УДК: 004.3, 004.9

Концепция информационной безопасности «роя» киберфизических систем

D.I. Pravikov, A.Yu. Shcherbakov

The Concept of Information Security of the "Swarm" of Cyber-Physical Systems

Abstract. *The article is devoted to consideration of possible approaches to ensuring information security, taking into account the peculiarities of cyber-physical systems in theoretical and practical aspects. The issues of information security assurance of a set of cyber-physical devices operating in the absence of a "secure perimeter" are considered. A solution to these issues is proposed by including the functions of forming an "intelligent swarm" with distributed mechanisms for ensuring information security in cyber-physical devices. An algorithm for ensuring information security of a "swarm" of cyber-physical devices is described.*

Keywords: *cyber-physical system, insecure environment, information security of the swarm, application environment descriptor, distributed ledger, man-in-the-middle attack, subject-object model.*

Д.И. Правиков[1]
А.Ю. Щербаков[2]
[1]Кандидат технических наук, руководитель Научно-образовательного центра новых информационно-аналитических технологий РГУ нефти и газа (НИУ) имени И.М. Губкина
E-mail: dip@gubkin.pro
[2]Доктор технических наук, начальник Центра развития криптовалют и цифровых финансовых активов (ЦРКЦФА) ВИНИТИ РАН.
E-mail: x509@ras.ru

Аннотация. *Статья посвящена рассмотрению возможных подходов к обеспечению информационной безопасности, учитывающих особенности киберфизических систем в теоретическом и практическом аспектах. Рассмотрены вопросы обеспечения информационной безопасности набора киберфизических устройств, функционирующих в условиях отсутствия «защищенного периметра». Предложено решение данных вопросов при помощи включения функций формирования «интеллектуального роя», обладающего распределенными механизмами обеспечения информационной безопасности, в киберфизических устройствах. Описан алгоритм обеспечения информационной безопасности «роя» киберфизических устройств.*

Ключевые слова: *киберфизическая система, незащищенная среда, информационная безопасность «роя», дескриптор прикладной среды, распределенный реестр, атака «человек посередине», субъектно-объектная модель.*

ВВЕДЕНИЕ

В настоящее время теория информационной безопасности находится в состоянии, которое можно охарактеризовать как приближение к точке бифуркации. С одной стороны существует уже общепризнанная теория, базирующаяся на субъектно-объектной модели, которая в основном используется для «традиционных» автоматизированных информационных систем. С другой стороны, резкое развитие киберфизических систем (КФС) и применение их для решения ряда задач привели к появлению запроса на формирование новых подходов к обеспечению информационной безопасности, учитывающих особенности КФС как в теоретическом, так и практическом плане.

Так, например, специалисты в области обеспечения информационной безопасности автоматизированных систем управления технологическими процессами (АСУ ТП) в ряде работ и в выступлениях на конференциях отмечают исчезновение «периметра» - одного из базовых постулатов классической теории информационной безопасности. Как следствие, для ряда случаев уже не применимо понятие «контролируемой зоны», а значит защищаемые элементы, в роли которых выступают киберфизические системы, должны функционировать фактически в незащищенной среде, тем не менее, обеспечивая заданные свойства безопасности. Эти проблемы в полной мере относятся и к системам обращения цифровых активов, блокчейн-платформам, платежным системам, которые корректно рассматривать только как комплексные киберфизические системы.

На текущий момент трудно судить как о наличии теории обеспечения информационной безопасности КФС, так и об общепризнанных подходах к ее формированию. Рассмотрению возможных подходов к решению указанных

проблем посвящена данная работа.

АНАЛИЗ

Обеспечение информационной безопасности киберфизических систем (как комплексов киберфизических устройств), является предметом изучения различных научных коллективов. Достаточно упомянуть работу [1]. При этом можно утверждать, что, несмотря на предпринимаемые усилия, в настоящее время не существует теории, позволяющей смоделировать и формализовать аспекты информационной безопасности комплекса киберфизических устройств. Современные тенденции, идущие от практики, связаны с появлением таких подходов, как архитектура «с нулевым доверием»[1], для которой существуют решения по обеспечению безопасности. Однако эти подходы не имеют соответствующего теоретического обоснования.

Такая постановка вопроса о безопасности комплекса киберфизических устройств имеет следующее объяснение.

