УДК 004.056

МОДЕЛЬ ЗАЩИЩЕННОГО ВЗАИМОДЕЙСТВИЯ КОМПОНЕНТОВ ЦИФРОВОГО ПРЕДПРИЯТИЯ

Мыськив И.И. (Университет ИТМО)
Научный руководитель – доцент, к.т.н. Заколдаев Д.А.
(Университет ИТМО)

Аннотация. На основе структуры типового Цифрового предприятия представлена графовая модель, также рассматривается обеспечение семантической целостности информации киберфизических систем Цифрового предприятия на основе модели безопасности использующих такие характеристики как доверие, репутацию и истинность для расчета оценки информации, и принятия решения о взаимодействии компонентов друг с другом.

Введение. Развитие научно-технического прогресса в области проектирования и производства изделий приводит нас к появлению нового подхода в организации технологических процессов, направленных на изготовление и разработку необходимого продукта и использования передовых решений и технологий:

- киберфизических систем (далее – КФС);
- интернета вещей (далее – IoT);
- облачные технологии;
- технологии сбора и обработки больших массивов производственных данных, аддитивные технологии и др.

Объединение всех этих решений в единую экосистему технологического цикла производства позволяет использовать алгоритм (бесшовного) технологического процесса автоматизированного изготовления изделий на Цифровых предприятиях (далее – ЦП).

Использование большого числа таких сложных гетерогенных распределенных информационных систем и взаимодействию их с физическим миром, значительно увеличивает риски, ландшафт угроз и вектора атак на информационную инфраструктуру предприятия, а успешная реализация деструктивных воздействий, направленных на нарушение целостности, доступности и конфиденциальности, способна привести не только к экономическому ущербу, но также к техногенным и экологическим катастрофам.

Также предприятия такого типа часто являются объектами критической информационной инфраструктуры и соответственно должны выполнять требования Федерального закона №187 «О безопасности критической информационной инфраструктуры Российской Федерации от 26 июля 2017 года», что говорит о важности в обеспечении безопасности предприятий подобного типа.

Цель. Для решения задачи обеспечения защиты семантической целостности от деструктивного информационного воздействия (далее – ДИВ) необходимо обеспечить защищенное информационное взаимодействие между компонентами, для достижения ими заданного состояния.

Для обеспечения защищенного информационного взаимодействия рассмотрим использование доверительной модели на основе оценки репутации, истинности и доверия Суть данной модели заключается в определении уровня доверия компонента-субъекта к компоненту-объекту. Также одной из ключевых особенностей этой доверительной модели заключается в том, что данную систему невозможно разрушить, так как отсутствует единый центр управления этой системой. Данный подход можно улучшить с помощью модели полицейских участков, суть модели полицейских участков заключается в разделении системы на отдельные участки в котором есть управляющий компонент отвечающий за безопасность своего выделенного участка.

Заключение. В данной работе предложена графовая модель ЦП описывающая различные типы компонентов, параметры и связи между ними. В части обеспечения

защищенного информационного взаимодействия была рассмотрена модель обеспечения семантической целостности информации на основе доверительной модели.

Низкий уровень доверия, не позволит компоненту-нарушителя оказывать ДИВ на принятие решений по достижению заданного стояния компонента, также если нарушитель захочет повысить уровень доверия компонента-нарушителя, то действия по повышению уровня доверия будут предполагать достижение заданного состояния, что нецелесообразно для нарушителя.

Мыськив И.И. (автор) Подпись

Заколдаев Д.А. (научный руководитель) Подпись