Математические методы и модели в обеспечении безопасности цифрового производства с использованием гомеостатического управления

М. А. Полтавцева[1], М. О. Калинин[2], Д. П. Зегжда[2], Е. Ю. Павленко[2]
Санкт-Петербургский политехнический университет Петра Великого
[1]poltavtseva@ibks.spbstu.ru, [2]max@ibks.spbstu.ru, [3]dmitry.zegzhda@ibks.spbstu.ru, [4]pavlenko@ibks.spbstu.ru

***Аннотация*. Изменения в управлении производственными системами, изменение характера и вида атак на них, привели к появлению новых требований к обеспечению информационной безопасности в промышленности. Так как описать полное множество атак на системы цифрового производства не представляется возможным, в работе предлагается новый подход к оценке безопасности таких систем, инвариантный к типу атаки. Авторы рассматривают подход к анализу состояния систем цифрового производства на базе самоподобия, а также предлагают фрактальные методы для математической оценки их защищенности. Устойчивость и гомеостатическое управление систем цифрового производства предлагаются в работе как основные подходы к обеспечению информационной безопасности.**

Ключевые слова: цифровое производство; математические методы в информационной безопасности; математические модели в информационной безопасности; гомеостатическое управление; безопасность цифрового производства

I. Особенности обеспечения безопасности цифрового производства

Цифровизация технологических отраслей деятельности, вызванная развитием Интернета вещей, сенсорных и облачных технологий, привела к видоизменению всей технологической инфраструктуры. Многие производственные и бизнес-процессы теперь реализуются интеллектуальными системами, которые являются не информационными, но киберфизическими системами (КФС), реализуя физические, реальные процессы путем имплементации информационных процессов [1]. Участники информационных процессов КФС – не люди, а «умные» устройства, способные осуществлять коммуникацию друг с другом и с окружающей средой, а также изменять свое состояние в соответствии с параметрами окружающей среды [2].

Широкие возможности по автоматизации технологических процессов стали триггером развития цифрового производства, открыв при этом широкие возможности для кибератак. Как показывает статистика, в 2017 году большинство атак на КФС было направлено на критические отрасли инфраструктуры, такие как энергетика, системы водоснабжения, транспортные объекты. При этом, в источнике [3] отмечается рост числа инцидентов безопасности во втором полугодии 2017 года по сравнению с первым полугодием.

Спектр атак на КФС крайне велик и описать их, в связи с чрезвычайно большим количеством возможных точек воздействия и zero-day уязвимостей, не представляется возможным, что осложняет решение задачи обеспечения безопасности систем цифрового производства. Помимо этого, следует отметить, что применение методов защиты, традиционных для информационных систем и сетей клиент-серверной архитектуры, не будет эффективным, как было показано ранее авторами в работах [4].

Данная работа расширяет научный задел авторов, посвященный разработке нового научного подхода к обеспечению безопасности КФС. Оценка безопасности КФС базируется на оценке самоподобия, поскольку в процессы КФС цифрового производства периодичны и практически не подвержены влиянию человека, таким образом, нарушение самоподобия их функционирования будет свидетельствовать о воздействии на них. Сохранение степени самоподобия процессов, реализуемых КФС, в определенных пределах, авторы предлагают называть обеспечением устойчивости управления системой к целенаправленным воздействиям. Свойство системы сохранять свое функционирование в заданном диапазоне входных и выходных характеристик в условиях целенаправленных деструктивных информационных воздействий называют киберустойчивостью [5].

В работах [6] авторами предложена гомеостатическая технология управления безопасностью КФС, она позволяет реализовать многоуровневое управление цифровым производством путем сочетания распределенного и централизованного иерархического управления, расширяющего число контуров управления и диапазон управляющих факторов. Для оценки состояния безопасности системы подход предполагает применение фрактальных показателей, учитывающих как

Исследование выполнено в рамках гранта Президента РФ для государственной поддержки ведущих научных школ Российской Федерации НШ-2992.2018.9 (Договор № 14. Y31.18.2992-НШ от 17.01.2018 г.).

информационную, так и функциональную составляющие, направленные на качество самоподобия системы. Самоподобие системы позволяет сохранить баланс в компенсации внешних факторов, что и составляет сущность гомеостатического управления. При этом, предложенные оценки самоподобия учитывают как долгосрочные зависимости в данных, проявляющиеся в периодичности на больших интервалах, так и краткосрочные зависимости, наблюдаемые на меньшем масштабе.

II. Фрактальные методы для оценки безопасности цифрового производства

Технологические процессы КФС цифрового производства могут быть рассмотрены как стационарные, то есть, как процессы, статистические свойства которых не меняются с течением времени [7]. Инвариантность характеристик позволяет предположить, что исследуемый технологический процесс обладает свойством фрактальности или самоподобия.

