DOI: 10.22184/1992-4178.2024.237.6.60.63

О проблемах интеграции информационно-измерительных систем в условиях противодействия компьютерным атакам

Е. Янов, к. т. н.[1]

УДК 658.5.012.7 | ВАК 2.2.11

Разработана информационно-измерительная система, не требующая прямого подключения к системам числового программного управления технологического оборудования, что позволяет минимизировать риски возникновения угроз информационной безопасности предприятия и выхода из строя всего оборудования в результате компьютерной атаки. Предложенная информационно-измерительная система способна осуществлять косвенный контроль состояния технологического оборудования с помощью специального диагностического модуля. Разработка внедрена на одном из предприятий оборонно-промышленного комплекса Тульской области и доказала свою эффективность в условиях промышленной эксплуатации.

Анализ тенденций развития современного машиностроительного производства свидетельствует о неуклонном росте доли аппаратно-программных комплексов (АПК) и информационно-измерительных систем (ИИС), задействованных в технологических переделах. АПК и ИИС интегрированы в производственные системы, управляемые с помощью сервера предприятия и связанные с информационными подсистемами верхнего уровня, сопряженными с основным и вспомогательным технологическим оборудованием. Цифровизация машиностроительного производства, безусловно, положительно сказывается на конкурентоспособности предприятия и эффективности выпуска продукции в условиях формирования технологического суверенитета.

Однако внедрение АПК и ИИС на предприятиях ряда отраслей связано с различными проблемами, в том числе с необходимостью обеспечения мер защиты от внешних воздействий и компьютерных атак, которые могут полностью остановить работу машиностроительного предприятия и вывести из строя его оборудование.

Так, в соответствии с Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 года № 187-ФЗ [1], установлены нормы регулирования отношений в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее – КИИ) в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

Для целей данного Федерального закона используются понятия, некоторые из которых, в рамках рассмотрения указанной проблематики, представлены ниже:

- критическая информационная инфраструктура – объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов;
- объекты критической информационной инфраструктуры – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры;
- значимый объект КИИ – объект критической информационной инфраструктуры (например, станок с ЧПУ), которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры;
- безопасность КИИ – состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак;

[1] «Тульская инженерная школа «Интеллектуальные оборонные системы» им. академика А.Г. Шипунова», заместитель директора, dexaik@mail.ru.

- автоматизированная система управления – комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами.

Категорирование объектов КИИ осуществляется в соответствии с постановлением Правительства РФ от 8 февраля 2018 года № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» (далее – постановление №127 [2]).

Категорирование осуществляется исходя из различных критериев. Рассмотрим критерии, применимые к машиностроительным производствам:

- экономическая значимость, выражающаяся в оценке возможного причинения прямого и косвенного ущерба субъектам КИИ и (или) бюджетам Российской Федерации;
- значимость объекта КИИ для обеспечения обороны страны, безопасности государства и правопорядка.

Устанавливаются три категории значимости объектов КИИ – первая, вторая и третья.

Категория значимости, к которой отнесен значимый объект КИИ, может быть изменена в порядке, предусмотренном для категорирования, в следующих случаях:

- по мотивированному решению федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности КИИ Российской Федерации, принятому по результатам проверки, проведенной в рамках осуществления государственного контроля в области обеспечения безопасности значимых объектов КИИ;
- в случае изменения значимого объекта КИИ, в результате которого такой объект перестал соответствовать критериям значимости и показателям их значений, на основании которых ему была присвоена определенная категория значимости;
- в связи с ликвидацией, реорганизацией субъекта критической информационной инфраструктуры и (или) изменением его организационно-правовой формы, в результате которых были изменены либо утрачены признаки субъекта КИИ.

Соответственно, при производстве продукции двойного и специального назначения на предприятиях машиностроительных производств, технологическое оборудование станочного парка является объектами КИИ – автоматизированными системами управления и другими значимыми системами, функционирование которых критически важно для жизнедеятельности государства, то же самое относится и к информационно-измерительным системам, интегрированным в производственные системы.

На рынке в настоящее время представлены различные отечественные ИИС, обеспечивающие контроль станочного парка [3]. Данные продукты отличаются организацией интерфейсов, ценами и применяемой в отношении их политикой лицензирования, но основным условием работы таких систем является необходимость их подключения к системам числового программного управления (СЧПУ) технологического оборудования.

В соответствии с требованиями информационной безопасности, подключение ИИС к СЧПУ объектов КИИ требует категорирования объектов КИИ и повышения их уровня значимости.

