ПРОБЛЕМА ОБЕСПЕЧЕНИЯ КИБЕРУСТОЙЧИВОСТИ ОБЛАЧНЫХ ПЛАТФОРМ УПРАВЛЕНИЯ КИБЕРФИЗИЧЕСКИМИ ОБЪЕКТАМИ

Скиба В.Ю.[1], Балябин А.А.[2], Петренко С.А.[3]

Ключевые слова: *управление киберфизическими объектами, угрозы безопасности информации, модель нарушителя, киберустойчивость, технологическая и эксплуатационная безопасность, верифицируемая безопасность.*

Аннотация

Цель работы: *обеспечение устойчивости функционирования облачной платформы управления киберфизическими объектами за счет выявления деструктивных воздействий, приводящих к возможности нарушения семантики вычислительного процесса.*

Методы исследования: *системный анализ, классификация деструктивных воздействий, моделирование, спецификация, формальные языки.*

Результаты исследования: *сформулированы отличительные особенности облачных платформ управления киберфизическими объектами, предложено множество соотношений языков входных данных при наличии уязвимости семантики вычислительного процесса, определено множество вероятных нарушителей безопасности информации облачных платформ управления киберфизическими объектам.*

Научная новизна: *для облачных платформ управления киберфизическими объектами сформулированы новые элементы научно-методического аппарата для решения задачи выявления деструктивных воздействий, приводящих к возможности нарушения семантики вычислительного процесса.*

Практическая значимость: *разработанные формальные языки могут быть использованы при разработке методик проведения сертификационных и иных испытаний с целью выявления ошибок семантики вычислительного процесса.*

DOI: 10.24412/1994-1404-2025-4-26-38

Введение

Современные системы управления киберфизическими объектами развиваются в направлении внедрения так называемых сквозных информационных технологий [1]. К таким технологиям относятся технологии искусственного интеллекта, машинного обучения и анализа больших данных, технологии интернета вещей, блокчейн, облачных вычислений и другие. Применение новых цифровых технологий обусловлено необходимостью обработки больших объемов данных и обеспечения безопасности и устойчивости функционирования киберфизических систем.

В то же время цифровизация систем управления киберфизическими объектами неизбежно приводит к усложнению их архитектуры и росту требований к вычислительной мощности. Для решения данной проблемы программное обеспечение таких систем развертывают

[1] ***Скиба Владимир Юрьевич,*** *доктор технических наук, старший научный сотрудник, главный инженер-исследователь Научного центра информационных технологий и искусственного интеллекта АНОО ВО «Научно-технологический университет «Сириус», федеральная территория «Сириус», Краснодарский край, Российская Федерация, профессор кафедры ИБМ-6 ФГАОУ ВО «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)», г. Москва. ORCID: 0000-0002-9805-7800.*

E-mail: skiba.vy@talantiuspeh.ru

[2] ***Балябин Артем Алексеевич,*** *младший научный сотрудник Научного центра информационных технологий и искусственного интеллекта АНОО ВО «Научно-технологический университет «Сириус», федеральная территория «Сириус», Краснодарский край, Российская Федерация. ORCID: 0009-0006-3949-154X.*

E-mail: balyabin.aa@talantiuspeh.ru

[3] ***Петренко Сергей Анатольевич,*** *доктор технических наук, профессор, руководитель группы Научного центра информационных технологий и искусственного интеллекта АНОО ВО «Научно-технологический университет «Сириус», федеральная территория «Сириус», Краснодарский край, Российская Федерация. ORCID: 0000-0003-0644-1731.*

E-mail: petrenko.sa@talantiuspeh.ru

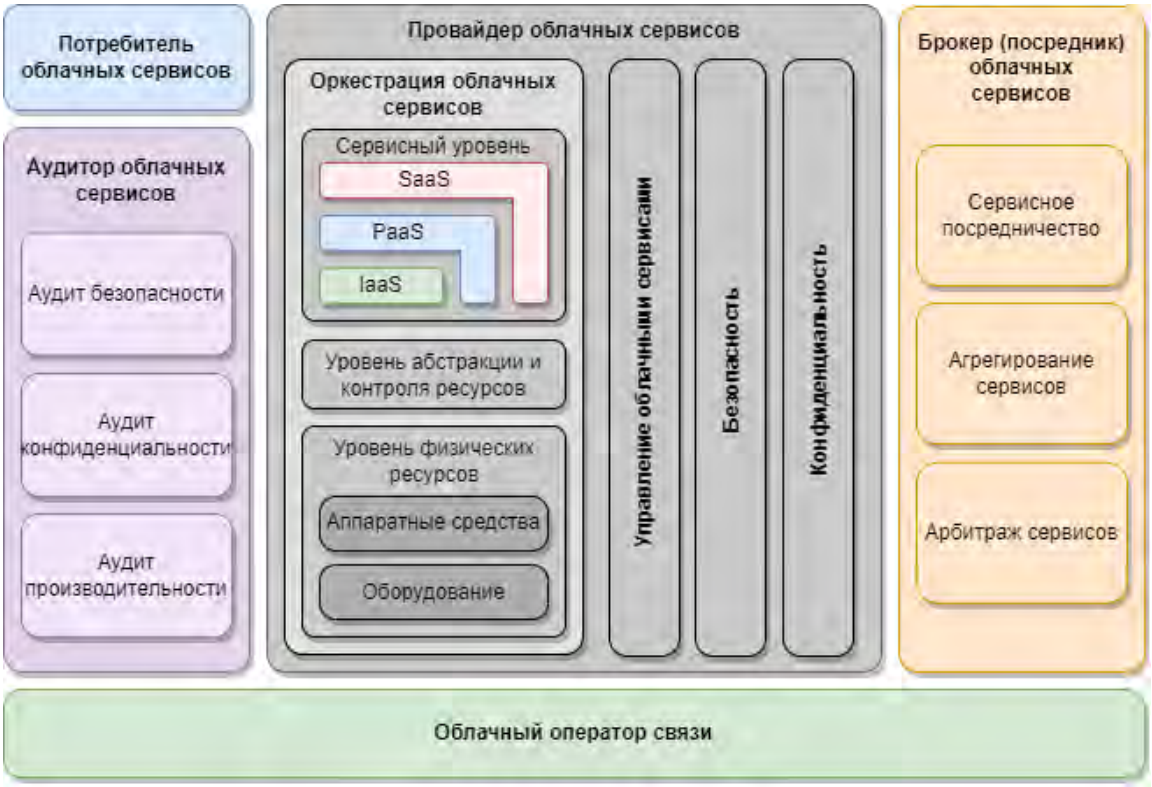

Рис.* 1. *Эталонная модель типовой облачной платформы

в облачной вычислительной среде. Облачные платформы предоставляют операторам возможность управления программным обеспечением, функционирующим на удаленных вычислительных машинах в специализированных центрах обработки данных [2].

Облачные платформы получили изначально широкое распространение в ведомственных распределенных автоматизированных информационных системах [3], а также успешно зарекомендовали себя при организации межведомственных и международных информационных взаимодействиях, предусматривающих в том числе и использование различных информационно-технических средств [4, 5, 6].

В статье представлены результаты исследования одного из способа разрешения проблемы обеспечения устойчивости современных облачных платформ управления киберфизическими объектами в условиях роста и целенаправленного характера кибератак за счет выявления деструктивных воздействий, приводящих к возможности нарушения семантики вычислительного процесса.

