УДК 004.056.53
doi:10.18720/SPBPU/2/id24-158

Алексеев Дмитрий Станиславович,
доцент, канд. техн. наук

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КИБЕРФИЗИЧЕСКОЙ СИСТЕМЫ НА ОСНОВЕ АНАЛИЗА ПАРАМЕТРОВ ФУНКЦИОНИРОВАНИЯ ЕЕ АППАРАТНОЙ ЧАСТИ

Россия, Кострома, ФГКВОУ ВО «Военная академия радиационной, химической и биологической защиты имени Маршала Советского Союза С.К. Тимошенко (г. Кострома)» Министерства обороны РФ,
d_alekseev@ksu.edu.ru

Аннотация. На концептуальном уровне предлагается модель обеспечения информационной безопасности киберфизической системы. Для защиты данных модель представляет собой систему, инвариантную к любой точке ее подключения в архитектуре киберфизической системы. С системных позиций сформулированы базовые требования к модели информационной безопасности. Представлена структурная модель обеспечения информационной безопасности киберфизической системы. Обнаружение несанкционированного воздействия определяется путем анализа отклонений косвенных признаков функционирования аппаратной части от их нормативных значений.

Ключевые слова: киберфизическая система, информационная безопасность, защита данных, мониторинг, система информационной безопасности.

Dmitry S. Alekseev,
Candidate of Technical Sciences (PhD), Associate Professor

ENSURING INFORMATION SECURITY OF CYBER-PHYSICAL SYSTEM ON THE BASIS OF ANALYZING PARAMETERS OF ITS HARDWARE FUNCTIONING

Military Academy of Radiation, Chemical and Biological Protection named after S.K. Timoshenko, Kostroma, Russia,
d_alekseev@ksu.edu.ru

Abstract. At the conceptual level, a model for ensuring information security of a cyber-physical system is proposed. For data protection the model represents a system invariant to any point of its connection in the architecture of cyber-physical system. Basic requirements to the information security model are formulated from the system positions. The structural model of information security of cyber-physical system is presented. Detection of unauthorized influence is determined by analyzing deviations of indirect signs of hardware functioning from their normative values.

Keywords: cyber-physical system, information security, data protection, monitoring, information security system.

Совершенствование методов несанкционированного доступа в киберфизические системы и стремительное развитие информационных технологий сохраняют до сих пор актуальной проблему обеспечения безопасности киберфизических систем [1].

Киберфизические устройства, с точки зрения информационной безопасности, нужно рассматривать как систему взаимодействующих между собой сервисов. Множество сервисов не является конечным и имеет тенденцию расширения своих элементов в течение жизненного цикла сложной технической системы. Особенно это характерно для современных производственных систем, где доля киберфизических систем существенно преобладает над организационно-техническими [2].

Информационные угрозы представляют собой явление однотипное, не обладающее уникальностью, практически всегда с одной и той же целью — нанесение ущерба процессам, которые поддерживаются соответствующими киберфизическими устройствами [3]. Поэтому необходимо выделить базовые принципы обнаружения и пресечения информационных угроз. При этом обеспечение информационной безопасности должно стать неотъемлемой частью проектирования киберфизических систем. Основная идея совершенствования информационной безопасности будет связана с использованием ее модели, инвариантной к месту его применения. Подобный подход может существенно снизить затраты на обработку данных, а также уменьшить стоимость средств защиты данных. Модель системы информационной безопасности киберфизических устройств, путем настройки или модификации, можно применять на любом уровне архитектуры к максимально большому количеству сервисов.

При функционировании киберфизических систем различают две условные группы потока данных. Первая группа — общий обезличенный поток данных, который связан с поддержкой функционирования технических и программных средств распределенных киберфизических устройств. Вторая группа — это выделенные из общего потока данные, поступающие в систему информационной безопасности (рис. 1).

Техническая реализация системы информационной безопасности киберфизических устройств предполагает ее функционирование на базе элементов аппаратной части. Среди таких устройств интерес для системы информационной безопасности представляют те, которые позволяют получать дополнительную информацию, отражающую поведение данных в выделенном потоке.

