носителей. Получены условия, определяющие целесообразность с точки зрения величины среднего времени восстановления разрушенных данных использования в распределенных системах неразрушенного ОР или АМН в качестве восстановительного резерва.

Работа выполнена в рамках темы: «Фундаментальные исследования по направлению «Модели, методы анализа и синтеза структуры и сценариев развития социально-экономических и технических систем управления, повышения их управляемости и безопасности функционирования в условиях неопределенности, структурных возмущений и чрезвычайных ситуаций» № 0052-2019-0011

Литература:

1. *Сомов С.К.* Сохранность информации в распределенных системах обработки данных. – М.: ИПУ РАН, 2019. – 254 с.

2. *Микрин Е.А., Сомов С.К.* Анализ эффективности стратегий восстановления информации в распределенных системах обработки данных // Информационные технологии и вычислительные системы. – 2016. – №3. – С. 5-19.

3. *Клейнрок Л.* Вычислительные системы с очередями. – М.: Мир, 1979. – 600 с.

Правиков Д.И.

Концепция информационной безопасности «роя» киберфизических систем

Аннотация: На основании анализа существующих подходов сделан вывод о необходимости разработки для комплексов киберфизических систем новых подходов к обеспечению их информационной безопасности. Показано, что комплекс киберфизических систем может быть описан как множество взаимодействующих прикладных программ. Для обеспечсения свойства незамкнутости комплекса киберфизических систем предложено управление безопасностью перенести в распределенный реестр, а определение санкционированности действий осуществлять на основании алгоритма консенсуса.

Ключевые слова: киберфизическая система, информационная безопасность, распределенный реестр, алгоритм консенсуса

Существующие теории информационной безопасности в основном построены на замкнутости защищаемых систем. При этом в основе наиболее распространенных методов обеспечения безопасности (моделей разграничения доступа) лежит субъекто-объектная теория, описанная, например, в [1]. Указанный подход очень хорошо подходит для обеспечения безопасности в автоматизированных информационных системах, предназначенных для хранения и обработки данных, но, как показывает практика, не вполне применим для киберфизических систем, где основной задачей является техническое управление.

В настоящее время обеспечение информационной безопасности киберфизических систем (как комплексов кибефизических устройств), являются предметом изучения и рассмотрения различных научных коллективов [2]. При этом современные тенденции, идущие от практики, показали появление таких подходов, как архитектура «с нулевым доверием», описанная в NIST Special Publication 800-207 Zero Trust Architecture, для которой существуют описанные подходы к обеспечению безопасности, но они не имеют соответствующего теоретического обоснования.

Возможное решение, основанного на использовании существующих теоретических разработо, было положено в основу изобретения [3], в соответствии с которым в «одноранговых коммуникационных сетях киберфизических устройств, включающем управление настройками маршрутизации, дополнительно вводят блок осуществления политики безопасности, в котором формируют правила политики безопасности в виде матрицы доступа между киберфизическими устройствами, получают запросы на сетевой доступ между киберфизическими устройствами, формируют и пересылают киберфизическим устройствам управляющие команды, внося изменения в их таблицы маршрутизации и тем самым определяя разрешенные правилами политики безопасности маршруты пересылки пакетов от одного устройства к другому».

Вместе с тем, предложенное изобретение, на наш взгляд, имеет ряд существенных ограничений. Попытки преодолеть недостатки

были предприняты, например, в [4], где предложена графовая модель функционирования промышленной системы (ПС), которую можно рассматривать как один из вариантов представления комплекса киберфизических устройств. Данная модель описывает сетевую инфраструктуру ПС в виде ориентированного графа G, множество вершин $V = \{v_1, \dots, v_N\}$ которого характеризует все компоненты ПС, способные к сетевому взаимодействию. Множество дуг $E = \{e_1, \dots, e_M\}$ графа отражает все возможные межкомпонентные связи, проявляющиеся как обмен данными между устройствами. Каждый компонент ПС, моделируемый вершиной v_i, характеризуется набором функций, которые он способен реализовывать.

