МНОГОАГЕНТНАЯ АУТЕНТИФИКАЦИЯ ЦИФРОВЫХ ДВОЙНИКОВ В КИБЕРФИЗИЧЕСКИХ СИСТЕМАХ

Балюк А.А.[1], Финько О.А.[2]

Постановка задачи: *основными катализаторами развития киберфизических систем в настоящее время являются рост искусственного интеллекта и создание цифровых двойников, имеющих сложную вертикальную структуру и обменивающихся данными для совместного обучения. В то же время наделение цифровых двойников полномочиями владельцев данных может привести к критическим последствиям в области обеспечения безопасности данных систем. Разработка эволюционных методов обеспечения безопасности информации, и в частности, методов аутентификации цифровых двойников, является принципиальным вопросом на пути развития киберфизических систем.*

Цель работы: *анализ аспектов и принципов построения системы и процесса аутентификации цифровых двойников в динамичных и масштабируемых киберфизических системах, организации исследуемого процесса, показателей его эффективности и критериев их оценивания.*

Используемые методы: *системный анализ, алгебра кортежей, методы проектирования и оценивания эффективности сложных систем.*

Новизна: *применение многоагентной структуры подсистемы аутентификации цифровых двойников, позволяющей достичь гарантированной осведомленности о состоянии безопасности системы в целом и соответствующим образом реагировать в случае компрометирующих событий. Реализацию интеллектуального управления аутентификацией предлагается осуществлять с использованием прикладных возможностей алгебры кортежей, учитывающей различия в структурах традиционных и интеллектуальных систем, а также трудности распараллеливания в распределенных системах. Для повышения устойчивости системы многоагентной аутентификации рассматривается возможность использования криптокодовых протоколов, позволяющих обеспечить восстановление достоверных аутентификационных данных при сбоях или отказах.*

Результат: *обоснование новых принципов и технологических решений в области высокоуровневого проектирования киберфизических систем.*

Ключевые слова: *робототехнические комплексы, искусственный интеллект, многоагентная система, алгебра кортежей, криптокодовые конструкции, нечеткий интеграл.*

DOI:10.21681/2311-3456-2022-5-100-113

Введение

Миграция технологий межмашинной связи (Machine-to-Machine, M2M) и беспроводных сенсорных сетей (WSN) в информационные системы облачных (туманных) вычислений привела к соединению кибернетического мира с физическим, к созданию киберфизических систем (КФС).

КФС представляет собой интеграцию вычислительных технологий, сетей и физических процессов, которая направлена на мониторинг и управление физическими процессами.

Отличительными особенностями КФС являются [1]:
1) наличие программного управления в каждом физическом объекте;
2) тесная интеграция систем и взаимосвязь объектов;
3) малые временные рамки и крупные пространственные масштабы;

1 Балюк Алексей Анатольевич, кандидат технических наук, Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М. Штеменко, г. Краснодар, Россия. E-mail: alexbaluk689@gmail.com

2 Финько Олег Анатольевич, доктор технических наук, профессор, Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М. Штеменко, г. Краснодар, ООО «Специальный технологический центр», г. Санкт-Петербург, Россия. E-mail: ofinko@yandex.ru

4) динамическая реорганизация / реконфигурация;
5) управление с обратной связью и высокая степень автоматизации;
6) высокие требования по надежности и безопасности.

К категории КФС можно отнести большинство составляющих современной техники: «умный город», «умный дом», «умные» медицинские устройства, беспилотные автомобили и летательные аппараты, робототехнические комплексы, а также системы военного назначения.

В новой парадигме промышленных производств «Индустрия – 4.0» реализация КФС рассматривается, в первую очередь, на основе применения технологии «умных» цифровых двойников (Smart Digital Twin). Данная технология подразумевает создание и использование для управления жизненным циклом объекта интеллектуальных цифровых двойников («отражений»), которые проективно инициируют действия в зависимости от различных обстоятельств, управляют всеми ресурсами и функционируют в одном ресурсно-функциональном домене (интеллектуальной площадке) [2].

По сути КФС – концепция «умной» системы, являющейся промышленным интернетом вещей с автоматизированным управлением на основе «умных» цифровых двойников.

Эффективность данных систем в значительной степени определяется характеристиками используемой системы безопасности информации, так как каждый киберфизический объект должен иметь возможность выбирать, какими ресурсами делиться с другими сторонами, изолировать себя для предотвращения утечки данных и иметь возможность отозвать доступ к ним.

Важной подсистемой, обеспечивающей опознавание субъекта доступа с необходимой уверенностью в том, что он является тем, за кого себя выдает, является подсистема аутентификации.

Известные методы аутентификации реализуются либо в физическом, либо в виртуальных компонентах, обслуживающих большое количество субъектов, а используемые протоколы аутентификации следуют своей частной логике, часто без комплексного учета потребностей ресурсов КФС в целом. Без решения проблемы, связанной с использованием дополнительных механизмов и координации процессов аутентификации в КФС невозможно обеспечить их качественное функционирование и масштабируемость.

Решение этой проблемы предположительно основывается на использовании многоагентной системы с интеллектуальным управлением, обеспечивающей адаптивность в разнообразных платформах КФС.

Первым этапом решения данной проблемы является:

— анализ аспектов и формулировка принципов исследуемого процесса;
— определение (обоснование) показателей его эффективности и критериев их оценивания.

1. Концепция цифровых двойников в КФС

Инновации КФС в настоящее время непрерывно продолжаются, и двумя основными катализаторами новых технологических прорывов являются рост искусственного интеллекта, основанного на машинном обучении, и создание цифровых двойников – проекций объектов физического мира на кибернетический.

Цифровой двойник представляет собой виртуальную копию, которая виртуально неотличима от своего физического аналога [3].

В отличие от цифровой модели, которая не обменивается данными с физическим объектом, изменения физического объекта приводят к автоматическому изменению цифрового двойника и наоборот [4]. Тем самым обеспечивается непрерывность проектирования в течение всего жизненного цикла объекта.

Одним из ключевых факторов достижения полномасштабной цифровой трансформации в КФС является наделение цифровых двойников способностью действовать на основе восприятий и встроенных знаний и организовывать свои действия с учетом полезности, максимизируя показатели производительности КФС в условиях частично наблюдаемых вариантов среды.

При этом новые достижения в области децентрализованного машинного обучения (Federated Learning, FL) позволяют цифровым двойникам совместно обучаться и обмениваться обучающими данными [5]. Являясь представителем физической сущности, интеллектуальный цифровой двойник действует как «умный цифровой агент», проективно инициируя действия в зависимости от различных обстоятельств.