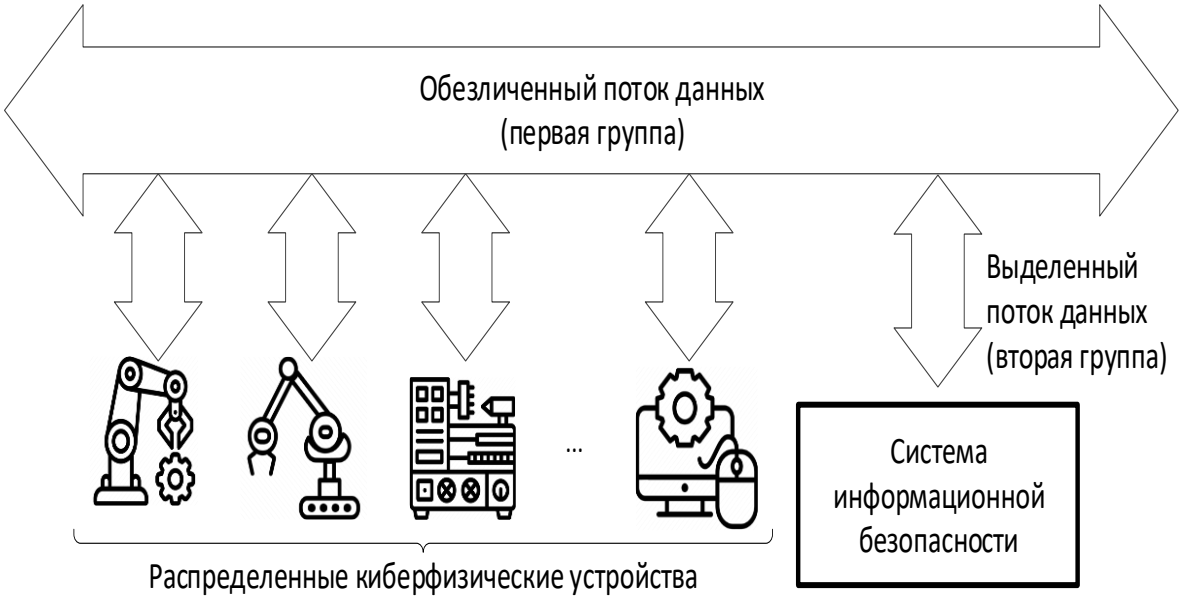

Рис. 1. Группы потоков данных киберфизической системы

В структуре модели системы информационной безопасности представлены аппаратные устройства (рис. 2), примерами которых являются процессор, оперативная память, порты ввода-вывода. То есть, изменение поведения потока данных регистрируется показателями функционирования этих аппаратных устройств компьютерной информационной системы. Показателями являются процент загруженности процессора, процент использованных байт оперативной памяти, количество полученных байт через сетевой адаптер. Эти показатели назовем косвенными признаками.

