ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ДВОЙНИКОВ С ЦЕЛЬЮ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

Водопьянов А. С.[1]

DOI: 10.21681/2311-3456-2024-4-140-144

Цель исследования *– работа посвящена исследованию методов использования цифровых двойников с целью обеспечения информационной безопасности киберфизических систем.*

Методология проведения работы*. При проведении исследований использовался системный анализ для анализа области применения цифровых двойников, их классификаций и моделей взаимодействия. При разработке прототипа цифрового двойника использовались математические модели, основанные на теории автоматов.*

Результат: *в результате исследования были рассмотрены понятия киберфизической системы и цифрового двойника, приведены существующие методы обеспечения информационной безопасности киберфизических систем, получены методы, повышающие информационную безопасность при синхронизации цифрового двойника и киберфизической системы, рассмотрены этапы обеспечения информационной безопасности с использованием цифрового двойника, причины преимущества цифрового двойника для промышленности, а также существующие протоколы по которым киберфизические системы взаимодействуют с киберпространством.*

Область применения результатов*. Полученные результаты не противоречат существующим нормативным документам по защите КИИ и могут быть использованы для повышения эффективности систем защиты информации в КИИ на этапах их проектирования и мониторинга работы.*

Научная новизна*. Предложена концептуальная модель цифровых двойников и классификация решаемых ими задач. Разработана модель цифрового двойника для проектирования систем управления информационной безопасностью.*

Ключевые слова: *синхронизация, концептуальная модель, конечные автоматы, критическая информационная инфраструктура.*

USING DIGITAL TWINS TO ENSURING INFORMATION SECURITY OF CYBERPHYSICAL SYSTEMS

Vodopyanov A. S.[2]

Purpose of the study *– the work is devoted to the study of methods for using digital twins to ensure information security of cyber-physical systems.*

Methodology of work*. When conducting research, system analysis was used to analyze the scope of digital twins, their classifications and interaction models. When developing a digital twin prototype, mathematical models based on automata theory.*

Result: *as a result of the study, the concepts of a cyber-physical system and a digital twin were considered, existing methods for ensuring information security of cyber-physical systems were given, methods were obtained that increase information security when synchronizing a digital twin and a cyber-physical system, the stages of ensuring information security using a digital twin were considered, the reasons for the advantages of a digital a double for industry, as well as existing protocols by which cyber-physical systems interact with cyberspace.*

Scope of application of the results*. The results obtained do not contradict existing regulatory documents on the protection of computer information systems and can be used to improve the efficiency of information security systems in computer information systems at the stages of their design and monitoring of operation.*

Scientific novelty*. A conceptual model of digital twins and a classification of the problems they solve are proposed. A digital twin model has been developed for the design of information security management systems.*

Keywords: *synchronization, conceptual model, finite state machines, critical information infrastructure.*

1 Водопьянов Александр Сергеевич, консультант Управления Федеральной службы по техническому и экспортному контролю Российской Федерации по Центральному федеральному округу. Москва, Россия. E-mail: AlexandrALex2024@yandex.ru

2 Alexander S. Vodopyanov, Consultant of the Office of the Federal Service for Technical and Export Control of the Russian Federation in the Central Federal District. Moscow, Russia. E-mail: AlexandrALex2024@yandex.ru.

Введение

Прогресс в сфере информационных и телекоммуникационных технологий дал старт новой (информационной) эпохе и появлению нового (информационного) общества, в котором информация и связь приобретают доминирующую ценность. В ходе развертывания информационной эпохи происходит формирование новой парадигмы влияния информационно-телекоммуникационных технологий на развитие самых разных отраслей промышленности, экономики и общества в целом.

Но вместе с прогрессом появляются и новые угрозы безопасности информации, они представляются в виде использовании различных новых методов хищения информации, использования новых типов вредоносного программного обеспечения, хакерских атаках, подмены результатов работы систем и их компонентов и многого другого. В том числе эти риски выражаются в киберфизических системах, имеющих в себе не только повседневные технологии, но и уникальные (особенные) методы и принципы работы, не задействованные нигде более, кроме как в данных решениях.

Работа киберфизических систем спасает жизни и обеспечивает устойчивое развитие экономики государства уже сегодня, но без должного уровня обеспечения их информационной безопасности, они могут представлять большую угрозу.