Использование цифровых двойников, обменивающихся знаниями на динамической основе, позволяет рассматривать КФС как многоагентную систему, для которой характерны следующие особенности:

1) распределенное решение проблем, которые разбиваются на параллельно решаемые частные проблемы, соответствующие различным источникам знаний;

2) проведение альтернативных рассуждений на основе использования различных источников знаний с механизмом устранения противоречий;

3) применение множества стратегий работы механизма вывода заключений;

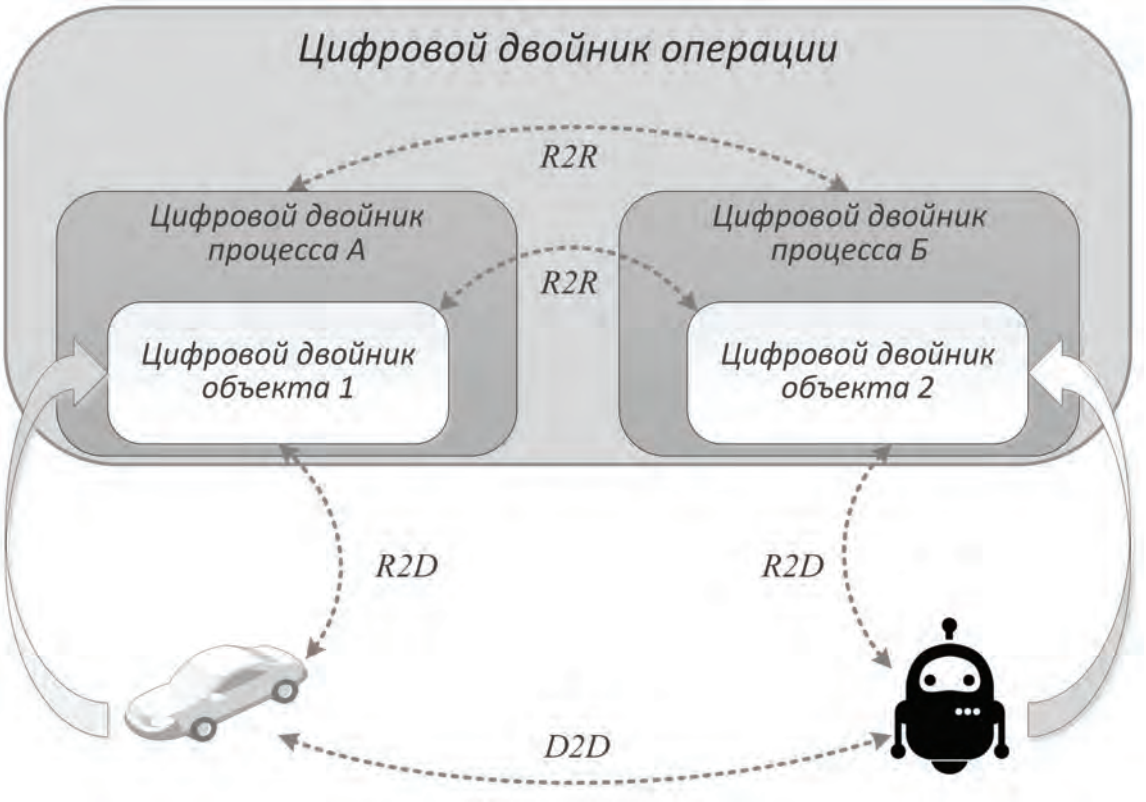

Рис. 1. Иллюстрация концепции цифровых двойников в КФС

4) использование различных математических моделей и внешних процедур, хранимых в базе моделей;

5) способность прерывания решения задач в связи с необходимостью получения дополнительных данных и знаний.

Многоагентная система цифровых двойников позволяет обеспечивать доступность ресурсов и услуг, а также возможность управления в режиме реального времени.

В рамках концепции КФС можно рассматривать следующие типы цифровых двойников [6]:

1) цифровые двойники объектов – отражают физические объекты;

2) цифровые двойники процессов – отражают какие-либо процессы, в которых участвую объекты;

3) цифровые двойники операции – отражают работу каждого процесса операции.

Цифровые двойники могут иметь как раздельные, так и общие ресурсы. Взаимодействия при этом осуществляются между устройствами (device-to-device, D2D), устройствами и их цифровыми двойниками (reflection-to-device, R2D), а также между цифровыми двойниками (reflection-to-reflection, R2R) (рис. 1).

Для образования цифровых двойников и их совместного обучения необходимо наделение их правами владельцев данных, что может привести к критическим последствиям в области обеспечения безопасности информации в КФС.

2. Требования, предъявляемые к аутентификации субъектов в многоагентных КФС

Аутентификация субъекта – процесс подтверждения подлинности предъявленного претендентом (субъектом доступа) идентификатора (идентификационной информации) и проверки принадлежности аутентификационной информации (фактора аутентификации, секрета) и идентификатора (идентификационной информации) конкретному субъекту или объекту доступа[3].

В роли субъекта доступа в КФС могут рассматриваться пользователи, сенсоры и исполнительные механизмы, внешние процессы, робототехнические средства, виртуальные объекты (аватары), программные агенты (боты), цифровые двойники и др.

3 Афанасьев А. А., Веденьев Л. Т., Воронцов А. А. и др. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. М.: Горячая линия – Телеком, 2009. 552 с.

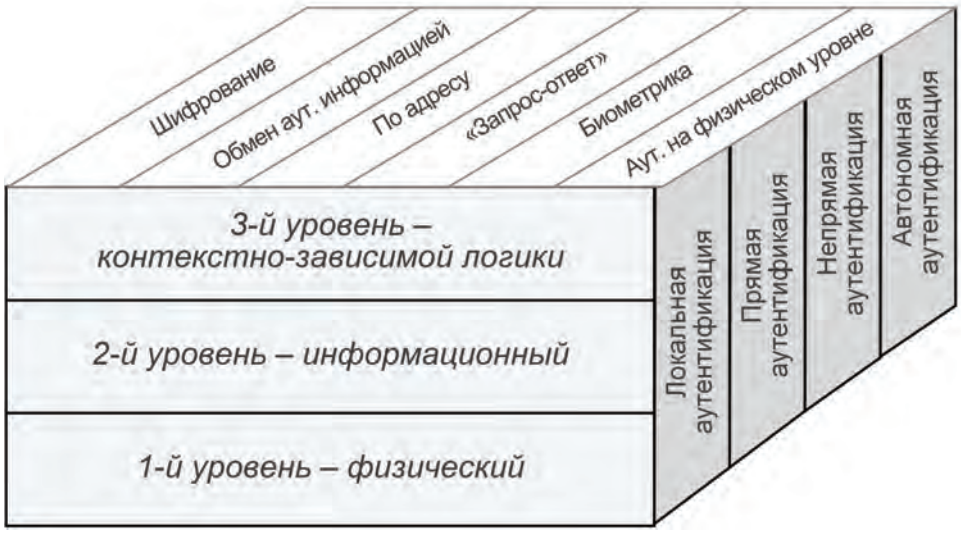

Рис. 2. Взаимосвязь шаблонов и механизмов аутентификации с уровнями логической структуры КФС

В архитектурных решениях программного обеспечения рассматриваются следующие виды проектных шаблонов аутентификации субъектов доступа[4]:

1) локальная аутентификация (вся система, включая механизм аутентификации, размещается внутри одного физического периметра безопасности);

2) прямая аутентификация (системой могут коллективно пользоваться удаленным образом множество различных пользователей);

3) непрямая аутентификация (система содержит несколько точек обслуживания, которые требуют управления доступом и могут размещаться в разных местах);

4) автономная аутентификация (применяется в системах с инфраструктурой открытого ключа, содержащих многочисленные автономные компоненты, которые способны принимать точные решения по управлению доступом даже в том случае, когда они не могут связываться с другими системами для получения авторитетных решений об аутентификации).

Основными механизмами аутентификации субъектов доступа являются механизмы шифрования, обмена аутентификационной информацией, аутентификации по адресу и по принципу «запрос-ответ».

К специальным механизмам аутентификации относят биометрическую идентификацию и аутентификацию на физическом уровне. Без биометрических параметров, то есть без инвариантных по времени свойств личности, нет возможности решить проблему автоматической идентификации личности посредством сенсорных устройств[5]. Аутентификация на физическом уровне обеспечивается альтернативным подходом (в том числе с использованием технологий машинного обучения) с использованием характеристик канала связи и устройств, а также данных, связанных с их местоположением [7-10].

