ПРЕДИСЛОВИЕ

В настоящее время постиндустриальное общество находится в состоянии перманентной цифровой революции, текущим этапом которой является глобальная компьютеризация и интеграция в сеть Интернет систем управления промышленными объектами, что неизбежно повышает их уязвимость с точки зрения информационной безопасности. Реальность этой угрозы полностью подтверждается на практике — почти каждую неделю средства массовой информации рассказывают о новых компьютерных преступлениях, взломах и сетевых атаках, целью которых являются промышленные объекты.

Переход к цифровой индустрии основан на массовом применении киберфизических систем, реализующих симбиоз информационных и физических процессов. Такие системы отличаются от традиционных средств автоматизированного управления наличием множества элементов различной природы, функциональной избыточностью, распределенностью и высокой степенью виртуализации. Примерами киберфизических систем являются беспилотные аппараты, роботизированное производство, промышленный Интернет вещей.

Коллективом кафедры ИБКС СПбПУ и нашими коллегами из МВТУ и МИФИ решен ряд научно-технических и технологических задач поддержания устойчивого функционирования неоднородных киберфизических систем в условиях воздействия целенаправленных киберугроз.

Перед авторами стояла весьма сложная и многоплановая задача — разработать технологии, направленные на выполнение традиционных требований безопасности и одновременно способные противодействовать новым видам кибератак на цифровые системы управления киберфизическими системами. В качестве решения, обусловленного развитием парадигмы информационной безопасности, авторы видят концепцию функциональной устойчивости промышленных систем к кибератакам, основанную на теории управления.

Практическим результатом исследований и разработок авторов являются комплексы инновационных решений по обеспечению кибербезопасности цифровой индустрии: доверенная операционная среда, средства обнаружения кибератак, управления инцидентами безопасности в высоконагруженных системах и экспериментальное тестирование защищенности. В качестве методологической основы для этих решений авторы разработали биоинспирированные методы оценки и поддержания безопасности на основе самоподобия и технологию саморегуляции цифровых управляющих систем с использованием теории фрактальных графов и имитационного моделиро-

вания. Обнаружение и управление инцидентами безопасности в высоконагруженных системах реализованы с применением фрактального анализа и Больших данных. Технологии распределенных реестров, групповой аутентификации и малоресурсные криптографические протоколы служат инструментом обеспечения доверия в распределенных системах управления цифровым производством.

Совокупность этих результатов, по мнению авторов, формирует методологические основы новой парадигмы информационной безопасности современных систем цифровой индустрии в виде набора методов и средств обеспечения функциональной устойчивости этих систем к кибератакам, опирающихся на теорию управления.

Оригинальная методология построения доверенной защищенной платформы информационных систем цифровой индустрии и аппарат раннего обнаружения киберугроз на основе применения биокогнитивных технологий были удостоены премии правительства РФ за разработку и внедрение комплекса средств и технологий обеспечения кибербезопасности автоматизированных банковских систем нового поколения.

Данная монография представляет основные теоретические достижения и практические результаты авторов в области функциональной устойчивости к кибератакам и охватывает целый комплекс вопросов от систематизации основных понятий кибербезопасности до создания отечественной доверенной платформы цифровой индустрии, доверенной среды обмена данными и групповой аутентификации.

Глава 1 (*Д. П. Зегжда, В. М. Крундышев*) систематизирует особенности современных киберугроз и объектов цифровой индустрии как киберфизических объектов. Приводятся основные понятия и определения, примеры технологий автоматизированного противостояния киберугрозам, основанные на методологии адаптивной реконфигурации инфраструктуры, что позволяет отражать кибератаки на ранней стадии.

Выявление и анализ закономерностей эволюции технологий информационной безопасности приведены в **главе 2** (*Д. П. Зегжда*). Последовательное развитие концепции безопасности киберфизических систем с позиции теории управления является ключевым положением, обосновывающем трактовку проблемы киберустойчивости как развитие парадигмы динамической защиты от кибератак. Такой подход позволяет трактовать кибербезопасность как естественное развитие информационной безопасности и определяет круг задач, которые необходимо решить для своевременного обнаружения и противодействия киберугрозам.

Фундаментальным вопросом реализации предложенного подхода является задача создания отечественной защищенной платформы для современных информационных систем, позволяющей обеспечить технологическую независимость, интеграцию современных технологий и отечественных средств защиты при сохранении совместимости с прикладными решениями. В решении этой задачи кафедра ИБКС СПбПУ имеет значительный опыт и определенный приоритет. В **главе 3** (*Д. П. Зегжда, М. О. Кали-*

нин, А. С. Марков, И. Ю. Жуков) приведены принципы построения защищенной импортонезависимой платформы на основе применения отечественной защищенной ОС («Фебос»), технологий виртуализации и программно-конфигурируемых гибридных систем с гибкой архитектурой.

Авторам удалось обосновать методологию построения гибридных сетей реализующих ИТК технологии нового поколения и проиллюстрировать ее применение на примере построения систем управления безопасностью в сетях беспилотных транспортных средств. Предложенная платформа применена при разработке отечественных средств контроля и анализа защищенности ресурсов банковских систем (*А. С. Марков, И. Ю. Жуков*). Вопросы управления безопасностью в сетях беспилотного транспорта представлены в разделах 3.2, 3.4, 3.7 (*В. М. Крундышев*)

В **главе 4** (*Д. П. Зегжда, Е. Ю. Павленко*) рассматриваются проблемы обеспечения устойчивого функционирования киберфизических систем в условиях деструктивных воздействий. Гомеостатическая методология обеспечения информационной безопасности киберфизических систем позволяет обнаруживать деструктивное воздействие и анализировать его возможные последствия, оценивать изменения состояния, переконфигурировать структуру и менять значения параметров киберфизической системы для возвращения ее в область устойчивых состояний.

