УДК 004.056

ОЦЕНКА И ОБЕСПЕЧЕНИЕ УСТОЙЧИВОСТИ УПРАВЛЕНИЯ КИБЕРФИЗИЧЕСКИМИ СИСТЕМАМИ В УСЛОВИЯХ КОМПЬЮТЕРНЫХ АТАК

Д.П. Зегжда
Санкт-Петербургский политехнический университет Петра Великого
Россия, 195251, Санкт-Петербург, Политехническая ул., 29
E-mail: dmitry@ibks.spbstu.ru

Е.Ю. Павленко
Санкт-Петербургский политехнический университет Петра Великого
Россия, 195251, Санкт-Петербург, Политехническая ул., 29
E-mail: pavlenko@ibks.spbstu.ru

Ключевые слова: киберустойчивость, киберфизическая система, устойчивость управления, информационная безопасность.

Аннотация: В данной статье авторами предложен подход к оценке устойчивости управления киберфизическими системами. Устойчивость предлагается использовать для расширения понятия информационной безопасности применительно к специфической предметной области киберфизических систем. Авторы определяют устойчивость как способность системы к корректному функционированию в условиях компьютерных атак. Для оценки устойчивости используется графовое представление системы, на основе которого вычисляется показатель избыточности рабочих маршрутов. Также предложен подход к обеспечению устойчивости управления киберфизическими системами в условиях компьютерных атак на основе динамического изменения работы цифровых систем управления.

1. Введение

Развитие интеллектуальных цифровых технологий и их внедрение в промышленные объекты привело к появлению систем нового типа – киберфизических систем (КФС), в которых физические промышленные процессы реализуются путем обмена управляющими сигналами между интеллектуальными компонентами системы (датчиками, сенсорами, актуаторами, контроллерами и т.п.). Цифровизация технологической инфраструктуры привела к доступности КФС и их компонентов из сети Интернет, что открыло широкие возможности для реализации компьютерных атак [1, 2].

Задача обеспечения информационной безопасности (ИБ) таких систем усложняется: для КФС характерны атаки, цель которых – получение возможности управления работой системы и реализуемыми в ней физическими процессами, а не нарушение конфиденциальности, целостности или доступности информации. Выход физических процессов из-под контроля может привести к катастрофическим последствиям, что делает задачу обеспечения ИБ КФС актуальной [3-7].

Существующие научные исследования в основном направлены на адаптацию методов и средств, применяемых в информационных системах, для использования в КФС. Однако такой подход не всегда может быть успешно применен, ввиду ряда особенностей, представленных в работе [8], а также в связи с тем, что для КФС, по аналогии с живой природой, реализация физических процессов, формирующих целевую функцию промышленной системы, является более приоритетной задачей, чем поддержание корректности функционирования каждого ее компонента в отдельности. Поэтому предлагается расширение понятия ИБ для КФС понятием устойчивости, в данном контексте представляющим собой способность КФС к корректному функционированию в условиях компьютерных атак [9,10].

2. Постановка задачи

С точки зрения обеспечения ИБ, КФС представляют собой новый объект, специфика которого – в объединении технологической составляющей системы, реализующей физические процессы, и информационной составляющей, задача которой – обеспечение цифрового управления той информационной средой, в рамках которой реализуются физические процессы. Уровень физических процессов характеризуется неизменностью состава и избыточностью компонентов. Уровень цифровых систем управления представлен информационными системами и сервисами, которые обеспечивают как функции нормальной эксплуатации (управление уровнем технологических процессов), так и функции обеспечения информационной безопасности [11].

В силу того, что цифровые системы управления подвержены киберугрозам, а обеспечить их безопасность за счет изоляции, контроля целостности и т.д. в реальных КФС практически невозможно, предлагается добавить к информационной составляющей КФС систему обеспечения устойчивости цифровых систем управления к компьютерным атакам. Задача такой системы заключается в мониторинге параметров информационной составляющей КФС и изменении работы цифровых систем управления для сохранения корректной информационной среды реализации физических процессов. Следовательно, необходимо разработать подход, обеспечивающий устойчивость управления КФС в условиях компьютерных атак, реализующий защиту от кибератак на цифровые системы управления.

В основу разрабатываемого подхода предлагается положить принцип избыточности ресурсов на уровне физических процессов и гибкость управления на уровне цифровых систем управления. Избыточность ресурсов на уровне физических процессов обеспечит широкие возможности по замене атакованных или вышедших из строя компонентов КФС, сигнализирующих о том, как протекает работа системы (сенсоров, актуаторов, контроллеров). Гибкость управления на уровне цифровых систем управления позволит оперативно вносить изменения в информационную среду реализации физических процессов, обеспечивая способность КФС к работе даже в условиях компьютерных атак.