Поскольку КФС – это архитектурная парадигма, то анализ подходов к использованию различных проектных шаблонов и механизмов аутентификации видится в соотнесении их с логической структурой системы (рис. 2).

Различие в используемых шаблонах аутентификации создает проблемы при организации ее осуществления на различных уровнях логической архитектуры КФС [11]:

1) первый уровень (физический) – включает в себя все элементы с непрерывной динамикой, поведение которых контролируется физическими законами, то есть физический мир, исполнительные механизмы и сенсоры;

2) второй уровень (информационный) – содержит элементы анализа данных, которые преобразуют дан-

4 Смит Р.Э. Аутентификация: от паролей до открытых ключей. М.: Издательский дом «Вильямс», 2002. 432 с

5 Болл Р. М., Коннел Д. Х., Панканти Ш., Ратха Н. К., Сеньор Эндрю У. Руководство по биометрии. М.: Техносфера, 2007. 368 с.

ные от сенсоров в абстрактную информацию, используемую в вычислительных элементах;

3) третий уровень (контекстно-зависимой логики) – моделирует на высоком уровне изменяющийся физический мир и определяет в реальном времени поведение системы.

Широкое распространение сенсоров и исполнительных механизмов, необходимость совместной обработки данных и постоянно увеличивающееся количество различных форм приложений предъявляют новые требования к аутентификации субъектов доступа в КФС. Рассмотрим данные требования.

1. Механизмы аутентификации должны быть устойчивыми к динамичности узлов и масштабируемости сети. С масштабируемостью связаны три уровня сложности: в физической инфраструктуре системы сбора данных; в механизме связи; в серверных и пользовательских приложениях [12]. Механизмы аутентификации в КФС должны адаптироваться к указанным сложностям при обеспечении соответствующих уровня качества обслуживания и безопасности информации.

2. Для обеспечения возможности обработки информации в реальном времени необходимы механизмы односторонней, взаимной и групповой аутентификации. При этом должна обеспечиваться конфиденциальность аутентификационной информации. Одним из перспективных направлений развития средств криптографической защиты в условиях мультиаренды ресурсов является гомоморфная криптография. Недостатком методов гомоморфного шифрования является накопление ошибок данных, обрабатываемых в зашифрованном тексте. Одним из возможных решений данной проблемы является использование систем аутентификации с допустимой погрешностью их сигналов-носителей и кодограмм аутентификации[6].

3. Механизмы аутентификации должны поддерживать постоянную осведомленность об общей системе и соответствующим образом реагировать в случае возникновения компрометирующих событий. Одной из основных характеристик угроз в КФС является то, что они также могут быстро распространяться, воздействуя как на кибер-, так и на физические объекты [13]. Для защиты от этих угроз необходимо использование механизма спецификации разрешений на аутентификацию.

4. Должна обеспечиваться возможность аутентификации объектов по их физическим параметрам. В настоящее время большинство разработчиков оборудования закупают конструктивные части у сторонних организаций. По мере производства и поставки в данные части могут быть злонамеренно внесены модификации и уязвимости [14]. Для нейтрализации угроз, влияющих на физические объекты, необходимы механизмы аутентификации, обеспечивающие подлинность самих физических объектов. Одним из возможных решений является использование адресной аутентификации физических объектов с использованием их цифровых двойников [15].

3. Многоагентная аутентификация цифровых двойников в КФС

С позиций системного анализа аутентификация представляет собой операцию, т.е. упорядоченную совокупность взаимосвязанных действий, направленных на достижение цели функционирования подсистемы аутентификации. Целью функционирования данной системы является подтверждение заявленных свойств сущности.

Для достижения указанной цели в многоагентных КФС предлагается структура, основанная на распределенном программном обеспечении с многоагентной структурой (рис. 3). Использование многоагентной аутентификации позволит учитывать последствия ее реализации и принимать решения в условиях частично наблюдаемых вариантов среды.

Под понятием *«многоагентная аутентификация»* будем понимать процесс подтверждения заявленных свойств сущностей, основанный на использовании системы с многоагентной структурой, в которой каждый агент аутентификации отвечает за координацию и выполнение соответствующих протоколов аутентификации.

В предлагаемой структуре (рис. 3):

1) главный агент – отвечает за выполнение обширных процедур управления, связанных с подчиненными локальными агентами, координацию всех коммуникаций, прогнозирование поведения системы и ее адаптивность, а также выполняет роль центра регистрации и валидации; по определенному набору признаков (к примеру, профиль субъекта аутентификации и его поведения) главный агент аутентификации должен быть способен определить уровень риска тех или иных действий субъекта и выбрать соответствующий механизм аутентификации, обеспечивая баланс между необходимым уровнем безопасности и затрачи-

6 Оков И. Н. Аутентификация речевых сообщений и изображений в каналах связи. СПб.: Изд-во политехн. ун-та, 2006. 392 с.

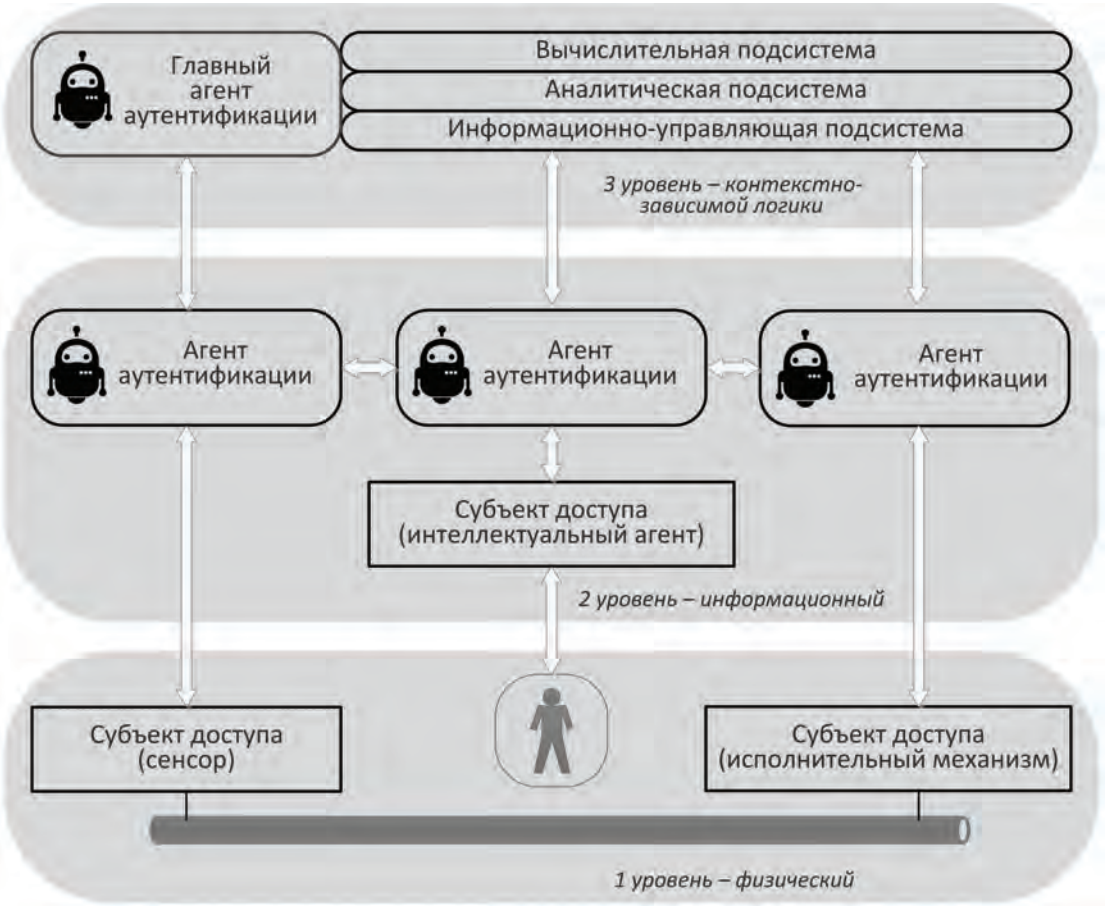

Рис. 3. Логическая структура подсистемы многоагентной аутентификации в КФС

ваемыми ресурсами путем оценки контекстуальных атрибутов в режиме реального времени;