Решение задачи обеспечения киберустойчивости автомобильных самоорганизующихся сетей VANET рассмотрено в **главе 5** (*Д. В. Иванов, Д. А. Москвин*). Использование предфрактальных графов для выявления самоподобных характеристик сети позволяет автоматизировать процесс обнаружения аномалий и обеспечивает саморегуляцию структуры сети.

Подход к оценке и управлению безопасностью на основе построения SIEM-системы, обеспечивающей автоматический анализ Больших данных для выявления внутренних связей событий и обнаружения инцидентов безопасности на основе принципа самоподобия, рассмотрен в **главах 6 и 7** (*Д. С. Лаврова*). Применение технологии SIEM проиллюстрировано на примере магистральных сетей и систем Интернета вещей. Оригинальным решением является применение методов мультифрактального анализа и статистических методов для выявления инцидентов безопасности в таких системах.

Надежность, безопасность и масштабируемость каналов коммуникации между компонентами киберфизической системы обеспечивается с помощью рассмотренных *А. С. Коноплевым* в **главе 8** блокчейн-подобных ориентированных ациклических графов, используемых для математического описания доверенной среды обмена данными.

Важную роль в обеспечении безопасности распределенных систем цифровой индустрии играют криптографические методы. Особенности разнородных распределенных систем, различные типы протоколов, характер вычислительных ресурсов учтены в методологии аутентификации, разработанной *Е. Б. Александровой* (**глава 9**). Обзор протоколов гомоморфной криптографии выполнил *Н. Н. Шенец*.

Неотъемлемой частью любого научного исследования является эксперимент. Технологии экспериментального тестирования защищенности киберфизической системы, реализованные *А. Д. Дахновичем и Д. А. Москвиным* (**глава 10**), позволяют обнаруживать значимые угрозы безопасности, спрогнозировать потенциальные механизмы их реализации, оценить множество возможных последствий и дать рекомендации для повышения защищенности системы.

Методы обработки и анализа Больших данных, предложенные *М. А. Полтавцевой* в **главе 11**, включая иерархический метод агрегации Больших данных при работе с временными рядами параметров, позволяют достичь высокой скорости оперативного анализа информации в современных высоконагруженных системах.

Авторы книги выражают благодарность руководству СПбПУ и лично ректору Андрею Ивановичу Рудскому, всему коллективу высшей школы кибербезопасности и защиты информации за поддержку и развитие научных идей, своим студентам и аспирантам за помощь в проведении экспериментальных исследований.

Профессор РАН, директор высшей школы
кибербезопасности и защиты информации СПбПУ,
доктор технических наук, профессор
Д. П. Зегжда

Предисловие рецензента

В настоящее время трудно встретить научную статью и тем более научно-техническое издание, посвященное автоматизированным системам или вопросам цифровизации, в которых не обсуждались бы такие понятия, как «киберугроза», «кибербезопасность», «киберустойчивость». Вместе с тем само понятие «кибербезопасность» на текущий момент не имеет четкого определения в отечественной библиографии, хотя существует ряд подходов к методологии ее обеспечения, технологии реализации и оценки. Такое положение обусловлено тем, что понятие «кибербезопасность» возникло вследствие тотальной компьютеризации и глобальной интернетизации автоматизированных систем, интеграции управляющих компьютерных систем, контроллеров и исполнительских механизмов, что привело к термину «киберфизические системы», примерами которых являются промышленный Интернет вещей, «Умный дом», грид-системы, автоматизированные системы управления производством и робототехнические системы. Распространение подобных систем послужило механизмом реализации четвертой промышленной революции (Industry 4.0) и привело к появлению новых отраслей, таких, как цифровое производство, цифровая экономика и цифровое управление.

Общей и, к сожалению, негативной особенностью этих систем является их подверженность внешним информационным разрушающим воздействиям, средой распространения которых служит Интернет, так или иначе включающий все перечисленные системы.

Разработка теоретических основ для анализа этого явления и создания методов обнаружения и противостояния внешним воздействиям, оценки уровня устойчивости и, в конечном счете, поддержания работоспособности киберфизических систем в условиях целенаправленных деструктивных воздействий и составляет область научной и технической деятельности под названием «кибербезопасность».

Учитывая, что активное развитие этой области знаний насчитывает не более 20–25 лет, существуют различные подходы к формальному определению понятия «кибербезопасность», в каждом из которых конечная цель и задачи, которые необходимо решить для ее достижения, формулируются по-разному. Спектр этих подходов простирается от формального распространения традиционных методов обеспечения информационной безопасности на киберфизические системы путем модификации понятий целостности, доступности и конфиденциальности до создания специализированных центров управления кибербезопасностью, обеспечивающих поддержание работоспособности комплексов киберфизических систем путем обнаружения и предотвращения внешних кибервоздействий.