Исходя из п.14 (1) постановления №127, при проведении категорирования объекта КИИ должны быть рассмотрены наихудшие сценарии, учитывающие проведение целенаправленных компьютерных атак на объекты КИИ, результатом которых являются прекращение или нарушение выполнения критических процессов и нанесение максимально возможного ущерба. В случае объединения парка технологического оборудования с ЧПУ, подключения АПК и ИИС, наихудший сценарий – это одновременный выход из строя всего оборудования.

Так как информационно-измерительные системы используют для сбора информации АПК, подключаемые к СЧПУ, а повышение категории значимости КИИ приводит к значительному увеличению расходов на обеспечение безопасности, зачастую несопоставимых с эффектом от внедрения ИИС, то это вынуждает предприятия отказываться от внедрения ИИС. Применение указанных систем также несет риск значительного увеличения затрат на восстановление работоспособности значимого объекта КИИ в случае возникновения инцидентов информационной безопасности.

Следовательно, становится актуальной задача разработки ИИС, контролирующих соблюдение техно-

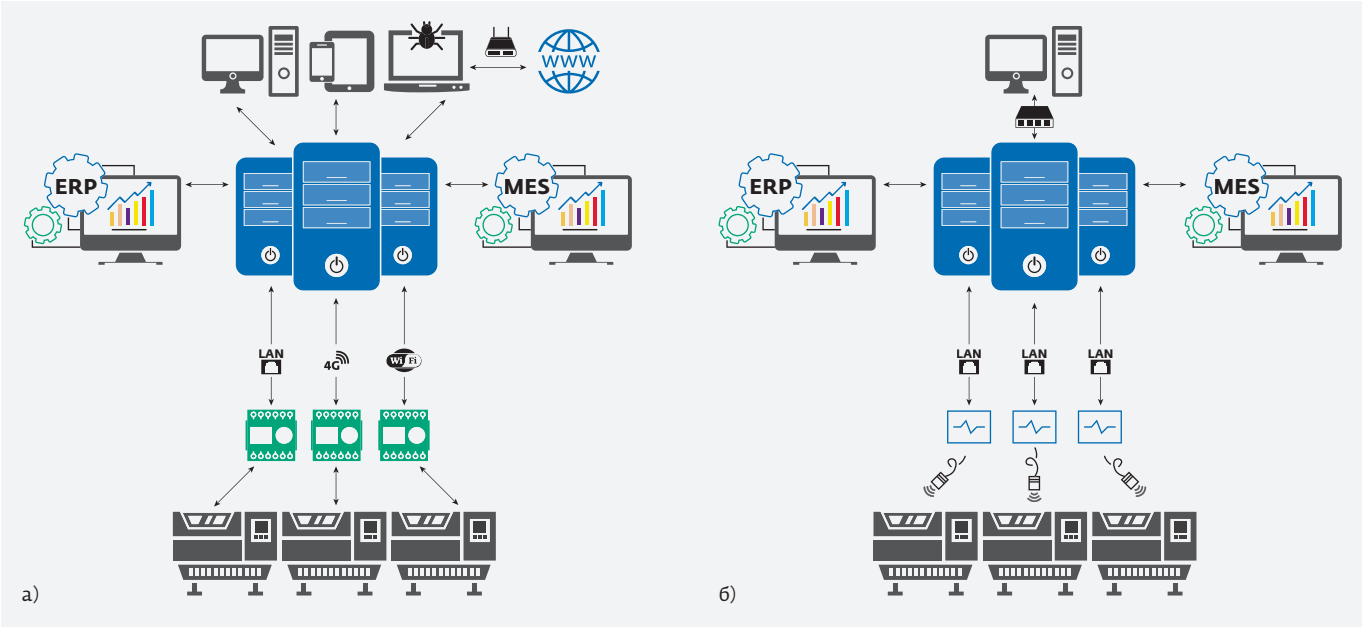

Рис. 1. Архитектура ИИС: а – типовой пример ИИС; б – разработанная ИИС

логической дисциплины в процессе работы технологических систем на основе методов и средств обеспечения оперативного контроля, сбора и обработки информации о технологических процессах и не требующих прямого подключения к СЧПУ технологического оборудования, с отдельными серверами, не связанными напрямую с сетями предприятия.