2) агенты аутентификации – отвечают за сбор данных и реализацию соответствующих процедур аутентификации; для обеспечения адаптивности системы агенты аутентификации должны обладать способностью максимизировать свои показатели производительности, то есть быть интеллектуальными агентами.

4. Теоретико-множественное моделирование многоагентной аутентификации в КФС

Важной особенностью рассматриваемой подсистемы является ее способность функционирования в условиях большого количества входящих в систему узлов. Такая масштабируемость обеспечивается заложенными в систему механизмами равноправного взаимодействия узлов и функциональных компонентов. Современные пиринговые системы данного типа характеризуются не только разнородностью и территориальной распределенностью, но и гибкой расширяемостью, а также способностью к саморазвитию в условиях полного отсутствия или минимального объема внешнего управления[7].

В общем случае модель системы многоагентной аутентификации $(MAAS)$ может быть задана в виде теоретико-множественных отношений и представляет собой следующий набор параметров:

$$MAAS = \{SD, GA, AA, R, ATR\},$$

где:

SD – множество субъектов доступа (они же являются владельцами ресурсов);

GA – множество главных агентов аутентификации;

AA – множество агентов аутентификации;

R – отношения на множествах объектов модели;

ATR – множество атрибутов объектов модели.

На множестве объектов заданы следующие отношения, определяющие структуру системы:

7 Маслобоев А. В., Путилов В. А. Разработка и реализация механизма управления информационной безопасностью мобильных агентов в распределенных мультиагентных информационных системах // Вестник МГТУ. 2010. Т. 13, № 4/2. С. 1015-1032.

$$R = \{GAAA,\ AAGA,\ SDAA,\ AASD\},$$

где:

$GAAA \subset GA \times AA$ – отношение «принадлежности» каждому главному агенту множества агентов аутентификации;

$AAGA \subset AA \times GA$ – отношение «принадлежности» каждому агенту аутентификации множества главных агентов;

$SDAA \subset SD \times AA$ – отношение «принадлежности» каждому субъектов доступа множества агентов аутентификации;

$AASD \subset AA \times SD$ – отношение «принадлежности» каждому агенту аутентификации множества субъектов доступа.

Каждый субъект доступа (владелец ресурсов) описывается следующим набором параметров:

$$SD = \{ID_{SD}, SP_{SD}, D_{SD}\},$$

где:

ID_{SD} – множество идентификаторов субъекта доступа;

SP_{SD} – множество секретных параметров (аутентификаторов) субъекта доступа;

D_{SD} – множество данных (ресурсов), которыми обладает субъект доступа.

Каждый главный агент аутентификации описывается следующим набором параметров:

$$GA = \{SR_{GA}, SV_{GA}, D_{GA}\},$$

где:

SR_{GA} – множество систем регистрации (множество способов установления связи субъекта доступа и его аутентификатора);

SV_{GA} – интеллектуальная система проверки (валидации) принадлежности субъекту доступа его аутентификатора;

D_{GA} – множество данных, которыми оперирует главный агент аутентификации:

$$D_{GA} = \{SD_{GA}, MAList_{GA}\},$$

где:

$SD_{GA} = \{IDList, SPList\}$ – множество субъектов доступа (владельцев ресурсов) в виде реестра их идентификаторов $IDList$ и аутентификаторов $SPList$;

$MAList_{GA}$ – реестр агентов аутентификации, которыми управляет главный агент.

Каждый агент аутентификации описывается следующим набором параметров:

$$AA = \{ISE_{AA}, ES_{AA}, GAList_{AA}\},$$

где:

ISE_{AA} – информационно-поисковая система для определения главного агента аутентификации (центра регистрации), регистрирующего субъекта доступа;

ES_{AA} – экспертная система определения механизма аутентификации субъекта доступа;

$GAList_{AA}$ – реестр главных агентов аутентификации (центров регистрации).

5. Интеллектуальное управление аутентификацией в КФС

Для реализации интеллектуального управления многоагентной аутентификацией в КФС необходимо взаимодействие структур искусственного интеллекта с традиционными структурами (базами данных, сетями и др.). При этом возникает ряд проблем, для решения которых требуются значительные затраты времени и средств. К ним относятся:

- различия в структуре данных в базах данных (таблицы, графы) и базах знаний (продукции, фреймы, семантические сети);
- трудности распараллеливания процедур при использовании традиционных структур и знаний в интеллектуальных системах.

Одной из наиболее подходящих универсальных математических систем для анализа таких интеграционных систем является алгебра кортежей.

Алгебра кортежей – это математическая система для моделирования и анализа многоместных отношений, в которой можно использовать все средства логического моделирования и анализа систем, входящие в математическую логику [16].

Все основные операции реляционной алгебры, такие как проекция, объединение, прямое произведение, разность и селекция, используемые для обработки запросов в традиционных базах данных, эффективно реализуются в алгебре кортежей.

Реализация информационно-поисковой системы для поиска центра регистрации субъекта доступа в агентах аутентификации при использовании математического аппарата алгебры кортежей будет основываться на запросах в виде AK-объектов с фиктивными атрибутами на месте искомой информации. Ответы также будут формируются в виде AK-объектов, в которых на месте искомых атрибутов появляется необходимая информация.

Экспертные системы агентов аутентификации должны основываться на использовании баз знаний, которые состоят из наборов правил, регламентирующих определенные преобразования данных. Этими правилами являются логические выражения определенного типа. Чаще всего в качестве таких выражений используют продукции, т.е. импликации типа:

«ЕСЛИ A_1 и A_2 и … и A_k, ТО B_1 или B_2 или … или B_n».

Применение правил вывода в качестве механизма получения следствий при заданных ограничениях часто требует перебора большого числа вариантов, так как заранее невозможно предсказать порядок и результат применения правил. Используя средства алгебры кортежей можно заменить комплекс правил одним AK-объектом. Для этого объединяются созданные в системе условия в один AK-объект и добавляется атрибут, характеризующий состояние всей системы. Получается AK-объект, который распознает все возможные ситуации для данного комплекта правил.

6. Устойчивая к ошибкам аутентификация на основе криптокодовых протоколов

Переход к многоагентной аутентификации обуславливает необходимость использования специальных криптокодовых протоколов, предназначенных для обеспечения защиты информации в многоканальных системах [17-20].

К достоинствам криптокодовых протоколов относится возможность обнаружения (исправления) искажений в передаваемых криптограммах, в том числе и в случае их стирания или обрыве линии. Тем самым обеспечивается повышение устойчивости системы многоагентной аутентификации.

