УДК 004.056 **DOI** 10.15622/ia.24.5.8

А.А. Балябин, С.А. Петренко

МОДЕЛЬ ОБЛАЧНОЙ ПЛАТФОРМЫ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ С КИБЕРИММУНИТЕТОМ

Балябин А.А., Петренко С.А. **Модель облачной платформы критической информационной инфраструктуры с кибериммунитетом.**

Аннотация. Исследование посвящено решению задачи синтеза модели облачной платформы критической информационной инфраструктуры с кибериммунитетом. Актуальность исследования обусловлена необходимостью разрешения проблемной ситуации, характеризующейся наличием противоречий в науке и практике. Противоречие в практике наблюдается между повышенными требованиями к устойчивости функционирования облачных платформ критической информационной инфраструктуры и ростом угроз, связанных с эксплуатацией новых, ранее неизвестных уязвимостей. Противоречие в науке состоит в невозможности обеспечения требуемой устойчивости таких платформ с использованием существующих моделей и методов. Так существующие подходы не в полной мере учитывают особенности облачных платформ критической информационной инфраструктуры, а именно, иерархическую архитектуру, наличие невыявленных уязвимостей, функционирование в условиях целенаправленных информационно-технических воздействий, повышенные требования к устойчивости и необходимость оперативного восстановления штатного функционирования. Поставлена задача синтеза новой модели облачной платформы критической информационной инфраструктуры с кибериммунитетом. Сформулирована гипотеза о том, что учет свойства кибериммунитета положительно влияет на устойчивость функционирования таких платформ в условиях информационно-технических воздействий. Методы исследования включают методы системного анализа, теории вероятностей, семантической теории программ, теории подобия и размерностей, а также методы компьютерной иммунологии. Обоснована идея кибериммунитета, состоящая в наделении облачной платформы способностью противодействовать известным и ранее неизвестным информационно-техническим воздействиям, оперативно восстанавливаться при возникновении нарушений и запоминать вредоносные входные данные, предотвращая их повторную обработку. Обоснованы показатели устойчивости функционирования облачных платформ критической информационной инфраструктуры. Разработана модель облачной платформы критической информационной инфраструктуры с кибериммунитетом. Научная новизна модели заключается в том, что в нее впервые внедрены такие элементы, как обнаружитель нарушений семантики вычислений, восстановитель штатного функционирования и кибериммунная память, в совокупности реализующие новое эмерджентное свойство кибериммунитета. Проведены теоретическое и экспериментальное исследования модели, по результатам которых подтверждена выдвинутая гипотеза. Практическая значимость результатов исследования заключается в доведении их до технических рекомендаций по архитектуре программного комплекса, которые могут быть использованы при разработке средств защиты облачных платформ критической информационной инфраструктуры, в частности, облачной платформы «ГосТех», в условиях информационно-технических воздействий.

Ключевые слова: облачные вычисления, семантика вычислений, критическая информационная инфраструктура, киберустойчивость, кибератаки, кибериммунитет.

1. Введение. В рамках реализации национального проекта «Экономика данных» в Российской Федерации ведется активная разработка и внедрение современных «сквозных» технологий, включая отечественные цифровые платформы и программное обеспечение, технологии искусственного интеллекта, блокчейн, квантовые вычисления и другие. Внедрение таких технологий необходимо для достижения цифровой трансформации государственного и муниципального управления, экономики и социальной сферы, обеспечения информационной безопасности и эффективного взаимодействия посредством сети Интернет.

Одним из примеров отечественных цифровых платформ является Единая цифровая платформа «ГосТех», позволяющая федеральным и региональным органам власти создавать государственные информационные системы (ГИС) и цифровые сервисы с использованием типовых программных решений, осуществлять мониторинг и управление ими. Платформа «ГосТех» может использоваться в качестве облачной платформы (ОП) для ГИС, относящихся к объектам критической информационной инфраструктуры (ОП КИИ).

В архитектуре типовых ОП можно условно выделить 4 уровня:

- системы виртуализации и гипервизоры;
- облачные операционные системы (ОС);
- промежуточные среды выполнения;
- прикладные облачные сервисы.

Следует отметить, что облачное программное обеспечение, функционирующее на различных уровнях ОП, характеризуется вложенной, иерархической структурой. В виртуальных средах (гипервизорах) могут быть параллельно запущены несколько изолированных ОС с контейнерными средами. Внутри контейнеров может выполняться множество микросервисов, таких как узел сети блокчейн, платформа машинного обучения, система управления базами данных, веб-сервер и другие.

Это говорит о наличии вертикальных (логических) связей между компонентами ОП. К типовым ОП относятся Microsoft Azure, Amazon Web Services, Google Cloud Platform и другие. Среди отечественных ОП известны, например, Yandex.Cloud, Selectel, MTC Web Services. Концептуальная модель такой ОП, учитывающая примерный стек технологий на каждом из уровней, представлена на рисунке 1.

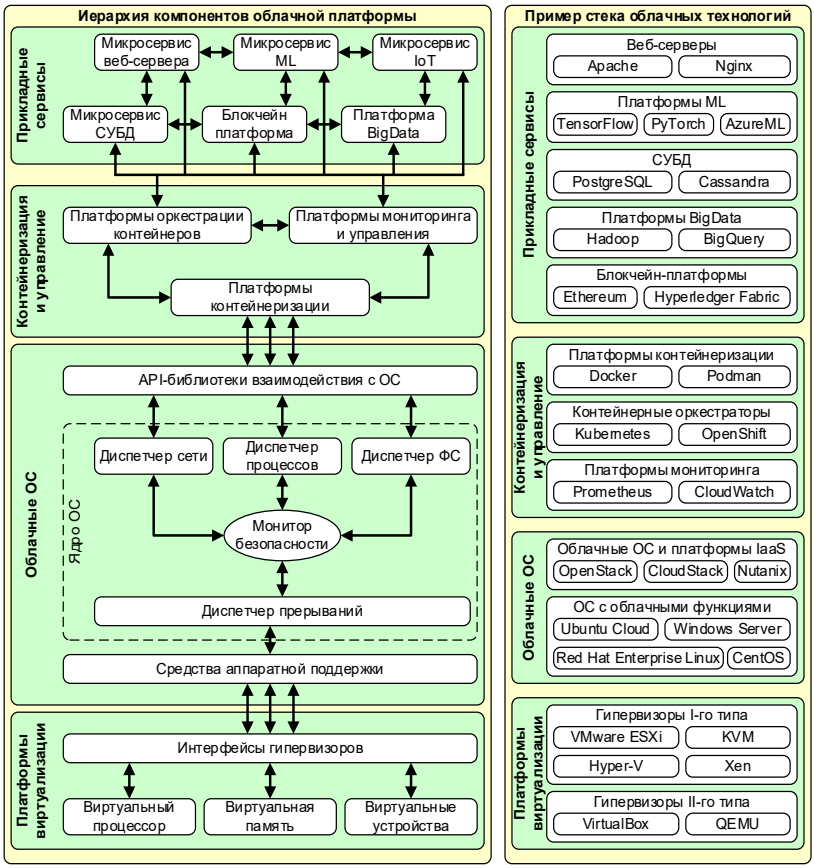

Рис. 1. Концептуальная модель ОП

Облачные платформы КИИ обладают некоторыми особенностями по отношению к типовым ОП.

Во-первых, в ОП КИИ может быть реализована мульти-облачная или гибридная архитектура, которая включает множество частных и публичных облачных сред. Такая архитектура предполагает наличие как вертикальных (логических), так и горизонтальных (информационных) связей между компонентами, что характеризует ОП КИИ как сложную иерархическую систему.

Во-вторых, ОП КИИ ориентированы на применение отечественных технологий и иных решений с открытым исходным кодом, однако в силу их ускоренной разработки и недостаточности

тестирования в них могут возникать новые, ранее неизвестные уязвимости. Это создает условия для реализации новых информационно-технических воздействий (ИТВ), направленных на нарушение семантики облачных вычислений (нарушение поведения программы, возникновение аномальных состояний при сохранении ее работоспособности), путем эксплуатации невыявленных уязвимостей.

В-третьих, информационные системы, создаваемые на базе ОП КИИ, предназначены для обеспечения деятельности органов власти. Успешная реализация ИТВ на такие платформы может привести к катастрофическим последствиям, поэтому к ним предъявляются повышенные требования в части безопасности и устойчивости их функционирования.

Таким образом, к значимым особенностям ОП КИИ относятся:

- сложная многоуровневая иерархическая архитектура;
- потенциальное наличие невыявленных уязвимостей;
- функционирование в условиях ИТВ, направленных на нарушение семантики вычислений;
- повышенные требования к устойчивости и необходимость оперативного восстановления штатного функционирования.

В то же время в мире наблюдается устойчивая тенденция роста количества и сложности киберугроз. Воздействия приобретают целенаправленный, комплексный, многоэтапный характер и зачастую ориентированы на новые технологии, для которых еще в недостаточной степени разработаны методы и средства защиты. Так в исследовании CheckPoint [1] отмечается, что в начале 2025 года наблюдался рост эксплуатации уязвимостей облачных сред, связанных с их некорректной конфигурацией и уязвимостями публичных интерфейсов (API). По данным исследования, проведенного ГК «Солар» [2], в Российской Федерации в 2024 году наиболее значимыми угрозами для промышленности и телекома оказались APT-группировки и средства удаленного доступа. В целом же с 2022 года ежегодный прирост количества кибератак на информационную инфраструктуру России составляет порядка 20-30% [3].

Совокупность вышеуказанных факторов позволяет сформулировать *противоречие в практике* между повышенными требованиями к безопасности и устойчивости функционирования ОП КИИ и ростом угроз, связанных в том числе с преодолением существующих средств защиты и эксплуатацией новых, ранее неизвестных уязвимостей.

2. Анализ предметной области. Существует ряд перспективных интеллектуальных и биоинспирированных подходов к

моделированию и управлению устойчивостью различных информационно-вычислительных систем в условиях ИТВ, а именно, подходы на основе:

- графовых моделей [4, 5];
- марковских цепей [6, 7];
- гироматов безопасности [8, 9];
- управляющих графов программ [10];
- нейронных сетей [11 – 17];
- искусственных иммунных систем и сетей [19 – 27];
- самовосстанавливающихся вычислений и кибериммунитета [29 – 34].