Рассмотрим типовую архитектуру построения информационно-измерительных систем, используемых на машиностроительных предприятиях (рис. 1а). В общем случае почти любая ИИС состоит из сервера, на котором установлено необходимое программное обеспечение, хранятся и обрабатываются данные. Сервер имеет непосредственную связь с персональными устройствами для передачи на них аналитической, статистической или иной запрашиваемой информации. Это могут быть как персональные компьютеры на рабочих местах, так и мобильные устройства. При этом каналы передачи информации могут быть как проводные, так и беспроводные, с использованием или без использования сотовых сетей, могут иметь или не иметь протоколы шифрования данных. С другой стороны, сервер предоставляет информацию для MES и ERP систем предприятия.

Информация (исходные данные) на сервер поступает с контроллеров АПК, интегрированных или связанных с СЧПУ технологического оборудования. АПК собирают информацию как с СЧПУ, так и с дополнительно установленных датчиков, если это необходимо.

Безусловно, такая архитектура ИИС имеет ряд преимуществ и распространена на предприятиях, но уязвима к инцидентам информационной безопасности. Так, заражение любого устройства в цепочке из множества устройств может привести к выходу из строя всего станочного парка предприятия, о чем говорилось выше. Здесь под инцидентом понимается факт нарушения и (или) прекращения функционирования объекта КИИ, в том числе произошедший в результате компьютерной атаки.

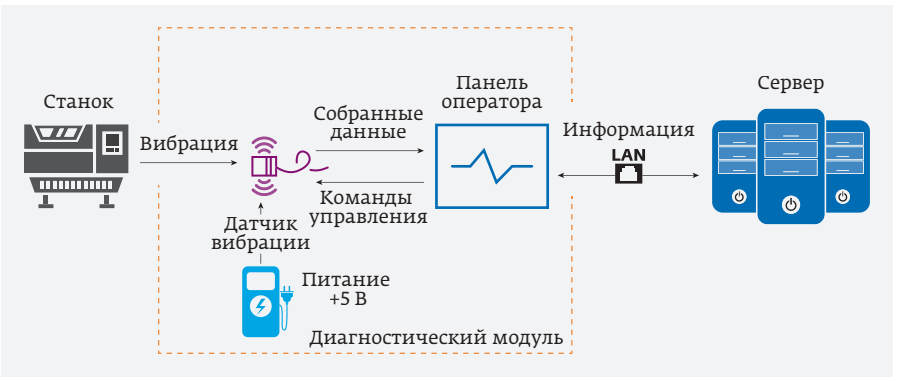

Рис. 2. Структура диагностического модуля

Задача обеспечения мер защиты от внешних воздействий и компьютерных атак при внедрении ИИС на предприятиях машиностроительных

производств может быть решена за счет применения ИИС, способных выполнять косвенный контроль состояния технологического оборудования. В рассматриваемом примере (рис. 1б) контролируется уровень вибрации в процессе механической обработки.

Для этого разработан специальный диагностический модуль контроля состояния технологических систем, осуществляющий мониторинг работы оборудования (рис. 2) [4]. В диагностический модуль встроен датчик контроля вибрации, который содержит МЭМС-акселерометр. Благодаря малым размерам акселерометр можно установить максимально близко к зоне резания, чтобы избежать затухания сигналов вибрации из-за прохождения через упругие элементы станка.

Косвенный контроль уровня вибрации позволяет исключить необходимость подключения ИИС к СЧПУ, при этом не повышается категория значимости объекта КИИ. Таким образом исключается риск компьютерной атаки одновременно на весь парк систем ЧПУ, подключенных к ИИС, а также причинения ущерба СЧПУ посредством воздействия через ИИС или распространения вредоносного программного обеспечения по сети, объединяющей ЧПУ.

В завершении стоит отметить, что разработанная ИИС внедрена на одном из предприятий оборонно-промышленного комплекса Тульской области и доказала свою эффективность и информативность в условиях промышленной эксплуатации.

ЛИТЕРАТУРА

1. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 года № 187-ФЗ
2. Постановление Правительства РФ от 8 февраля 2018 года № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».
3. **Анцев А.В., Янов Е.С., Воротилин М.С.** Информационно-измерительные системы мониторинга работы станочного парка предприятия // Известия Тульского государственного университета. Технические науки. 2023. № 9. С. 495–498.
4. **Янов Е.С.** Аппаратно-программный комплекс мониторинга технологических систем и процессов / Е.С. Янов, А.В. Анцев, М.С. Воротилин, Е.И. Минаков // СТИН. 2024. №5. С. 32–35.