Введение

Книга посвящена проблеме предотвращения компьютерных атак на технологическую инфраструктуру, к которой относятся автоматизированные системы управления технологическими процессами, системы Интернета вещей и киберфизические системы.

Интеграция физических и вычислительных процессов привела к развитию современных производственных технологий, видоизменив промышленные системы и сделав большую часть производства автономной от человека. Переход к цифровому производству открыл широкие возможности по реализации компьютерных атак на объекты производственной инфраструктуры. Вектор таких атак сместился в сторону несанкционированного воздействия и нарушения корректности функционирования промышленных объектов.

Компьютерные атаки затрагивают информационную инфраструктуру, в среде которой происходит выполнение физических процессов. Именно эта информационная среда и ее компоненты становятся объектами атак. Успешная реализация компьютерных атак способна привести к катастрофическим последствиям в связи с необратимостью физических процессов, реализуемых промышленными системами.

В таких условиях актуальной является комплексная и многоступенчатая задача предотвращения атак на промышленные системы. Автором предложен комплекс математических методов, обеспечивающих прогнозирование, обнаружение и нейтрализацию атак на промышленные объекты. Основу концепции составляют принципы, позволяющие обеспечить корректное функционирование системы в условиях деструктивных информационных воздействий, инвариантное к типу деструктивного воздействия, с автоматической саморегуляцией системой своего состояния при раннем обнаружении атаки.

В книге подробно освещаются математические аспекты прогнозирования и обнаружения компьютерных атак. Основным математическим аппаратом здесь являются временные ряды, сформиро-

ванные из значений параметров компонентов промышленных систем. Выбор аппарата временных рядов связан с тем, что значения параметров информационной инфраструктуры сложных промышленных систем характеризуют протекание физических процессов в системе. Как правило, большинство промышленных систем имеет выраженную целевую функцию, представляющую собой набор физических процессов, которые должны выполняться с определенной периодичностью и характеризоваться значениями параметров, находящимися в определенном диапазоне. Анализ поведения временных рядов, сформированных из значений таких параметров, позволяет обеспечить контроль реализации системой своей целевой функции.

Представленные методы анализа временных рядов связаны с обнаружением аномалий и прогнозированием значений временных рядов, в совокупности они обеспечивают раннее обнаружение кибератак и нежелательных тенденций, происходящих в системе.

Автор выражает искреннюю благодарность Д.П. Зегжде за внимательное прочтение рукописи, ряд ценных советов и предложений, рецензенту Р.М. Юсупову, рекомендации которого способствовали улучшению книги.

Особую благодарность выражаю П.Д. Зегжде за большую научную и методическую помощь в ходе подготовки рукописи.

Глубокую благодарность автор выражает П.А. Аверьяновой, Е.А. Зайцевой, А.А. Штыркиной, А.В. Ярмак, оказавшим существенную помощь в разработке математических методов обнаружения и предотвращения компьютерных атак и в проведении экспериментальных исследований эффективности разработанных методов.

Неоценимую помощь в подготовке рукописи к печати автору оказали Е.Б. Александрова и сотрудники ООО «Научно-техническое издательство «Горячая линия — Телеком».

Искренние слова благодарности за терпение и поддержку в течение написания рукописи я выражаю своей семье — родителям и мужу.