РЕЦЕНЗИЯ НА МОНОГРАФИЮ «КИБЕРБЕЗОПАСНОСТЬ ЦИФРОВОЙ ИНДУСТРИИ. ТЕОРИЯ И ПРАКТИКА ФУНКЦИОНАЛЬНОЙ УСТОЙЧИВОСТИ К КИБЕРАТАКАМ»

Юсупов Р.М.[1]

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[2], 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 кибербезопас-

2 Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Д. П. Зегжда, Е. Б. Александрова, М. О. Калинин, А. С. Марков и др. М.: Горячая линия – Телеком, 2019. – 560 с.

1 Юсупов Рафаэль Мидхатович, член-корреспондент РАН, доктор технических наук, профессор, научный руководитель СПИИРАН, Санкт-Петербург, Россия. E-mail: yusupov@iias.spb.su

ности 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.