Сложность структуры эталонной модели облачной платформы управления киберфизическими объектами

Анализ различных моделей информационных систем, построенных с использованием облачных вычислений, для построения модели угроз для таких систем проведен в [7]. По итогам анализа сделан вывод, что при построении модели угроз главную роль играю уровни виртуализации и сервисов. Также авторы предложили новую модель [8], которая основывалась на уточнении эталонной модели национального института стандартов и технологий США (англ. The National Institute of Standards and Technology, NIST)[4], представленной на Рис. 1.

По степени контроля и возможности управления облачным программным обеспечением выделяют следующие основные модели предоставления облачных сервисов [1, 9]:

Software-as-a-Service (SaaS) — пользователю доступно только прикладное программное обеспечение. Управление остальными уровнями облачной инфраструктуры осуществляет провайдер облачных сервисов;

Platform-as-a-Service (PaaS) — пользователю доступно прикладное программное обеспечения, а также средства разработки, тестирования и развертывания. Управление операционной системой, средствами виртуализации, вычислительными ресурсами и физической вычислительной инфраструктурой осуществляет провайдер облачных сервисов;

[4] National Institute of Standards and Technology Special Publication 500-292. NIST Cloud Computing Reference Architecture. Recommendations of the National Institute of Standards and Technology / Liu F., Tong J. and other // Cloud Computing Program, Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930, September 2011, 35 pp. URL: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=909505 (Дата обращения: 18.09.2025)

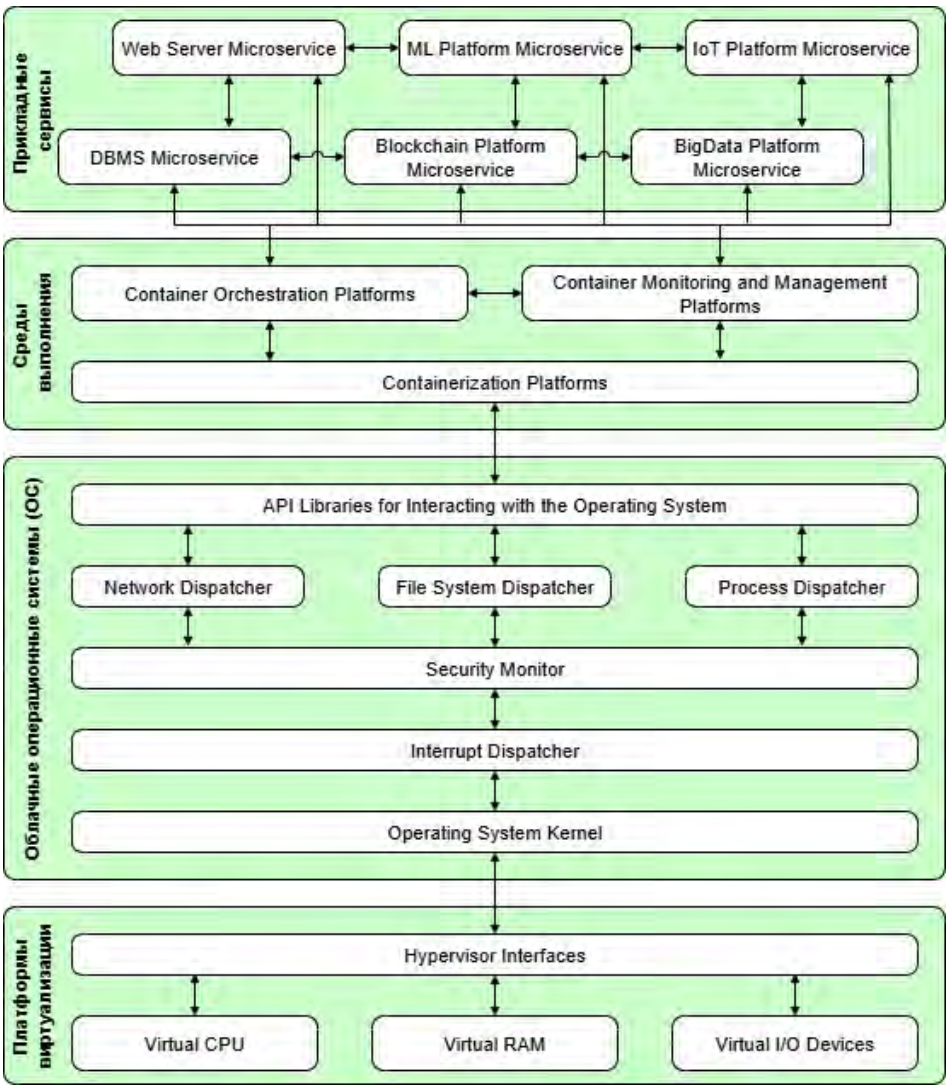

Рис.** 2. **Концептуальная модель облачной платформы для управления киберфизическими объектами

Infrastructure-as-a-Service (IaaS) — пользователю доступно любое прикладное и системное программное обеспечение, операционная система и средства виртуализации. Управление физической вычислительной инфраструктурой осуществляет провайдер облачных сервисов.

Таким образом, в концептуальной модели типовой облачной платформы управления киберфизическими объектами (Рис. 2) совокупность сервисов и средств управления функционирует на удаленных вычислителях в соответствии с одной из описанных моделей, а доступ к ним осуществляется посредством сети Интернет на 4 уровнях представления (примеры приведены на Рис. 3). При этом необходимо отметить, что главную роль имеют уровни виртуализации и сервисов.

Первый уровень представлен средствами виртуализации и гипервизорами. Программное обеспечение, функционирующее на данном уровне, отвечает за управление виртуальными машинами, изоляцию их друг от друга и контроль доступа к аппаратным средствам: процессору, памяти, устройствам хранения и другим.

Второй уровень представлен облачными операционными системами. Системное программное обеспечение, функционирующее на данном уровне, отвечает за управление вычислительными ресурсами и правами доступа, а также обеспечивает функционирование промежуточных сред выполнения.

Третий уровень представлен промежуточными средами выполнения. Программное обеспечение, функционирующее на данном уровне, отвечает за развертывание, мониторинг и управление прикладными облачными сервисами.

Четвертый уровень представлен собственно прикладными облачными сервисами. На данном уровне могут быть развернуты системы управления базами данных, веб-серверы, платформы машинного обучения, обработки больших данных, интернета вещей, блокчейн-платформы и другие.

Важной особенностью архитектуры облачных платформ является вложенный иерархический характер функционирующего в них программного обеспечения.

Так гипервизор позволяет управлять несколькими операционными системами, внутри которых может быть развернуто множество контейнерных сред с прикладными облачными сервисами.

Данная особенность позволяет говорить о наличии вертикальных (логических) связей между компонентами типовой облачной платформы.

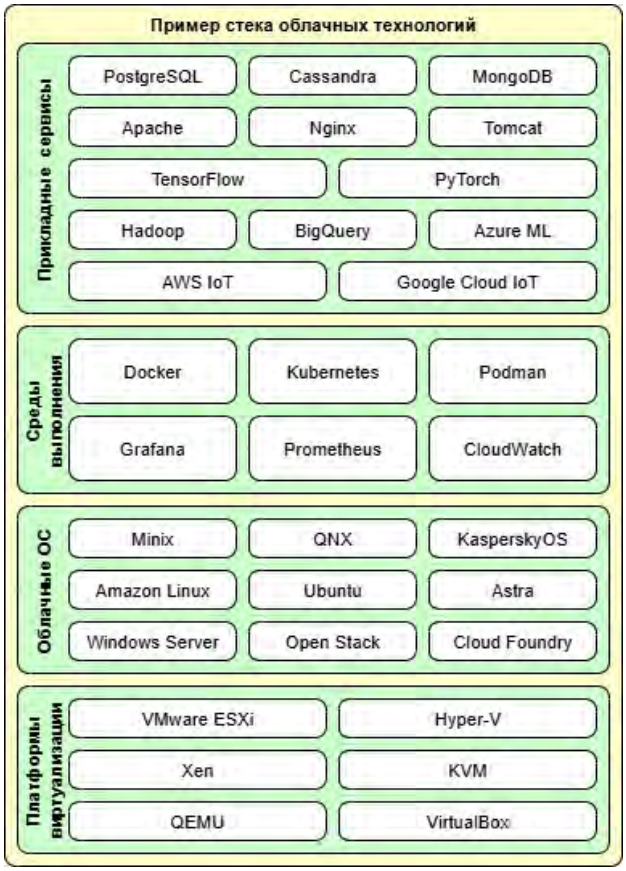

Рис.* 3. *Пример стека облачных технологий

Примерами существующих облачных платформ являются Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, Yandex Cloud и другие. Все они предоставляют схожие возможности управления облачными вычислительными ресурсами.