Рассмотрим подробнее данные подходы и их применимость для моделирования ОП КИИ.

В работе [4] предлагается обеспечивать информационную безопасность и устойчивость киберфизических систем (КФС) на основе принципов гомеостаза. Для этого КФС моделируется при помощи графов. Устойчивость функционирования КФС оценивается на основе анализа структурных свойств моделирующих графов, таких как избыточность и спектр графа [5]. Противодействие ИТВ, снижающим устойчивость функционирования КФС, предлагается осуществлять путем синтеза сценариев переконфигурирования. Фрактальные графы учитывают иерархический характер ОП КИИ, однако не позволяют учитывать ранее неизвестные уязвимости, связанные с нарушением семантики облачных вычислений.

В работе [6] исследуются компьютерные атаки на программно-конфигурируемые сети, с использованием математического аппарата цепей Маркова. В работе [7] их устойчивость оценивается с использованием вероятностно-временных показателей реализации кибератак. Цепи Маркова позволяют учесть стохастический характер возникновения нарушений, однако, моделирование сложных иерархических информационно-вычислительных систем в условиях ИТВ, направленных на нарушение семантики вычислений, может быть затруднительным.

В работах [8, 9] предлагается наделять интеллектуальные системы кибербезопасности свойством антиципации, позволяющим противодействовать кибератакам путем синтеза упреждающего поведения. Моделирование таких систем предлагается осуществлять на основе самообучающейся системы самоорганизующихся гироматов. Такая модель позволяет учесть многоуровневый иерархический характер ОП КИИ, наличие восстанавливающих воздействий, накопление информации о нарушениях, однако, является

«высокоуровневой» и не позволяет описывать ИТВ, направленные на нарушение семантики вычислений.

В работе [10] предлагается исследовать программное обеспечение на предмет наличия дефектов с использованием универсальных графовых представлений кода, учитывающих взаимодействия между компонентами. Управляющие графы позволяют описать иерархию взаимодействия вычислительных программ, однако, их выразительных свойств достаточно лишь для описания синтаксических структур. Для исследования нарушений семантики вычислений необходимо использовать дополнительные модели и методы.

Известны исследования, посвященные применению нейронных сетей и машинного обучения для задач выявления атак на IoT-системы [11], системы Smart Grid [12], киберфизические системы [13], а также для задач совершенствования систем обнаружения вторжений на основе классических алгоритмов машинного обучения [14], федеративного обучения [15], глубокого обучения [16], автокодировщика [17]. Нейросетевая модель позволяет выявлять как известные, так и некоторые ранее неизвестные ИТВ, однако, она не позволяет осуществлять восстановление штатного функционирования системы. Кроме того, системы обнаружения вторжений на основе алгоритмов машинного обучения и искусственного интеллекта могут быть уязвимы к различным атакам, направленным на искажение данных обучающей выборки [18].

В работе [19] предлагается применить искусственную иммунную систему для обнаружения вторжений. В работе [20] искусственные иммунные системы предлагается применять для создания интеллектуальной системы мониторинга безопасности промышленного интернета вещей. В работе [21] предлагается подход на основе интеллектуальных методов обнаружения сетевых атак с использованием нейронных, нейронечетких и иммунных детекторов. Подходы, описанные в исследованиях [22 – 24], основаны на адаптации алгоритмов функционирования иммунных систем и иммунного ответа для противодействия компьютерным атакам. К этому же направлению относятся подходы на основе алгоритмов дендритных клеток [25], отрицательного отбора [26], клональной селекции [27]. Модели, предложенные в данных исследованиях, применимы для распределенных многоагентных систем и позволяют обнаруживать как известные, так и ранее неизвестные ИТВ, однако не учитывают семантику вычислений и не позволяют осуществлять восстановление штатного функционирования систем.

В целом в работе [28] отмечается необходимость количественного оценивания устойчивости функционирования объектов КИИ в условиях воздействия угроз нарушения информационной безопасности и невозможность осуществления такой оценки существующими методами без ряда допущений.

Результаты анализа позволяют сформулировать *противоречие в науке* между повышенными требованиями к безопасности и устойчивости функционирования ОП КИИ и невозможностью их обеспечения с использованием существующих моделей и методов.

Выявленные противоречия в науке и практике характеризуют проблемную ситуацию, разрешение которой является *актуальной* научной задачей. Перспективной для разрешения данной проблемной ситуации является идея организации самовосстанавливающихся вычислений и кибериммунитета. Методологические основы данного научного направления сформированы в монографиях [30, 31].

Настоящее исследование продолжает и развивает исследования [32 – 34], в которых определены основные угрозы безопасности и устойчивости функционирования ОП КИИ, и посвящено разработке модели ОП КИИ с кибериммунитетом в условиях ИТВ, направленных на нарушение семантики облачных вычислений.

3. Постановка задачи исследования. Выполним постановку задачи синтеза модели ОП КИИ с кибериммунитетом.

Дано:

L – ОП КИИ, функционирующая на N уровнях, так что $L = \{L_i \mid i \in [1, N]\}$, где L_i – подсистема i-го уровня;

$X = \{X_i \mid i \in [1, N]\}$ – множество входных данных ОП КИИ, где X_i – входные данные на i-ом уровне;

$Y = \{Y_i \mid i \in [1, N]\}$ – множество выходных данных ОП КИИ, где Y_i – выходные данные на i-ом уровне;

$A = \{A_i \mid i \in [1, N]\}$ – множество параметров вредоносных воздействий на ОП КИИ, где A_i – параметры вредоносных воздействий i-ом уровне;

$D = \{D_i \mid i \in [1, N]\}$ – множество параметров нейтрализующих воздействий на ОП КИИ, где D_i – нейтрализующие воздействия на i-ом уровне;

$f = \{f_i \mid i \in [1, N]\}$ – множество вычислительных программ ОП КИИ, где f_i – вычислительная программа на i-ом уровне;

$C = \{C_i \mid i \in [1, N]\}$ – множество подсистем кибериммунитета ОП КИИ, где C_i – подсистема кибериммунитета на i-ом уровне;

$K = \{K_i \mid i \in [1, N]\}$ – множество подсистем управления устойчивостью функционирования ОП КИИ, где K_i – подсистема управления устойчивостью функционирования на i-ом уровне;

$R = \{R_i \mid i \in [1, N]\}$ – множество показателей устойчивости функционирования ОП КИИ, где R_i – показатели устойчивости функционирования на i-ом уровне.

Под *кибериммунитетом* в настоящей работе будем понимать свойство ОП КИИ, заключающееся в способности противодействовать ИТВ, не допуская нарушений, оперативно восстанавливать машинные вычисления в случае возникновения таких нарушений, и обеспечивать требуемые значения показателей устойчивости функционирования.

Необходимо: разработать математическую модель M ОП КИИ L с кибериммунитетом, устанавливающую закономерность изменения множества выходных данных Y и множества показателей устойчивости ее функционирования R от множества входных данных X, множества значений параметров дестабилизирующих воздействий A и множества параметров нейтрализующих воздействий D, с учетом наличия множества подсистем кибериммунитета C и множества подсистем оценивания и управления устойчивостью R. При этом на значения X, Y, A, D наложены условия допустимости: $X \subseteq X_{\text{доп}}$, $Y \subseteq Y_{\text{доп}}$, $A \subseteq A_{\text{доп}}$, $D \subseteq D_{\text{доп}}$.

Формальная постановка задачи синтеза модели: найти

$$M :\prec L, X, Y, A, D, f, C, K \succ \rightarrow Y, R$$
$$X \subseteq X_{\text{доп}}, Y \subseteq Y_{\text{доп}}, A \subseteq A_{\text{доп}}, D \subseteq D_{\text{доп}}.$$

Гипотеза исследования. Учет свойства кибериммунитета положительно влияет на устойчивость функционирования ОП КИИ в условиях ИТВ.

4. Обоснование идеи кибериммунитета. Иерархию вычислительных программ ОП КИИ можно представить в виде универсальной машины Тьюринга (МТ) большой вложенности:

$$T_{N_i} : \left(T_{N_{i-1}} \times \left(\ldots \times \left(T_{N_0} \times X_{N_0}^{n_0} \right)^{n_1} \ldots \right)^{n_{i-1}} \right)^{n_i} \rightarrow Y_{N_i},$$

где T_{N_i} – универсальная МТ N_i -го уровня; $X_{N_i}^{n_i}$ – набор из n_i входных данных для универсальной МТ T_{N_i}; Y_{N_i} – выходные данные универсальной МТ T_{N_i}.

Каждая такая МТ реализует некоторую вычислимую функцию над строками $f: X \to Y$ так, что $\forall x \in X, \exists y \in Y: f(x) = y$ где X – множество входных данных (строк); Y – множество выходных данных (результатов преобразования строк). При этом МТ одного уровня могут применяться последовательно, формируя композиции функций $f_1 \circ f_2 \circ ... \circ f_n$, которые без потери общности могут быть заменены составной функцией f.

Пусть T_1 – МТ, соответствующая спецификации программы и задающая функцию $f: X \to Y$, а T_2 – МТ, соответствующая фактической ее реализация и задающая функцию $g: X \to Y$. В работах [32, 33] показано, что если программа, реализуемая машиной T_2, содержит семантическую ошибку, то множество ее входных данных подразделяется на два непересекающихся подмножества $X = X^+ \cup X^-$, $X^- \neq \varnothing$, где $X^+ = \{x \mid x \in X, f(x) = g(x)\}$ – множество строк, одинаково преобразуемых обеими МТ, $X^- = \{x \mid x \in X, f(x) \neq g(x)\}$ – множество строк, результаты преобразования которых различаются. Это является причиной возникновения новых, ранее неизвестных уязвимостей, сохраняющих синтаксическую корректность программы, но нарушающих семантику вычислений (смысл выполняемых вычислительных операций). Тогда реализация новых ИТВ становится возможной при эксплуатации таких уязвимостей атакующим путем нахождения строк, принадлежащих множеству X^-, и передачи их программе в качестве входных данных.

Любой алгоритм, реализуемый МТ, может быть представлен в виде вычислительной программы, которая, в свою очередь, имеет структуру управления и может быть описана графом $\Gamma(B,T)$, где $B = \{b_i \mid i \in [1,k]\}$ – множество линейных блоков, содержащих последовательности вычислительных операций; k – количество линейных блоков; $T = \{B \times B\}$ – множество связей по управлению между линейными блоками.