По мнению авторов данной книги, методология обеспечения кибербезопасности должна быть основана на применении методов автоматизированного ситуационного адаптивного управления, искусственного интеллекта (нейросети, распознавание образов) и технологии Больших данных для обнаружения кибервоздействий, оценки защищенности и принятия решений о мерах противодействия.

Применение интеллектуальных технологий, нейросетевого самообучения и прогнозирования позволяет обеспечить адаптивное управление или саморегуляцию в пределах возможной динамической реконфигурации для обеспечения устойчивости киберфизической системы к киберугрозам. Предлагаемый подход позволяет создать методологию обеспечения кибербезопасности как совокупность методов и средств адаптивного управления для обнаружения и атрибуции внешних кибервоздействий, их нейтрализации и сохранения устойчивости функционирования системы. Создание методологии кибербезопасности цифровой индустрии как совокупности средств противостояния киберугрозам на основе интеллектуального управления составляет основную задачу данной книги.

Такой подход вполне соответствует нарастающим тенденциям интеллектуализации автоматизированных систем. В условиях глобальной цифровизации он может быть распространен практически на все системы производственного, энергетического, транспортного и экономического назначения.

Данная монография подготовлена коллективом сотрудников, входящих в научную школу кибербезопасности, действующую в Санкт-Петербургском политехническом университете в течение более 20 лет. Коллектив известен рядом проектов, научных и практических результатов, получивших высокую оценку специалистов.

Данная монография, возможно, представляет собой первую в России попытку систематизации задач кибербезопасности и обобщения технологий, применяемых для решения этих задач, проиллюстрированную конкретными примерами реализации как на основе собственного опыта авторов, так и с учетом самых передовых решений из мировой практики.

Предложенная систематизация задач и технологий обеспечения кибербезопасности характеризуется следующими положениями:

- перечень рассмотренных в книге технологий защиты достаточно разнообразен, что позволяет получить представление о необходимом наборе средств обеспечения устойчивости функционирования распределенных систем;
- объект защиты рассматривается в непрерывной связи с внешней средой Интернета с учетом всех типов удаленных кибервоздействий, что обеспечивает полноту охвата проблемы;
- описание отдельных технологий защиты снабжено минимально достаточными теоретическими сведениями, что облегчает изучение и особенно важно для раздела, посвященного криптографическим методам защиты.

Первые главы раскрывают позиции авторов относительно проблемы кибербезопасности как кибернетической задачи, связанной с разработкой системы интеллектуального управления, регулирующей непрерывный контакт защищаемого объекта с агрессивной внешней киберсредой, что позволяет представить проблему безопасности как обеспечение устойчивости функционирования в условиях внешних деструктивных кибервоздействий.

Практические результаты этого подхода представлены в главе, посвященной методам автоматического поддержания устойчивости к внешним кибервоздействиям путем реконфигурации структуры системы.

Ряд разделов связан с комплексом практических работ, проводимых авторами в интересах финансовых структур, результаты которых удостоились премии Правительства Российской Федерации в 2018 г.

Отметим, что книга содержит весьма актуальный материал, хотя и неоднородный по характеру описываемых технологий и их сложности, что вполне компенсируется обилием практических рекомендаций. В отношении круга поднятых проблем можно считать, что книга не имеет аналогов.

К основным особенностям книги следует отнести ее многоплановость. Ее можно рассматривать как монографию по технологиям кибербезопасности, содержащую как теоретические особенности некоторых методов защиты, так и практическое руководство по решению задач обнаружения и противодействия киберугрозам и применению криптографических методов, включая гомоморфные вычисления. Книга не перегружена общими теоретическими выкладками, отвлекающими специалистов от скорейшего ознакомления с практическими примерами.

Такое изложение свидетельствует о большом практическом опыте авторов и выгодно отличает данное издание от других книг четко выверенным балансом между теорией и практической реализацией рассматриваемых методов.

Из вышесказанного следует, что лежащая перед читателем книга — весьма нетривиальное издание, представляющее интерес для ученых и специалистов по проблемам безопасности в эпоху цифровизации, а особенно для стремительно расширяющегося круга практиков, посвятивших себя применению интеллектуальных технологий для задач обеспечения киберустойчивости цифрового производства и экономики.

Член-корреспондент РАН,
научный руководитель СПИИ РАН,
доктор технических наук, профессор
Р. М. Юсупов

1 ОСНОВНЫЕ ПОНЯТИЯ КИБЕРБЕЗОПАСНОСТИ ИНДУСТРИАЛЬНЫХ СИСТЕМ

1.1. Цифровая трансформация производства

Современный производственный процесс претерпевает существенные изменения из-за повсеместного внедрения информационных технологий и систем. Предприятия энергетики, машиностроения, нефтехимии, транспорта, логистики и прочих отраслей за последнее десятилетие перешагнули незримую черту, отделяющую физический мир машин и агрегатов от виртуального мира компьютерных программ, и, по сути, превратились в киберфизические системы, где объектами физического мира управляют инструкции машинного кода [1]. Потребность в производстве новой более сложной высокотехнологичной продукции изменяет требования к системам автоматизированного управления, общее число которых стремительно растет. Возрастает разнообразие информационных систем, разрабатываются и внедряются новые, ранее не существовавшие типы систем, а также увеличиваются связности между ними. Электронными датчиками и контроллерами оборудуются практически все промышленные элементы и благодаря им в процесс организации потоков вещества и энергии при производстве добавляются еще и информационные потоки.