Единая цифровая технологическая платформа «ГосТех»

Правовые основы создания, развития и эксплуатации государственных информационных систем на Единой цифровой технологической платформе «ГосТех» (далее — платформа «ГосТех», цифровая платформа «Гостех»)[5] отражены в следующих правовых актах:

- Концепция Концепции создания и функционирования единой государственной цифровой платформы «ГосТех»[6];
- Положения о системе «Управление платформой «ГосТех» и «Госмаркете»[7];
- Положение о платформе «ГосТех» и изменения в постановление Правительства Российской Федерации № 676[8].

Цифровая платформа «ГосТех» предназначена, в первую очередь, для проектирования, разработки и реализации государственных информационных систем (далее — ГИС), к ее отличительным особенностям относятся следующее.

1. В облачной платформе общего назначения большинство взаимодействий происходит в пределах одного изолированного клиента, например, между вычислительными сервисами и хранилищами данных, что подразумевает наличие вертикальных логических связей между компонентами. Цифровая платформа «ГосТех» должна обеспечивать взаимодействие и интеграцию различных ГИС, в том числе и предназначенных для управления киберфизическими системами.
2. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации представило для общественного обсуждения проект Федерального закона[9], в соответствии с отдельными требованиями которого предусматривается, что на цифровой платформе «ГосТех» поставщики облачных услуг по предоставлению программного обеспечения и (или) по предоставлению вычислительных ресурсов должны будут обеспечивать соответствие информационно-телекоммуникационной инфраструктуры и (или) программного обеспечения требованиям, предъявляемым к защите информации в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации, и (или) предъявляемым к обеспечению безопасности критической информационной инфраструктуры (далее – КИИ) Российской Федерации.
3. Облачные вычислительные среды, создаваемые на базе цифровой платформы «ГосТех» могут иметь гибридную архитектуру, объединять публичные и частные облачные решения, а также включать несколько центров обработки данных. Данная особенность цифровой платформы «ГосТех» позволяет говорить о наличии в ней не только вертикальных, но и горизонтальных (информационных) связей между компонентами. Таким образом, архитектура облачных платформ управления киберфизическими объектами, соз-

[5] Единая цифровая платформа ГосТех. URL: https://platform.gov.ru/. (Дата обращения: 18.09.2025).

[6] Утверждена распоряжением Правительства Российской Федерации от 21 октября 2022 г. № 3102-р (Собрание законодательства Российской Федерации. 31.10.2022. № 44. Ст. 7594).

[7] Утверждено Постановлением Правительства Российской Федерации от 30 ноября 2022 г. № 2194 (с изменениями и дополнениями).

[8] Утверждено постановление Правительства Российской Федерации от 16 декабря 2022 г. № 2338 (с изменениями и дополнениями).

[9] Проект Федерального закона о внесении изменений в федеральный закон «Об информации, информационных технологиях» и о защите информации». URL: https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=156884 (Дата обращения: 18.09.2025).

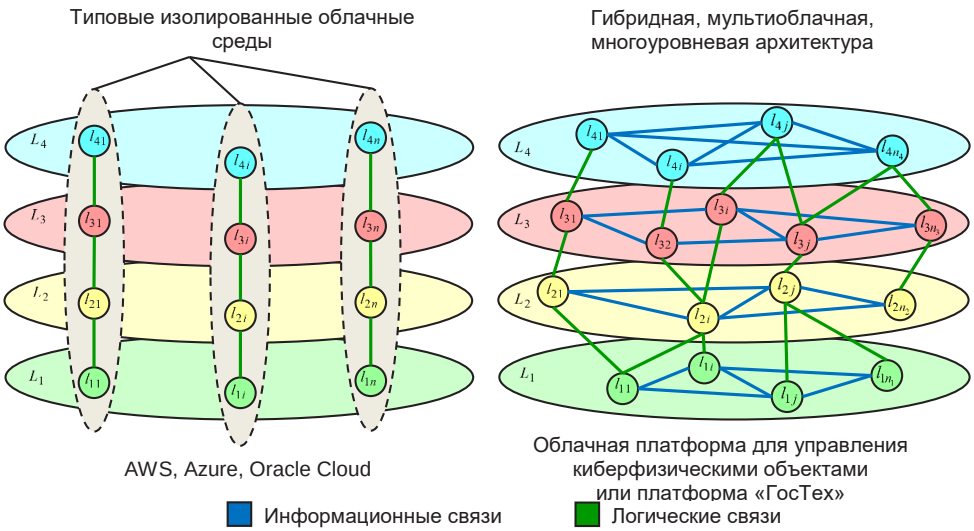

Рис. 4. Архитектурные отличия облачных платформ для управления киберфизическими объектами от типовых изолированных облачных сред

даваемых на базе цифровой платформы «ГосТех», обладает сложным многоуровневым характером и высокой степенью связности, как показано на Рис. 4**.**

На базе цифровой платформы «ГосТех» создаются библиотеки типовых программных компонентов, упрощающие процесс создания и управления облачными сервисами. Однако в силу ускоренного замещения иностранных технологий, потенциально содержащих недекларированные возможности, и недостаточного тестирования вновь создаваемых программных решений, такие решения могут содержать невыявленные уязвимости [10, 11, 12, 13]. Наличие уязвимостей обуславливает возможность реализации ранее неизвестных информационно-технических воздействий, направленных на нарушение семантики облачных вычислений [0].

Таким образом, к отличительным особенностям облачных платформ управления киберфизическими объектами можно отнести:

- сложную многоуровневую иерархическую архитектуру, подразумевающую наличие вертикальных и горизонтальных связей между компонентами;
- подверженность новым, ранее неизвестным информационно-техническим воздействиям, направленным на нарушение семантики вычислений;
- высокие требования к устойчивости и критичность нарушений.

Оценка угроз безопасности информации облачной платформы управления киберфизическими объектами

Для облачных платформ управления киберфизическими объектами также актуально утверждение, что глобальное информационное пространство одновременно используется [14—19]:

с одной стороны, для расширения доступа физических и юридических лиц к информации, цифровым сервисам и финансовым инструментам и повышения эффективности цифровой экономики (экономики данных), а

с другой стороны, криминальными структурами, международными террористическими организациями и государствами, проводящими недружественную политику в отношении Российской Федерации.

Одними из самых серьезных угроз являются угрозы эксплуатации ранее неизвестных уязвимостей «нулевого дня» (0-day) [0] и недекларируемых возможностей. При этом недекларируемые возможности могут быть следствием внесения средств скрытого информационного воздействия. В отсутствии самокорректирующих сред для обеспечения проактивной безопасности такие угрозы могут быть реализованы даже невысоко квалифицированными злоумышленниками [10, 11, 12, 13, 19, 20].