Для обеспечения возможности контроля семантики вычислений необходимо осуществить гомоморфное отображение управляющего

графа программы $\Gamma(B,T)$ в эталонную модель $M(S,A)$, представляющую собой граф, вершины которого содержат инварианты, описывающие допустимые состояния программы в линейных блоках в терминах формальных семантик и не зависящие от конкретной реализации программы, с сохранением переходов между ними. На рисунке 2 представлен пример семантической модели программы и выявляемых с помощью нее нарушений.

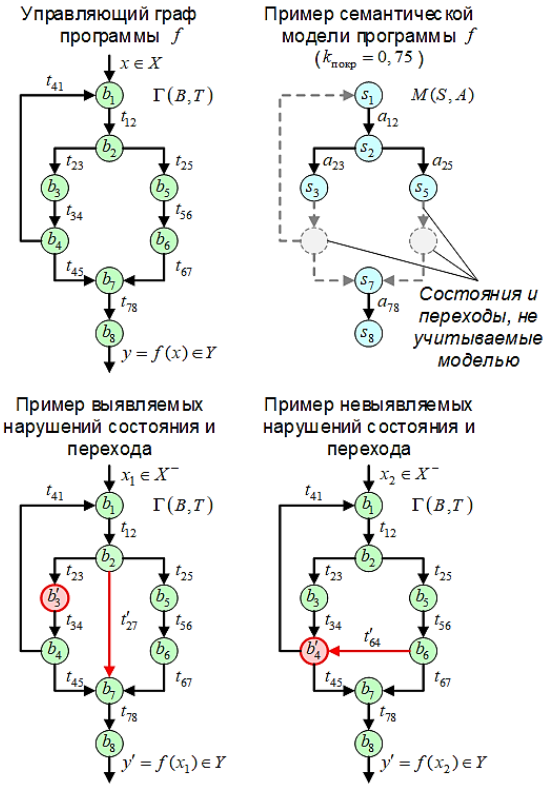

Рис. 2. Примеры управляющего графа, семантической модели программы, выявляемых и невыявляемых нарушений

Для контроля корректности семантики облачных вычислений в процессе функционирования ОП КИИ в условиях ИТВ потребуется внедрить в вычислительные программы дополнительную структурно-функциональную избыточность. Это может привести к недопустимому

увеличению времени их выполнения. Для решения данной проблемы может быть введен коэффициент покрытия кибериммунитета $k_{\text{покр}}$, определяющий долю линейных блоков, подлежащих контролю (на рисунке 2 $k_{\text{покр}} = 0,75$), однако неполное покрытие программы механизмами кибериммунитета приведет к пропуску некоторых нарушений, каждое из которых может быть расценено как потенциально критическое (приводящее к полному отказу системы или возникновению необратимых последствий). Для исследования влияния $k_{\text{покр}}$ на устойчивость функционирования и время выполнения программ ОП КИИ введем ряд показателей.

5. Обоснование показателей устойчивости. Примем некоторые допущения относительно функционирования ОП КИИ [29].

1. Программы ОП КИИ (сетевой драйвер, система управления базами данных, веб-сервер) осуществляют обработку входных данных последовательно, в порядке их поступления, и функционируют циклически так, что после завершения цикла обработки они переходят к ожиданию следующих входных данных. Таким образом, невозможно возникновение нескольких нарушений в единицу времени.

2. Нарушения обусловлены внешними факторами и не зависят от внутренних параметров ОП КИИ. Кроме того, для вредоносных входных данных, поступивших на предыдущих итерациях функционирования ОП КИИ, отсутствует эффект последействия. То есть, ранее произошедшие нарушения, не оказывают влияния на текущую итерацию функционирования ОП КИИ. При этом вредоносными являются только те входные данные, обработка которых непосредственно привела к нарушению семантики вычислений.

3. Образцы вредоносных входных данных сохраняются в кибериммунной памяти, а вновь поступающие входные данные принимаются только при отсутствии их среди сохраненных вредоносных образцов. После каждого обнаружения случайного или преднамеренного нарушения осуществляется восстановление штатного функционирования ОП КИИ. При этом, входные данные, переданные администратором и не являющиеся вредоносными, но приведшие к нарушению, также будут классифицированы как вредоносные (нарушающие функционирование ОП КИИ). С точки зрения управления безопасностью, это потребует дальнейшего анализа и устранения причин такого нарушения.

4. ИТВ характеризуются массовой отправкой нарушителем вредоносных входных данных, которые вместе с остальными

входными данными последовательно обрабатываются в порядке их поступления. Новые, ранее неизвестные ИТВ связаны с отправкой нарушителем новых вредоносных входных данных.

Введем теперь показатели устойчивости функционирования ОП КИИ. Одним из таких показателей является вероятность успешного противодействия ИТВ $P_{\text{прот}}$, которую можно выразить через обратную вероятность нарушения $P_{\text{прот}} = 1 - P_{\text{нар}}$.

Среднее время между пропусками атак $T_{\text{ср.атак}}$ характеризует способность ОП КИИ противодействовать ИТВ и является показателем средней продолжительности ее функционирования между возникновением нарушений. Данный показатель можно определить как отношение времени вычислений программы с учетом проверок наличия нарушений за $n_{\text{ц}}$ циклов к ожидаемому количеству нарушений за это время:

$$T_{\text{ср.атак}} = \frac{n_{\text{ц}}(T_{\text{выч}} + T_{\text{обн}})}{n_{\text{ц}}(1 - P_{\text{прот}})} = \frac{T_{\text{выч}} + T_{\text{обн}}}{1 - P_{\text{прот}}}. \quad (1)$$

Вероятность успешного восстановления $P_{\text{восст}}$ характеризует способность ОП КИИ оперативно восстанавливать штатное функционирование после обнаружения нарушения. Предполагается, что всякое обнаруженное нарушение семантического состояния или перехода может быть нейтрализовано, а значит $P_{\text{восст}} = P_{\text{обн}}$, где $P_{\text{обн}}$ определяется типом применяемой формальной семантики и будет обоснована позднее.

Среднее время восстановления $T_{\text{ср.восст}}$ характеризует оперативность восстановления функционирования ОП КИИ после нарушения. Данный показатель можно вычислить как отношение времени, затрачиваемого на восстановление функционирования ОП КИИ за $n_{\text{ц}}$ циклов, к ожидаемому числу восстановлений за это время:

$$T_{\text{ср.восст}} = \frac{n_{\text{ц}} T_{\text{восст}}}{n_{\text{ц}} P_{\text{восст}}} = \frac{T_{\text{восст}}}{P_{\text{восст}}}. \quad (2)$$

Вероятность работоспособности ОП КИИ $P_{\text{раб}}$ является показателем того, в данный момент ОП КИИ не находится в состоянии

нарушения. Это означает, что ОП КИИ противодействует ИТВ, сохраняя работоспособное и корректное состояние, или к данному моменту возникшее ранее нарушение было нейтрализовано. Данный показатель схож по смыслу с коэффициентом готовности и может быть вычислен как:

$$P_{\text{раб}} = \frac{T_{\text{ср.атак}}}{T_{\text{ср.атак}} + T_{\text{ср.восст}}}. \quad (3)$$

Вероятность достижения цели $P_{\text{цели}}$ характеризует интегральную способность ОП КИИ противодействовать ИТВ, не допуская нарушений семантики, оперативно восстанавливать машинные вычисления при их возникновении и сохранять устойчивое состояние, в котором возможно достижение цели функционирования ОП КИИ. Данный показатель можно вычислить как:

$$P_{\text{цели}} = (P_{\text{прот}} + (1 - P_{\text{прот}})P_{\text{восст}})P_{\text{раб}}. \quad (4)$$

Полное время выполнения программного цикла $T_{\text{вып}}$, учитывающее время непосредственно вычислений, динамического формирования семантических инвариантов и сравнение их с эталонными для обнаружения нарушений семантики облачных вычислений, а также время, затрачиваемое на восстановление штатного функционирования программ ОП КИИ, можно вычислить как:

$$T_{\text{вып}} = T_{\text{выч}} + T_{\text{обн}} + T_{\text{восст}}. \quad (5)$$

Основными оцениваемыми показателями устойчивости функционирования ОП КИИ в условиях ИТВ можно считать вероятность достижения цели $P_{\text{цели}}$ и время выполнения программного цикла $T_{\text{вып}}$.

Формализуем теперь модель ОП КИИ с учетом принятых допущений и введенных показателей устойчивости.

6. Формализация модели облачной платформы критической информационной инфраструктуры с кибериммунитетом. Введем ряд обозначений для ОП КИИ на i-ом уровне [29].

$X_i = \{X_{ij} \mid j \in [1, n_j]\}$ – множество входных данных (строк), принимаемых программами ОП КИИ i-го уровня, n_i – количество вычислительных программ i-го уровня;

$Y_i = \{Y_{ij} \mid j \in [1, n_i]\}$ – множество выходных данных программ ОП КИИ i-го уровня;

$k_{\text{изв}i}$ – доля известных ИТВ в общем количестве ИТВ на i-ом уровне, $k_{\text{изв}i} \in [0,1]$. Оценивание данного параметра может осуществляться с помощью экспертных методов или в результате учений с имитацией действий атакующих;

$k_{\text{вред}i}$ – доля вредоносных входных данных в общем количестве входных данных i-го уровня, $k_{\text{вред}i} \in [0,1]$. Оценивание данного параметра может также осуществляться с помощью экспертных методов или в результате учений с имитацией действий атакующих;

$A_i = \{k_{\text{изв}i}, k_{\text{вред}i}\}$ – множество параметров ИТВ на i-ом уровне;

$k_{\text{покр}i}$ – коэффициент покрытия кибериммунитета i-го уровня, определяющий долю линейных блоков программы, для которых осуществляется контроль семантики, $k_{\text{покр}i} \in [0,1]$. Данный коэффициент является основным варьируемым параметром, используемым при оценивании устойчивости ОП КИИ;

$D_i = \{k_{\text{покр}i}\}$ – множество параметров нейтрализующих воздействий на i-ом уровне;