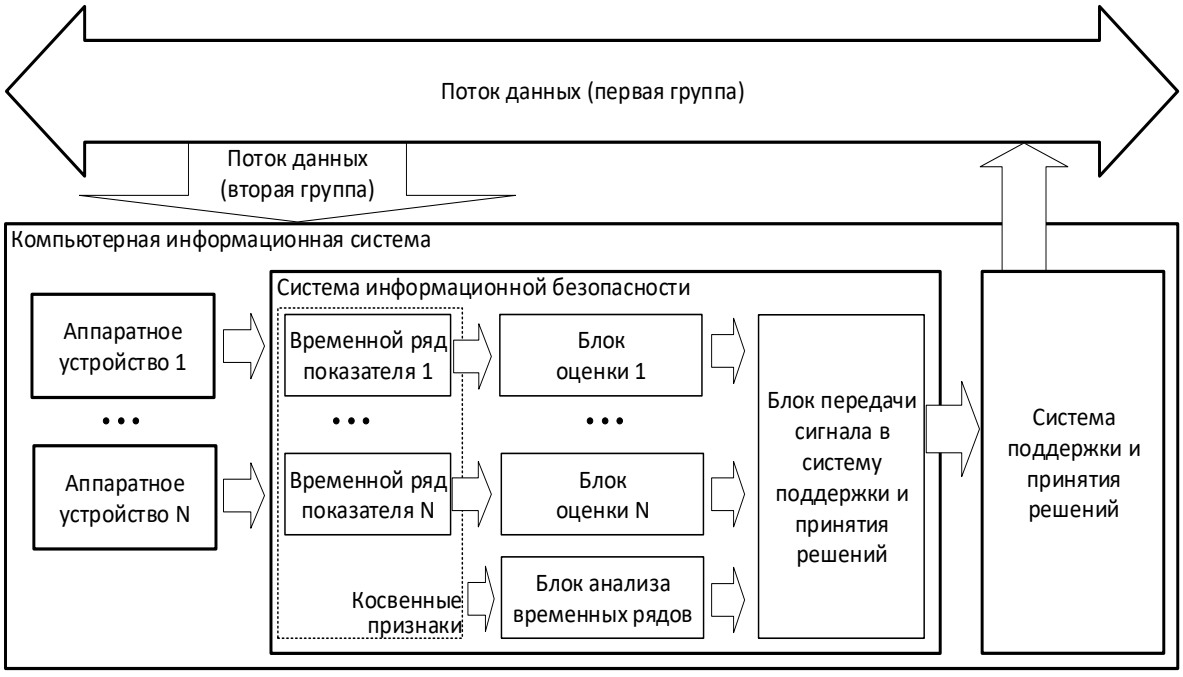

Рис. 2. Структура модели системы информационной безопасности

Продемонстрируем обработку косвенных признаков на примере показателя загрузки центрального процессора. Когда система функционирует в штатном режиме, то среднее значение процента загрузки центрального процессора имеет некоторую нормативную величину. Деструктивные процессы в киберфизической системе влияют на объем обрабатываемого потока данных в компьютерной информационной системе, что приводит к изменению процента загрузки процессора. Такие изменения регистрируются в показателях системы информационной безопасности.

Косвенные признаки используются для решения двух задач.

Во-первых, в системе информационной безопасности выполняется оценка показателей функционирования аппаратных устройств. Отклонение от нормативной величины показателей формирует в блоке передачи сигнала управляющие команды, соответствующие текущему состоянию киберфизической системы, для передачи в систему поддержки и принятия решений. Система поддержки и принятия решений создается известными способами с применением современных технологий [4, 5]. В настоящей работе внимание на функционирование системы поддержки и принятия решений не акцентируется.

Во-вторых, косвенные признаки используются для расчетов в блоке анализа временных рядов. Порядок обработки временных рядов требует отдельного пояснения с точки зрения системного подхода.

Информационные потоки, циркулирующие в киберфизических системах подвержены сезонным циклам. Это может быть связано с технологическими, экономическими, природными и иными циклами. Сущность анализа параметров функционирования аппаратной части компьютерной информационной системы заключается в детектировании отклонений, природой которых в распределенных киберфизических устройствах являются воздействия на элементы ввода данных с некоторой периодичностью. Будем предполагать, что потоки входных данных несут в себе признаки сезонности и представляют из себя некоторый колебательных процесс, вследствие чего первая группа потока данных представляет собой транспортную среду для волновых явлений.

Детектирование в компьютерной информационной системе волновых явлений из потока данных второй группы выполняется в блоке анализа временных рядов на основе алгоритмов быстрого преобразования Фурье с целью определения тактовых частот волновых процессов. При построении модели также исходим из того, что каждый детектируемый процесс компьютерной информационной системы имеет свою частотную и фазовую характеристики, которые могут существенно отличаться друг от друга и которые находят отражение в косвенных признаках функционирования элементов аппаратной части.

Фактически выполняется математическая обработка выборок временных рядов по известной формуле [6, 7] дискретного преобразования Фурье (1):

$$X_k = \sum_{n=0}^{N-1} x_n e^{-\frac{i2\pi}{N}kn}, \quad k = 0,\ldots,N-1, \tag{1}$$

где N — количество значений сигнала, измеренных за период;

x_n — измеренные значения сигнала в дискретных временных точках;

X_k — комплексные амплитуды синусоидальных сигналов, слагающих исходные сигналы (обозначают одновременно амплитуду и фазу);

$|X_k|/N$ — амплитуда k-го синусоидального сигнала;

$\arg(X_k)$ — фаза k-го синусоидального сигнала;

k — частота k-й синусоиды, измеренная в колебаниях за период.

Образец частного случая спектра выборки временного ряда данных при работе модели представлен на рисунке 3.