Подход должен выполнять оценку устойчивости КФС к компьютерным атакам, что означает необходимость определения, при каких последствиях компьютерных атак система сможет продолжать реализовывать цифровое управление физическими процессами. В случае если система не обладает достаточной устойчивостью, необходимо реализовать управляющее воздействие цифровой системой управления так, чтобы обеспечить необходимую устойчивость.

3. Оценка устойчивости управления КФС к компьютерным атакам

Для формализации решаемой задачи используем теорию графов и перейдем к графовому представлению КФС. КФС может быть представлена в виде графа $G =< V, E >$, где: $V = \{v_1, v_2, \dots, v_k\}$ – множество вершин графа, которые представляют собой компоненты КФС, а $E = \{e_1, e_2, \dots, e_p\}$ – множество ребер, служащих для описания межкомпонентных связей КФС. Под межкомпонентными связями следует понимать обмен компонентов КФС управляющими сигналами.

Пусть $R = \{S_{ij}\}$ – множество всех возможных маршрутов на графе G, элементы которого представляют собой совокупность различных путей из вершины v_i в вершину v_j. Тогда любой физический процесс, направленный на выполнение целевой функции КФС, есть набор маршрутов $R' \subseteq R$ на множестве всех маршрутов на графе G, что в функциональном смысле представляется набором функций $F = \{f_1, f_2, \dots, f_t\}$, ассоциированным с вершинами графа.

В соответствии с введенными выше обозначениями, любой физический процесс $R_i \in R'$, направленный на выполнение целевой функции КФС, может быть описан в функциональном смысле как последовательность функций $R_i^F = \{f_z, f_x, \dots, f_l\}$ или же как последовательность вершин графа $R_i^V = \{v_n, v_m, \dots, v_q\}$, которые обладают возможностью реализации необходимой функции.

Устойчивость управления КФС напрямую зависит от избыточности рабочих маршрутов: чем больше существует запасных рабочих маршрутов, тем более устойчива КФС к кибератакам, результатом которых в терминах введенного графового представления является удаление ребер или удаление вершин. Таким образом, устойчивость цифрового управления КФС к компьютерным атакам может быть определена в виде отношения числа рабочих маршрутов R' к общему число вершин V.

4. Обеспечение устойчивости управления КФС в условиях компьютерных атак

Обеспечение устойчивости КФС предлагается реализовывать посредством применения управляющего воздействия на цифровую систему управления за счет изменения параметров работы компонентов, задействованных в реализации физических процессов, или изменения связей между компонентами информационной среды, в рамках которой реализуются эти процессы.

Изменение связей может проявляться как в создании новых, так и в удалении существующих. Создание новых связей происходит при кооперации компонентов КФС с целью принятия и перераспределения функций, выполняемых компонентом, безопасность которого нарушена. Удаление связей происходит при компрометации или выходе компонента из строя: очевидно, что через данный компонент либо опасно с точки зрения безопасности продолжать отправку управляющих команд и значений параметров, либо это неэффективно, поскольку компонент не работает и не сможет ни интерпретировать данные, ни передать их другим компонентам для дальнейшей обработки.

Корректировка логики протекания процесса в терминах графовой модели означает изменение рабочего маршрута, характеризующего физический процесс, реализуемый КФС. Это может происходить в случае, если какой-либо из компонентов системы вышел из строя или был скомпрометирован, или если из строя вышла целая подсистема.

Однако для применения подхода к обеспечению устойчивости граф должен обладать высокой связностью, а также избыточностью по всем типам компонентов КФС. Исследование устойчивости графа, моделирующего КФС, показало, что граф, имеющий большое число вершин, которые могут быть задействованы при построении рабочих маршрутов, характеризующих физические процессы, необходимые для реализации целевой функции КФС, будет устойчивым к компьютерным атакам, в том числе, к атакам, в результате которых происходит разрыв связи между компонентами системы (рисунок 1). Таким образом, избыточность системы позволит повысить ее устойчивость к компьютерным атакам.