Сгенерированное в двоичном виде отправителем исходное сообщение M, подлежащее зашифрованию, разбивается на блоки фиксированной длины:

$$M = M_1 \| M_2 \| \dots \| M_i \| \dots \| M_n,$$

где «||» – символ операция конкатенации, n – количество блоков фиксированной длины в каждом рассматриваемом сообщении M.

i-ый блок сообщения M_i представляется в полиномиальной форме:

$$M_i(z) = \sum_{j=0}^{s-1} m_j^{(i)} z^j,$$

где z – фиктивная переменная; $m_j^{(i)} \in \{0,1\}$; $i = 1, 2, \dots, n$.

Соответственно, для получения последовательности блоков шифртекста $C_1(z), C_2(z), \dots, C_n(z)$ потребуется выполнение n операций зашифрования, а для получения блоков $M_1(z), M_2(z), \dots, M_n(z)$ открытого текста – n операций расшифрования. Процедуры зашифрования и расшифрования (в общем случае – на индивидуальных ключах) представляются в виде:

$$\begin{cases} C_1(z) \to E_{k_{e,1}} : M_1(z), \\ C_2(z) \to E_{k_{e,2}} : M_2(z), \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ C_n(z) \to E_{k_{e,n}} : M_n(z); \end{cases}$$

$$\begin{cases} M_1(z) \to D_{k_{d,1}} : C_1(z), \\ M_2(z) \to D_{k_{d,2}} : C_2(z), \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ M_n(z) \to D_{k_{d,n}} : C_n(z); \end{cases}$$

где:

$C_i(z)$ – блок шифртекста;

$M_i(z)$ – блок открытого текста;

$k_{e,i}, k_{d,i}$ – ключи зашифрования и расшифрования соответственно (при $k_{e,i} = k_{d,i}$ – систему шифрования называют симметричной, а при $k_{e,i} \neq k_{d,i}$ – асимметричной).

Блоки шифртекста $C_i(z)$ интерпретируются как наименьшие неотрицательные вычеты по модулям $m_i(z)$, таким что $\gcd(m_i(z), m_j(z)) = 1$, где $i \neq j$; $i, j = 1, n$. Причем $\deg C_i(z) \leq \deg m_i(z)$, где $\deg(\cdot)$ – степень полинома; $i = 1, n$. Совокупность блоков шифртекста $C_1(z), C_2(z), \dots, C_n(z)$ представляется как единый суперблок шифртекста модулярного полиномиального кода по системе модулей: $m_1(z), m_2(z), \dots, m_n(z)$.

После выполнения операции расширения модулярного полиномиального кода из каждой i-ой последовательности блоков шифртекстов $\xi(z) = (C_{i,1}(z), C_{i,2}(z), \dots, C_{i,l}(z))$ формируется имитовставка (или хеш-код) $H_i(z)$, $i = 1, n+r$. Процедура выработки имитовставки имеет вид:

$$\begin{cases} H_1(z) \to I_{h_1} : \xi_1(z), \\ H_2(z) \to I_{h_2} : \xi_2(z), \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ H_{n+r}(z) \to I_{h_{n+r}} : \xi_{n+r}(z), \end{cases}$$

где: I_{h_i} – оператор выработки имитовставки на ключе h_i ($i = 1, n+r$).

При передаче или хранении суперблоков шифртекстов с вычисленными имитовставками возникают ошибки вследствие преднамеренных или непред-

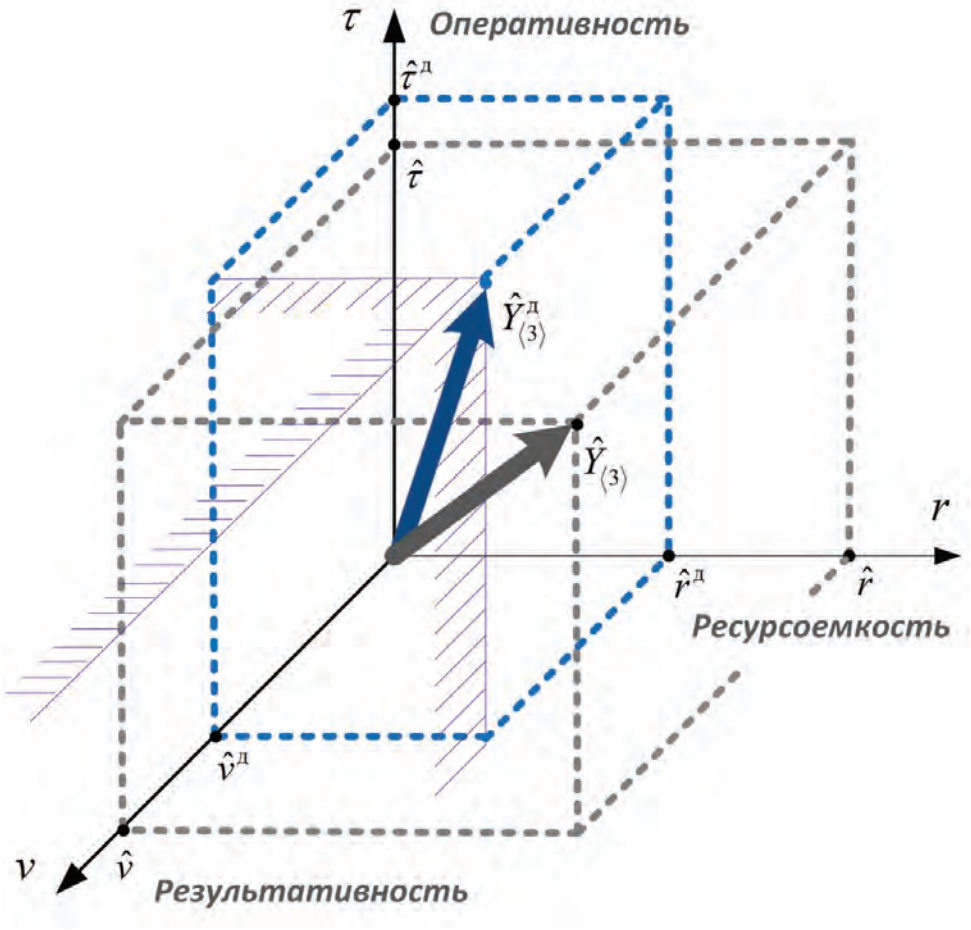

Рис. 4. Возможные реализации векторов $\hat{Y}_{\langle 3\rangle}$ *и* $\hat{Y}^{Д}_{\langle 3\rangle}$

намеренных (случайных) воздействий. Обнаружение нарушения целостности в принятой последовательности суперблоков шифртекста с имитовставками $\left(\xi'_1(z), H'_1(z)\right); \ldots; \left(\xi'_n(z), H'_n(z)\right); \ldots; \left(\xi'_{n+r}(z), H'_{n+r}(z)\right)$ с локализацией номера i ложного блока выполняется путем сравнения имитовставок, полученных из канала связи $H'_1(z), \ldots, H'_n(z), \ldots, H'_{n+r}(z)$ и имитовставок, вычисленных в подсистеме приема данных:

$$\begin{cases} \tilde{H}_1(z) \to I_{h_1} : \xi'_1(z), \\ \tilde{H}_2(z) \to I_{h_2} : \xi'_2(z), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \tilde{H}_{n+r}(z) \to I_{h_{n+r}} : \xi'_{n+r}(z). \end{cases}$$

Восстановление целостности данных осуществляется любым известным методом коррекции ошибок модулярных полиномиальных кодов.