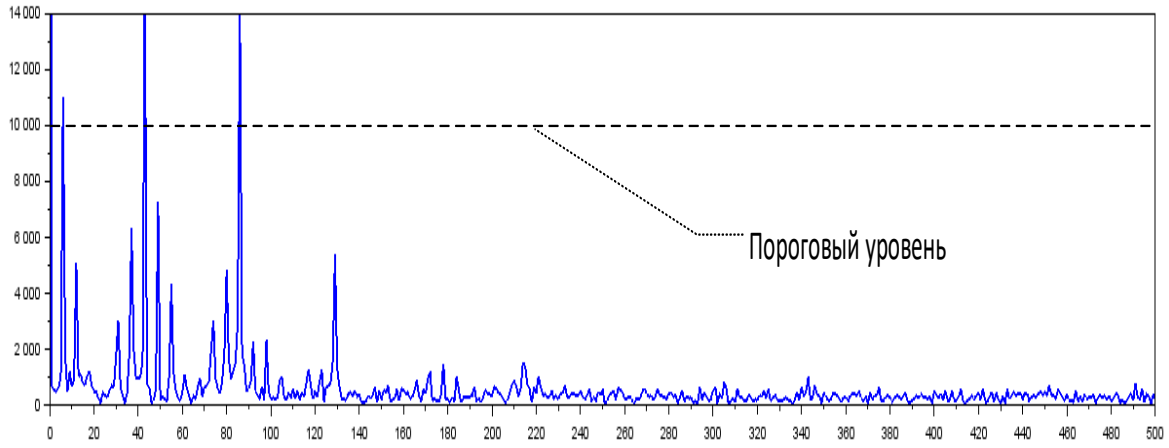

Рис. 3. Пример спектра временного ряда

Спектральный анализ выборок временных рядов позволяет получить сведения о тактовых частотах волновых колебаний, содержащихся в косвенных данных компьютерной информационной системы. В ходе расчетов выполняется сортировка показателей амплитуд спектра и выбирается ряд максимальных, ограниченных по количеству заданным заранее пороговым уровнем сигнала. Например, для амплитуды порогового уровня сигнала в 10000 единиц (см. рис. 3), ряд образуют три тактовые частоты волновых процессов с величинами 43, 84 и 7 Гц. Частоты приведены в порядке уменьшения их амплитуд. Рассчитанные параметры тактовых частот используются для формирования интерференционной картины (рис. 4).

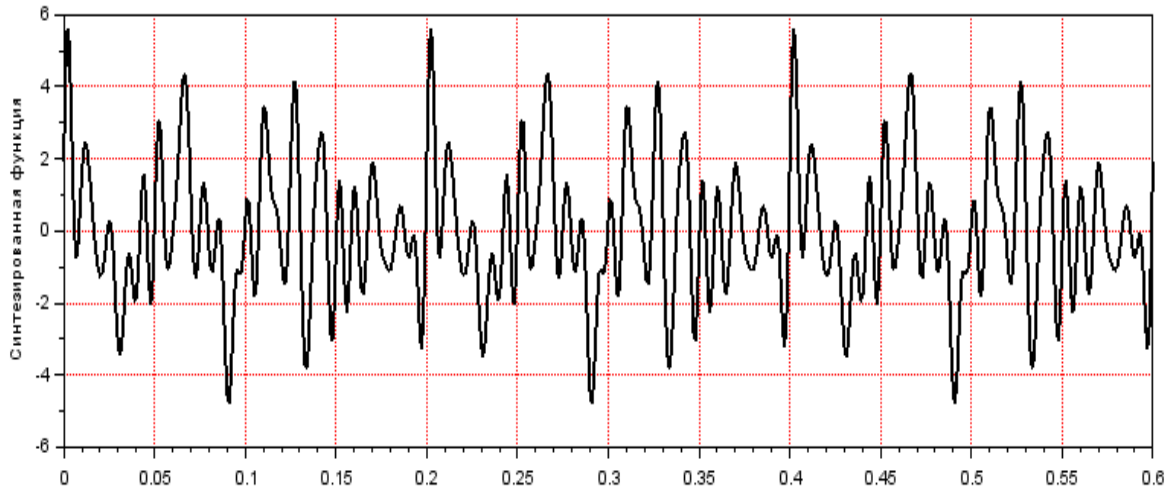

Рис. 4. Результат построения интерференционной картины на основе проведения вычислительных экспериментов

Области интерференционной картины, имеющие выраженные всплески и амплитуды сигналов более установленного уровня, помечаются как резонансы. Каждый резонанс регистрируется и для него фиксируется время и процессы, принявшие участие в его формировании. Полученный перечень резонансов и их параметров используется для определения и прогнозирования состояния киберфизической системы.