Разработанные ранее теоретические положения и подходы опирались на постулат замкнутости защищаемой системы [2]. В субъектно-объектной модели определены и перечислены все пассивные сущности (объекты) и активные сущности (субъекты), права доступа и правила продукции (устанавливают, что произойдет, если некоторый субъект произведет разрешенное действие с некоторым объектом). Для систем подобного типа вводилась роль администратора, который фактически должен был контролировать перечни субъектов и объектов, а также задавать права доступа и полномочия.

В упомянутой выше работе [2] вводились две аксиомы защищенных компьютерных систем (КС):

Аксиома 1. В защищенной КС всегда присутствует активная компонента (субъект), выполняющая контроль операций субъектов над объектами. Данная компонента фактически отвечает за реализацию некоторой политики безопасности.

Аксиома 2. Для выполнения в защищенной КС операций над объектами необходима дополнительная информация (и наличие содержащего ее объекта) о разрешенных и запрещенных операциях субъектов с объектами.

Гипотетически комплекс, состоящий из киберфизических устройств, также можно было бы рассматривать как некоторую систему, состав которой зафиксирован, а безопасность обеспечивается в рамках субъекто-объектной модели. Вместе с тем, возникает проблема реализации аксиом 1 и 2 для комплексов киберфизических устройств.

Анализ различных источников показал, что одно из возможных решений было положено в основу изобретения [3], в соответствии с которым в одноранговых коммуникационных сетях киберфизических устройств осуществляется управление настройками маршрутизации, дополнительно вводится блок осуществления политики безопасности; в данном блоке «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 имеет следующие ограничения:

1. Оно порождает новый объект атаки – блок осуществления политики безопасности, в отношении информационной безопасности которого в изобретении отсутствуют предложения.

2. Оно применимо для киберфизических устройств, реализующих только один прикладной процесс, т.к. приравнивает информационный обмен между киберфизическими устройствами к обмену между программами. Для киберфизических устройств с набором прикладных процессов подход, описанный в изобретении, не применим.

3. Не исключено, что при значительном количестве киберфизических устройств (де-

[1] NIST Special Publication 800-207. Zero Trust Architecture. https://doi.org/10.6028/NIST.SP.800-207

сятки и сотни) сложность администрирования возрастает в степенной зависимости, что делает управление безопасностью неподконтрольным на уровне возможностей обычного человека.

Более того, если мы будем рассматривать вопрос реализации указанных аксиом для комплексов киберфизических устройств, возникает вопрос, где будет располагаться компонента, выполняющая контроль субъектов над объектами и, соответственно, где и в каком виде будет размещаться информация, описывающая разрешенные операции субъектов над объектами, при условии того, что сами киберфизические устройства могут динамически как включаться комплекс, так и исключаться из него.

Рассмотрим киберфизическое устройство, функционирующее в составе комплекса других аналогичных устройств. Оно имеет подключение к локальной вычислительной сети и, в соответствии с проектом цифровизации функционального процесса, в общем случае на вход получает сигналы (управления и данных), выходом устройства также являются сигналы, которые также подразделить на данные (снимаемые с датчиков) и результаты обработки информации, полученные в результате вычислений.

В работе [4] 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:

$$f_{v_i} = \left\{f_{v_i}^{(1)}, f_{v_i}^{(2)}, \dots, f_{v_i}^{(k)}\right\}.$$

Модель отражает взаимодействие компонентов ПС друг с другом, процессы, необходимые для реализации целевой функции ПС, и саму целевую функцию. Целевая функция F ПС представляется в модели двумя способами одновременно: в виде множества маршрутов на графе и в виде набора функциональных последовательностей с заданными типами отношений между функциями: $F = \{F_1, F_2, \dots, F_n\}$.

Данную модель можно интерпретировать следующим образом. Вершины описывают киберфизические устройства, функция f – это прикладная программа, функционирующая на киберфизическом устройстве. Соответственно дуги моделируют связи, которые, с одной стороны, возникают между киберфизическими устройствами, но в детализации описывают взаимодействие прикладных программ.

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.

Представленная графовая модель отражает все типы компьютерных атак на систему.

Полное перечисление возможных видов атак на промышленную систему представлено в работе [5]. Данная работа интересна тем, что на основании описания представленных видов атак, их все можно свести к набору элементарных действий:

1. Удалить информационный обмен между двумя прикладными программами (где он был).

2. Создать информационный обмен между двумя прикладными программами (где его не было).

3. Добавить новую прикладную программу (без информационного обмена).

4. Удалить существующую прикладную программу (вне зависимости от ее участия в информационном обмене).

5. Добавить новую прикладную программу и организовать ее информационный обмен с двумя другими существующими прикладными программами (комбинация действий 1, 2 и 3).