M_i – эталонная семантическая модель программы i-го уровня;

k_i – среднее количество линейных блоков программ i-го уровня, $k_i \in \mathbb{N}$;

m_i – среднее количество инструкций в каждом линейном блоке программ i-го уровня, $m_i \in \mathbb{N}$;

n_i – среднее количество параметров в каждой инструкции i-го уровня, $n_i \in \mathbb{N}$;

$f_i = \{M_i, k_i, m_i, n_i\}$ – вычислительная программа i-го уровня;

I_i – кибериммунная память i-го уровня;

O_i – обнаружитель нарушений i-го уровня;

V_i – восстановитель штатного функционирования i-го уровня;

$C_i = \{I_i, O_i, V_i\}$ – подсистема кибериммунитета i-го уровня;

K_i – подсистема оценивания и управления устойчивостью i-го уровня;

$P_{\text{моди}}$ – вероятность возникновения модификации вычислений при обработке вредоносных входных данных на i-ом уровне. Данная вероятность определяется на основе информации о вероятностях появления различных типов модификаций вычислительных структур;

$P_{\text{обни}}$ – вероятность обнаружения нарушений, вызванных обработкой вредоносных входных данных на i-ом уровне. Данная вероятность определяется с использованием оценки коэффициента $k_{\text{изви}}$;

$P_{\text{проти}}$ – вероятность успешного противодействия ИТВ на i-ом уровне. Данная вероятность определяется с использованием известных параметров моделирования и оценок коэффициентов $k_{\text{изви}}$ и $k_{\text{вреди}}$;

$T_{\text{ср.атаки}}$ – среднее время между пропусками ИТВ (атак) на i-ом уровне, $T_{\text{ср.атаки}} \in \mathbb{N}$ (ед. времени);

$P_{\text{восстi}}$ – вероятность успешного восстановления после нарушения на i-ом уровне. Данная вероятность определяется на основе значения $P_{\text{обни}}$;

$T_{\text{ср.восстi}}$ – среднее время, затрачиваемое на восстановление после ИТВ на i-ом уровне, $T_{\text{ср.восстi}} \in \mathbb{N}$ (ед. времени);

$P_{\text{раб}i}$ – вероятность нахождения ОП КИИ на i-ом уровне в работоспособном состоянии в произвольный момент времени. Данная вероятность определяется с использованием известных параметров моделирования и оценок коэффициентов $k_{\text{изви}}$ и $k_{\text{вреди}}$;

$P_{\text{целиi}}$ – вероятность достижения цели функционирования ОП КИИ в условиях ИТВ на i-ом уровне. Данная вероятность определяется с использованием известных параметров моделирования и оценок коэффициентов $k_{\text{изви}}$ и $k_{\text{вреди}}$;

$T_{\text{выпi}}$ – время выполнения программного цикла, включая время вычислений, время обнаружения и время восстановления нарушений на i-ом уровне, $T_{\text{выпi}} \in \mathbb{N}$ (ед. времени);

$R_i = \{P_{\text{прот}i}, T_{\text{ср.атак}i}, P_{\text{восст}i}, T_{\text{ср.восст}i}, P_{\text{раб}i}, P_{\text{цели}i}, T_{\text{вып}i}\}$ – множество показателей устойчивости функционирования ОП КИИ i-го уровня;

$T_{\text{выч}i}$ – время вычислений программы i-го уровня, $T_{\text{выч}i} \in \mathbb{N}$ (ед. времени);

$T_{\text{обн}i}$ – время проверки вычислений на предмет наличия нарушений на i-ом уровне (время обнаружения нарушений), $T_{\text{обн}i} \in \mathbb{N}$ (ед. времени);

$T_{\text{восст}i}$ – время восстановления штатного функционирования программы i-го уровня, $T_{\text{восст}i} \in \mathbb{N}$ (ед. времени);

t_0 – время выполнения элементарной операции (при расчетах принимается $t_0 = 1$ ед. времени).

Обоснование аналитических выражений вероятностей $P_{\text{прот}i}$, $P_{\text{мод}i}$, $P_{\text{обн}i}$, $P_{\text{цели}i}$ в работе будет дано позднее.

Общая схема предлагаемой модели ОП КИИ с кибериммунитетом представлена на рисунке 3.

Рассмотрим подробнее подсистему кибериммунитета ОП КИИ.

Подсистема кибериммунитета ОП КИИ C_i предназначена для обнаружения нарушений семантики облачных вычислений, возникающих при обработке вредоносных входных данных $x \in X_i^- \subset X_i$, оперативного восстановления машинных вычислений, а также сохранения вредоносных образцов для предотвращения повторной обработки вредоносных входных данных и превентивного реагирования на схожие ИТВ в будущем.

Для наделения программ свойством кибериммунитета и обеспечения возможности обнаружения нарушений, как упоминалось ранее, в программу вносится избыточность, а также формируется ее эталонная семантическая модель. Линейные блоки программы могут быть представлены в виде последовательностей арифметических выражений. Тогда для формирования эталонной семантической модели можно использовать теорию подобия и размерностей [35]. Соотношения размерностей сохраняют свойства операндов арифметических выражений в динамике выполнения программы и служат инвариантами ее семантических состояний в линейных блоках.

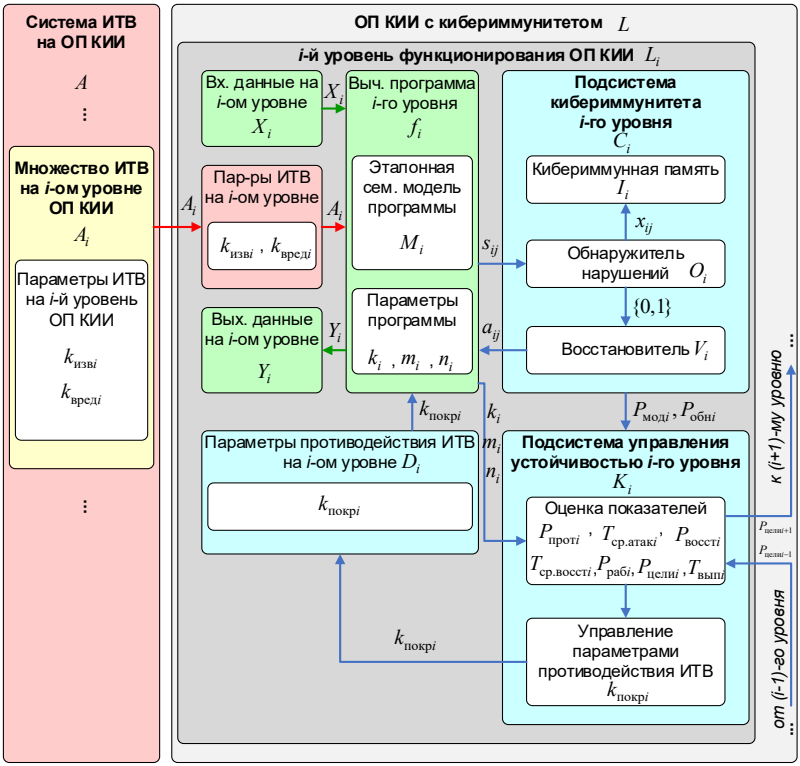

Рис. 3. Модель ОП КИИ с киберимунитетом

Обозначим гомоморфное отображение управляющего графа программы в эталонную семантическую модель как $\mu :< B,T >\to< S,A >$, где множество линейных блоков программы B отображается в множество семантических состояний S, а множество переходов между блоками T отображается в множество переходов между семантическими состояниями A. По завершении преобразования в линейные блоки $\forall b_j \in B, b_j = (b_{j1},...,b_{jm_i})$ вносятся метки для последующего контроля семантики вычислений так, что $b_j = (KT_j^{in}, b_{j1},...,b_{jm_i}, KT_j^{out})$, где KT_j^{in} и KT_j^{out} – метки начала и конца линейного блока соответственно.

Вычислительный процесс представляет собой последовательную смену семантических состояний под управлением

переходов $s_{i1} \xrightarrow{a12} s_{i2} \xrightarrow{a23} \ldots \xrightarrow{a_{ij-1}} s_{ij}$. Обнаружитель нарушений O_i формирует семантический инвариант программы, описывающий ее состояние в текущем линейном блоке, и осуществляет проверку его принадлежности эталонной семантической модели программы. В функциональном виде это может быть записано как $\eta :< S, M >\rightarrow \{0,1\}$, при этом:

$$\eta\left(s_{ij}, M_i\right) = \begin{cases} 1, \text{если } s_{ij} \in S_i \wedge \exists a_{ij} : s_{ij-1} \xrightarrow{a_{ij}} s_{ij} \\ 0, \text{иначе} \end{cases}.$$

При обнаружении семантического состояния s'_{ij}, не удовлетворяющего эталонной модели, восстановитель V_i, реализующий функцию $\xi :< S, S >\rightarrow A$, осуществляет синтез перехода для приведения вычислительной программы в корректное состояние в зависимости от принятой стратегии восстановления: начальное, предыдущее или конечное, как показано на рисунке 4.

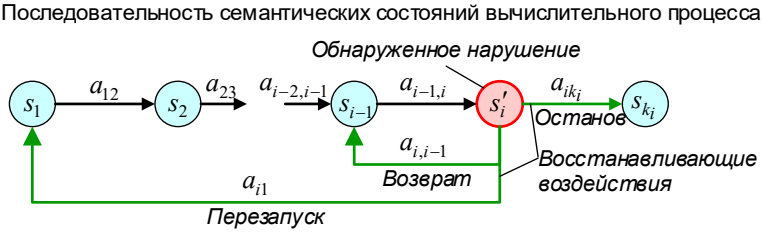

Рис. 4. Пример обнаружения и восстановления нарушения

Слова $x \in X_i^-$, которые привели к нарушению, накапливаются в памяти кибериммунитета I_i так, что $I_i \subseteq X_i^- \subset X_i$. В дальнейшем данные слова используются при проверке вновь поступающих входных данных для превентивного реагирования на аналогичные ИТВ. Таким образом происходит последовательное формирование приобретаемого кибериммунитета и самообучение ОП КИИ.

Таким образом, кибериммунитет является новым эмерджентным свойством, которое обеспечивается совокупностью

элементов модели ОП КИИ: обнаружителя O_i, восстановителя V_i и кибериммунной памяти I_i, с учетом коэффициента покрытия $k_{\text{покр}i}$.

Рассмотрим теперь подсистему управления устойчивостью функционирования ОП КИИ.