Существующие методы защиты киберфизических систем

Понятие киберфизических систем часто рассматривают совместно с понятием систем интернета вещей. Оба типа систем имеют схожие элементы, однако киберфизические системы являются более широким понятием и имеют более сложную архитектуру [4]. Киберфизическая система – это система, которая может эффективно интегрировать кибер- и физические компоненты, используя современные сенсорные, вычислительные и сетевые технологии [7].

Главная схожесть архитектур заключается в том, что на нижнем уровне киберфизических систем и систем интернета вещей лежит сенсорная сеть. Сенсорная сеть представляет собой динамическую, самоорганизующуюся и распределенную сеть датчиков и исполнительных устройств. Она предназначена для решения задач автоматизации, диагностики, телеметрии и межмашинного взаимодействия. Значительное внимание уделяется также прикладным возможностям киберфизических систем, позволяющим эффективно связывать объекты физического мира – производственные системы, транспортные средства, объекты энергетики, – с киберфизическим миром через вычислительные, информационно-коммуникационные сети, формируя единую информационно-управляющею среду [8].

Защита киберфизических систем строится в основном на защите стека технологий, лежащих в её основе, это мониторинг и анализ трафика элементов киберфизической системы, применение на её элементах механизмов идентификации, аутентификации и управления доступом, а также использование более стойких алгоритмов криптографической защиты информации, эти решения имеют высокую надёжность как метод защиты, но при этом могут оказывать в том числе и негативное влияние на целостность и доступность элементов киберфизических систем.

Традиционные средства защиты, такие как межсетевые экраны, средства антивирусной защиты, средства обнаружения и предотвращения вторжений и др., часто эффективны не в полной мере для защиты IoT-инфраструктуры из-за того, что трафик, генерируемый системой специфичен и сложен в анализе, а устройства взаимодействуют напрямую друг с другом.

Киберфизические системы могут получать доступ к киберпространству по различным сетевым протоколам, таким как Wi-Fi, WiMAX, GPRS и технологиям 3G/4G/LTE. Другие облегченные протоколы, такие как MQTT, CoAP, AMQP, Websocket, Node используются для передачи данных с периферийных устройств в облако для дальнейшего хранения и обработки. Каждый протокол имеет свои преимущества перед другими в зависимости от скорости, задержки, пропускной способности, надежности, безопасности и масштабируемости [9].

В общем виде система обнаружения вторжений для киберфизических систем осуществляет сбор трафика или его статистики и сравнивает собранные данные с эталоном, и любое отклонение от эталона может свидетельствовать об атаке [2]:

- изменение количества узлов в сети – это напрямую указывает на наличие нелегитимного узла;
- изменение уровня мощности сигнала узла – резкое изменение уровня принимаемого сигнала может свидетельствовать о подмене передающего узла;
- изменение маршрутов доставки данных – большинство киберфизических систем имеют ячеистую топологию, а одним из критериев выбора маршрута доставки является качество сигнала. Поэтому изменение маршрута может быть вызвано добавлением нового узла или подменой существующего, а соответственно, и влиянием на качество передачи;
- увеличение или уменьшение числа кадров, изменение типа трафика – в киберфизических системах узлы генерируют, как правило, однотипный трафик, поэтому изменение количества трафика

и его типа, например рост числа служебных пакетов, может указывать на присутствие злоумышленника;
- ухудшение характеристик производительности сети – снижение пропускной способности, увеличение задержек также может указывать на присутствие злоумышленника в системе;
- уменьшение или увеличение времени реакции на запросы – данный факт может указывать на подмену легитимного узла, например, более производительным устройством, в случае более быстрой реакции на запросы;
- изменение временных периодов отправки данных – узлы.

Каждый параметр отклонения в отдельности может давать ложный результат, поэтому их следует использовать в совокупности, но это усложняет задачу защиты киберфизических систем.

Использование цифрового двойника для обеспечения информационной безопасности киберфизических систем

Термин «цифровой двойник» появился более десяти лет назад и до сих пор не имеет четкого определения. Тем не менее интерес к этому направлению постоянно возрастает и особенно в тех областях, где много неформализуемых задач, нечетких значений параметров, случайных и непредвиденных ситуаций в автоматизированных системах управления, критических информационных инфраструктурах и социально значимых информационных системах. DT во многом могут решать часть этих задач на этапах проектирования, внедрения и мониторинга этих систем [5].

Использование цифровых двойников, является также одним из новых подходов в обеспечении информационной безопасности киберфизических систем.