Таким образом, на основании проведенного обзора литературы можно сделать вывод о том, что информационная безопасность киберфизических устройств является предметом исследований. Поскольку функционал киберфизических устройств фактически определяется загруженным прикладным программным обе-

спечением, информационную безопасность системы киберфизических устройств можно свести к обеспечению информационной безопасности взаимодействия прикладных программ. Как следствие, само киберфизическое устройство, включая его системное программное обеспечение, должно обеспечить требуемые функции безопасности.

ИССЛЕДОВАНИЕ

Для начала определим, что множество функций (прикладных программ) и отношения информационного обмена между ними задают ориентированный граф. Таким образом, будет осуществлен переход от самих киберфизических устройств к набору функционирующих на них прикладных программ.

Тогда (пока на неформальном уровне), 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 одного из постулатов, 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 типа Man-In-The-Middle (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 инициали-зируется – 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 котором 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 содержатся 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, доступно использование таких возможностей, как связанное хранение данных, когда структура данных и алгоритмы контроля целостности не допускают изменения содержания данных и их последовательности, или алгоритмы обеспечения консенсуса.

Предположим, есть Алиса, есть Боб, включается третье устройство (и это не должно реализовывать атаку «человек посредине»).

Третье устройство говорит, что у него есть программа **c**, которая готова принимать данные от программы **a** (такая есть у Алисы), а посылать –программе **b** (такая программа есть у Боба).

В дескрипторе прикладной среды описание входов и выходов каждой прикладной программы должно быть подписано администратором всего комплекса. В данном случае термин «подписано» апеллирует к возможности проверки авторства и сохранения неизменности описания входов и выходов. Важно отметить, что в киберфизической среде нецелесообразно использовать механизмы электронной подписи в их классическом варианте, достаточно ограничиться симметричными алгоритмами на основе вычисления и проверки имитовставок (модель угроз: администратор может контролировать набор прикладных программ с определенной точностью, не просчитывая возможные коллизии и ситуации, связанные с нарушением безопасности).

Тогда устройство Алисы получает дескриптор программной среды, считывает запрос, подписанный администратором приоритетным, и меняет свой дескриптор среды, отменяя передачу данных от программы **a** Бобу на передачу данных программе **c**. Боб, получая свою копию программной среды, также считывает запрос, подписанный администратором, и меняет уже свой дескриптор среды, отменяя получение данных от Алисы и меняя его на программу **c**. Тогда в блоке реестра должны появиться записи, отменяющие обмен Алисы и Боба и реализующие его через прикладную программу **c** на вновь подключаемом устройстве.

Данный блок записей реестра должен быть подписан не только Алисой, Бобом, новым устройством, но и администратором системы.

Может возникнуть вопрос, каким образом Алиса и Боб понимают, что запись в реестр осуществляет администратор, а не злоумышленник? Ответ на этот вопрос также может быть сведен к алгоритму достижения консенсуса. Так, один из алгоритмов может быть основан на Proof-of-Stake. Говоря другими словами, за администратора системы признается такая активная сущность, которая либо больше всех в течение заданного промежутка времени администрировала систему, либо получила право (подтвержденное криптографической процедурой или также консенсусом) на администрирование от той, которая больше всех администрировала систему.

Таким образом, приведенный выше алгоритм может обеспечить информационную безопасность «роя» киберфизических устройств за счет:

1. Сведения вопросов информационной

безопасности к вопросам безопасного взаимодействия и модификации набора прикладного программного обеспечения, функционирующего в комплексе киберфизических устройств (аналога субъектно-объектной модели).

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

3. Администрирование распределенного реестра на основании алгоритма консенсуса (фактически децентрализованное администрирование и управление безопасностью).

Как представляется, приведенные выше подходы могут быть реализованы программным образом. При этом поддержка описанных функций должна быть реализована на уровне операционной системы, осуществляющей управление киберфизическим устройством.

Наделение киберфизических устройств функциями формирования безопасного «роя» может рассматриваться как одно из возможных направлений теоретических исследований и практических реализаций.

ВЫВОДЫ

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

СПИСОК ЛИТЕРАТУРЫ

1. 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. DOI: 10.25729/2413-0133-2019-3-11.
2. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие. М.: Книжный мир, 2009. 352 с.
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: автореф. дис. … д-ра техн. наук. 05.13.19. Санкт-Петербург, 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. DOI: 10.17586/0021-3454-2019-62-3-226-234.