Новые или ранее неизвестные уязвимости могут возникать вследствие программных ошибок, влияющих на поведение программы. При этом необходимо учитывать, что методика проведения анализа влияния изменений программного обеспечения не имеет детального описания и не закреплена на законодательном уровне [21], а сам анализ влияния изменений программного обеспечения требует необходимой компетенции у проводящего его эксперта и представляет собой требующую значительных временных затрат и трудоемкую процедуру.

Схема жизненного цикла уязвимости «нулевого дня», предложенная в [22], приведена на Рис. 5.

В соответствии с [23] любая вычислительная программа реализует некоторый алгоритм, который можно также моделировать с помощью машины Тьюринга (далее — МТ). МТ задает некоторую функцию над строками:

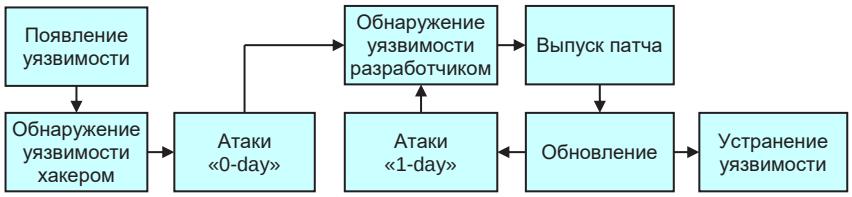

Рис. 5. Схема жизненного цикла уязвимости «нулевого дня»

$f: L_{вх} \to L_{вых}$,

где $L_{вх}$ — язык входных данных МТ;

$L_{вых}$ — язык выходных данных МТ.

При этом, если функция является всюду вычислимой, то $\forall x \in L_{вх}\ \exists y \in L_{вых}: f(x) = y$, как показано на Рис. 6. В дальнейшем будем полагать, что рассматриваемые МТ задают именно всюду вычислимые функции.

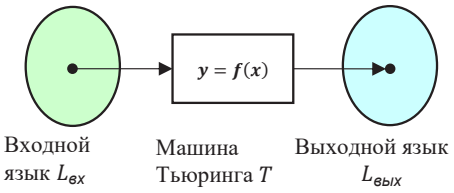

Рис. 6. Машина Тьюринга как функция над строками

Пусть теперь T_1 — МТ, соответствующая спецификации программы и задающая функцию $f: L_{вх} \to L_{вых}$, а T_2 — МТ, соответствующая фактической реализации программы и задающая функцию $g: L_{вх} \to L_{вых}$.

Будем считать, что фактическая реализация программы на МТ T_2 содержит ошибку семантики относительно спецификации, описываемой МТ T_1, если существуют такие слова языка входных данных $L_{вх}$, для которых значения функций f и g отличаются.

Математически это можно записать как:

$$\exists x \in L_{вх}: g(x) \neq f(x), f(x) \in L_{вых}, g(x) \in L_{вых}$$

С точки зрения управления безопасностью, возникновение аномальных состояний программы, при которых результат ее выполнения отличается от ожидаемого в соответствии со спецификацией, говорит о наличии уязвимости. Тогда входные данные, приводящие программу в такое аномальное состояние, можно считать вредоносными. На Рис. 7 представлена графическая интерпретация ошибки семантики, приводящей к возникновению аномалий обработки входных данных.

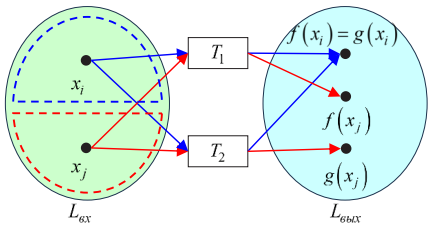

Рис. 7. Нарушение семантики вычислений при совпадении языков

Сформулируем и докажем следующее утверждение.

Утверждение 1. Пусть T_1 — МТ, соответствующая спецификации программы и задающая функцию $f: L_{вх} \to L_{вых}$ без ошибок; T_2 — МТ, соответствующая фактической реализации этой программы и задающая функцию $g: L_{вх} \to L_{вых}$. Если реализация программы содержит уязвимость, то:

$L_{вх} = L^{+}_{вх} \cup L^{-}_{вх}$,

где $L^{-}_{вх} \neq \emptyset$;

$L^{+}_{вх} = \{x | f(x) = g(x)\}$ — подъязык легитимных входных данных;

$L^{-}_{вх} = \{x | f(x) \neq g(x)\}$ — подъязык вредоносных входных данных.

Доказательство. Пусть реализация вычислительной программы, моделируемая МТ T_2, содержит уязвимость. Тогда существует некоторое непустое подмножество слов языка входных данных $L_{вх}$, для которых значения функций f и g отличаются:

$\exists X^{-} \subset L_{вх}, X^{-} = \{x_1, \ldots, x_n\}, n > 0$

и $\forall x \in X^{-}, f(x) \neq g(x)$.

Поскольку $f(x) \in L_{вых}$ и $g(x) \in L_{вых}$, то можно построить МТ T_3, распознающую только слова $x \in X^{-}$, для которых $f(x) \neq g(x)$. Известно, что язык распознается МТ тогда и только тогда, когда он порожден некоторой формальной грамматикой. Таким образом, поскольку подмножество слов X^{-} распознается МТ T_3, то оно является языком $X^{-} = L^{-}_{вх}$:

$L^{-}_{вх} = \{x | f(x) \neq g(x)\}$,

$L^{+}_{вх} = L_{вх} \backslash L^{-}_{вх} = \{x | f(x) = g(x)\}$.

Что и требовалось доказать.

В рассмотренном выше случае предполагалось, что языки входных данных МТ, соответствующих спецификации вычислительной программы и ее реализации, содержащей уязвимость, совпадают, однако в общем случае это не обязательно.

Графическая интерпретация возможных соотношений языков входных данных машин при наличии уязвимости (Рис. 8) содержит следующие варианты:

a — возникновение уязвимости не привело к изменению языка входных данных МТ;

b — возникновение уязвимости привело к расширению языка входных данных МТ и появлению некоторого подмножества новых принимаемых слов;

c — возникновение уязвимости привело к сужению языка входных данных МТ и невозможности распознавания некоторых легитимных слов;

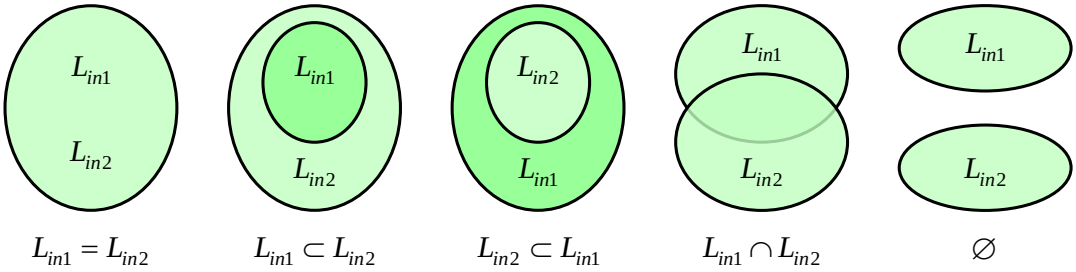

***Рис.** 8. Виды нарушений семантики с точки зрения входных данных: а — языки совпадают; б — расширение; в — сужение; г — пересечение; д — несовпадение*

d — возникновение уязвимости привело одновременно к невозможности распознавания некоторых легитимных слов и появлению новых принимаемых слов;

e — возникновение уязвимости привело к полному изменению алгоритма функционирования вычислительной программы и языка принимаемых входных данных. Будем считать, что в этом случае МТ спецификации и реализации не совпадают и реализуют разные функции.