Современную эпоху можно назвать эпохой интернетизацией общества. Интернет выступает универсальной средой, которая позволяет с помощью открытых протоколов передачи данных и управления транзитивно замкнуть все информационные аспекты экономики и социальной жизни в единое цифровое пространство — киберпространство, включающее не только данные, но и системы их передачи, обработки и хранения, системы управления этими процессами, средства защиты, а также их динамически изменяющиеся взаимосвязи.

В книге «Четвертая промышленная революция» [2] подробно описывается процесс изменения экономики производства, вызванный стремительными темпами технического развития, широтой применения информационно-телекоммуникационных технологий во всех сферах и системностью использования цифровых устройств. Термин «Индустрия 4.0» впервые прозвучал в 2011 году на Ганноверской ярмарке для обозначения процесса коренного преобразования глобальных цепочек создания стоимости [2, 3], в основе которого — технологии «умного» производства, «умного» оборудования и «умных» бытовых устройств. Фактически гибкое взаимодействие различ-

ных физических систем посредством цифровых технологий меняет вид не только промышленности, но и экономики в целом.

Несмотря на то что программно-аппаратное управление внедрили в производство давно, ситуация в последние годы существенно отличается от того, что было раньше. Во-первых, масштабом проникновения цифровых технологий в контексте как отраслей и сфер деятельности, так и отдельного производственного процесса. Современный период даже называют «вторым машинным веком» [4], подчеркивая разницу между традиционными технологиями использования аппаратного и программного обеспечения, которые неуклонно развивались в течение всего двадцатого века, и новыми тенденциями и решениями глобальной цифровизации и искусственного интеллекта. Именно синтез технологий, от расшифровки генома до нанотехнологий, и систем возобновляемых энергоресурсов составляет фундаментальное отличие. Во-вторых, безусловно, скоростью изменений — в отличие от предыдущих индустриальных революций промышленная революция 4.0 развивается не линейно, а по экспоненте [2].

Основную ценность общества «Индустрии 4.0» представляет собой не продукция, а информация и потенциал информационного воздействия за счет повсеместного использования автоматизации и обмена данными, киберфизических систем, Интернета вещей и облачных сервисов. По прогнозам, потенциал промышленного Интернета вещей (IIOT, Industrial Internet of Things) [5] — сети физических объектов, платформ, систем и приложений со встроенными технологиями обмена данными друг с другом, внешней средой и людьми — оценивается аналитиками более чем в тридцать триллионов долларов и продолжит возрастать [6].

«Индустрия 4.0» характеризуется прорывом и бурным развитием нескольких технологических отраслей. Компания McKinsey группирует их в четыре категории [7], которые в развернутом виде представлены на рис. 1.1.

Все эти технологические кластеры напрямую связаны с цифровой трансформацией производства и киберфизическими системами. Они включают не только сами системы контроллеров и взаимодействующих промышленных устройств, но и новые возникающие области, такие как:

- изменение интерфейсов АСУ с развитием графических интерфейсов, применением технологий touch-screen и технологий расширенной/виртуальной реальности. Несмотря на то что бурное развитие этой области происходит в сегменте пользовательских устройств, его продвижение в область АСУ ТП тоже не за горами;
- технологии обработки данных, генерируемых устройствами в процессе функционирования и взаимодействия. Согласно [7] 40 % таких данных никогда не сохранялось, а оставшиеся 60 % хранятся короткое время локально и почти не подвергаются анализу и обработке. Комплексный контроль цифрового производства требует сбора и обработки всей этой информации в центрах обработки и вычислительных системах;
- технологии анализа данных и искусственного интеллекта возглавляют этот список. Они необходимы для получения реальной выгоды от со-

Рис. 1.1. Технологии четвертой промышленной революции

бранных и обработанных данных о производстве, оперативного и долговременного контроля и планирования производственного процесса. Итогом технологического рывка должны стать устойчивые к внешним изменениям самоадаптирующиеся производственные системы.

Таким образом, технологии «Индустрии 4.0» формируют киберпространство. Киберпространство — глобальная сфера в информационном пространстве, представляющая собой сочетание взаимодействующих компьютеризированных промышленных устройств, автоматизированных и аналитических систем на базе интегрированных информационных технологий, в основе которого лежат глобальные сети передачи данных. Кибернетический подход распространяется на все системы обработки потоков: энергетических, материальных, физических.

Рассматривая цифровую трансформацию технологического процесса, можно говорить о компьютеризации и интеллектуализации всех его стадий. Принципиально выделяются два этапа создания конечного продукта:

1) проектирование продукта;

2) промышленное производство продукта.

При этом неважно, что именно выступает в качестве конечной стадии производства, то есть является итоговым продуктом: машины, механизмы, бытовые изделия, интеллектуальные системы, электрическая или тепловая энергия, гидроэнергия и так далее (рис. 1.2).