Среди основных преимуществ цифровых двойников для промышленности [6] отметим, что они:

- позволяют реализовать дистанционный мониторинг и управление физическим объектом в реальном времени (РВ) там, где это невозможно другими средствами;
- обеспечивают большую автономию персонала в случае необходимости, таким образом повышая эффективность и безопасность производства, что особенно ценно с учетом опыта пандемии 2020 г.;
- создают условия для предиктивного обслуживания и планирования ремонтов оборудования за счет обработки и интеллектуального анализа в РВ больших объемов данных о работе промышленных активов;
- делают возможным анализ производственных сценариев и оценку риска путем проигрывания нештатных ситуаций без ущерба для реального производства;
- поддерживают и ускоряют принятие решений за счет расширенной аналитики данных в РВ;
- упрощают документирование и коммуникации, используя легкодоступную on-line информацию, и в сочетании с автоматизированной отчетностью повышают прозрачность бизнес-процессов.

Следовательно, при рассмотрении взаимодействия между технологическими процессами предприятия и процессами управления информационной безопасности, специалист по защите информации нуждается в исследовании обратной связи.

Технология цифровых двойников может позволить собирать цифровые следы с учётом уровня информационного риска при эмпирически определённых ситуациях.

Это может быть реализовано в форме имитационных моделей, обучающихся на основе сценариев реального использования с учетом особенностей технологического процесса и накопленных оперативных данных, а также виртуальных или аппаратных лабораторных стендах.

Цифровой двойник может быть как подключен к системе напрямую, обмениваясь с ней данными, так и использоваться в асимметричной схеме, когда обмен данными происходит в оговоренном заранее дискретном временном режиме.

Обеспечение безопасности с использованием технологии цифрового двойника гибкое и может проводиться на всех этапах жизненного цикла, позволяя моделировать различные события безопасности.

На этапе создания, это возможность изучения безопасного дизайна, обнаружения неправильной конфигурации программного обеспечения и тестирования механизмов безопасности [3].

На этапе эксплуатации, цифровой двойник может позволить обнаруживать вторжения, внедрять механизмы аутентификации, идентификации и использовать криптостойкие алгоритмы шифрования, без дополнительной нагрузки на физическую систему.

На этапе вывода из эксплуатации, цифровой двойник может помочь сохранять конфиденциальность информации в киберфизической системе.

В отличии от тех же «песочниц», использование цифрового двойника может усилить контроль за безопасностью киберфизических систем по следующим причинам:

1. Цифровой двойник может быть спроектирован таким образом, чтобы оставаться активным, не изолируя реальную среду на определённое время t, с встроенными функциями изоляции тупиковых областей тестирования.

2. Обладать свойствами размножения (ветвления) потоков команд и данных для параллельного изучения поведения (анализа) в сегментах двойника.
3. Быть не единственным и иметь «клонов» для реализации при защите информационной инфраструктуры метода «медовых ловушек».
4. Заставлять работать систему в условиях со смещённым временем, для анализа угроз, связанным со срабатыванием по времени.

Основными данными при обеспечении безопасности киберфизической системы может быть [10]:

- ❖ первичное измерительное оборудование (датчики и приборы);
- ❖ преобразование измеряемых параметров в цифровой формат;
- ❖ достаточная вычислительная мощность и хранилище данных;
- ❖ совершенная сетевая инфраструктура;
- ❖ внедрение предиктивной аналитики, позволяющей отслеживать и диагностировать состояния системы, а также прогнозировать возможные сбои.

При этом на всех этапах необходимо и контролировать выполнение требований о защите информации, а именно:

- ❖ к процессу хранения, передачи и обработки защищаемой в киберфизической системе информации;
- ❖ к киберфизической системе;
- ❖ к взаимодействию киберфизической системы с цифровым двойником;
- ❖ к условиям функционирования киберфизической системы;
- ❖ к содержанию работ по созданию (модернизации) киберфизической системы на различных стадиях и этапах ее создания (модернизации);
- ❖ к организациям (должностным лицам), участвующим в создании (модернизации) и эксплуатации киберфизической системы;
- ❖ к документации на киберфизическую систему.

Усилить безопасность взаимодействия цифрового двойника и киберфизической системы может, к примеру синхронизация в определённый период времени, что может снизить возможности злоумышленника при проведении целевых компьютерных атак на инфраструктуру [1].

Если описать данный метод с использованием конечных автоматов, то взаимодействие киберфизической системы и цифрового двойника представляется отношением элементов системы к их проекции в домене ($C \in X$).