Вероятность успешного противодействия ИТВ можно определить как $P_{\text{прот}i} = 1 - P_{\text{нар}i}$, где $P_{\text{нар}i}$ – вероятность пропуска нарушения. Здесь вероятность пропуска нарушения можно определить как $P_{\text{нар}i} = P_{S_3}(P_{S_1} + P_{S_2})$, где P_{S_1} – вероятность того, что нарушение произошло в контролируемом участке управляющего графа, но не было обнаружено; P_{S_2} – вероятность того, что нарушение произошло за пределами контролируемых участков управляющего графа; P_{S_3} – вероятность того, что нарушение привело к нетождественной модификации вычислительных операторов. Вероятности P_{S_1} и P_{S_2} можно оценить как:

$$P_{S_1} = \frac{\#X_i^- - \#X_i^- P_{\text{обн}i}}{\#X_i} k_{\text{покр}i}\left(1 - P_{\text{обн}i}\right), \tag{6}$$

$$P_{S_2} = \frac{\#X_i^- - \#X_i^- P_{\text{обн}i}}{\#X_i}\left(1 - k_{\text{покр}i}\right), \tag{7}$$

где $\#$ – мощность множества.

Вероятность P_{S_3} – есть условная вероятность $P_{\text{моди}}$ модификации вычислительных операторов. Обозначим долю вредоносных входных данных как $k_{\text{вреди}} = \#X_i^- / \#X_i$. Тогда с учетом формул (6) и (7) получим:

$$P_{\text{прот}i} = 1 - P_{\text{моди}} k_{\text{вреди}} (1 - P_{\text{обн}i})(1 - k_{\text{покр}i} P_{\text{обн}i}). \tag{8}$$

Поскольку эталонная семантическая модель программы формируется на основе ее управляющего графа, а ИТВ обнаруживается тогда и только тогда, когда оно приводит нарушению состояния или перехода, то вероятность ошибок I-го рода (ложных обнаружений) стремится к 0, что в целом характерно для

инвариантных методов [30]. Вероятность же ошибок II-го рода (ложных пропусков) определяется вероятностью пропуска ИТВ $P_{\text{нар}i}$.

В работе [35] под модификацией вычислений понимается злонамеренное нетождественное изменение арифметических операторов программы $Op\{+,-,*,/\}$ ($P_{Op_l|Op_j} = 0,25$). Если принять, что появление данных арифметических операторов в управляющем графе равновероятно ($P_{Op_j} = 0,25$), то вероятность возникновения модификации $P_{\text{мод}i}$ составит:

$$P_{\text{мод}i} = \sum_{j=1}^{4} P_{Op_j} \left(\sum_{\substack{l=1 \\ j \neq l}}^{4} P_{Op_l|Op_j} \right) = \sum_{j=1}^{4} 0,25 \left(\sum_{\substack{l=1 \\ j \neq l}}^{4} 0,25 \right) = 0,75 .$$

Вероятность обнаружения нарушения $P_{\text{обн}i}$ зависит коэффициента $k_{\text{изв}i}$, определяющего то, какую часть составляют известные ИТВ на ОП КИИ. Допустим, известные ИТВ обнаруживаются всегда, а ранее неизвестные – с вероятностью, зависящей типа модификации. Арифметические операторы «+» и «–» неразличимы с точки зрения соотношений размерностей их операндов ($[L] = [P]$), а значит модификацию одного из них на другой невозможно обнаружить. Обозначим вероятность того, что модификация будет различима с точки зрения размерностей, как $p = 1 - (P_{+-} + P_{-+}) = 0,875$. Тогда вероятность обнаружения (а значит и восстановления) нарушений можно определить как:

$$P_{\text{обн}i} = P_{\text{восст}i} = k_{\text{изв}i} 1 + (1 - k_{\text{изв}i}) p . \quad (9)$$

Допускается, что время непосредственного вычисления программного цикла $T_{\text{выч}i}$ определяется временем выполнения всех вычислительных инструкций программы с учетом количества их параметров. Если также принять допущение, что параметры k_i , m_i и n_i одинаковы для всех программ i -го уровня ОП КИИ, то время вычислений можно оценить как $T_{\text{выч}i} = k_i m_i n_i t_0$.

Время, затрачиваемое дополнительно на контроль и обнаружение нарушений в процессе функционирования программы $T_{\text{обн}i}$, зависит от времени формирования и проверки матриц

размерностей в линейных блоках и пропорционально коэффициенту покрытия кибериммунитета $k_{\text{покр}i}$. Для формирования матриц размерностей (функция μ) потребуется для каждого из k_i блоков вычислить $m_i(m_i-1)/2$ соотношений размерностей (для учета попарных связей) и выполнить $(2n_i-1)$ элементарных операций взятия размерностей (обход дерева разбора арифметического выражения слева направо), после чего для обнаружения нарушения потребуется выполнить $k_i m_i n_i$ элементарных операций сравнения элементов текущей и эталонной матриц (функция η обнаружителя). Нарушение присутствует если один или более элементов матриц не совпадают. Тогда время $T_{\text{обн}i}$ можно определить как:

$$T_{\text{обн}i} = k_{\text{покр}i}\left(k_i \frac{m_i(m_i-1)}{2}(2n_i-1)+k_i m_i n_i\right)t_0 . \quad (10)$$

Восстановление штатного функционирования осуществляется путем перезапуска или возврата к предыдущей контрольной точке. В обоих случаях необходимо выполнить переразметку программы в памяти путем выполнения элементарных операций чтения и записи всего образа программы (функция ξ восстановителя). Тогда время восстановления можно оценить как $T_{\text{восст}i} = 2k_i m_i n_i t_0$.

Поскольку ОП КИИ обладает вертикальными межуровневыми связями, то вероятность достижения цели функционирования ОП КИИ на i -ом уровне $P_{\text{цели}i}$ зависит от аналогичного показателя на $(i-1)$ -ом уровне и с учетом формулы (4) определяется как:

$$P_{\text{цели}i} = P_{\text{цели}i-1}(P_{\text{прот}i}+(1-P_{\text{прот}i})P_{\text{восст}i})P_{\text{раб}i} . \quad (11)$$

7. Теоретическое исследование модели. Исследуем системное свойство устойчивости ОП КИИ в условиях ИТВ на разработанной модели. Для этого сформулируем и докажем утверждение.

Утверждение 1. Увеличение значения коэффициента покрытия кибериммунитета $k_{\text{покр}i}$ повышает устойчивость ОП КИИ и время выполнения программ на i -ом уровне в условиях ИТВ.

Доказательство. Основные показатели устойчивости функционирования ОП КИИ определяются формулами (1)-(5), (8)-(11) и представляют собой непрерывные величины.

Вероятность противодействия ИТВ $P_{\text{прот}i}$, в соответствии с формулой (8), монотонно возрастает при увеличении $k_{\text{покр}i}$.

Среднее время между пропусками ИТВ $T_{\text{ср.атак}i}$ определяется формулой (1) и зависит от времени вычислений $T_{\text{выч}i}$, времени обнаружения нарушений $T_{\text{обн}i}$ и вероятности $P_{\text{прот}i}$. При этом $T_{\text{выч}i}$ и $T_{\text{восст}i}$ не зависят от $k_{\text{покр}i}$, а $T_{\text{обн}i}$, в соответствии с формулой (10), монотонно возрастает при увеличении $k_{\text{покр}i}$. Значит $T_{\text{ср.атак}i}$ также монотонно возрастает при увеличении $k_{\text{покр}i}$.

Вероятность восстановления $P_{\text{восст}i}$ (9) и среднее время восстановления $T_{\text{ср.восст}i}$ (2) не зависят от $k_{\text{покр}i}$.

Вероятность нахождения ОП КИИ в работоспособном состоянии $P_{\text{раб}i}$ определяется формулой (3), зависит от $T_{\text{ср.атак}i}$ и $T_{\text{ср.восст}i}$, и с учетом вышесказанного монотонно возрастает при увеличении $k_{\text{покр}i}$.

Вероятность достижения цели $P_{\text{цели}i}$ определяется формулой (11) и зависит от $P_{\text{цели}i-1}$, $P_{\text{прот}i}$, $P_{\text{восст}i}$ и $P_{\text{раб}i}$. Пусть $P_{\text{цели}i-1}=1$. Поскольку $P_{\text{прот}i}$ и $P_{\text{раб}i}$ монотонно возрастают при увеличении $k_{\text{покр}i}$, а $P_{\text{восст}i}=const$ и $P_{\text{восст}i}<1$, то $P_{\text{цели}i}$ монотонно возрастает при увеличении $k_{\text{покр}i}$.

Время выполнения программного цикла $T_{\text{вып}i}$ определяется формулой (5) и зависит от $T_{\text{выч}i}$, $T_{\text{обн}i}$ и $T_{\text{восст}i}$. Поскольку $T_{\text{обн}i}$ монотонно возрастает, а $T_{\text{выч}i}$ и $T_{\text{восст}i}$ не изменяются при увеличении $k_{\text{покр}i}$, то $T_{\text{вып}i}$ также монотонно возрастает при увеличении $k_{\text{покр}i}$.

Таким образом, все рассмотренные показатели устойчивости не уменьшаются, а основной показатель $P_{\text{цели}i}$ – увеличивается при увеличении $k_{\text{покр}i}$. *Ч.т.д.*

По результатам доказательства Утверждения 1 можно сделать следующий вывод. Увеличение $k_{\text{покр}i}$ повышает устойчивость ОП КИИ, но приводит к увеличению времени выполнения программ. В целом учет свойства кибериммунитета положительно влияет на устойчивость функционирования ОП КИИ в условиях ИТВ, а значит Гипотезу исследования можно считать *подтвержденной* теоретически.

8. Экспериментальное исследование модели. Целью эксперимента является исследование изменения показателей устойчивости ОП КИИ при варьировании $k_{\text{покр}i}$, определение существования минимального и максимального допустимых значений $k_{\text{покр}i}$ при наличии требований к показателям и проверка Гипотезы исследования. Зададим параметры моделирования: $P_{\text{цели}i-1} = 1$, $P_{\text{мод}i} = 0,75$, $k_{\text{изв}i} = 0,4$, $k_i = 1000$, $m_i = 5$, $n_i = 2$.