Упомянутая работа [4] интересна тем, что компьютерные атаки описаны в виде преобразований графа G. Они разделяются на структурные, представляющие собой унарные операции над G, и функциональные, заключающиеся в изменении параметров вершин и дуг.

Полное перечисление возможных видов атак на промышленную систему представлено в работе [5], в которой все возможные атаки сведены к набору элементарных действий.

Таким образом, проведенный обзор литературы показывает, возможность описания комплекса киберфизических устройств в виде набора взаимодействующих прикладных программ.

Тогда, пусть у нас существует комплекс киберфизических устройств, работу которого мы считаем безопасной. Для него справедливы следующие постулаты.

Постулат 1. В созданном комплексе киберфизических устройств набор прикладных программ является взаимоувязанным, что подразумевает, что выход одной прикладной программы является входом для другой. Если прикладная программа получает данные извне, то эти данные являются входными для всего комплекса. Если у данных, генерируемых программой нет потребителя, то эти данные являются выходом всего комплекса.

Постулат 2. Любая прикладная программа, находящаяся на одном из киберфизических устройств, объединенных в комплекс, не может иметь входного потока данных, кроме как входного потока для всей системы или от другой прикладной программы, зарегистрированной в комплексе.

Постулат 3. Любая прикладная программа направляет свои данные для другой прикладной программы, зарегистрированной в комплексе, либо на выход всего комплекса, описанный и заданный извне.

Исходя из описанных постулатов можно утверждать, что изменение комплекса киберфизических устройств, приводящее к нарушению 1, 2 или или 3, нарушает безопасность всего комплекса.

Вместе с тем, перечисленный в работе [5] перечень элементарных действий характерен и для штатной модернизации системы. В результате, если руководствоваться только тремя постулатами, будут выявляться воздействия на систему, обнаруживаемые, условно говоря, на уровне противоаварийной защиты. Более сложным случаем является, например, атака MiM, сходная в плане своей реализации со штатной модернизацией системы. Таким образом, задача выявления атак сводится к задаче различения администрирования от несанкционированного воздействия, при условии того, что объект, реализующий положения упомянутой Аксиомы 2 должен находиться за пределами отдельного киберфизического устройства.

Решение данной задачи предлагается осуществлять на основании подхода, определяющего санкционированность или несанкционированность совершаемых действий. Действие, в том числе элементарное, считается санкционированным, если запрос на его реализацию подтверждается всеми сторонами. Применительно к рассматриваемому случаю это будет означать, что совершенное действие получило подтверждение от администратора (в роли которого может выступать автоматическая система администрирования или искусственный интеллект), а также от других киберфизических устройств, перестраивающих свой информационный обмен. В результате запрос на изменение потока данных должен получить подтверждение, выработанное на основании некоего алгоритма консенсуса. Это, в свою очередь (пока теоретически) приводит к тому, что потенциальный злоумышленник при реализации атаки MiM должен инициировать получение подтверждений уже от нескольких источников, что существенно усложняет саму атаку.

В этом случае подключение нового устройства к уже существующему комплексу планируется проводить по следующему алгоритму.

Шаг 1. Перед подключением киберфизическое устройство инициализируется – запускается особый режим операционной системы, который опрашивает каждую загруженную в устройство прикладную программу на предмет ожидаемых входов и выходов. Определим данный файл как дескриптор прикладной среды. В указанном файле для каждой программы должно быть указано, от программ с какими идентификаторами ожидаются данные и программам с какими идентификаторами данные будут передаваться.

Шаг 2. Операционная система запрашивает и получает адрес распределенного реестра (идеальный вариант – каждое устройство имеет свою копию распределенного реестра), в котором уже содержаться загруженные в него ранее дескрипторы киберфизических устройств, описывающие наборы прикладных программ. Дескриптор прикладной среды выгружается в формате отдельных записей, каждая из которых описывает отдельную прикладную программу.

Шаг 3. Каждое из киберфизических устройств на основании размещения дескриптора нового устройства принимает решение о переключении информационных потоков.