Анализ параметров функционирования аппаратной части киберфизической системы позволяет определить наличие в ней волновых процессов. Их интерференционная картина представляет сведения о периодах повышенной нагрузки при функционировании киберфизической системы. Компьютерная информационная система использует алгоритм обработки потоков данных, учитывает закономерности в их поведении, которые имеют предопределённые тренды и сезонности. Выработка управляющих воздействий компьютерной системой в центр принятия решений осуществляется в соответствии с настройками мониторинга потоков данных и нагрузок на систему. Система мониторинга может быть интегрирована в различные контуры управления и выбор сигналов управления определяется масштабом угроз.

Местоположение компьютерной информационной системы принципиального значения не имеет, предполагает универсальность применения на любом уровне архитектуры киберфизической системы и определяется исходя из решений технических проектов. Следует также отметить, что алгоритмы обработки любых потоков данных киберфизической системы будут одинаковыми и представлять собой инвариантную информационную систему.

Разработанное решение системы информационной безопасности соответствует всем принципам сложной системы. Система обеспечивает защиту от деструктивных воздействий, имеет четкую структуру и иерархию подсистем. За счет применения в системе поддержки и принятия решений технологий искусственного интеллекта система обладает свойствами, не присущими каждой подсистеме в отдельности. Устойчивые связи системы информационной безопасности обеспечивают формирование управляющих воздействий в контуре обратной связи.

Таким образом, предложено новое решение обеспечения информационной безопасности киберфизических систем. Оно связано с мониторингом косвенных признаков функционирования элементов аппаратной части, таким как процессор, оперативная память и порты ввода-вывода. Моделирование потоков данных и отражение их влияния на косвенные признаки показало возможность эффективного применения подобного способа.

Список литературы

1. Кушко Е.А., Грачёв Д.А., Паротькин Н.Ю., Золотарёв В.В. О вопросах безопасности киберфизических систем [Электронный ресурс] // Доклады ТУСУР. – 2022. – № 4. – URL: https://cyberleninka.ru/article/n/o-voprosah-bezopasnosti-kiberfizicheskih-sistem (дата обращения: 17.09.2023).

2. Иващенко А.В., Никифорова Т.В. Цифровизация организационной структуры управления производственным предприятием // Известия Самарского научного центра РАН. – 2021. – № 2. – URL: https://cyberleninka.ru/article/n/tsifrovizatsiya-organizatsionnoy-struktury-upravleniya-proizvodstvennym-predpriyatiem (дата обращения: 17.09.2023).

3. Ainslie S., Thompson D., Maynard S., Ahmad A. Cyber-threat intelligence for security decision-making: a review and research agenda for practice [Electronic Source] // Computers & Security. – 2023. – Vol. 132. – URL: https://doi.org/10.1016/j.cose.2023.103352 (date of access: 17.09.2023).

4. Щекочихин О.В., Алексеев Д.С., Шведенко В.Н. Архитектура интеллектуального модуля детектирования угроз при защите информации // Приборы и системы. Управление, контроль, диагностика. – 2017. – № 6. – С. 11–16. – EDN YZKCRV.

5. Rodriguez-Garcia P., Li Yu., Lopez-Lopez D., Juan A.A. Strategic decision making in smart home ecosystems: a review on the use of artificial intelligence and Internet of things // Internet of Things. – 2023. – Vol. 22. – DOI: https://doi.org/10.1016/j.iot.2023.100772.

6. Cerovecki C., Hörmann S. On the CLT for discrete Fourier transforms of functional time series // Journal of Multivariate Analysis. – 2017. – Vol. 154. – Pp. 282–295. – DOI: https://doi.org/10.1016/j.jmva.2016.11.006.

7. Галанина Н.А., Песошин В.А., Иванова Н.Н. Разработка и анализ поразрядных устройств дискретного преобразования Фурье // Вестник ЧГУ. – 2015. – №1. – URL: https://cyberleninka.ru/article/n/razrabotka-i-analiz-porazryadnyh-ustroystv-diskretnogo-preobrazovaniya-furie (дата обращения: 17.09.2023).