На рисунке 5 представлены графики зависимостей показателей устойчивости функционирования ОП КИИ на i-ом уровне в условиях ИТВ от коэффициента покрытия кибериммунитета $k_{\text{покр}i}$. Как видно, при увеличении $k_{\text{покр}i}$ значения основных показателей устойчивости также возрастают. При этом следует отметить, что такие показатели как вероятность восстановления (рисунок 5(в)) и среднее время восстановления (рисунок 5(г)) не зависят от $k_{\text{покр}i}$ напрямую, однако при наличии кибериммунной защиты ($k_{\text{покр}i} > 0$) вероятность $P_{\text{восст}i}$ оказывается выше, а время $T_{\text{ср.восст}i}$ – ниже, чем при ее отсутствии ($k_{\text{покр}i} = 0$, $p = 0$).

Таким образом, увеличение $k_{\text{покр}i}$ положительно влияет на способность ОП КИИ противодействовать ИТВ, не допуская нарушений, и восстанавливать штатное функционирование при их возникновении, а учет свойства кибериммунитета в целом повышает устойчивость функционирования ОП КИИ, что согласуется с теоретическими выводами.

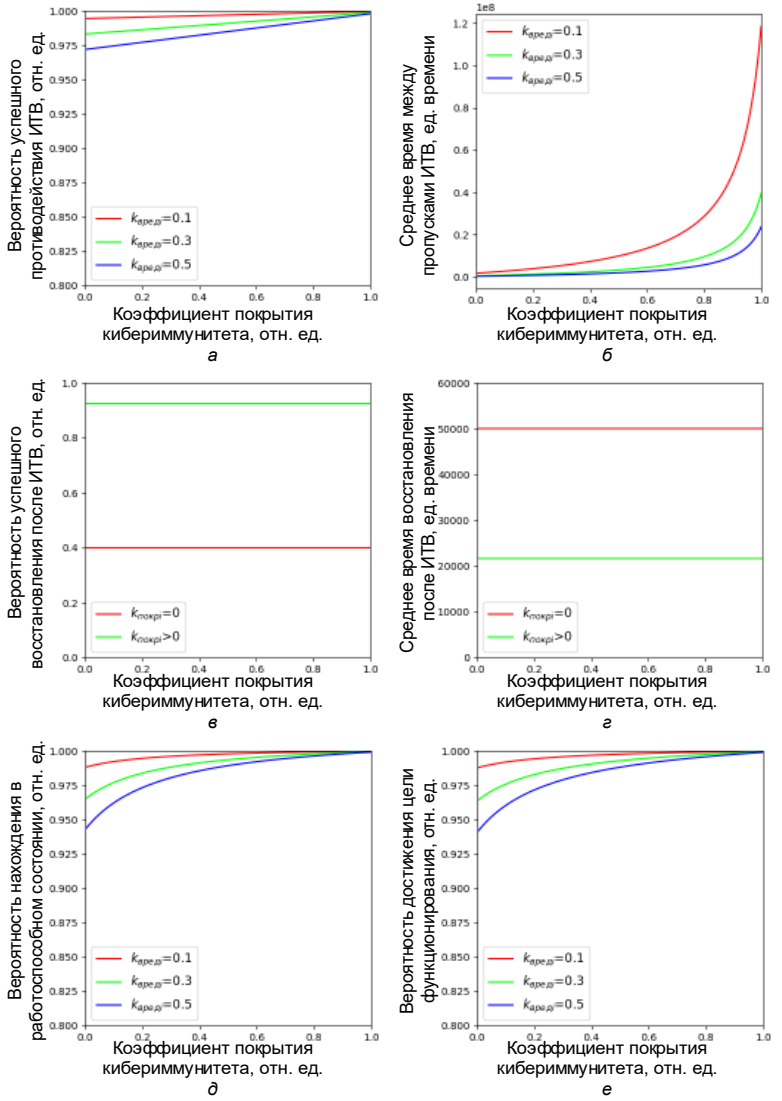

Рис. 5. Зависимости от коэффициента покрытия кибериммунитета $k_{\text{покр}i}$: *а* – вероятности успешного противодействия ИТВ $P_{\text{прот}i}$; *б* – ср. времени между пропусками ИТВ $T_{\text{ср.атак}i}$; *в* – вероятности успешного восстановления $P_{\text{восст}i}$; *г* – ср. времени восстановления $T_{\text{ср.восст}i}$; *д* – вероятности нахождения в работоспособном состоянии $P_{\text{раб}i}$; *е* – вероятности достижения цели $P_{\text{цели}}$

Пусть теперь требуется, чтобы $P_{\text{цели}} \geq 0,96$ и $T_{\text{вып}i} \leq 46000$ при $N = 4$ (количество уровней ОП КИИ). В таблице 1 представлены результаты исследования показателей устойчивости ОП КИИ для различных значений коэффициента $k_{\text{вред}i}$. Отметим, что $P_{\text{цели}i}$ характеризует вероятность достижения цели ОП КИИ на i-ом уровне, а $P_{\text{цели}}$ – общую вероятность достижения цели ОП КИИ. При этом $P_{\text{цели}} \propto P_{\text{цели}i}^{N}$, поскольку нарушение на нижележащем уровне влияет на все вышележащие, а значит общая вероятность достижения цели ОП КИИ зависит от вероятности достижения ее на всех N уровнях.

Таблица 1. Результаты исследования показателей устойчивости функционирования ОП КИИ в условиях ИТВ

$k_{\text{покр}i}$	$P_{\text{прот}i}$	$T_{\text{ср.атак}i}$	$P_{\text{восст}i}$	$T_{\text{ср.восст}i}$	$P_{\text{раб}i}$	$P_{\text{цели}i}$	$T_{\text{вып}i}$	$P_{\text{цели}}$
$k_{\text{вред}i} = 0,1$								
0	0,9550	222222	0,4000	50000	0,8163	0,7943	30000	0,3980
0,0457	0,9946	2195568	0,9250	21622	0,9902	0,9898	**31828**	**0,9600**
0,2000	0,9954	3926380	0,9250	21622	0,9945	0,9942	38000	0,9769
0,4000	0,9965	7336861	0,9250	21622	0,9971	0,9968	**46000**	**0,9872**
0,5000	0,9970	9922480	0,9250	21622	0,9978	0,9976	50000	0,9904
0,8000	0,9985	28717948	0,9250	21622	0,9992	0,9991	62000	0,9965
$k_{\text{вред}i} = 0,3$								
0	0,8650	74074	0,4000	50000	0,5970	0,5486	30000	0,0906
0,2000	0,9862	1308793	0,9250	21622	0,9837	0,9827	38000	0,9327
0,3787	0,9890	2293745	0,9250	21622	0,9907	0,9898	**45148**	**0,9600**
0,4000	0,9894	2445620	0,9250	21622	0,9912	0,9904	**46000**	**0,9623**
0,5000	0,9909	3307493	0,9250	21622	0,9935	0,9928	50000	0,9716
0,8000	0,9956	9572649	0,9250	21622	0,9977	0,9974	62000	0,9897
$k_{\text{вред}i} = 0,5$								
0	0,7750	44444	0,4000	50000	0,4706	0,4071	30000	0,0275
0,2000	0,9771	785276	0,9250	21622	0,9732	0,9715	38000	0,8909
0,4000	0,9823	1467372	0,9250	21622	0,9855	0,9842	**46000**	**0,9382**
0,5000	0,9849	1984496	0,9250	21622	0,9892	0,9881	50000	0,9532
0,5541	0,9863	2346069	0,9250	21622	0,9909	0,9898	**52164**	**0,9600**
0,8000	0,9927	5743590	0,9250	21622	0,9962	0,9957	62000	0,9829

Видно, что при отсутствии кибериммунной защиты ($k_{\text{покр}i} = 0$) ОП КИИ теряет устойчивость ($P_{\text{цели}} \to 0$). Увеличение же значения $k_{\text{покр}i}$ повышает устойчивость ОП КИИ по всем обоснованным ранее показателям, однако это сопровождается увеличением времени

выполнения программ $T_{\text{вып}i}$. В случае $k_{\text{вред}i} = 0{,}1$ заданные требования обеспечиваются за счет варьирования значения коэффициента $k_{\text{покр}i}$ в диапазоне от 0,0457 до 0,4000, а в случае $k_{\text{вред}i} = 0{,}3$ – в диапазоне от 0,3787 до 0,4000. Иная ситуация наблюдается при $k_{\text{вред}i} = 0{,}5$. Здесь требование к $P_{\text{цели}}$ обеспечивается при $k_{\text{покр}i}$ не ниже 0,5541, однако для выполнения требования к $T_{\text{вып}i}$ допустимы значения $k_{\text{покр}i}$ не выше 0,4000, а значит в данном случае не существует значения $k_{\text{покр}i}$, при котором одновременно выполняются оба требования.

Полученная вероятность ошибок II-го рода (пропуск ИТВ) не превышает 0,03 (оценка на основе $\beta = 1 - P_{\text{прот}i}$), что согласуется с результатами исследований инвариантных методов обнаружения аномалий, приведенными в работе [30].

В дальнейшем целесообразно определить критерий существования решения, а также разработать методику синтеза оптимального значения $k_{\text{покр}i}$ с учетом требований к $P_{\text{цели}}$ и $T_{\text{вып}i}$.

Таким образом, результаты экспериментальных исследований устойчивости функционирования ОП КИИ в условиях ИТВ согласуются с теоретическими выводами, а значит, Гипотезу исследования можно считать *подтвержденной*.

9. Возможности практического применения результатов исследования. На рисунке 6 представлена возможная архитектура программного комплекса обеспечения устойчивости функционирования ОП КИИ.

Основными элементами программного комплекса являются:

- транслятор с SDK для внедрения кибериммунитета;
- подсистема управления устойчивостью, включающая модуль оценивания текущей устойчивости ОП КИИ и модуль управления параметрами кибериммунитета;
- подсистема кибериммунитета, включающая базу данных (БД) кибериммунитета, обнаружитель нарушений и восстановитель штатного функционирования.