Таким образом, для оказания скрытого информационного воздействия на облачную платформу управления киберфизическими объектами необходимо и достаточно передать уязвимой вычислительной программе облачного сервиса вредоносные входные данные. Здесь под скрытым информационным воздействием понимается воздействие, направленное на нарушение устойчивости функционирования таких платформ, реализующее угрозу запуска вычислительного процесса на МТ с входными данными, приводящими его в состояние, не удовлетворяющее его эталонной семантической модели.

Графическая интерпретация возможных типов нарушений семантики вычислительных процессов представлена на Рис. 9.

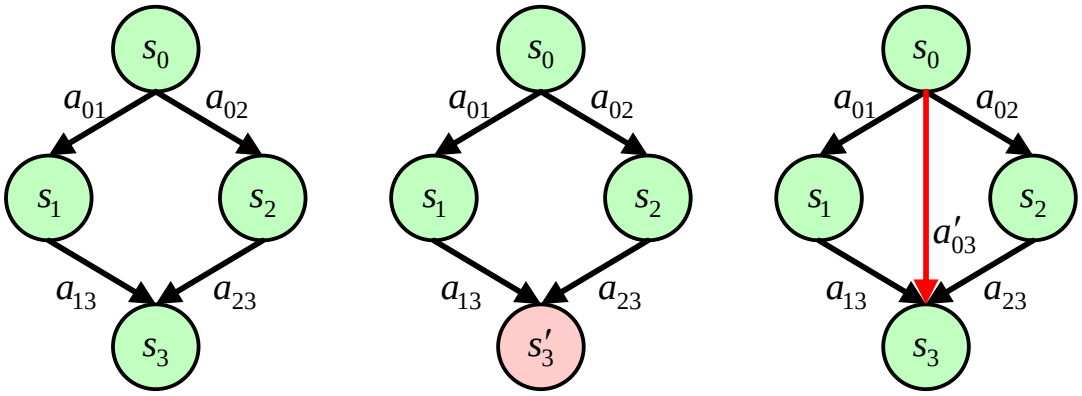

***Рис.** 9. Типы нарушений семантики вычислений: а — нет нарушения; б — нарушение состояния; в — нарушение перехода*

Для формирования модели угроз и корректной постановки задачи обеспечения устойчивости функционирования облачных платформ управления киберфизическими объектами необходимо рассмотреть актуальные способы воздействия, реализация которых может приводить к описанным нарушениям семантики вычислительного процесса, а также определить возможности потенциальных нарушителей.

Как определено ранее, облачная модель вычислений предполагает наличие удаленного вычислителя, доступ к которому осуществляется посредством сети Интернет. Программы облачных сервисов обрабатывают входные данные, поступающие извне через сетевые интерфейсы, и потенциально содержат невыявленные ошибки семантики, а значит подвержены удаленным воздействиям, в том числе с использованием вредоносных сетевых пакетов.

Такие сетевые пакеты, как правило, содержат «полезную нагрузку» в виде шелл-кода, реализующего один из способов воздействия.

В Табл. 1 представлен перечень актуальных угроз устойчивости функционирования облачных платформ управления киберфизическими объектами с учетом возможных способов воздействия по классификации MITRE ATT&CK[10] и соответствующих им типов нарушений семантики вычислений.

[10] ATT&CK Matrix for Enterprise. URL: https://attack.mitre.org/ (Дата обращения: 18.09.2025).

Табл. 1

Перечень актуальных угроз устойчивости функционирования облачных платформ управления

Нарушение состояния	T1055. Внедрение кода в процесс
	T1202. Косвенное выполнение команд
	T1543. Создание/изменение системных процессов
	T1546. Выполнение кода по наступлению события
Нарушение перехода	T1559. Перехват межпроцессного взаимодействия
	T1574. Перехват потока управления
Нарушение состояния или перехода	T1129. Эксплуатация уязвимостей разделяемых модулей
	T1190. Эксплуатация уязвимостей общедоступного ПО
	T1203. Эксплуатация уязвимостей в клиентском ПО
	T1648. Эксплуатация уязвимостей облачных сервисов

Здесь угрозы безопасности информации, связанные с эксплуатацией уязвимостей вынесены в отдельную группу, поскольку они могут влиять как на сами семантические состояния вычислительного процесса, так и на переходы между ними.

Отметим, что данный перечень не является исчерпывающим и отражает актуальные угрозы, влияющие на устойчивость функционирования широкого класса типовых облачных платформ управления киберфизическими объектами. Более подробно классификация угроз нарушения безопасности, а также их актуализация в связи с изменением международной обстановки и с появлением квантовых угроз, рассмотрены в работах [11, 14, 15, 16, 17, 19].

На основе методического документа ФСТЭК России «Методика оценки угроз безопасности информации», определяющего базовый перечень потенциальных нарушителей безопасности информации систем и сетей, исследовательских работ [24—30], а также статистической информацией о компьютерных атаках на информационные ресурсы Российской Федерации, возможно определить вероятных нарушителей безопасности информации облачных платформ управления киберфизическими объектами.

С учетом особенностей функционирования исследуемых облачных платформ и их распределенного характера, источниками угроз, как правило, становятся внешние нарушители, либо внутренние нарушители, вступающие в сговор с внешними. Перечень возможных нарушителей, их категорий и потенциала приведен в Табл. 2.

Табл. 2.

Возможные источники угроз безопасности информации типовой облачной платформы

Вид нарушителя	Категория нарушителя	Потенциал (уровень возможностей) нарушителя
Специальные службы иностранных государств	Внешний	Высокий (Н4)
Террористические, экстремистские группировки	Внешний	Средний (Н3)
Преступные группы (криминальные структуры)	Внешний	Базовый повышенный (Н2)
Администраторы облачных ИВС	Внутренний	Базовый повышенный (Н2) В случае сговора — Н3/Н4
Авторизованные пользователи облачных ИВС	Внутренний	Базовый (Н1) В случае сговора — Н2/Н3/Н4
Отдельные физические лица (хакеры)	Внешний	Базовый (Н1)

Действия внутренних нарушителей могут быть как преднамеренными, так и непреднамеренными, действия же внешних нарушителей всегда являются преднамеренными. Уровень возможностей указанных нарушителей может меняться в зависимости от наличия сговора с нарушителями, обладающими большим уровнем возможностей. Цели, преследуемые указанными нарушителями, будем считать совпадающими

с возможными негативными последствиями от реализации соответствующих угроз нарушения функционирования облачной платформы управления киберфизическими объектами.

В настоящее время большинство кибератак на объекты критической инфраструктуры Российской Федерации совершается с территории иностранных государств.

С учетом сложности и целенаправленного характера кибератак, наиболее вероятным источником угроз безопасности информации для облачной платформы управления киберфизическими объектами следует считать специальные службы иностранных государств, что, однако, не исключает возможность реализации угроз безопасности информации злоумышленниками, обладающими меньшим потенциалом.

Заключение

В настоящей работе была поставлена задача обеспечения устойчивости функционирования облачной платформы управления киберфизическими объектами за счет выявления деструктивных воздействий, приводящих к возможности нарушения семантики вычислительного процесса.

При этом, к вероятным нарушителям устойчивости функционирования облачных платформ управления киберфизическими объектами отнесены:

- специальные службы иностранных государств;
- террористические и экстремистские организации;
- организованные хакерские группировки;
- отдельные мотивированные лица.

