УДК 004.056.2

ВЫЯВЛЕНИЕ НАРУШЕНИЙ СОДЕРЖАТЕЛЬНОЙ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ В КИБЕР-ФИЗИЧЕСКОЙ СИСТЕМЕ В СЛУЧАЕ НЕПОЛНОТЫ ДАННЫХ

Мариненков Е.Д. (федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)
Научный руководитель – к.т.н., Викснин И.И.
(федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

Аннотация. В работе представлен подход к обеспечению защищенного информационного взаимодействия элементов киберфизической системы, основанный на комбинации показателей репутации, доверия и истинности, и теории. Формирование показателей доверия, репутации и истинности позволяет выявлять и противодействовать "мягким «атакам, которые не могут быть выявлены классическими методами, подходами и механизмами обеспечения информационной безопасности. Представленный подход позволяет формировать данные показатели при неполноте данных на основе теории игр. В работе приведены результаты компьютерного моделирования и сравнение эффективности представленного метода.

Введение.

Существуют различные виды атак на данные, передаваемые между элементами в системе. Атаки могут быть как пассивные, когда злоумышленником не оказывается прямого влияния на систему, так и активные, когда в ходе атаки происходит несанкционированная модификация информационных активов, свойств системы, её состояния. В качестве средств противодействия атакам могут быть использованы различные средства защиты, обеспечивающих конфиденциальность, целостность и доступность информации. Однако, существуют атаки, когда уже авторизованные в системе, изначально считающиеся легитимными элементы начинают передавать недостоверные данные по причине сбоев в системе, отказов устройств или несанкционированного вмешательства в программно-аппаратные составляющие. Использование этих неверных данных для оптимизации групповых действий может привести к снижению эффективности работы системы или, в крайнем случае, к нанесению ущерба людям. Такие атаки на содержательную целостность информации получили в литературе название "мягких" атак. Для противодействия "мягким" атакам на киберфизические системы (КФС) может быть использован подход с использованием показателей репутации и доверия. В настоящей работе автор затрагивают проблему нарушения содержательной целостности данных в группе мобильных роботов и предлагает модель обнаружения подобных нарушений, основанную на показателях доверия и репутации с использованием элементов теории игр.

Основная часть.

В подходе используются показатели истинности, репутации и доверия, которые позволяют оценить передаваемые между элементами данные и сформировать решение о доверии или не доверии элементу, передающему данные. Далее будут приведены определения формируемых показателей.

Истинность – показатель, отображающий субъективную оценку переданных данных другими элементами. Корректность определяется с помощью устройств физического уровня КФС или при общении с другими доверенными элементами.

Репутация – показатель, основанный на ретроспективе оценки истинности каждого из элементов, позволяющий определять элементам легитимность других в рамках системы. Репутация рассчитывается таким образом, чтобы показатель линейно возрастал в случае определения допустимого значения истинности и экспоненциально убывал в обратных случаях.

Доверие – показатель, характеризующий субъективную оценку поведения элемента другими элементами. Вычисляется на основе комбинации истинности и репутации и позволяет сформировать конечную оценку элемента.
В качестве ограничения каждый из вышеперечисленных показателей находится в отрезке [0;1].
Существующим недостатком описанного подхода является формирование показателя истинности в случае неполноты данных – когда элемент не может оценить информацию посредством своих устройств и не имеет возможности получить оценку от других доверенных элементов. В подобных подходах в этом случае используется показатель равный 0,5.
Автором была представлена данная ситуация в виде игры, где есть два игрока: элемент, передающий информацию (U) и элемент, принимающий и оценивающий информацию (G).
У игрока U существует две стратегии: передать неверные данные или передать верные данные. У игрока G также существуют две стратегии: принять данные как верные или не принимать данные и использовать уже имеющиеся. Учитывая, что максимальный выигрыш игрок G получит, когда примет верные данные, а игрок U – когда игрок G примет неверные данные, получим равновесие Нэша в исходе, когда игрок G не примет данные, а игрок U соврет. Таким образом было принято формировать показатель истинности в подобных ситуациях равный 0.

Выводы.
Описанный подход был внедрен в разработанный ранее симулятор и сравнен с подходом без использования теории игр. Моделирование показало, что подход с использованием теории игр повышает точность решений элементов на 1%, правильно-истинные решения в 4.5 раз и снижает ошибку второго рода в 7.7 раз. Также результаты показали, что ошибка первого рода возрастает в 12,3 раз, что говорит о том, что данный подход необходимо доработать. Дальнейшие исследования будут связаны с внедрением вероятностей при формировании матрицы платежей, что позволит снизить ошибку первого рода.