Следовательно, значимые состояния элементов системы и их проекций в домене можно представить как множество этих состояний $S_c = \{S_{c0}, S_{c1}, S_{c2}, \ldots, S_{cn-1}\}$, $S_x = \{S_{x0}, S_{x1}, S_{x2}, \ldots, S_{xm-1}\}$, при этом значимых состояний двойника будет меньше, чем состояний физической системы ($n>m$), по причине того, что физическая часть системы остаётся главным контроллером домена цифрового двойника.

Множествами представляются и входные данные для физической системы и её цифрового двойника $I_c = \{I_{c0}, I_{c1}, \ldots, I_{cp-1}\}$, $I_x = \{I_{x0}, I_{x1}, \ldots, I_{xp-1}\}$.

При проведении синхронизации данных и контроля в период времени t, ключевое состояние киберфизической системы примет следующий вид: $S_{c,t} \in S_c$, следовательно такое же состояние примет и цифровой двойник $S_{x,t} \in S_x$. Входные данные также изменят своё состояние и будут представлены в следующем виде: $I_{c,t} \in I_c$ и цифровой двойник $I_{x,t} \in I_x$. Следовательно, можно вывести что начальные состояния киберфизической системы и цифрового двойника это $S_{c,0}$ и $S_{x,0}$.

Исходя из всего вышесказанного функции переходов выглядят как прямое произведение групп ключевых состояний и входных данных системы: $\delta_c: S_c \times I_c \longrightarrow S_c$ и $\delta_x: S_x \times I_x \longrightarrow S_x$.

Для обеспечения необходимого уровня их защиты при синхронизации, в предложенной схеме необходимо использовать шифрование по времени t $e_c \longrightarrow e_x$ или $e_x \longrightarrow e_c$.

Таким образом, полученный автомат можно увидеть на рисунке 1.

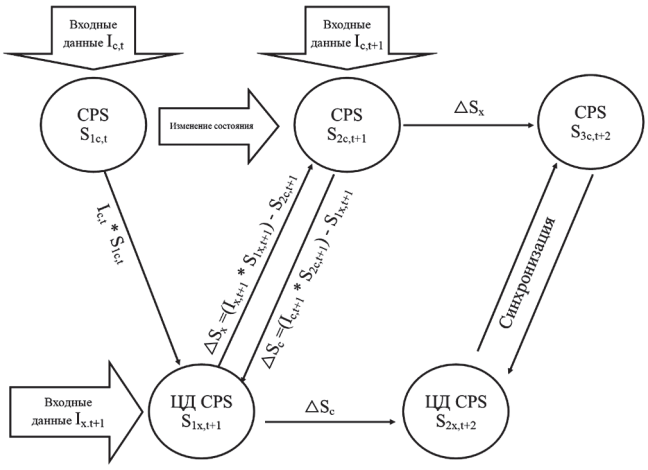

Рис. 1. Структура конечного автомата, двунаправленного порядка

Перед первой синхронизацией оператор отправляет ввод данных I_c в физический двойник

и система принимает первое ключевое состояние S_{1c}, следовательно в цифровом двойнике нет пока такого же состояния, после синхронизации, цифровой двойник получает на вход данные физической системы I_c и на основе её состояния S_{1c} принимает своё первое ключевое состояние S_{1x}.

В следующем временном интервале t+1, первое ключевое состояние цифрового двойника S_{1x} должно быть равно первому ключевому состоянию физической системы S_{1c} и когда физическая система получает на вход новую партию данных I_c она вычисляет разницу ΔS_c и отправляет её в цифровой двойник, который на её основе переходит уже в своё следующее ключевое состояние.

При двунаправленном обмене данными, оператор может подать набор данных I_x в цифровой двойник, тогда уже цифровой двойник будет использовать их для получения первого ключевого состояния S_{1x} и вычисления разницы необходимой для перехода физической системы в её новое состояние ΔS_x.

Следовательно, в момент времени t+2, если входных данных нет, ключевые состояния физической системы и цифрового двойника могут остаться прежними.

Если представить, что взаимодействие киберфизической системы и цифрового двойника однонаправленное (Рисунок 2), то мы получим другую структуру автомата. В этом случае синхронизация не потребуется, следовательно физическая система будет только передавать данные цифровому двойнику, что не позволит получить доступ из сети к физической системе злоумышленником.

Следовательно функция перехода будет выглядеть следующим образом: $\delta_c: S_c \times I_c \longrightarrow S_c$ и $\delta_x: S_c \times I_c \longrightarrow S_c$, $n = m$ так как домен для синхронизации не используется и оператор может только снимать показания телеметрии.