По результатам анализа актуальных угроз и нарушителей безопасности можно сделать следующие выводы:

- вероятный нарушитель обладает высоким уровнем подготовки, достаточными компетенциями и ресурсами, способен выявлять недостатки программного обеспечения, внедрять недекларированные возможности, самостоятельно разрабатывать новые методы и средства воздействия, а также осуществлять комплексные целенаправленные кибератаки, используя весь спектр возможностей;
- кибератаки на облачные платформы управления киберфизическими объектами, направленные на эксплуатацию ранее неизвестных уязвимостей облачных сервисов, перехват потока управления и внедрение кода, могут быть осуществлены удаленно посредством сети Интернет с использованием сетевых пакетов, содержащих вредоносные входные данные, обработка которых приводит к нарушению семантики вычислений;
- нарушение устойчивости функционирования облачных платформ управления киберфизическими объектами вследствие успешных кибератак может привести к катастрофическим последствиям.

Таким образом, в условиях роста угроз безопасности необходима разработка новых элементов научно-методического аппарата обеспечения устойчивости функционирования облачных платформ управления киберфизическими объектами.

Исследование выполнено за счет гранта Российского научного фонда № 25-11-20037 «Технология самовосстановления киберфизических систем национальной критической информационной инфраструктуры в условиях беспрецедентного роста угроз безопасности на основе искусственного интеллекта» (руководитель — д.т.н. Петренко С.А.).

Литература

1. Балябин А.А., Петренко С.А. О самовосстановлении киберфизических систем КИИ РФ в условиях кибератак на основе кибериммунитета // The 2025 Symposium on Cybersecurity of the Digital Economy - CDE'25: Сборник трудов IX Международной научно-технической конференции, Иннополис, 05—06 марта 2025 года. Санкт-Петербург: Общество с ограниченной ответственностью Издательский Дом Афина, 2025. С. 64 - 75. EDN IIDVHJ.
2. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications / Al-Fuqaha A., Guizani M. and other // IEEE Communications Surveys & Tutorials, Vol. 17, № 4, pp. 2347-2376, Fourthquarter 2015, DOI: 10.1109/COMST.2015.2444095.
3. Заборовский В.С., Лукашин А.А., Скиба В.Ю. О возможности внедрения технологий облачных вычислений в ведомственных (корпоративных) распределенных автоматизированных информационных системах // Инженерный журнал: наука и инновации. 2013. № 3(15). 6 С. EDN RCRZWB.
4. Заборовский В.С., Лей Д., Скиба В.Ю., Стрекалов С.В. Цифровая информационно-логистическая платформа оперативного управления внешнеторговой деятельностью поставщиков высокотехнологичной продукции // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2018. Т. 11, № 4. С. 7 — 20. DOI: 10.18721/JCSTCS.11401. EDN YZNZWH.
5. Петренко С.А., Петренко А.С., Ожиганова М.И. Концепция обеспечения устойчивости функционирования платформы цифрового рубля Банка России в условиях роста угроз безопасности // Защита информации. Инсайд, 2024. № 5(119). С. 6 — 13. EDN DQRQXE.

6. Котенко И.В., Саенко И.Б., Коцыняк М.А., Лаута О.С. Оценка киберустойчивости компьютерных сетей на основе моделирования кибератак методом преобразования стохастических сетей // Труды СПИИРАН. 2017. № 6(55). С. 160 — 184. DOI 10.15622/sp.55.7. EDN ZVMTPH.
7. Симоненкова Д.С., Велигура А.Н. Эталонные модели информационных систем, построенных с использованием технологий облачных вычислений // Безопасность информационных технологий. 2013. Т. 20, № 3. С. 28 — 32. EDN RTVBBP.
8. Simonenkova D.S., Veligura A.N. Visual representation of the model of security threats for cloud-based information system // Scientific Visualization. 2015. Vol. 7, № 2. pp. 81-95. EDN UBFGXT.
9. Balyabin A. Model of a self-healing computing process of a cloud computing system under conditions of information and technical impacts," in 2023 XXVI International Conference on Soft Computing and Measurements (SCM), 2023, pp. 147—151. DOI: 10.1109/SCM58628.2023.10159053. EDN UVWXEH.
10. Казарин О.В., Скиба В.Ю. Реализация практически значимых проактивно безопасных компьютерных систем // Защита информации. Инсайд. 2015. № 3(63). С. 40 — 43. EDN TTGSZH.
11. Казарин О.В., Скиба В.Ю. Методология обеспечения проактивной безопасности компьютерных систем // Защита информации. Инсайд. 2013. № 2(50). С. 52 — 60. EDN TKJJVB.
12. Казарин О.В., Скиба В.Ю. Парадигма проактивной безопасности компьютерных систем // Защита информации. Инсайд. 2009. № 5(29). С. 68 — 75. EDN TNBGZZ.
13. Казарин О.В., Скиба В.Ю. Парадигма проактивной безопасности компьютерных систем // Защита информации. Инсайд. 2009. № 6(30). С. 62 — 67. EDN TMZVYD.
14. Казарин О.В., Скиба В.Ю., Шаряпов Р.А. Новые разновидности угроз международной информационной безопасности // Вестник РГГУ. Серия «Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность», 2016, № 1 (3). С. 54 — 72. EDN WAIXQZ.
15. Skiba V.Yu., Petrenko S.A., Gnidko K.O., Petrenko A.S. Concept of ensuring the resilience of operation of national digital platforms and blockchain ecosystems under the new quantum threat to security // Computing, Telecommunications and Control. 2025. Vol. 18, № 2. pp. 56 — 73. DOI 10.18721/JCSTCS.18205. EDN DCDMZF.
16. Skiba V.Yu., Petrenko S.A., Murzina A.A., Popova K.R. New types of threats and assessment of quantum stability of information systems in the field of foreign trade activity // Computing, Telecommunications and Control. 2024. Vol. 17, № 4. pp. 16 — 34. DOI 10.18721/JCSTCS.17402. EDN TFFIFM.
17. Скиба В.Ю., Петренко С.А., Мурзина А.А., Попова К.Р. Оценка квантовой устойчивости информационных систем таможенных органов Российской Федерации в современных условиях // Вестник Российской таможенной академии, 2024, № 4(69). С. 32 — 45. EDN DCCFTC.
18. Konyavsky V.A., Ross G.V., Sychev A.M., Skiba V.U. Information protection in systems of critical information infrastructures // Journal of the Balkan Tribological Association. 2021. Vol. 27, № 4. pp. 479 — 496. EDN IJJGBN.
19. Проактивная безопасность квантовых АИС / Скиба В.Ю., Тургиев Э.З., Лисов Д.Н., Салокина (Полякова) Н.А., Сергеев В.С. // The 2024 Symposium on Cybersecurity of the Digital Economy — CDE'24: Сборник трудов VIII международной научно-технической конференции, Иннополис, 23 — 25 сентября 2024 года. Санкт-Петербург: ООО Издательский Дом «Афина», 2024. С. 71 — 77. EDN ZMLHJL.
20. Казарин О.В., Скиба В.Ю. Применение самокорректирующихся сред для обеспечения проактивной безопасности компьютерных систем // Известия высших учебных заведений. Приборостроение. 2010. Т. 53, № 1. С. 34 — 39. EDN KYQFEZ.
21. Легкодумов А.А., Козеев Б.Н., Беликов В.В., Корольков А.В. Методы анализа влияния изменений программного обеспечения на целевые функции и функции безопасности // Russian Technological Journal. 2024. Т. 12, № 2. С. 7 — 15. DOI 10.32362/2500-316X-2024-12-2-7-15. EDN GBYWDW.
22. Петренко С.А., Балябин А.А. Модель квантовых угроз безопасности информации для национальных блокчейн-экосистем и платформ // Вопросы кибербезопасности. 2025. № 1(65). С. 7 — 17. DOI 10.21681/2311-3456-2025-1-7-17. EDN YYRSOI.
23. Балябин А.А. Модель угроз безопасности и киберустойчивости облачных платформ КИИ РФ // The 2023 Symposium on Cybersecurity of the Digital Economy - CDE'23: Сборник трудов VII международной научно-технической конференции, Иннополис, 11—12 апреля 2023 года. Иннополис: Университет Иннополис, 2024. С. 31-41. EDN KVFCMA.
24. Аверьянов В.С., Карцан И.Н. Оценка защищенности киберфизических систем на основе общего графа атак // Южно-Сибирский научный вестник. 2022. № 1(41). С. 30 — 35. DOI 10.25699/SSSB.2022.41.1.013. EDN: RUVLRD.
25. Зубарев И.В., Радин П.К. Основные угрозы безопасности информации в виртуальных средах и облачных платформах // Вопросы кибербезопасности. 2014. № 2(3). С. 40 — 45. EDN SEUFPR.
26. Максимова Е.А. Когнитивное моделирование деструктивных злоумышленных воздействий на объектах критической информационной инфраструктуры // Труды учебных заведений связи. 2020. Т. 6, № 4. С. 91 — 103. DOI 10.31854/1813-324X-2020-6-4-91-103. EDN LIRTXZ
27. Петренко С.А., Ступин Д.Д. Национальная система раннего предупреждения о компьютерном нападении. Университет Иннополис. Санкт-Петербург: Издательский Дом «Афина», 2017. 440 с. EDN YTKXOJ