Значимость оценки самоподобия цифрового производства заключается в том, что любое нарушение корректности выполнения хотя бы одного процесса отразится в потоке данных, поскольку функционирование цифрового производства управляется посредством обмена информацией между ее компонентами. Поэтому предлагается обнаруживать киберугрозы, анализируя самоподобие временных рядов, сформированных из параметров компонентов КФС.

A. Оценка самоподобия на базе вычисления показателя Хёрста

Показатель Херста H – определяет степень самоподобия процесса. Чем ближе этот параметр к единице, тем более ярко проявляются фрактальные свойства [8], в то время как равенство H=0.5 свидетельствует об отсутствии самоподобия. В соответствии с источником [9], для вычисления значения коэффициента Херста может быть использована статистика нормированного размаха или R/S статистика. Для этого необходимо вычислить размах R ряда, представляющий собой разность между максимальным и минимальным значением ряда, и стандартное отклонение ряда S:

$$R = \max_{1 \le u \le N} \left(\sum_{i=1}^{u}(x_i - X_{cp})\right) - \min_{1 \le u \le N} \left(\sum_{i=1}^{u}(x_i - X_{cp})\right),$$

$$S = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i - X_{cp})^2},$$

где $X_{cp} = \frac{1}{N-1}\sum_{i=1}^{N} x_i$ представляет собой среднее арифметическое ряда наблюдений за N периодов. Тогда показатель Херста H вычисляется следующим образом: $H = log\frac{R/S}{log(\alpha N)}$, где α – заданная константа, α > 0.

B. Оценка самоподобия на базе вычисления мультифрактальных показателей

В работе [10] предложено использование фрактальных методов для оценки безопасности и контроля устойчивости функционирования киберфизической системы, так как протекаемые в КФС технологические процессы обладает свойством самоподобия, нарушение которого может свидетельствовать об отклонениях и аномалиях в системе.

В качестве эвристик, используемых для обнаружения аномалий в работе киберфизической системы, были выбраны следующие характеристики мультифрактального спектра, изображенного на рис. 1 [11]:

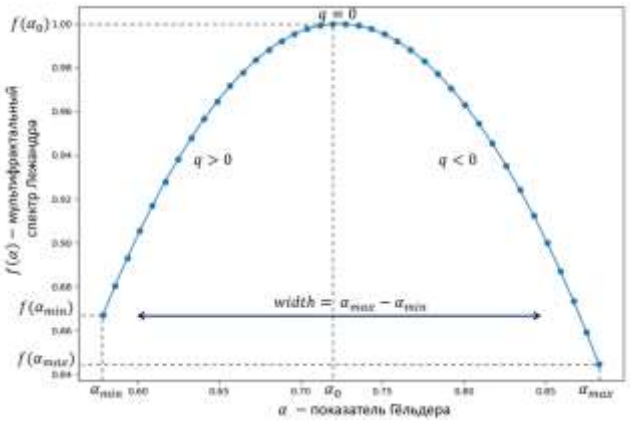

Рис. 1. Мультифрактальный спектр

- значение ширины спектра (*width*), вычисляемое по формуле $width = \alpha_{max} - \alpha_{min}$;
- значение показателя Гельдера в максимуме мультифрактального спектра α_0;
- значение ширины правой «ветви», вычисляемое по формуле $width_{right} = \alpha_{max} - \alpha_0$;
- значение ширины левой «ветви», вычисляемое по формуле $width_{left} = \alpha_0 - \alpha_{min}$;
- значение высоты левой «ветви», вычисляемое по формуле $high_{left} = f(\alpha_0) - f(\alpha_{min})$;
- значение высоты правой «ветви», вычисляемое по формуле $high_{right} = f(\alpha_{max}) - f(\alpha_0)$.

III. Экспериментальные исследования

A. *Исследуемая экспериментальная киберфизическая система*

В рамках исследования эффективности применения показателей безопасности и устойчивости для оценки состояния КФС в условиях целенаправленных внешних деструктивных воздействий была использована экспериментальная установка, организованная в Центре исследований кибербезопасности университета технологии и дизайна Сингапура [12]. Испытательный стенд реализует процесс очистки сточных вод, который условно можно разделить на шесть различных стадий: сбор и подготовка поступающих на сооружение сточных вод, предварительная обработка сточных вод, во время которой оценивается качество воды, ультрафильтрация и обратная промывка, дехлорирование, обратный осмос, сбор очищенной воды, обратная промывка и очистка (рис. 2).