Проектирование современного промышленного продукта — это сложный процесс, связанный с применением моделирования, САПР-решений и систем расчетов. В результате создается проект будущего продукта или его «цифровой двойник» [8]. Процесс проектирования при переходе к «Индустрии 4.0» не претерпел существенных изменений, кроме применения новых более

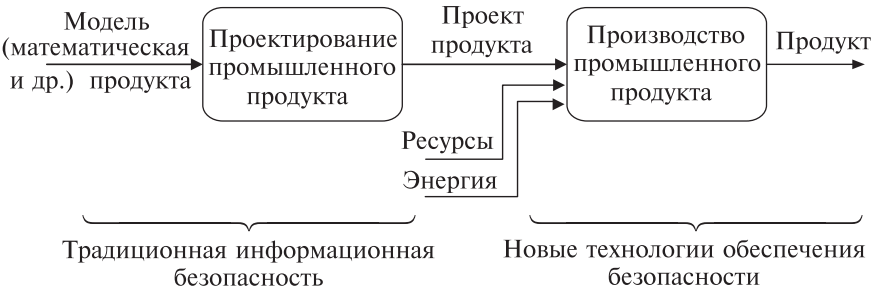

Рис. 1.2. Этапы передового производства

интеллектуальных средств автоматизации. Для обеспечения защищенности систем проектирования могут применяться уже традиционные технологии обеспечения информационной безопасности компьютерных систем последней четверти века.

Процесс производства, в свою очередь, помимо внедрения более интеллектуальных и совершенных АСУ ТП систем привел не просто к появлению SCADA-систем мониторинга и управления процессом производства изделия, но и к интеграции их с корпоративными информационными сетями и ресурсами предприятия для формирования единой цифровой среды управления и мониторинга производства, возникновению киберсистем.

Трансформация производственной информатизации представлена на рис. 1.3, и сейчас можно говорить не о двух (старый и новый, киберфизический), а о трех этапах изменения промышленной среды.

Первый этап включает в себя традиционные информационные системы и информационно-телекоммуникационные системы. Второй этап — кибернетизацию производственного процесса и повсеместное внедрение промышленных контроллеров. Он представляет собой эпоху киберфизических систем и является реальностью сегодняшнего дня. Третий — взгляд в будущее. По мнению ряда специалистов [9, 10], он предполагает цифровую интеграцию не только физических систем, но и организационных: киберне-

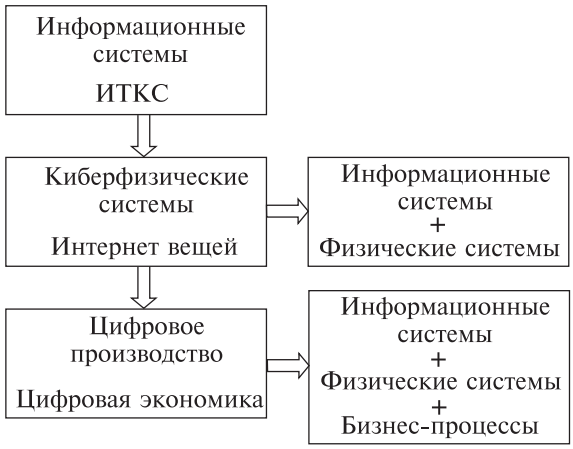

Рис. 1.3. Трансформация производственной компьютеризации

тизацию бизнес-процессов предприятий. Уже в ближайшем будущем ожидается повсеместное внедрение технологии 5G/5G+, которое существенно повысит устойчивость и надежность беспроводной связи между машинами и устройствами. Наличие высокоскоростной и устойчивой связи даст мощный толчок к созданию умных городов, сетей беспилотного транспорта и цифрового производства. На этом этапе можно говорить о применении информационных технологий во всех сферах производственной деятельности. Однако наличие такой среды предоставляет новые уникальные возможности для злоумышленников в реализации таких сетевых атак, как «черная дыра», «серая дыра», массированная DDoS-атака, которые могут привести к серьезным последствиям. Поэтому уже сейчас исследователи и разработчики изучают возможность создания принципиально новых методов противодействия таким кибератакам.

1.2. Киберфизические системы

Рассмотрим общую схему производства, которая характерна для современных промышленных систем, вступающих в эру цифровой экономики. Как и в предыдущем поколении производственных структур, в основе находятся системы управления физическими процессами (рис. 1.4). Над ними располагается управляющий слой контроллеров, осуществляющих сбор данных с физических объектов и генерирующих непосредственные управляющие воздействия в соответствии с развернутым на них программным обеспечением. Контроллеры связаны в сети SCADA-систем, а те, в свою очередь, через общую коммуникационную среду — с корпоративной сетью предприятия. Необходимо отметить, что в качестве среды взаимодействия, как правило, выступает глобальная сеть Интернет.