7. Оценка эффективности подсистемы аутентификации в КФС

Будем рассматривать следующие основные показатели качества операции[8] в подсистеме аутентификации:

1) результативность v – характеризуется получаемым в результате операции целевым эффектом;

2) ресурсоемкость r – характеризуется расходом операционных ресурсов;

3) оперативность τ – характеризуется расходом операционного времени, т.е. времени, потребного достижения целей операции.

В совокупности указанные показатели определяют комплексный показатель качества операции $Y_{\langle 3\rangle} = \langle v, r, \tau \rangle$.

При сравнительном оценивании качества результата операции возможно возникновение противоречий из-за неоднозначности ситуации принятия

8 Петухов Г. Б., Якунин В. И. Методологические основы внешнего проектирования целенаправленных процессов и целеустремленных систем. М.: АСТ, 2006. 504 с.

решения, поскольку по одним показателям более качественным может оказаться одно решение, а под другим – другое. Такая задача принятия решения является многокритериальной.

Применительно к показателям $Y_{\langle 3\rangle}$ качества результатов аутентификации эти требования носят односторонний характер. Так, возможный целевой эффект $\hat{v}$ должен быть не менее требуемого (минимально допустимого) $\hat{v}^4$, возможные затраты $\hat{r}$ ресурсов должны быть не выше максимально допустимых $\hat{r}^4$, называемых предельными, цель должна быть достигнута за время $\hat{\tau}$, не превышающее директивного $\hat{\tau}^4$.

Тогда область $\left\{\hat{Y}^4_{\langle 3\rangle}\right\}$ допустимых значений результатов операции будет представлять собой трехмерный октант (рис. 4):

$$\left\{\hat{Y}^{\text{д}}_{\langle 3\rangle}\right\} = \left[\hat{v}^{\text{д}}, \infty\right) \times \left(-\infty, \hat{r}^{\text{д}}\right) \times \left(-\infty, \hat{\tau}^{\text{д}}\right),$$

с вершиной в точке $\hat{Y}^{\text{д}}_{\langle 3\rangle} = \left(\hat{v}^{\text{д}}, \hat{r}^{\text{д}}, \hat{\tau}^{\text{д}}\right)$.

Рассмотрим указанные показатели качества подсистемы аутентификации.

1. Результативность.

Так как целью решения задачи аутентификации является подтверждение заявленных свойств субъекта доступа, то можно говорить о скачкообразном изменении свойств аутентифицируемого объекта. Для таких операций говорят о качественном характере полезного эффекта.

При этом эффект проявляется в виде наступления какого-либо события, что возможно только при выполнении соответствующих условий. Обычно эти условия формулируются в виде требований к показателям качества системы, к которым в данном случае относятся основные эксплуатационно-технические характеристики F_i, $i = \overline{1, n}$.

Результат свертывания данных величин приводит к обобщенным скалярным функциям. При этом фигурирующие в них весовые коэффициенты призваны отражать относительные «важности» отдельных частных свойств результатов операции для достижения ее цели.

Распространенным методом выражения различий критериев по «важности» является назначение каждому из них некоторого веса с последующим суммированием этих весов в рамках операции свертки. Однако при использовании данного подхода не учитывается нелинейный характер влияния показателей друг на друга и в целом на обобщенный показатель[9].

В случае, когда отсутствуют объективные физические шкалы для оценки показателей, предпочтительно использование размытого варианта ожидаемой полезности, примером которого является вычисление нечеткого интеграла λ-нечеткой меры Сугено:

$$X = \int h \circ G_\lambda = \sup_{\alpha \in [0,1]} \min\left\{\alpha, G_\lambda\left(F_\alpha\right)\right\},$$

где: $F_\alpha = \left\{F_i \mid h\left(F_i\right) \geq \alpha\right\}$ – множество параметров, степень влияния которых превышает порог α;

$h : X \to [0,1]$ – оценочная функция, которая строится путем нормировки частных параметров F_i, $i \in N\left(N = \{1, 2, \ldots, n\}\right)$;

$(\circ)$ – символ вычисления нечеткого интеграла.

Мера Сугено для рассматриваемого случая имеет следующий вид:

$$G_\lambda\left(\left\{F_i, i \in N'\right\}\right) = \frac{1}{\lambda}\left(\prod_{i \in N'}\left(1 + \lambda g_i\right) - 1\right);$$

$$N' \subseteq N$$

где g_i – плотность распределения этой нечеткой меры.

Значение λ находится из условия нормировки:

$$\frac{1}{\lambda}\left(\prod_{i=1}^{n}\left(1 + \lambda g_i\right) - 1\right) = 1, \quad -1 < \lambda < \infty.$$

Тогда возможный целевой эффект характеризуется случайной величиной:

$$\hat{v} = \begin{cases} 1, \text{ если } X \in \left\{X^{\text{д}}_{\langle n\rangle}\right\}, \\ 0, \text{ если } X \notin \left\{X^{\text{д}}_{\langle n\rangle}\right\}, \end{cases}$$

где $\left\{X^4_{\langle \text{n}\rangle}\right\}$ – область допустимых значений нечеткого интеграла λ-нечеткой меры Сугено.

В качестве частного показателя полезного эффекта может выступать математическое ожидание соответствующей случайной величины. При этом, если некоторая величина $\hat{v}_j$ имеет двухточечное распределение, то есть ее возможными значениями являются 0 и 1, то математическое ожидание такой случайной величины равно:

$$M\left\{\hat{v}_j\right\} = P\left(\hat{v}_j = 1\right) = P\left(X \in \left\{X^{\text{д}}_{\langle n\rangle}\right\}\right).$$

2. Ресурсоемкость.

Ресурсоемкость оценивается со стороны количества и качества затрат ресурсов, которые в общем случае характеризуются n-мерным вектором:

$$\hat{R}_{\langle n\rangle} = \left\langle \hat{r}_1, \hat{r}_2, \ldots, \hat{r}_n \right\rangle.$$

9 Леоненков А. В. Нечеткое моделирование в среде MATLAB и fuzzyTECH. СПб.: БХВ-Петербург, 2005. 736 с.

В качестве основного показателя затрат обычно рассматривается их математическое ожидание, которое в данном случае будет представлять собой векторную величину:

$$M_{\langle n\rangle}\left\{\hat{R}_{\langle n\rangle}\right\}=\left\langle M\left\{\hat{r}_1\right\}, M\left\{\hat{r}_2\right\}, \ldots, M\left\{\hat{r}_n\right\}\right\rangle .$$

3. Оперативность.

Показателем оперативности аутентификации является длительность $\hat{\tau}$ периода выполнения задачи, которая также является случайной величиной, и для ее оценивания должны применяться ее вероятностные характеристики:

$$P\left(\hat{\tau}\le\hat{\tau}^{\text{Д}}\right)=\int_{-\infty}^{\infty}F_{\hat{\tau}}(\tau)dF_{\hat{\tau}^{\text{Д}}}(\tau) .$$

Математическая формулировка критерия оптимальности многоагентной аутентификации в КФС в векторной форме представляется в виде:

$$O:\left(\hat{Y}_{\langle 3\rangle}\in\left\{\hat{Y}^{\text{Д}}_{\langle 3\rangle}\right\}\right)\cap\left(\hat{Y}_{\langle 3\rangle}=Y^{\text{ОПТ}}_{\langle 3\rangle}\right)\cong$$

$$\cong\left(\hat{Y}_{\langle 3\rangle}\in\left\{\hat{Y}^{\text{Д}}_{\langle 3\rangle}\right\}^{\text{ОПТ}}\right)\cong U ,$$

где:

$\hat{Y}^{\text{ОПТ}}_{\langle 3\rangle}$ – оптимальное значение показателя качества результата аутентификации;

$\left\{\hat{Y}^{\text{Д}}_{\langle 3\rangle}\right\}^{\text{ОПТ}}$ – множество (область) допустимых значений показателя качества оптимального результата аутентификации;

$\cap$ – символ булева пересечения событий (конъюнкции высказываний);

U – достоверное событие;

$\cong$ – знак равносильности высказываний (событий).