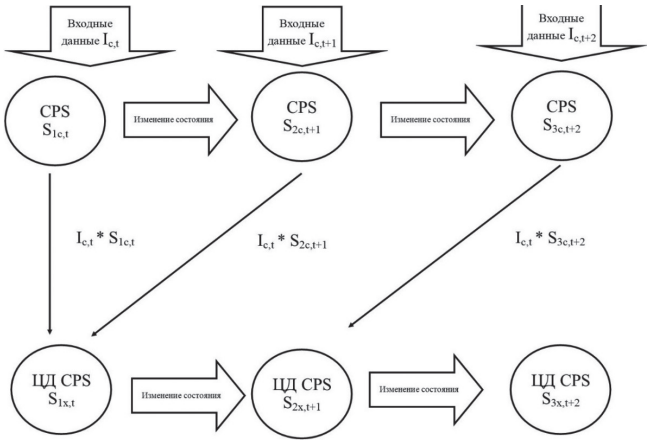

Рис. 2. Структура конечного автомата однонаправленного порядка

Вывод

Концепция цифровых двойников представляется новым направлением исследований в области информационной безопасности. На данный момент опубликовано лишь несколько статей, которые поверхностно касаются того, что может казаться возможным с использованием технологии цифровых двойников. Данный способ обеспечения безопасности киберфизических систем, с использованием технологий цифрового двойника лишь один из многих и позволяет немного повысить уровень защищённости при эксплуатации киберфизических систем, проблема данного решения заключается в сложности интеграции дополнительных модулей в поставляемое оборудование и их обслуживании.

Литература

1. *G. Lampropoulos, Kerstin V. Siakas – Enhancing and securing cyber-physical systems and Industry 4.0 through digital twins // A critical review July 2022Journal of Software: Evolution and Process 35(2011), DOI:10.1002/smr.2494.*
2. *M. Eckhart, A. Ekelhart – Digital Twins for Cyber-Physical Systems Security: State of the Art and Outlook // Security and Quality in Cyber-Physical Systems Engineering (pp.383–412), 2019. DOI:10.1007/978-3-030-25312-7_14.*
3. *Richard J. Somers, James A. Douthwaite, David J. Wagg, Neil D. Walkinshaw – Digital-twin-based testing for cyber–physical systems: A systematic literature review // Information and Software Technology Volume 156, 2022. DOI: 10.1016/j.insof.2022.107145.*
4. *Кушко Е. А., Грачёв Д. А., Паротькин Н. Ю., Золотарёв В. В. О вопросах безопасности киберфизических систем // Доклады Томского государственного университета систем управления и радиоэлектроники. 2022. № 4, том 2, С. 101–109 DOI: 10.21293/1818-0442-2022-25-4-101-109.*
5. *Минзов А. С., Невский А. Ю., Баронов О. Р., Немчанинова С.В. Цифровые двойники в системах управления // Вопросы кибербезопасности 2024 № 2(60). С.29–35. DOI: 10.21681/2311-3456-2024-2-29-35.*
6. *Дозорцев В. М. – Цифровые двойники в промышленности: генезис, состав, терминология, технологии, платформы, перспективы. Часть 1. Возникновение и становление цифровых двойников. Как существующие определения отражают содержание и функции цифровых двойников? // Автоматизация в промышленности DOI: 10.25728/avtprom.2020.09.01.*
7. *Расим Алгулиев, Ядигар Имамердиев, Людмила Сухостат – Обеспечение Информационной Безопасности Киберфизических Систем // Proqram mühəndisliyinin aktual elmipraktikiproblemləri. I respublika konfransı Bakı, 17 may 2017-ci il DOI: 10.25045/NCSoftEng.2017.07*
8. *Шкодырев В. П. Киберфизические системы как технологическая платформа синергетической интеграции перспективных прорывных технологий // Системный анализ в проектировании и управлении. 2020. DOI:10.18720/SPBPU/2/id20-109.*
9. *Смышляева А. А., Резникова К. М., Савченко Д. В. Современные технологии в Индустрии 4.0 – киберфизические системы // Интернет-журнал «Отходы и ресурсы», 2020. №3, DOI: 10.15862/02INOR320.*
10. *Мехтиев Ш. А. Анализ некоторых проблем надежности киберфизических систем // Информационные технологии в науке, образовании и производстве. 2022. №18(1). С. 42–47. DOI: 10.25045/NCInfoSec.2017.06.*