Необходимо отметить, что приведенные три шага не означают реализации управления информационными потоками на технологии распределенного реестра. Исходя из попыток, описанных, в частности, в [6], создание полноценного распределенного реестра с механизмами, ориентированными на обработку криптовалют нецелесообразно. Вместе с тем, возможно использование отдельных элементов, таких как связанное хранение данных, когда структура данных и алгоритмы контроля целостности не допускают изменения содержания данных и их последовательности и алгоритмы обеспечения консенсуса.

Можно предложить алгоритм, который обеспечивает информационную безопасность «роя» киберфизических устройств за счет:

– сведения вопросов информационной безопасности к вопросам безопасного взаимодействия и модификации набора

прикладного программного обеспечения, функционирующего в комплексе киберфизических устройств (аналога субъектно-объектной модели);

– вынесения описания прав и порядка взаимодействия прикладного программного обеспечения (аналога таблицы разграничения прав доступа) в распределенный реестр.

– администрирования распределенного реестра на основании алгоритма консенсуса (фактически децентрализованное администрирование и управление безопасностью).

Таким образом, обеспечение информационной безопасности набора киберфизических устройств, функционирующих в условиях отсутствия «защищенного периметра», является актуальной научной и практической задачей. Решение указанной задачи возможно наделением киберфизических устройств функциями формирования «интеллектуального роя», обладающего распределенными механизмами обеспечения информационной безопасности. Предложено реализовать указанные механизмы на уровне операционной систем, осуществляющей управление отдельным киберфизическим устройством.

Литература.

1. *Щербаков А.Ю.* Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие. – М.: Книжный мир, 2009 – 352 с.

2. *Колосок И.Н., Коркина Е.С.* Анализ кибербезопасности цифровой подстанции с позиций киберфизической системы // Информационные и математические технологии в науке и управлении. – 2019. – № 3 (15). – С. 121-131.

3. *Калинин М.О.* Способ осуществления правил политики безопасности в одноранговых коммуникационных сетях киберфизических устройств. Российский патент 2020 года по МПК H04L12/721 G06F21/60. RU2714217C1.

4. *Лаврова Д.С.* Методология предотвращения компьютерных атак на промышленные системы на основе адаптивного прогнозирования и саморегуляции. – Автореферат диссертации на соискание ученой степени доктора технических наук. – СПбТУ, 2019. – 37 с.

5. *Лаврова Д.С., Зегжда Д.П., Зайцева Е.А.* Моделирование сетевой инфраструктуры сложных объектов для решения задачи противодействия кибератакам // Вопросы кибербезопасности. – 2019. – № 2 (30). – С. 13-20.

6. *Афанасьев М. Я., Федосов Ю. В., Крылова А. А., Шорохов С. А.* Организация киберфизических производственных систем с использованием технологий блокчейн и смарт-контрактов // Известия высших учебных заведений. Приборостроение. – 2019. – Т. 62. № 3. – С. 226-234.

Изотова И.А., Мысак М.Ю., Фейзов В.Р.

Технология кибербразведки как инструмент выстраивания проактивной защиты

Аннотация: Работа посвящена актуальной на сегодняшний день проблеме низкого уровня осведомленности организаций о технологии кибербразведки и вопросам применения данных о киберугрозах при выстраивании системы обеспечения кибербезопасности. В работе проанализированы методы применения данных кибербразведки в целях повышения уровня защищенности организации путем выстраивания проактивной защиты. Вопросы, изучаемые в работе, заинтересуют руководителей служб информационной безопасности (ИБ), а также центров мониторинга и реагирования организаций кредитно-финансового сектора.

Ключевые слова: кибербразведка, данные о киберугрозах, кибербезопасность, повышение уровня защищенности, кредитно-финансовый сектор

Современный мир невозможно представить без информационных технологий, и финансовая сфера не стала исключением. Пандемия лишь ускорила процесс цифровизации в кредитно-финансовом секторе, что сместило приоритеты в сторону дистанционного обслуживания клиентов и организации удаленных рабочих мест для сотрудников. Это было бы невозможно без достижений в области информационных технологий, которые стали неотъемлемой частью финансовых услуг. Распространение сфер