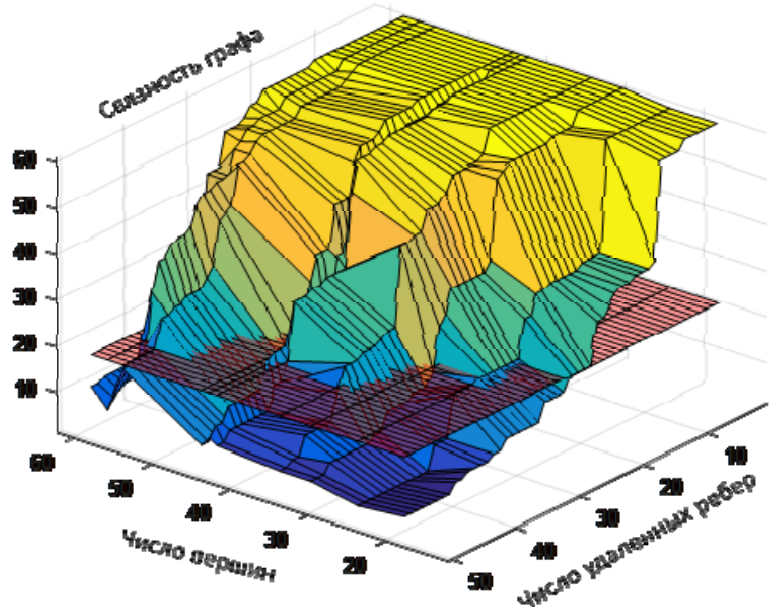

Рис. 1. Граф зависимости устойчивости графа от количества вершин и числа удаленных ребер.

Также для всех компонентов системы, которых должно быть избыточное количество, должна быть обеспечена возможность взаимодействия и коммуникации (что на практике может быть осложнено тем, что устройства разработаны разными производителями и используют различные протоколы коммуникации).

5. Заключение

Предложен подход к оценке устойчивости управления киберфизическими системами в условиях компьютерных атак на основе вычисления показателя избыточности рабочих маршрутов. Также предложен подход к обеспечению устойчивости управления киберфизическими системами в условиях компьютерных атак на основе динамического изменения работы цифровых систем управления. Предложенные подходы являются универсальными, так как в их основе лежит общее графовое представление киберфизических систем.

Исследование выполнено в рамках гранта Президента РФ для государственной поддержки ведущих научных школ Российской Федерации НШ-2992.2018.9 (соглашение 075-02-2018-504).

Список литературы

1. Лаврова Д.С. Подход к разработке SIEM-системы для Интернета Вещей // Проблемы информационной безопасности. Компьютерные системы. 2016. № 2. С. 50-60.
2. Полетыкин А.Г., Жарко Е.Ф., Менгазетдинов Н.Э., Промыслов В.Г. Новое поколение систем верхнего уровня и концепция Industry 4.0 // Управление развитием крупномасштабных систем MLSD'2017. 2017. С. 101-107.
3. Менгазетдинов Н.Э., Полетыкин А.Г., Промыслов В.Г. Новые кибернетические угрозы и методы обеспечения кибербезопасности в цифровых системах управления // Энергетик. 2012. № 7. С. 18-23.
4. Зегжда Д.П., Павленко Е.Ю. Гомеостатическая стратегия безопасности киберфизических систем // Проблемы информационной безопасности. Компьютерные системы. 2017. № 3. С. 9-22.
5. Зегжда П.Д., Зегжда Д.П., Павленко Е.Ю. Гомеостатическая стратегия управления безопасностью киберфизических систем // Материалы 26-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 2017. С. 51-52.
6. Зегжда Д.П., Павленко Е.Ю. Показатели безопасности Цифрового Производства // Проблемы информационной безопасности. Компьютерные системы. 2018. № 2. С. 118-130.
7. Павленко Е. Ю. Обеспечение безопасности киберфизических систем с использованием принципа гомеостаза // Материалы 27-й научно-технической конференции «Методы и технические средства обеспечения безопасности информации». 2018. С. 94-95.
8. Зегжда Д.П. Устойчивость как критерий информационной безопасности киберфизических систем // Проблемы информационной безопасности. Компьютерные системы. 2016. № 2. С. 13–18
9. Зегжда Д.П., Павленко Е.Ю. Обеспечение киберустойчивости программно-конфигурируемых сетей на основе ситуационного управления // Проблемы информационной безопасности. Компьютерные системы. 2018. № 1. С. 160-168.
10. Зегжда Д.П., Павленко Е.Ю. Обеспечение устойчивости функционирования киберфизических систем на основе динамического переконфигурирования // Проблемы информационной безопасности. Компьютерные системы. 2018. № 4. С. 130-139.
11. Бабаев Д.И., Полетыкин А.Г., Промыслов В.Г., Тимофеев М.Ю. Управление архитектурой кибербезопасности АСУ ТП атомных электростанций // Проблемы управления. 2018. № 3. С. 47-55.