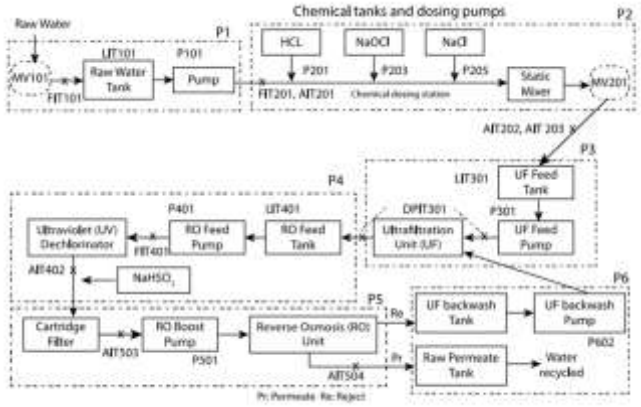

Рис. 2. Схема работы используемой экспериментальной КФС

В рамках каждого подпроцесса функционирует заданный набор устройств. Архитектура киберфизической системы включает в себя:

- сенсоры (расходомеры, датчики давления, уровня воды, анализаторы химических свойств воды и др.);
- актуаторы и другие исполнительные механизмы (моторные клапаны, насосы, дехлораторы и т.д.);
- логические контроллеры, отвечающие за управление исполнительными механизмами;
- сетевые устройства, а также ПЭВМ и рабочие станции, предназначенные для обработки и хранения данных, мониторинга и визуализации состояния системы.

Атакующие воздействия могут быть направлены как на отдельные компоненты одного подпроцесса, так и на компоненты в рамках нескольких подпроцессов. Интенсивность внешних воздействий определяется количеством и расположением элементов, компрометация которых ведет к успешной реализации атаки, и может ранжироваться следующим образом [12]:

- Воздействие на отдельный компонент в рамках одного этапа обработки (Single Stage Single Point, SSSP).
- Воздействие на несколько компонентов в рамках одного этапа обработки (Single Stage Multi Point, SSMP).
- Атака охватывает несколько этапов обработки, на каждом из которых осуществляется компрометация одного компонента (Multi Stage Single Point, MSSP).
- Атака охватывает несколько этапов обработки, на каждом из которых осуществляется компрометация нескольких компонентов (Multi Stage Multi Point, MSMP).

Набор анализируемых данных для каждого процесса функционирующей системы представляет собой многомерный временной ряд, образованный показателями датчиков, задействованных в текущем процессе. Для выявления киберугроз возможно использование показателя Херста, динамика изменения которого позволяет отследить нарушение самоподобия процесса (рис. 3).

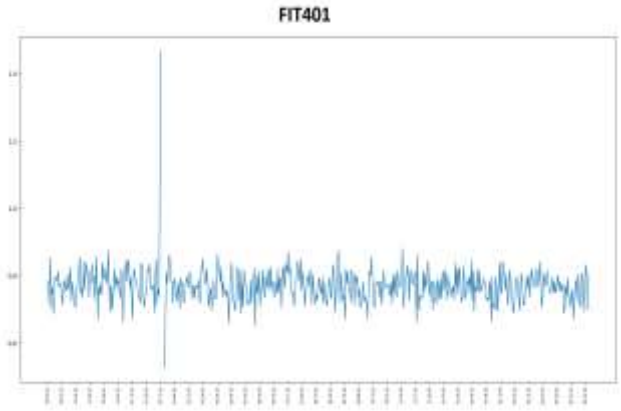

Рис. 3. Обнаружение атак на датчик FIT-401 с помощью анализа изменения показателя Херста

Анализ значений функции мультифрактального спектра позволяет сделать вывод об изменениях в структуре показателей датчиков. На рис. 4 представлены графики изменения ширины мультифрактального спектра, ширины и высоты левой «ветви» спектра для расходомера FIT-401, расположенного в блоке дехлорирования. На рис. 5 приведена динамика изменения параметров мультифрактального спектра (показатель Гельдера в максимуме спектра, ширина и высота правой «ветви» спектра) для датчика уровня воды LIT-301. Наличие выбросов и отклонений от медианных значений может свидетельствовать об атакующих воздействиях на конкретный компонент киберфизической системы. В частности, целенаправленное изменение текущих значений FIT-401 привело к отключению насоса, направляющего дехлорированную воду в блок обратного осмоса;

фальсификация значений LIT-301 стала причиной отсутствия воды в баке, повреждения насоса при первой атаке, а также переполнения бака – при второй атаке.