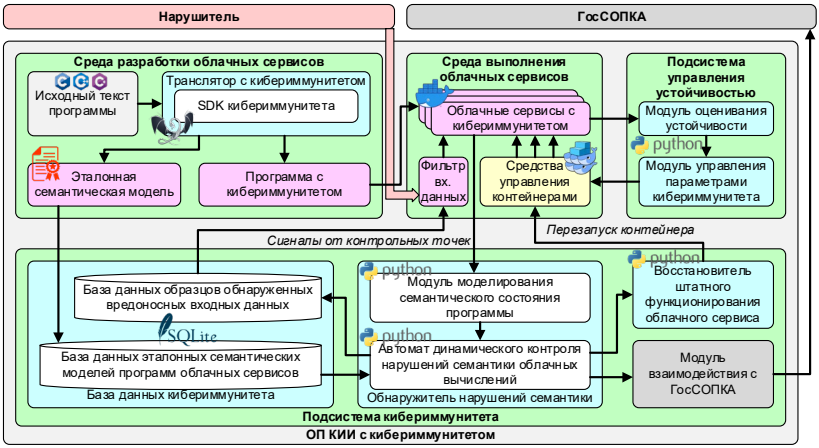

Рис. 6. Возможная архитектура программного комплекса обеспечения устойчивости функционирования ОП КИИ

Исходная программа облачного сервиса с помощью дополнений компилятора clang преобразуется в программу с кибериммунитетом путем внедрения элементов структурно-функциональной избыточности (меток начала и конца линейных блоков), при этом формируется ее эталонная модель в терминах формальных семантик (в частности, размерностей). Полученная программа с кибериммунитетом запускается в Docker-контейнере и циклически обрабатывает входные данные, находясь под воздействием ИТВ. В процессе функционирования программы сигналы о прохождении контрольных точек от внедренных меток передаются в обнаружитель нарушений, где текущее семантическое состояние программы в линейном блоке моделируется и сравнивается с эталонным (поэлементным сравнением матриц размерностей). При обнаружении нарушения состояния в результате атаки внедрения кода или нарушения перехода в результате атаки перехвата потока управления образец вредоносных входных данных заносится в БД SQLite и более не допускается. После этого восстановитель формирует команду перезапуска Docker-контейнера или возврата к предыдущему состоянию, если осуществляется их сохранение, и передает ее оркестратору. В процессе функционирования устойчивость ОП КИИ оценивается по показателям вероятности достижения цели и времени выполнения программного цикла и, при необходимости, осуществляется управление множеством контролируемых линейных блоков на основе коэффициента покрытия кибериммунитета.

В ходе накопления информации об отраженных ИТВ в БД SQLite могут сохраняться схожие образцы вредоносных входных данных одного формата. Поскольку данный формат неизвестен заранее, целесообразно осуществлять периодическую оптимизацию БД путем замены схожих образцов шаблонами. Имея несколько схожих образцов и применяя методы статистической индукции, можно своевременно нейтрализовать весь подкласс ранее неизвестных ИТВ, использующих вредоносные входные данные такого формата.

Таким образом, *практическая значимость* результатов исследования заключается в доведении их до технических рекомендаций по архитектуре программного комплекса. Данные технические рекомендации включают в себя разработку программных модулей, в совокупности реализующих новое эмерджентное свойство кибериммунитета, и могут быть применены для обеспечения устойчивости функционирования ОП КИИ, в частности «ГосТех».

10. Заключение. В работе предложена модель ОП КИИ с кибериммунитетом, позволяющая при принятых допущениях получать оценки введенных и обоснованных показателей устойчивости. *Научная новизна* модели заключается в том, что в нее впервые внедрены такие элементы, как обнаружитель нарушений семантики вычислений, восстановитель штатного функционирования и кибериммунная память. Данные элементы в совокупности реализуют новое эмерджентное свойство кибериммунитета, определяющее способность ОП КИИ противодействовать известным и новым, ранее неизвестным ИТВ, не допуская нарушений, и оперативно восстанавливать штатное функционирование при их возникновении.

Проведены теоретическое и экспериментальное исследования модели. Доказано утверждение о том, что увеличение значения коэффициента покрытия кибериммунитета повышает устойчивость функционирования ОП КИИ в условиях ИТВ по всем введенным показателям, но также приводит к увеличению времени выполнения программ. Для заданных условий экспериментально определены границы допустимых значений коэффициента покрытия кибериммунитета, в пределах которых одновременно обеспечиваются требования к вероятности достижения цели функционирования и времени выполнения программ ОП КИИ. По результатам исследований *подтверждена* выдвинутая Гипотеза исследования о том, что учет свойства кибериммунитета положительно влияет на устойчивость функционирования ОП КИИ в условиях ИТВ.

Практическая значимость результатов исследования заключается в доведении их до технических рекомендаций по

архитектуре программного комплекса, которые могут быть использованы при разработке средств защиты ОП КИИ, в частности, облачной платформы «ГосТех», в условиях ИТВ.

В *направления дальнейших исследований* входит: разработка методики синтеза оптимального значения коэффициента покрытия кибериммунитета с учетом требований к показателям устойчивости и времени выполнения программ, а также критерия его существования; исследование возможностей применения методов статистической индукции для превентивного реагирования на ранее неизвестные ИТВ на основе информации об известных вредоносных входных данных.

Литература

1. Официальный сайт компании CheckPoint. The State of Cyber Security 2025. URL: https://www.checkpoint.com/security-report/ (дата обращения: 09.06.2025).
2. Официальный сайт компании «Солар». Тренды кибератак на промышленность и телеком в 2025 году. URL: https://rt-solar.ru/analytics/reports/5522/ (дата обращения: 09.06.2025).
3. Официальный сайт «РИА Новости». Гендиректор «Солара» рассказал о росте числа кибератак на Россию. URL: https://ria.ru/20250606/gk-2021325615.html (дата обращения: 09.06.2025).
4. Зегжда Д.П., Александрова Е.Б., Калинин М.О., и др. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам // Москва: Научно-техническое издательство «Горячая линия-Телеком». 2021. 560 с.
5. Павленко Е.Ю., Штыркина А.А., Зегжда Д.П. Оценка устойчивости киберфизических систем на основе спектральной теории графов // Проблемы информационной безопасности. Компьютерные системы. 2019. № 1. С. 60–68.
6. Саенко И.Б., Котенко И.В., Лаута О.С., Скоробогатов С.Ю. Методика оценки устойчивости программно-конфигурируемых сетей в условиях компьютерных атак // I-methods. 2023. Т. 15. № 1.
7. Саенко И.Б., Котенко И.В., Лаута О.С., Скоробогатов С.Ю. Модели компьютерных атак на программно-конфигурируемые сети // Наукоемкие технологии в космических исследованиях Земли. 2023. Т. 15. № 1. С. 37–47. DOI: 10.36724/2409-5419-2023-15-1-37-47.
8. Бирюков Д.Н., Ломако А.Г., Ростовцев Ю.Г. Облик антиципирующих систем предотвращения рисков реализации киберугроз // Труды СПИИРАН. 2015. № 2(39). С. 5–25. DOI: 10.15622/sp.39.1.
9. Андрушкевич Д.В., Бирюков Д.Н., Тимашов П.В. Порождение сценариев предотвращения компьютерных атак на основе логико-онтологического подхода // Труды Военно-космической академии имени А.Ф. Можайского. 2021. № 677. С. 118–134.
10. Кубрин Г.С., Зегжда Д.П. Выявление дефектов в многокомпонентном программном обеспечении с применением набора универсальных графовых представлений кода // Проблемы информационной безопасности. Компьютерные системы. 2024. № S2(60). С. 65–75. DOI: 10.48612/jisp/nb67-m5g8-mpae.

11. Chevtchenko S.F., et al. Anomaly Detection in Industrial Machinery Using IoT Devices and Machine Learning: A Systematic Mapping // IEEE Access. 2023. vol. 11. pp. 128288–128305. DOI: 10.1109/ACCESS.2023.3333242.
12. Nand K., Zhang Z., Hu J. A Comprehensive Survey on the Usage of Machine Learning to Detect False Data Injection Attacks in Smart Grids // IEEE Open Journal of the Computer Society. 2025. vol. 6. pp. 1121–1132. DOI: 10.1109/OJCS.2025.3585248.
13. Hao W., Yang T., Yang Q. Hybrid Statistical-Machine Learning for Real-Time Anomaly Detection in Industrial Cyber–Physical Systems // IEEE Transactions on Automation Science and Engineering. 2023. vol. 20. no. 1. pp. 32–46. DOI: 10.1109/TASE.2021.3073396.
14. Ozdogan E. A Comprehensive Analysis of the Machine Learning Algorithms in IoT IDS Systems // IEEE Access. 2024. vol. 12. pp. 46785–46811. DOI: 10.1109/ACCESS.2024.3382539.
15. Новикова Е.С., Котенко И.В., Мелешко А.В., Израилов К.Е. Обнаружение вторжений на основе федеративного обучения: архитектура системы и эксперименты // Вопросы кибербезопасности. 2023. № 6(58). С. 50–66. DOI: 10.21681/2311-3456-2023-6-50-66.
16. Aljuaid W.H., Alshamrani S.S. A deep learning approach for intrusion detection systems in cloud computing environments // Applied sciences. 2024. vol. 14. no. 13. DOI: 10.3390/app14135381.
17. Alrayes F.S., Zakariah M., Amin S.U., Iqbal Khan Z., Helal M. Intrusion Detection in IoT Systems Using Denoising Autoencoder // IEEE Access. 2024. vol. 12. pp. 122401–122425. DOI: 10.1109/ACCESS.2024.3451726.
18. Liu X., Xie L., Wang Y., Zou J., Xiong J., Ying Z. Privacy and Security Issues in Deep Learning: A Survey // IEEE Access. 2021. vol. 9. pp. 4566–4593. DOI: 10.1109/ACCESS.2020.3045078.
19. Бурлаков М.Е., Ивкин А.Н. Система обнаружения вторжения на основе искусственной иммунной системы // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. 2019. № 29. С. 209–224.
20. Шамсутдинов Р.Р., Васильев В.И., Вульфин А.М. Интеллектуальная система мониторинга информационной безопасности промышленного интернета вещей с использованием механизмов искусственных иммунных систем // Системная инженерия и информационные технологии. 2024. Т. 6. № 4(19). С. 14–31. DOI: 10.54708/2658-5014-SIIT-2024-no4-p14.
21. Браницкий А.А., Котенко И.В. Обнаружение сетевых атак на основе комплексирования нейронных, иммунных и нейронечетких классификаторов // Информационно-управляющие системы. 2015. № 4(77). С. 69–77. DOI: 10.15217/issn1684-8853.2015.4.69.
22. Dutt I., Borah S., Maitra I.K. Immune System Based Intrusion Detection System (IS-IDS): A Proposed Model // IEEE Access. 2020. vol. 8. pp. 34929–34941. DOI: 10.1109/ACCESS.2020.2973608.
23. Aldhaheri S., Alghazzawi D., Cheng L., Alzahrani B., Al-Barakati A. DeepDCA: Novel Network-Based Detection of IoT Attacks Using Artificial Immune System // Appl. Sci. 2020. vol. 10(6). DOI: 10.3390/app10061909.
24. Gijsen B., Montalto R., Panneman J., Falconieri F., Wiper P., Zuraniewski P. Self-Healing for Cyber-Security // Sixth International Conference on Fog and Mobile Edge Computing (FMEC). 2021. pp. 1–7. DOI: 10.1109/FMEC54266.2021.9732575.
25. Pinto C., Pinto R., Gonçalves G. Towards Bio-Inspired Anomaly Detection Using the Cursory Dendritic Cell Algorithm // Algorithms. 2022. vol. 15(1). DOI: 10.3390/a15010001.

