники — все это уже реальность современного нефтегаза» [1].

Вместе с тем, применение таких технологий имеет ряд особенностей. Прежде всего, – это масштабные инвестиции в средства обеспечения. Их внедрение в уже существующие автоматизированные системы управления производством (АСУП) или автоматизированные системы управления технологическими процессами (АСУТП) ведёт к изменениям сразу на трёх уровнях информирования о принятии решений и полной перестройки всех систем оперативного управления производственными процессами. Существующее нормативное обеспечение технологических процессов в автоматизированных системах (АС), включая процессы обеспечения безопасности, жёстко регулируют процессы. Например, выполнение требований [2] (п.4.4) при внедрении систем «Индустрии 4.0» потребует полной замены всего парка датчиков первого уровня, модернизации мощностей на втором уровне и замены всего разработанного ранее программного обеспечения (ПО) на новое в соответствии с [3].

Последнее обстоятельство хочется отметить особо. Дело в том, что на большинстве объектов ТЭК продолжительное время существовали собственные системы автоматизации, которые разрабатывались и поддерживались существующими на них коллективами программистов или сторонними организациями-разработчиками ПО. Создаваемое ими ПО в нормативной документации принято называть специальным (СПО). Переход объектов ТЭК к единому цифровому циклу производственных цепочек требует либо вписать данное СПО в новые системы (что часто невозможно в принципе), либо переписать его заново на новых средствах разработки, что в разы увеличивает затраты. Отказ от предыдущих поколений систем СПО на объектах ТЭК может привести к нарушению стабильной работы многократно тестируемых программных систем обеспечения комплексной безопасности (информационной, технической, пожарной и т.п.), а также в некоторых случаях отдельных или всех систем жизнеобеспечения и оповещения персонала.

Помимо этого, следует отметить, что многолетний опыт применения предыдущих поколений средств разработки СПО для объектов нефтегазового комплекса и объектов ТЭК показывает, что быстрое внедрение новых систем СПО всегда влечёт за собой долгий период их тестирования и «подгонки» под условия конкретного объекта ТЭК и даже отдельных технологических процессов, выполняемых на его базе. Наиболее близким по времени к внедрению цифровых двойников является платформа ERP-систем.

Опыт их применения показывает [4], что за конкретные участки отвечают так называемые ERP-модули, выполняющие роль СПО в традиционном смысле. Они призваны выполнять основные функции конкретных исполнителей на рабочих местах в автоматизированном (или автоматическом для систем обеспечения безопасности) режиме. При этом само внедрение представляет собой сложный многоэтапный и многоступенчатый процесс. В нём принято определять восемь основных этапов: подготовка к внедрению (указание целей и задач для внедрения новых ИТ), анализ бизнеса (определение текущих задач и перспектив развития бизнеса и структур используемых при этом данных), выбор ERP-системы (анализ существующих предложений систем в данном сегменте рынка в соответствии с целями и задачами, полученными на предыдущих этапах), выбор поставщика, управление проектом (собственно доработка модулей под потребности объекта ТЭК с назначением ответственных и координацией усилий различных специалистов), тестирование (пробная эксплуатация в течение какого-то, иногда продолжительного, времени), обучение персонала работе с новой системой (сроки обучения на разных участках различны), ввод в эксплуатацию (как правило, постепенный). Временной анализ этих пунктов внедрения показывает, что для исключения риска снижения текущего уровня комплексной безопасности этот процесс для новой системы СПО на объектах ТЭК должен занимать не менее чем 3-5 лет. Следовательно, внедрение цифровых двойников должно проводиться с такими же временными интервалами.

Вместе с тем, в РГУ нефти и газа им. И.М. Губкина разработан новый набор методов синтеза СПО, который, не будучи определён как технология, может существенно упростить внедрение новых элементов системы СПО цифровых двойников на объектах ТЭК [5-

7]. Данный набор методов позволяет хранить данные о целях и задачах для внедрения новых ИТ, текущих задачах бизнеса и структурах используемых данных в одинаковых структурах независимо от направления их использования, а также использовать фиксированные требования к доработкам модулей (в терминах ERP-систем) СПО. Помимо этого, данный набор методов позволяет на содержательном (семантическом) уровне описывать интерфейс пользователя, что может существенно упростить обучение персонала при переходе на новое СПО. Использование фиксированных требований к доработкам модулей может существенно упростить тестирование при доработке модулей [7]. Это позволит не только сократить временные и финансовые издержки, но и снизить риск возникновения опасных событий, которые могут привести к реализации угроз комплексной безопасности объектов нефтегазового комплекса.

Литература:

1. Цифровые технологии в нефтяной отрасли [Электронный ресурс]. – URL https://zen.yandex.ru/media/sibneft/cifrovye-tehnologii-v-neftianoi-otrasli-5def8fcbd7859b00af01311f (дата обращения 16.07.2020).

2. СТО 70238424.27.100.010-2011 Автоматизированные системы управления технологическими процессами (АСУТП) ТЭС. Условия создания. Нормы и требования [Электронный ресурс]. – URL: http://docs.cntd.ru/ document/1200093673 (дата обращения 16.07.2020).

3. Системы автоматизации. Схемы автоматизации. Указания по выполнению. Пособие к ГОСТ 21.408-93 [Электронный ресурс].– URL: https://ohranatruda.ru/upload/iblock/9b8/4293836573.pdf (дата обращения 17.07.2020).

4. *Дуванский В.* Применение ERP-системы на предприятии [Электронный ресурс]. – URL: https://dicis.ru/blog/programma-erp-chto-eto-takoe (дата обращения 17.07.2020).

5. *Крючков А.В.* Методология универсализации синтеза специального программного обеспечения крупной автоматизированной системы управления предприятием//Технологии техносферной безопасности. – 2015 – № 3 (61). – С. 264-268.

6. *Крючков А.В.* Иерархические требования к специальному программному обеспечению автоматизированной системы управления предприятием//Технологии техносферной безопасности. – 2015 – № 1 (59). – С. 135-144.

7. *Бутузов С.Ю., Крючков А.В.* Сервис удалённой разработки специального программного обеспечения в интересах МЧС России//Технологии техносферной безопасности. – 2013 – № 6 (52). – С. 18.

Курако Е.А., Орлов В.Л.

К вопросу перевода информационных систем на отечественное программное обеспечение

Аннотация: Рассматриваются проблемы функционирования информационных систем в разных операционных средах. Определяются основные направления деятельности при преобразовании программного обеспечения в процессе перевода из одной среды в другую. Даются предварительные оценки трудоемкости и эффективности перевода при сохранении уровня безопасности.

Ключевые слова: информационные системы, операционные системы, Windows, Linux, преобразование, уровень безопасности

В 2000-е годы большинство информационных систем проектировалось с использованием операционной системы (ОС) Windows. Это было понятно, так как система была широко распространена, достаточно надежна и обладала развитым инструментарием, позволяющим работать с офисными приложениями, базами данных, организовывать различные формы отображения и формировать области ввода данных.

Но закрытость операционной системы фактически понижала уровень надежности и, самое главное, уровень защиты информации, так как отсутствовали сведения о том, как поведет себя ОС в различных ситуациях, не будут ли введены в действие скрытые закладки и не будет ли перехвачено управление программно-аппаратными комплексами.