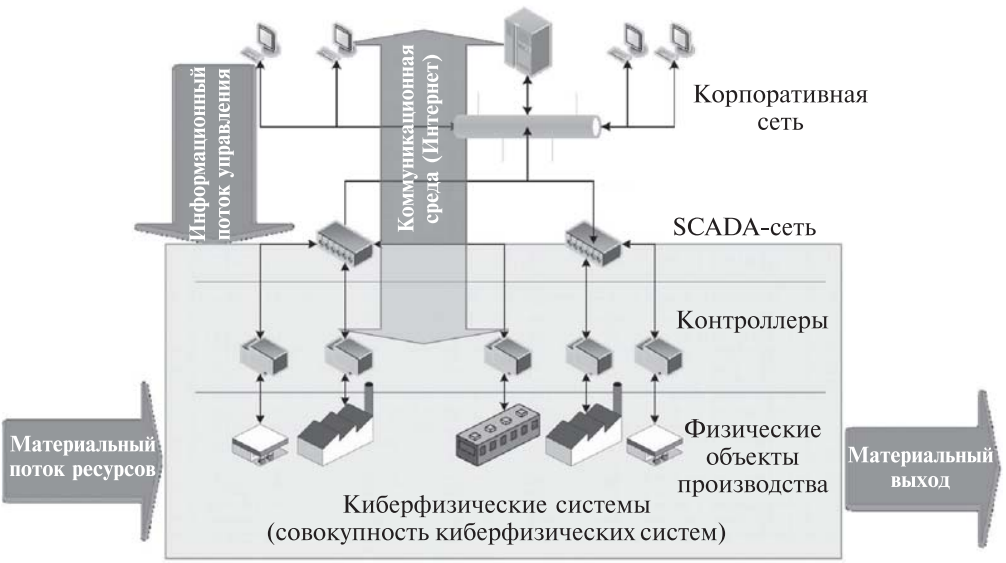

Рис. 1.4. Общая схема цифрового производства

Компьютеризация производства привела к слиянию исполнительных модулей с модулями взаимодействия систем и переходу к цифровому взаимодействию, обмену данными и управляющими командами. Если раньше каждый узел представлял собой отдельный компонент с контуром управления, функция управления которого определялась в соответствии с теорией автоматизированного управления и типами обратных связей, то в настоящее время такой узел не просто компьютеризирован, переведен на цифровое управление и сам по себе является киберфизическим объектом, но и активно взаимодействует с множеством других узлов, организуя производственный процесс практически без участия человека.

Формальные понятия киберфизических объектов и систем приведены в [11]. Киберфизический объект (КФО) — это концептуальная парадигма представления производственных технологических схем в виде конгломерата средств преобразования различных видов материи и энергии и информационно-телекоммуникационной среды, обеспечивающей как обмен информацией между компонентами, так и устойчивое функционирование всей системы в условиях внешних воздействий с помощью автоматизированного управления. Киберфизические системы (КФС) можно определить как наборы взаимодействующих киберфизических объектов, которые включают набор взаимосвязанных физических компонентов, реализующих технологический процесс; информационных компонентов, осуществляющих управление процессом в разной степени автоматизации; коммуникационную среду, обеспечивающую обмен информацией внутри системы и с окружающей средой и передачу управляющих команд исполнительным механизмом [11].

Отличительными признаками киберфизической системы являются:

- высокая степень компьютеризации системы, постоянный телекоммуникационный контакт (обмен информацией) с аналогичными системами и взаимодействие с глобальной сетью Интернет;
- наличие центра (подсистемы) автоматического управления функционированием системы и обеспечение ее устойчивой работоспособности при наличии различных возмущающих воздействий со стороны окружающей среды, включая целенаправленные и случайные воздействия;
- наличие единой информационной среды или киберпространства, представляющего собой совокупность программно-аппаратных средств обработки и передачи информации, обмена внутри системы и с окружающей средой, системы автоматического управления физическими компонентами посредством логически программируемых контроллеров и поддержание заданного сценария работы с возможностью адаптивного управления, а также средства обеспечения защиты информации в виде криптосерверов, межсетевых экранов, антивирусов и так далее;
- наличие интеллектуализации управления путем гомеостаза построения сценариев работы на основе автопрогноза и адаптационного управления, что обеспечивает автономность систем и снижает степень зависимости от оператора.

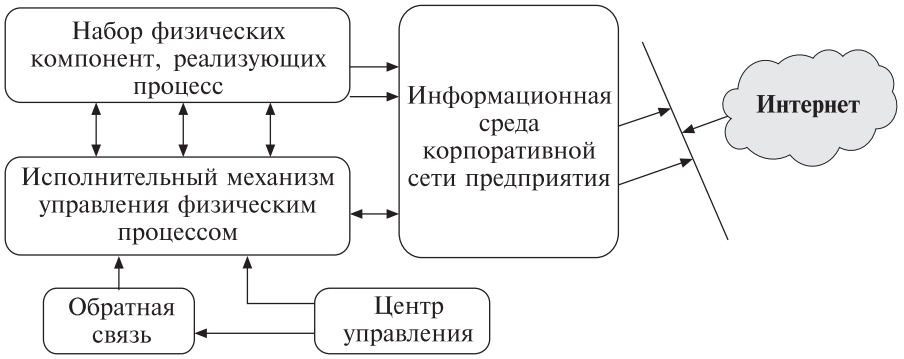

Рис. 1.5. Логическая структура киберфизической системы

Из-за сочетания физической, информационной и коммуникационной составляющих, если для традиционных САР функцией управления является физическая величина, то в современной киберфизической системе это информационное воздействие. На основе киберфизических систем формируется киберсреда цифрового производства, состоящая из:

- центра управления, включающего:
  - корпоративную информационную среду;
  - АСУ предприятия;
- средств обеспечения технологического процесса, в том числе:
  - АСУ технологических процессов (в общем случае всех протекающих на предприятии);
  - коммуникационная сеть;
  - физические компоненты, реализующие процесс производства и управляемые программируемыми контроллерами;
  - исполнительные механизмы АСУ ТП;
- средств обеспечения безопасности производства, включающие:
  - средства информационной безопасности;
  - средства управления системами защиты.