28. A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies / Alouffi B., Hasnain M. and other // IEEE Access, Vol. 9, pp. 57792 — 57807, 2021, DOI: 10.1109/ACCESS.2021.3073203.
29. Стрижков В.А. Анализ стратегий защиты информации от инсайдерской угрозы в облачных вычислениях // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2024. № 10-2. С. 91 — 95. DOI 10.37882/2223-2966.2024.10-2.28. EDN: FYTJSV.
30. Сеналиев Р.Б., Яриков В.Г. Проблемы и решения безопасности в облачных вычислениях // НБИ технологии. 2024. Т. 18, № 3. С. 52 — 58. DOI 10.15688/NBIT.jvolsu.2024.3.6. EDN: RHRVCT.

SECTION:
INFORMATION PROTECTION METHODS AND SYSTEMS

THE PROBLEM OF ENSURING CYBER RESILIENCE OF CLOUD PLATFORMS FOR MANAGING CYBER-PHYSICAL OBJECTS

***Skiba V.Yu.*[11], *Balybin A.A.*[12], *Petrenko S.A.*[13]**

Keywords: *cyber-physical object management, information security threats, intruder model, cyber resilience, technological and operational security, verifiable security.*

Abstract

Purpose of work: *ensuring the resilience of operation of the cloud platform for managing cyber-physical objects by identifying destructive impacts that could lead to the possibility of violating the semantics of the computing process.*

Research methods: *systems analysis, classification of destructive impacts, modeling, specification, formal languages.*

Results of the study. *The distinctive features of cloud platforms for managing cyber-physical objects are formulated, a set of relationships between input data languages is proposed in the presence of vulnerability in the semantics of the computing process, a set of probable violators of information security of cloud platforms for managing cyber-physical objects is identified.*

Scientific novelty. *For cloud platforms for managing cyber-physical objects, new elements of a scientific and methodological apparatus have been formulated to solve the problem of identifying destructive influences that lead to the possibility of violating the semantics of the computing process.*

Practical significance. *The developed formal languages can be used in the development of methods for conducting certification and other tests in order to identify errors in the semantics of the computing process.*

References

1. Baljabin A.A., Petrenko S.A. O samovosstanovlenii kiberfizicheskih sistem KII RF v uslovijah kiberatak na osnove kiberimmuniteta // The 2025 Symposium on Cybersecurity of the Digital Economy - CDE'25: Sbornik trudov IX Mezhdunarodnoj nauchno-tehnicheskoj konferencii, Innopolis, 05—06 marta 2025 goda. Sankt-Peterburg: Obshhestvo s ogranichennoj otvetstvennost'ju Izdatel'skij Dom Afina, 2025. S. 64 - 75. EDN IIDVHJ.
2. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications / Al-Fuqaha A., Guizani M. and other // IEEE Communications Surveys & Tutorials, Vol. 17, № 4, pp. 2347-2376, Fourthquarter 2015, DOI: 10.1109/COMST.2015.2444095.

[11] ***Vladimir Yu. Skiba,*** *Doctor of Technical Sciences, Senior Researcher, Chief Research Engineer at the Scientific Center for Information Technology and Artificial Intelligence, Sirius Scientific and Technological University, Sirius Federal Territory, Krasnodar region, Russian Federation, Professor of the IBM-6 Department, Federal State Autonomous Educational Institution of Higher Education «Bauman Moscow State Technical University», Moscow. ORCID: 0000-0002-9805-7800.*
E-mail: skiba.vy@talantiuspeh.ru

[12] ***Artem A. Balybin,*** *junior research fellow at the Scientific Center for Information Technology and Artificial Intelligence, Sirius Scientific and Technological University, Sirius Federal Territory, Krasnodar region, Russian Federation. ORCID: 0009-0006-3949-154X.*
E-mail: balyabin.aa@talantiuspeh.ru

[13] ***Sergei A. Petrenko,*** *Doctor of Technical Sciences, professor, group leader at the Scientific Center for Information Technology and Artificial Intelligence, Sirius Scientific and Technological University, Sirius Federal Territory, Krasnodar region, Russian Federation. ORCID: 0000-0003-0644-1731.*
E-mail: petrenko.sa@talantiuspeh.ru