Критерий оптимальности для рассматриваемого случая:

$$O: P_{\text{ДЦ}}=P^{\text{ОПТ}}_{\text{ДЦ}}=P\left(\hat{Y}_{\langle 3\rangle}\in\left\{\hat{Y}^{\text{Д}}_{\langle 3\rangle}\right\}^{\text{ОПТ}}\right),$$

где:

$P_{\text{ДЦ}}$ – вероятность достижения цели процесса аутентификации субъектов доступа;

$P^{\text{ОПТ}}_{\text{ДЦ}}$ – вероятность достижения оптимального значения показателя качества результата аутентификации.

При решении задачи оптимального синтеза процесса многоагентной аутентификации в КФС и обеспечивающей ее функционирование подсистемы следует учитывать требования, предъявляемые к каждой из представленных характеристик.

Заключение

Развитие КФС в настоящее время осуществляется по пути создания интеллектуальных цифровых двойников, способных обмениваться обучающими данными. Для этого цифровые двойники наделяются правами владельцев ресурсов, что предъявляет новые требования к аутентификации субъектов доступа в динамичных и масштабируемых КФС.

Обеспечение выполнения указанных требований основывается на использовании подсистемы многоагентной аутентификации с интеллектуальным управлением, реализуемым на основе математических методов анализа многоместных отношений.

Переход к многоагентной аутентификации обуславливает полезность использования криптокодовых протоколов, позволяющих обеспечить аутентификацию субъектов в многоканальных системах.

Для оценки эффективности подсистемы многоагентной аутентификации в КФС предлагается использовать размытый вариант ожидаемой полезности, вычисляемый с использованием нечеткого интеграла.

Литература

1. Cardin O. Classification of cyber-physical production systems applications: Proposition of an analysis framework // Computers in Industry, 2018, DOI: 10.1016/j.compind.2018.10.002.
2. Wen Tong, Peiying Zhu. 6G: The Next Horizon. From Connected People and Things to Connected Intelligence // Cambridge University Press, 2021. ISBN 978-1-108-83932-7
3. Huang Z., Shen Y., Li J., Fey M., Brecher C. AI-Driven Digital Twins // Sensors, 2021, 21, 6340. HTTPS: //doi.org/10.3390/s21196340.
4. Fuller A., Fan Z., Day C., Barlow C. Digital Twin: Enabling Technologies, Challenges and Open Research // IEEE Access, 2020. DOI 10.1109/ACCESS.2020.2998358.
5. Jamil S., Rahman M., Fawad. A comprehensive Survey of Digital Twins and Federated Learning for Industrial Internet of Things (IIoT), Internet of Vehicles (IoV) and Internet of Drones (IoD) // Appl. Syst. Innov. 2022, 5, 56. HTTPS://doi.org/10.3390/asi5030056.
6. De Silva Mendonca R., de Oliveira Lins S., de Bessa I.V., de Carvalho Ayres F.A.Jr., de Medeiros R.L.P., de Lucena V.F.Jr. Digital Twin Applications: A Survey of Recent Advances and Challenges // Process, 2022, 10, 744. HTTPS: doi.org/10.3390/pr10040744.
7. Enad E.H., Younis S. Machine Learning based Decision Strategies for Physical Layer Authentication in Wireless Systems // 2020 2nd Annual International Conference on Information and Sciences (AiCIS), 2020, pp. 114-118. DOI: 10.1109/AICIS51645.2020.00028.
8. Jiang J.-R. Short Survey on Physical Layer Authentication by Machine-Learning for 5G-based Internet of Things // 2020 3rd IEEE International Conference on Knowledge Innovation and Invention (ICKII), 2020, pp. 41-44. DOI: 10.1109/ICKII50300.2020.9318879.
9. Yoon J., Lee Y., Hwang E. Machine Learning-based Physical Layer Authentication using Neighborhood Component Analysis in MIMO Wireless Communications // 2019 International Conference on Information and Communication Technology Convergence (ICTC), 2019, pp. 63-65.
10. Fang H., Wang X., Tomasin S. Machine Learning for Intelligent Authentication in 5G and Beyond Wireless Networks // IEEE Wireless Communications, 2019, Vol. 26, N. 5, pp. 55-61. DOI: 10.1109/MWC.001.1900054.
11. Bordel S.B., Alcarria R., Robles T., Martín D. Cyber-physical systems: Extending pervasive sensing from control theory to the Internet of Things // Pervasive and Mobile Computing, 40. DOI: 10.1016/j.pmcj.2017.06.011.
12. Ferrag M.A., Maglaras L.A., Janicke H., Jiang J., Shu L. Authentication Protocol for Internet of Things: A Comprehensive Survey // Security and Communication Networks, 2017. HTTPS://doi.org/10.1155/2017/6562953.
13. Alguliev R., Imamverdiyev Y., Sukhostat L., Cyber-phesical systems and their security issues // Computer in Industry, 100, 2018, pp. 212-223. HTTPS://doi.org/10.1016/j.compind. 2018.04.017.
14. Shaikh H.A., Monjil M.B., Chen S., Farahmandi F., Asadizanjani N., Tehranipoor M., Rahman F. Digital Twin for Secure Semiconductor Lifecycle Management: Prospects and Applications // Future Hardware Security Research Series, 2022.
15. Патент № 2763165 Российская Федерация, МПК G01S 13/78 (2006.01). Способ и система опознавания малогабаритных робототехнических средств: № 2021102008: заявл. 28.01.2021: опубликовано 28.12.2021 / Балюк А.А., Махов Д.С., Финько О.А., Шпырня И.В.; заявитель КВВУ. – 14 с.
16. Кулик Б.А. Логика и математика: просто о сложных методах логического анализа / Б.А. Кулик; под общ. ред. А.Я. Фридмана. – СПб.: Политехника, 2020. – 141 с.
17. Samoylenko D., Eremeev M., Finko O., Dichenko S. Protection of Information from Imitation on the Basis of Crypt-Code Structures // Advances in Soft and Hard Computing ACS 2018. Advances in Intelligent Systems and Computing. Springer. Cham, 2019, pp. 317-331.
18. Диченко С.А., Финько О.А. Гибридный крипто-кодовый метод контроля и восстановления целостности данных для защищенных информационно-аналитических систем // Вопросы кибербезопасности. 2019, № 6(34), с. 17-36. DOI:10.21681/2311-3456-2019-6-17-36
19. Dichenko S.A., Finko O.A. Controlling and Restoring the Integrity of Multi-Dimensional Data Arrays Through Cryptocode Constructs // Programming and Computer Software. 2021, 47, № 6, pp. 415-425.
20. Диченко С.А., Финько О.А. Контроль и восстановление целостности многомерных массивов данных посредством криптокодовых конструкций // Программирование, 2021, № 6, С. 3-15. eLIBRARY ID: 46621832

INFORMATION SECURITY OF CYBER-PHYSICAL SYSTEMS: AUTHENTICATION OF DIGITAL TWINS

Balyuk A.A.[10], Finko O.A.[11]