Киберфизическая система обладает следующими свойствами [12]:

- наличие избыточности и резервирование ресурсов системы (допуская возможность пустого резервирования узлов);
- функциональная связность. Под функциональной связностью понимается возможность создания внутри системы целевых функций из комбинации ее отдельных узлов. Уровень декомпозиции функций в данном случае — есть глубина гомеостаза;
- построение целевой функции (или функций) системы из заданного набора функций ее компонентов.

Логическая структура киберфизической системы представлена на рис. 1.5.

Примеры практического применения киберфизических систем:

Производственная среда. Улучшение производственных процессов возможно за счет обмена информацией в реальном времени между промышленным оборудованием, производственной цепочкой поставок, постав-

щиками, системами управления бизнесом и клиентами. Повышение эффективности процессов достигается благодаря автоматическому мониторингу и контролю всего производственного процесса и адаптации производства для удовлетворения предпочтений клиентов. Повышение прозрачности и управляемости цепочек поставок.

Здравоохранение и медицина. Реализация дистанционного мониторинга физических показателей пациентов в реальном времени с целью уменьшения потребностей в госпитализации (например, пациентов с болезнью Альцгеймера) или для улучшения ухода за инвалидами и пожилыми людьми. Кроме того, киберфизические системы применяются в нейробиологических исследованиях для изучения функций организма человека с использованием нейроинтерфейсов — посредника между мозгом и оборудованием терапевтической робототехники.

Транспорт. Транспортные средства и объекты придорожной инфраструктуры могут взаимодействовать, обмениваясь информацией о дорожном движении, местоположении и проблемах на дорогах, и тем самым предотвращать транспортные инциденты и дорожные пробки, повышая уровень безопасности и в конечном счете экономя время и деньги [13].

Сельское хозяйство. Сбор важной информации о климате, почве и других данных для более точного управления сельскохозяйственными работами. Датчики киберфизических систем могут вести постоянный мониторинг различных показателей, таких как орошение почвы, влажность воздуха и здоровье растений, для поддержания оптимальных условий окружающей среды.

Умные здания. Сокращение энергопотребления, повышение безопасности и защищенности, а также создание более комфортных условий для жителей. Например, киберфизические системы могут поддерживать мониторинг энергопотребления и использовать системы регулирования для реализации концепции дома с нулевым потреблением электроэнергии. Кроме того, их можно применять для определения степени ущерба для зданий в результате непредвиденных событий и предотвращения разрушения конструкций.

Вычислительная среда. Киберфизические системы позволяют точнее определять поведение систем и пользователей, что способствует повышению производительности и более эффективному управлению ресурсами. Например, можно оптимизировать работу приложений с учетом контекста и действий пользователей или отслеживать доступность ресурсов. Так, социальные сети и сайты электронной коммерции хранят информацию о действиях пользователей и затребованном контенте, анализируют эту информацию, чтобы предсказывать, что может заинтересовать пользователя, и рекомендовать друзей, публикации, ссылки, страницы, события или продукты [14].

Примеры КФС, внедряемых в различные отрасли деятельности:

Международный аэропорт Пекина реализует технологическую концепцию «Аэропорт как город» [15]. Данная концепция предполагает внедре-

ние цифровых технологий в инфраструктуру аэропорта и реализуется посредством интеграции большого числа интеллектуальных датчиков с инфраструктурой аэропорта. Ключевой функцией интеллектуальной системы Пекинского аэропорта является автоматизация предполетного контроля безопасности, который заключается в проверке посадочного талона пассажира, фотографировании лица пассажира для идентификации его личности, проверки провозимой пассажиром ручной клади. Вся собранная датчиками информация автоматически агрегируется и анализируется. Выполняется связывание информации о пассажире с данными о содержимом его багажа. При обнаружении подозрительного багажа персонал аэропорта получит сообщение, содержащее данные о пассажире и фото его багажа. Это позволяет минимизировать временные затраты на поиск пассажира, которому принадлежит багаж, что особенно актуально в условиях большого пассажиропотока. По словам начальника технического отдела компании Beijing Capital Airport Aviation Security, такая интеллектуальная система проверки безопасности пассажиров включает в себя четыре подсистемы автоматической передачи информации, уведомлений, распознавания лиц и проверки действий пассажира.

Медицинские учреждения сети Calvary в Австралии. Применяется система сетевого мониторинга Paessler PRTG [16] для контроля температурного режима в палатах, запасов плазмы, мониторинга ИТ инфраструктуры. Система PRTG координирует вывоз отходов и их отправку на перерабатывающие заводы, а также внедрена на кухни медучреждений для контроля работы посудомоечных машин. Основными элементами мониторинга являются интеллектуальные сенсоры. Один сенсор обычно контролирует один сетевой параметр, а на одно устройство требуется в среднем 5–10 сенсоров.

«Умный» завод Siemens в Германии. На заводе Siemens в Амберге автоматизировано около 75 % производства. Подавляющее большинство из 1150 штатных работников завода в основном управляют компьютерами и отслеживают процесс [17]. Большая часть производственных компонентов завода способна обмениваться информацией, не требуя вмешательства человека.

Система ContiPressureCheck от компании Continental, включающая в себя «умные» автомобильные шины iTyre с установленными на заводе датчиками ContiPressureCheck. Датчики непрерывно контролируют давление и температуру в шинах, данные записываются и отображаются на дисплее транспортного средства [18]. При отклонении давления от заданного значения система ContiPressureCheck выдает предупреждение, что повышает безопасность движения, поскольку водитель получает возможность своевременно предпринять меры по устранению проблемы. Данная система способна обеспечивать автоматический контроль состояния шин в масштабе автомобильного парка, поскольку она совместима с системами телематики и результаты измерений давления и температуры шин можно просматривать на общем экране и передавать их на внешние устройства.