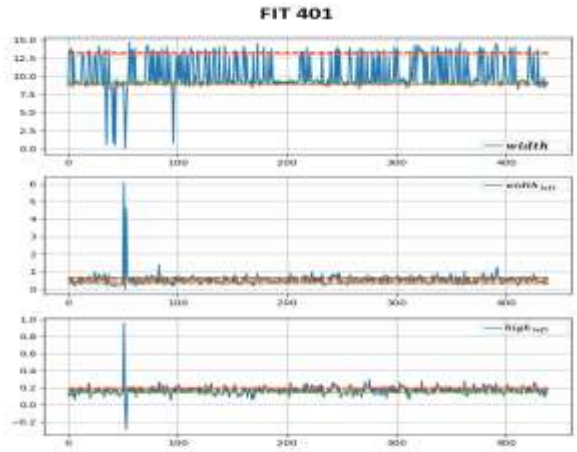

Рис. 4. Выявление атак на датчик FIT-401 с помощью характеристик мультифрактального спектра

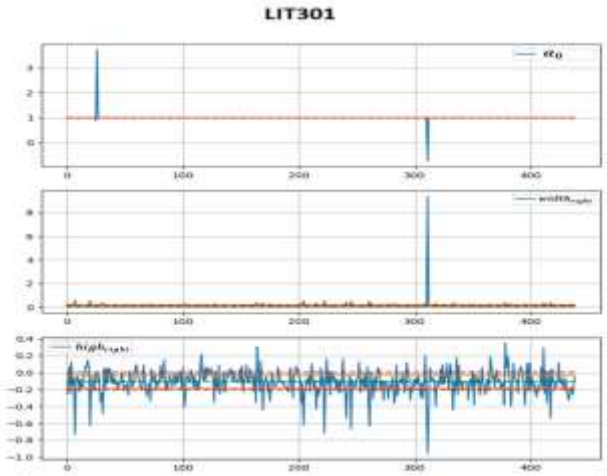

Рис. 5. Выявление атак на датчик LIT-301 с помощью характеристик мультифрактального спектра

IV. Заключение

В данной работе авторами был предложен математический аппарат, используемый для оценки безопасности систем цифрового производства. Анализ характерных особенностей и выявление инвариантности протекания технологических процессов, свойственной системам цифрового производства, позволяет применить фрактальные методы для обнаружения киберугроз и нарушения устойчивости киберфизической системы.

В качестве основных показателей, используемых для оценки устойчивости киберфизической системы, были выбраны коэффициент Херста и характеристики мультифрактального спектра. Проведенные экспериментальные исследования демонстрируют целесообразность и эффективность предложенных методов, а использование самоподобия технологических процессов для оценки безопасности является новым подходом, позволяющим осуществлять обнаружение киберугроз в сложных, гетерогенных системах цифрового производства.

Список литературы

[1] Зегжда П.Д., Полтавцева М.А., Лаврова Д.С. Систематизация киберфизических систем и оценка их безопасности// Проблемы информационной безопасности. Компьютерные системы. 2017. №2. С. 127-138.

[2] Лаврова Д.С. Подход к разработке SIEM-системы для Интернета Вещей // Проблемы информационной безопасности. Компьютерные системы. 2016. №2. С. 50-60.

[3] Kaspersky Lab ICS CERT. Ландшафт угроз для систем промышленной автоматизации, второе полугодие 2017. URL: https://ics-cert.kaspersky.ru/reports/2018/03/26/threat-landscape-for-industrial-automation-systems-in-h2-2017.

[4] Zegzhda D. P., Pavlenko, E. Y. Cyber-physical system homeostatic security management// Automatic Control and Computer Sciences, 51(8), 805-816.

[5] Zegzhda D. P. Sustainability as a criterion for information security in cyber-physical systems//Automatic Control and Computer Sciences. 2016. 50(8). P. 813-819.

[6] Зегжда Д.П., Павленко Е.Ю. Гомеостатическая стратегия безопасности киберфизических систем// Проблемы информационной безопасности. Компьютерные системы. 2017. № 3. С. 9-22.

[7] Lavrova D.S. An approach to developing the SIEM system for the Internet of Things // Automatic Control and Computer Sciences. 2016. №8. P. 673-681.

[8] Треногин Н. Г., Соколов Д. Е. Фрактальные свойства сетевого трафика в клиент-серверной информационной системе // Вестн. НИИ Сибир. гос. ун-та телекоммуникаций и информатики. 2003. №1. С. 163-172.

[9] Петров В.В., Платов В.В. Исследование самоподобной структуры телетрафика беспроводной сети // Радиотехнические тетради. 2004. № 30. С. 58-62.

[10] Зегжда Д.П., Павленко Е.Ю. Показатели безопасности цифрового производства// Проблемы информационной безопасности. Компьютерные системы. 2018 г. №2.

[11] Зегжда П.Д., Лаврова Д.С., Штыркина А.А. Мультифрактальный анализ трафика магистральных сетей интернет для обнаружения атак отказа в обслуживании//Проблемы информационной безопасности. Компьютерные системы. 2018 г. №2.

[12] Goh J. et al. A dataset to support research in the design of secure water treatment systems //International Conference on Critical Information Infrastructures Security, Springer, Cham.2016. P. 88-99.