Formulation of the problem: *the main catalysts for the development of cyber-physical systems are currently the growth of artificial intelligence and the creation of digital twins that have a complex vertical structure and exchange data for joint learning. At the same time, the empowerment of digital twins as data owners can lead to critical consequences in the field of ensuring the security of data systems. The development of evolutionary methods for ensuring information security, and in particular, methods for authenticating digital twins, is a fundamental issue on the way to the development of cyber-physical systems.*

Objective: *analysis of aspects and principles of building a system and the process of authenticating digital twins in dynamic and scalable cyber-physical systems, organizing the process under study, indicators of its effectiveness and criteria for their evaluation.*

Methods used: *system analysis, tuple algebra, methods for designing and evaluating the efficiency of complex systems.*

Novelty: *the use of a multi-agent structure of the digital twin authentication system, which makes it possible to achieve guaranteed awareness of the security status of the system as a whole and respond appropriately in case of compromising events. The implementation of intelligent authentication management is proposed to be carried out using the application capabilities of tuple algebra, which takes into account differences in the structures of traditional and intelligent systems, as well as the difficulties of parallelization in distributed systems. To increase the stability of the multi-agent authentication system, the possibility of using cryptocode protocols is considered, which makes it possible to ensure the restoration of reliable authentication data in case of failures.*

Result: *substantiation of new principles and technological solutions in the field of high-level design of cyber-physical systems.*

Keywords: *robotic complexes, artificial intelligence, multi-agent system, algebra of motorcades, cryptocode constructions, fuzzy integral.*

References

1. Cardin O. Classification of cyber-physical production systems applications: Proposition of an analysis framework // Computers in Industry, 2018, DOI: 10.1016/j.compind.2018.10.002.
2. Wen Tong, Peiying Zhu. 6G: The Next Horizon. From Connected People and Things to Connected Intelligence // Cambridge University Press, 2021. ISBN 978-1-108-83932-7
3. Huang Z., Shen Y., Li J., Fey M., Brecher C. AI-Driven Digital Twins // Sensors, 2021, 21, 6340. HTTPS: //doi.org/10.3390/s21196340.
4. Fuller A., Fan Z., Day C., Barlow C. Digital Twin: Enabling Technologies, Challenges and Open Research // IEEE Access, 2020. DOI 10.1109/ACCESS.2020.2998358.
5. Jamil S., Rahman M., Fawad. A comprehensive Survey of Digital Twins and Federated Learning for Industrial Internet of Things (IIoT), Internet of Vehicles (IoV) and Internet of Drones (IoD) // Appl. Syst. Innov. 2022, 5, 56. HTTPS://doi.org/10.3390/asi5030056.
6. De Silva Mendonca R., de Oliveira Lins S., de Bessa I.V., de Carvalho Ayres F.A.Jr., de Medeiros R.L.P., de Lucena V.F.Jr. Digital Twin Applications: A Survey of Recent Advances and Challenges // Process, 2022, 10, 744. HTTPS: doi.org/10.3390/pr10040744.
7. Enad E.H., Younis S. Machine Learning based Decision Strategies for Physical Layer Authentication in Wireless Systems // 2020 2nd Annual International Conference on Information and Sciences (AiCIS), 2020, pp. 114-118. DOI: 10.1109/AICIS51645.2020.00028.
8. Jiang J.-R. Short Survey on Physical Layer Authentication by Machine-Learning for 5G-based Internet of Things // 2020 3rd IEEE International Conference on Knowledge Innovation and Invention (ICKII), 2020, pp. 41-44. DOI: 10.1109/ICKII50300.2020.9318879.
9. Yoon J., Lee Y., Hwang E. Machine Learning-based Physical Layer Authentication using Neighborhood Component Analysis in MIMO Wireless Communications // 2019 International Conference on Information and Communication Technology Convergence (ICTC), 2019, pp. 63-65.
10. Fang H., Wang X., Tomasin S. Machine Learning for Intelligent Authentication in 5G and Beyond Wireless Networks // IEEE Wireless Communications, 2019, Vol. 26, N. 5, pp. 55-61. DOI: 10.1109/MWC.001.1900054.

10 Aleksey A. Balyuk, Ph.D., Krasnodar Higher Military Order of Zhukov and the October Revolution Red Banner School named after General of the Army S.M. Shtemenko, Krasnodar, Russia. E-mail: alexbaluk689@gmail.com

11 Oleg A. Finko, Dr.Sc., Professor, Russian Academy of Rocket and Artillery Sciences, Krasnodar Higher Military Order of Zhukov and the October Revolution Red Banner School named after General of the Army S.M. Shtemenko, Krasnodar, Special Technological Center, St. Petersburg, Russia. E-mail: ofinko@yandex.ru

11. Bordel S.B., Alcarria R., Robles T., Martín D. Cyber-physical systems: Extending pervasive sensing from control theory to the Internet of Things // Pervasive and Mobile Computing, 40. DOI: 10.1016/j.pmcj.2017.06.011.
12. Ferrag M.A., Maglaras L.A., Janicke H., Jiang J., Shu L. Authentication Protocol for Internet of Things: A Comprehensive Survey // Security and Communication Networks, 2017. HTTPS://doi.org/10.1155/2017/6562953.
13. Alguliev R., Imamverdiyev Y., Sukhostat L., Cyber-phesical systems and their security issues // Computer in Industry, 100, 2018, pp. 212-223. HTTPS://doi.org/10.1016/j.compind. 2018.04.017.
14. Shaikh H.A., Monjil M.B., Chen S., Farahmandi F., Asadizanjani N., Tehranipoor M., Rahman F. Digital Twin for Secure Semiconductor Lifecycle Management: Prospects and Applications // Future Hardware Security Research Series, 2022.
15. Patent № 2763165 Rossijskaja Federacija, MPK G01S 13/78 (2006.01). Sposob i sistema opoznavanija malogabaritnyh robototehnicheskih sredstv: № 2021102008: zajavl. 28.01.2021: opublikovano 28.12.2021 / Baljuk A.A., Mahov D.S., Fin'ko O.A., Shpyrnja I.V.; zajavitel' KVVU. – 14 s.
16. Kulik B.A. Logika i matematika: prosto o slozhnyh metodah logicheskogo analiza / B.A. Kulik; pod obshh. red. A.Ja. Fridmana. – SPb.: Politehnika, 2020. – 141 s.
17. Samoylenko D., Eremeev M., Finko O., Dichenko S. Protection of Information from Imitation on the Basis of Crypt-Code Structures // Advances in Soft and Hard Computing ACS 2018. Advances in Intelligent Systems and Computing. Springer. Cham, 2019, pp. 317-331.
18. Dichenko S.A., Fin'ko O.A. Gibridnyj kripto-kodovyj metod kontrolja i vosstanovlenija celostnosti dannyh dlja zashhishhennyh informacionno-analiticheskih sistem // Voprosy kiberbezopasnosti. 2019, № 6(34), s. 17-36. DOI:10.21681/2311-3456-2019-6-17-36
19. Dichenko S.A., Finko O.A. Controlling and Restoring the Integrity of Multi-Dimensional Data Arrays Through Cryptocode Constructs // Programming and Computer Software. 2021, 47, № 6, pp. 415-425.
20. Dichenko S.A., Fin'ko O.A. Kontrol' i vosstanovlenie celostnosti mnogomernyh massivov dannyh posredstvom kriptokodovyh konstrukcij // Programmirovanie, 2021, № 6, S. 3-15. eLIBRARY ID: 46621832