Завод Mitsubishi Electric в г. Нагоя, Япония. Автоматизация работы завода в городе Нагоя заключается в реализации процесса сбора серводвигателей. По данным [19], после каждого шага процесса выполняется автоматический контроль качества, при котором внедренные измерительные системы и компоненты сравнивают реальные значения с допустимыми пороговыми. Если, например, статорная обмотка признается дефектной, изделие удаляется из дальнейшего процесса производства и генерируется информирующее сообщение для контролирующего процесс работника завода. При этом каждая производственная единица имеет дисплей, что делает удобным доступ к информации о производстве в режиме реального времени и позволяет рабочим немедленно реагировать на проблемные ситуации. Сбор серводвигателя выполняется поэтапно до тех пор, пока устройство не будет собрано, успешно пройдя все автоматические проверки качества. Таким образом, после завершения процесса остаются только бездефектные, полностью проверенные двигатели. На заводе в Нагоя внедрение технологий умного производства увеличило скорость работы оборудования на 190 %, продуктивность — на 180 %, а стоимость производства сократилась на 65 %. Время выполнения заказов уменьшилось на 50 % [19].

Киберфизические системы — источник большого объема интенсивно поступающих разнородных неструктурированных данных, извлечение знаний из которых способно обеспечить решение задачи киберустойчивости. В связи с этим возникает потребность в развитии таких технологий, как Большие данные и искусственный интеллект. Также существует потребность в быстрой обработке данных сверхвысокого объема и в обработке разнородных и неструктурированных данных для агрегации, фильтрации, нормализации, классификации и статистического анализа. Искусственный интеллект позволит извлекать знания из разнородных данных, реализовать обучение и накопление опыта, а также осуществлять предиктивный анализ. Все это возможно благодаря использованию машинного обучения, нейронных сетей, моделирования и распознавания образов.

Цифровизация промышленности привела к появлению в индустрии новых проблем обеспечения информационной безопасности. Единое киберпространство, образуемое взаимодействующими системами на основе общих универсальных протоколов и принципов удаленного управления, приводит к транзитивному замыканию всех действующих компонентов управляющих систем производственной, финансовой и социальной сфер. Глобальная доступность объектов киберпространства порождает проблему обеспечения устойчивой работы современного производства в условиях случайных и целенаправленных компьютерных атак, приводящих к долговременному и труднообнаруживаемому воздействию на управление технологическими процессами. Так изменяется само понятие и подход к безопасности АСУ ТП и производственных систем: возникает задача сохранения их работоспособности в условиях нового ландшафта угроз.

1.3. Новые угрозы безопасности

Цифровая трансформация и интернетизация экономики являются драйверами современного подхода к обеспечению кибербезопасности.

Объединение КФС друг с другом и с внешним кибермиром многократно упрощает их эффективное использование и развитие, но одновременно делает их уязвимыми перед угрозой кибератак. Специалисты промышленных предприятий и исследователи информационной безопасности отмечают опасность, которую несет технологическому процессу и оборудованию внедрение киберфизических технологий. Однако, по признанию большинства вовлеченных в этот процесс или причастных к нему людей, решение задач киберзащиты промышленных предприятий происходит чрезвычайно медленно. Как правило, при этом приводятся различные причины и факторы, затрудняющие и замедляющие движение в направлении защиты промышленных объектов или вовсе препятствующие такому движению.

В традиционных компьютерных сетях объектом защиты являлась совокупность данных ограниченного доступа, а задача защиты информации заключалась в обеспечении конфиденциальности, целостности и доступности. В связи с активным развитием динамических межмашинных цифровых инфраструктур (например, IoT, IIoT, WSN, MANET, VANET) объект защиты приобретает новое представление как элемент киберсреды, где традиционные операции чтения/записи имеют физические последствия, при этом основной задачей стало обеспечение сохранности и надежности кибер-систем, и как следствие, жизни людей [20]. Из-за особенностей современных цифровых инфраструктур и стремительно растущего объема данных, подвергающихся обработке, традиционные методы защиты становятся неэффективными, поэтому перед исследователями стоит задача создания новых методов обеспечения кибербезопасности, которые отвечают актуальным вызовам времени, — методов управления доступом между системами в динамической инфраструктуре, глобального регулирования информационных и управляющих потоков.

Универсальность сетевых протоколов Интернета и принципов удаленного управления распределенными системами позволяет транзитивно замкнуть все управляющие системы производственной, финансовой и общественно-политической сфер в единое киберпространство. Глобальная доступность киберфизических объектов порождает проблему обеспечения устойчивой работы цифрового производства в условиях случайных и целенаправленных компьютерных атак, приводящих к долговременному и труднообнаруживаемому воздействию на управление технологическими процессами, что может повлечь катастрофические последствия. В табл. 1.1 представлена эволюция киберугроз.

Огромное число пользователей, узлов, потоков информации и управления, нечеткий периметр одноранговых инфраструктур, автоматизация администрирования разнородных компонентов, мониторинг и управление делают киберсреду практически безграничной. В то же время для киберсреды