3. Zaborovskij V.S., Lukashin A.A., Skiba V.Ju. O vozmozhnosti vnedrenija tehnologij oblachnyh vychislenij v vedomstvennyh (korporativnyh) raspredelennyh avtomatizirovannyh informacionnyh sistemah // Inzhenernyj zhurnal: nauka i innovacii. 2013. № 3(15). 6 S. EDN RCRZWB.
4. Zaborovskij V.S., Lej D., Skiba V.Ju., Strekalov S.V. Cifrovaja informacionno-logisticheskaja platforma operativnogo upravlenija vneshnetorgovoj dejatel'nost'ju postavshhikov vysokotehnologichnoj produkcii // Nauchno-tehnicheskie vedomosti Sankt-Peterburgskogo gosudarstvennogo politehnicheskogo universiteta. Informatika. Telekommunikacii. Upravlenie. 2018. T. 11, № 4. S. 7 — 20. DOI: 10.18721/JCSTCS.11401. EDN YZNZWH.
5. Petrenko S.A., Petrenko A.S., Ozhiganova M.I. Koncepcija obespechenija ustojchivosti funkcionirovanija platformy cifrovogo rublja Banka Rossii v uslovijah rosta ugroz bezopasnosti // Zashhita informacii. Insajd, 2024. № 5(119). S. 6 — 13. EDN DQRQXE.
6. Kotenko I.V., Saenko I.B., Kocynjak M.A., Lauta O.S. Ocenka kiberustojchivosti komp'juternyh setej na osnove modelirovanija kiberatak metodom preobrazovanija stohasticheskih setej // Trudy SPIIRAN. 2017. № 6(55). S. 160 — 184. DOI 10.15622/sp.55.7. EDN ZVMTPH.
7. Simonenkova D.S., Veligura A.N. Jetalonnye modeli informacionnyh sistem, postroennyh s ispol'zovaniem tehnologij oblachnyh vychislenij // Bezopasnost' informacionnyh tehnologij. 2013. T. 20, № 3. S. 28 — 32. EDN RTVBBP.
8. Simonenkova D.S., Veligura A.N. Visual representation of the model of security threats for cloud-based information system // Scientific Visualization. 2015. Vol. 7, № 2. pp. 81-95. EDN UBFGXT.
9. Balyabin A. Model of a self-healing computing process of a cloud computing system under conditions of information and technical impacts," in 2023 XXVI International Conference on Soft Computing and Measurements (SCM), 2023, pp. 147—151. DOI: 10.1109/SCM58628.2023.10159053. EDN UVWXEH.
10. Kazarin O.V., Skiba V.Ju. Realizacija prakticheski znachimyh proaktivno bezopasnyh komp'juternyh sistem // Zashhita informacii. Insajd. 2015. № 3(63). S. 40 — 43. EDN TTGSZH.
11. Kazarin O.V., Skiba V.Ju. Metodologija obespechenija proaktivnoj bezopasnosti komp'juternyh sistem // Zashhita informacii. Insajd. 2013. № 2(50). S. 52 — 60. EDN TKJJVB.
12. Kazarin O.V., Skiba V.Ju. Paradigma proaktivnoj bezopasnosti komp'juternyh sistem // Zashhita informacii. Insajd. 2009. № 5(29). S. 68 — 75. EDN TNBGZZ.
13. Kazarin O.V., Skiba V.Ju. Paradigma proaktivnoj bezopasnosti komp'juternyh sistem // Zashhita informacii. Insajd. 2009. № 6(30). S. 62 — 67. EDN TMZVYD.
14. Kazarin O.V., Skiba V.Ju., Sharjapov R.A. Novye raznovidnosti ugroz mezhdunarodnoj informacionnoj bezopasnosti // Vestnik RGGU. Serija «Dokumentovedenie i arhivovedenie. Informatika. Zashhita informacii i informacionnaja bezopasnost'», 2016, № 1 (3). C. 54 — 72. EDN WAIXQZ.
15. Skiba V.Yu., Petrenko S.A., Gnidko K.O., Petrenko A.S. Concept of ensuring the resilience of operation of national digital platforms and blockchain ecosystems under the new quantum threat to security // Computing, Telecommunications and Control. 2025. Vol. 18, № 2. pp. 56 — 73. DOI 10.18721/JCSTCS.18205. EDN DCDMZF.
16. Skiba V.Yu., Petrenko S.A., Murzina A.A., Popova K.R. New types of threats and assessment of quantum stability of information systems in the field of foreign trade activity // Computing, Telecommunications and Control. 2024. Vol. 17, № 4. pp. 16 — 34. DOI 10.18721/JCSTCS.17402. EDN TFFIFM.
17. Skiba V.Ju., Petrenko S.A., Murzina A.A., Popova K.R. Ocenka kvantovoj ustojchivosti informacionnyh sistem tamozhennyh organov Rossijskoj Federacii v sovremennyh uslovijah // Vestnik Rossijskoj tamozhennoj akademii, 2024, № 4(69). S. 32 — 45. EDN DCCFTC.
18. Konyavsky V.A., Ross G.V., Sychev A.M., Skiba V.U. Information protection in systems of critical information infrastructures // Journal of the Balkan Tribological Association. 2021. Vol. 27, № 4. pp. 479 — 496. EDN IJJGBN.
19. Proaktivnaja bezopasnost' kvantovyh AIS / Skiba V.Ju., Turgiev Je.Z., Lisov D.N., Salokina (Poljakova) N.A., Sergeev V.S. // The 2024 Symposium on Cybersecurity of the Digital Economy — CDE'24: Sbornik trudov VIII mezhdunarodnoj nauchno-tehnicheskoj konferencii, Innopolis, 23 — 25 sentjabrja 2024 goda. Sankt-Peterburg: OOO Izdatel'skij Dom «Afina», 2024. S. 71 — 77. EDN ZMLHJL.
20. Kazarin O.V., Skiba V.Ju. Primenenie samokorrektirujushhihsja sred dlja obespechenija proaktivnoj bezopasnosti komp'juternyh sistem // Izvestija vysshih uchebnyh zavedenij. Priborostroenie. 2010. T. 53, № 1. S. 34 — 39. EDN KYQFEZ.
21. Legkodumov A.A., Kozeev B.N., Belikov V.V., Korol'kov A.V. Metody analiza vlijanija izmenenij programmnogo obespechenija na celevye funkcii i funkcii bezopasnosti // Russian Technological Journal. 2024. T. 12, № 2. S. 7 — 15. DOI 10.32362/2500-316X-2024-12-2-7-15. EDN GBYWDW.
22. Petrenko S.A., Baljabin A.A. Model' kvantovyh ugroz bezopasnosti informacii dlja nacional'nyh blokchejn-jekosistem i platform // Voprosy kiberbezopasnosti. 2025. № 1(65). S. 7 — 17. DOI 10.21681/2311-3456-2025-1-7-17. EDN YYRSOI.
23. Baljabin A.A. Model' ugroz bezopasnosti i kiberustojchivosti oblachnyh platform KII RF // The 2023 Symposium on Cybersecurity of the Digital Economy - CDE'23: Sbornik trudov VII mezhdunarodnoj nauchno-tehnicheskoj konferencii, Innopolis, 11—12 aprelja 2023 goda. Innopolis: Universitet Innopolis, 2024. S. 31-41. EDN KVFCMA.
24. Aver'janov V.S., Karcan I.N. Ocenka zashhishhennosti kiberfizicheskih sistem na osnove obshhego grafa atak // Juzhno-Sibirskij nauchnyj vestnik. 2022. № 1(41). S. 30 — 35. DOI 10.25699/SSSB.2022.41.1.013. EDN: RUVLRD.

25. Zubarev I.V., Radin P.K. Osnovnye ugrozy bezopasnosti informacii v virtual'nyh sredah i oblachnyh platformah // Voprosy kiberbezopasnosti. 2014. № 2(3). S. 40 — 45. EDN SEUFPR.
26. Maksimova E.A. Kognitivnoe modelirovanie destruktivnyh zloumyshlennyh vozdejstvij na ob#ektah kriticheskoj informacionnoj infrastruktury // Trudy uchebnyh zavedenij svjazi. 2020. T. 6, № 4. S. 91 — 103. DOI 10.31854/1813-324X-2020-6-4-91-103. EDN LIRTXZ
27. Petrenko S.A., Stupin D.D. Nacional'naja sistema rannego preduprezhdenija o komp'juternom napadenii. Universitet Innopolis. Sankt-Peterburg: Izdatel'skij Dom «Afina», 2017. 440 s. EDN YTKXOJ
28. A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies / Alouffi B., Hasnain M. and other // IEEE Access, Vol. 9, pp. 57792 — 57807, 2021, DOI: 10.1109/ACCESS.2021.3073203.
29. Strizhkov V.A. Analiz strategij zashhity informacii ot insajderskoj ugrozy v oblachnyh vychislenijah // Sovremennaja nauka: aktual'nye problemy teorii i praktiki. Serija: Estestvennye i tehnicheskie nauki. 2024. № 10-2. S. 91 — 95. DOI 10.37882/2223-2966.2024.10-2.28. EDN: FYTJSV.
30. Senaliev R.B., Jarikov V.G. Problemy i reshenija bezopasnosti v oblachnyh vychislenijah // NBI tehnologii. 2024. T. 18, № 3. S. 52-58. DOI 0.15688/NBIT.jvolsu.2024.3.6. EDN: RHRVCT.