26. Bereta M. Negative selection algorithm for unsupervised anomaly detection // Applied sciences. 2024. vol. 14. no. 23. DOI: 10.3390/app142311040.
27. Jerbi M., Dagdia Z.C., Bechikh S., Said L.B. Immune-based system to enhance malware detection // IEEE congress on evolutionary computation (CEC). 2023. pp. 1–8. DOI: 10.1109/CEC53210.2023.10254159.
28. Воеводин В.А. О постановке задачи оценивания устойчивости функционирования объектов критической информационной инфраструктуры // Вопросы кибербезопасности. 2025. № 1(65). С. 41–49. DOI: 10.21681/2311-3456-2025-1-41-49.
29. Балябин А.А., Петренко С.А. Модель самовосстановление киберфизических систем КИИ РФ в условиях кибератак на основе кибериммунитета // Сборник трудов IX Международной научно-технической конференции (CDE'25). 2025. С. 76–91.
30. Петренко С.А. Кибериммунология: научная монография // Санкт-Петербург: Издательский дом «Афина». 2021. 240 с.
31. Петренко С.А. Киберустойчивость индустрии 4.0: научная монография // Санкт-Петербург: Издательский дом «Афина». 2020. 256 с.
32. Balyabin A.A. Threats to the Resilience of Cloud Platforms // XXVII International Conference on Soft Computing and Measurements (SCM). 2024. pp. 246–249. DOI: 10.1109/SCM62608.2024.10554080.
33. Balyabin A.A. Ensuring the Resilience of Cloud Platforms Based on Cyber Immunity // XXVII International Conference on Soft Computing and Measurements (SCM). 2024. pp. 233–237. DOI: 10.1109/SCM62608.2024.10554277.
34. Балябин А.А. Модель облачной платформы КИИ РФ с кибериммунитетом в условиях информационно-технических воздействий // Защита информации. Инсайд. 2024. № 5(119). С. 35–44.
35. Харжевская А.В., Ломако А.Г., Петренко С.А. Представление программ инвариантами подобия для контроля искажения вычислений // Вопросы кибербезопасности. 2017. № 2(20). С. 9–20. DOI: 10.21581/2311-3456-2017-2-9-20.

Балябин Артём Алексеевич — младший научный сотрудник, научный центр информационных технологий и искусственного интеллекта, Научно-технологический университет "Сириус". Область научных интересов: исследование безопасности программного обеспечения, формальная верификация, обратный инжиниринг программных комплексов, организация самовосстанавливающихся вычислений, кибериммунология, искусственный интеллект, блокчейн, квантовые вычисления. Число научных публикаций — 112. balyabin.aa@talantiuspeh.ru; проспект Олимпийский, 1, 354340, Федеральная территория "Сириус", Россия; р.т.: +7(911)260-0620.

Петренко Сергей Анатольевич — д-р техн. наук, профессор, руководитель группы, научный центр информационных технологий и искусственного интеллекта, Научно-технологический университет "Сириус". Область научных интересов: квантовая информатика и информационная безопасность, информационные технологии и искусственный интеллект. Число научных публикаций — 560. petrenko.sa@talantiuspeh.ru; проспект Олимпийский, 1, 354340, Федеральная территория "Сириус", Россия; р.т.: +7(903)742-8543.

Поддержка исследований. Исследование выполнено за счет гранта Российского научного фонда (№ 25-11-20037, https://www.rscf.ru/project/25-11-20037/).

DOI 10.15622/ia.24.5.8

A. BALYABIN, S. PETRENKO

MODEL OF A CRITICAL INFORMATION INFRASTRUCTURE CLOUD PLATFORM WITH CYBER IMMUNITY

Balyabin A., Petrenko S. **Model of a Critical Information Infrastructure Cloud Platform with Cyber Immunity.**

Abstract. The research is devoted to solving the problem of synthesizing a model of a critical information infrastructure cloud platform with cyber immunity. The relevance of the research is due to the need to resolve a problematic situation characterized by contradictions in science and practice. The contradiction in practice is observed between increased requirements for the resilience of critical information infrastructure cloud platforms and the growth of threats associated with the exploitation of previously unknown vulnerabilities and the overcoming of protective measures. The contradiction in science is that it is impossible to ensure the required resilience of such platforms using existing models and methods. Thus, existing approaches do not fully account for the specific features of critical information infrastructure cloud platforms, such as hierarchical architecture, the presence of undetected vulnerabilities, operation under targeted cyberattacks, increased requirements for resilience, and the need for rapid restoration of normal operation. This paper aims to synthesize a new model of a critical information infrastructure cloud platform with cyber immunity. A hypothesis has been formulated that endowing cloud platforms with the property of cyber immunity has a positive effect on their resilience when subjected to cyberattacks. Research methods include methods of system analysis, probability theory, theory of formal semantics, theory of similarity and dimensional analysis, as well as cyber immunology methods. The concept of cyber immunity has been substantiated, which involves providing cloud platforms with the ability to counteract known and previously unknown cyberattacks, quickly restore normal operation, and memorize malicious input data, thereby preventing their processing in the future. The indicators of the resilience of critical information infrastructure cloud platforms have also been substantiated. A new model of a critical information infrastructure cloud platform with cyber immunity has been developed. The scientific novelty of the proposed model lies in the introduction, for the first time, of components such as a semantic violation detector, a normal operation restorer, and cyber immune memory. These components collectively implement a new emergent property of cyber immunity. Theoretical and experimental studies of the model have been conducted, confirming the proposed hypothesis. The practical significance of the research results lies in providing technical recommendations on the architecture of the software complex, which can be applied in the development of means for protecting critical information infrastructure cloud platforms, in particular, the GosTech cloud platform, against cyberattacks.

Keywords: cloud computing, computation semantics, critical information infrastructure, cyber resilience, cyberattacks, cyber immunity.

References

1. Официальный сайт компании CheckPoint. The State of Cyber Security 2025. Available at: https://www.checkpoint.com/security-report/ (accessed 09.06.2025). (In Russ.).
2. Официальный сайт компании «Солар». Тренды кибератак на промышленность и телеком в 2025 году. Available at: https://rt-solar.ru/analytics/reports/5522/ (accessed 09.06.2025). (In Russ.).

3. Официальный сайт «РИА Новости». Гендиректор «Солара» рассказал о росте числа кибератак на Россию. Available at: https://ria.ru/20250606/gk-2021325615.html (accessed 09.06.2025). (In Russ.).
4. Zegzhda D.P., Aleksandrova E.B., Kalinin M.O., et al. Kiberbezopasnost' tsifrovoy industrii. Teoriya i praktika funktsional'noy ustoychivosti k kiberatakam [Cybersecurity of the Digital Industry: Theory and Practice of Functional Resilience to Cyberattacks]. Moscow: Nauchno-tekhnicheskoe izdatel'stvo «Goryachaya liniya-Telekom». 2021. 560 p. (In Russ.).
5. Pavlenko E.Yu., Shtyrkina A.A., Zegzhda D.P. [Estimating the Cyber-Physical System Sustainability Based on Spectral Graph Theory]. Problemy informatsionnoy bezopasnosti. Komp'yuternye systemy – Problems of information security. Computer systems. 2019. no. 1. pp. 60–68. (In Russ.).
6. Saenko I.B., Kotenko I.V., Lauta O.S., Skorobogatov S.Yu. [Sustainability Assessment Methodology Software-Configurable Networks in the Conditions of Computer Attacks]. I-methods. 2023. vol. 15. no. 1. (In Russ.).
7. Saenko I.B., Kotenko I.V., Lauta O.S., Skorobogatov S.Yu. [Computer Attack Models on Software-Configurable Networks]. Naukoemkie tekhnologii v kosmicheskikh issledovaniyakh Zemli – High technologies in earth space research. 2023. vol. 15. no. 1. pp. 37–47. DOI: 10.36724/2409-5419-2023-15-1-37-47. (In Russ.).
8. Biryukov D., Lomako A., Rostovtsev Y. The Appearance of Anticipating Cyber Threats Risk Prevention Systems. SPIIRAS Proceedings. Труды СПИИРАН. 2015. no. 2(39). pp. 5–25. DOI: 10.15622/sp.39.1. (In Russ.).
9. Andrushkevich D.V., Biryukov D.N., Timashov P.V. [Synthesis of Computer Attack Prevention Scenarios Based on a Logical-Ontological Approach]. Trudy Voenno-kosmicheskoy akademii imeni A.F. Mozhayskogo – Proceedings of the A.F. Mozhaysky Military Space Academy. 2021. no. 677. pp. 118–134. (In Russ.).
10. Kubrin G.S., Zegzhda D.P. [Vulnerability Detection in Multicomponent Software Using a Set of Generalized Code Graph Representations]. Problemy informatsionnoy bezopasnosti. Komp'yuternye systemy – Problems of information security. Computer systems. 2024. no. S2(60). pp. 65–75. DOI: 10.48612/jisp/nb67-m5g8-mpae. (In Russ.).
11. Chevtchenko S.F., et al. Anomaly Detection in Industrial Machinery Using IoT Devices and Machine Learning: A Systematic Mapping. IEEE Access. 2023. vol. 11. pp. 128288–128305. DOI: 10.1109/ACCESS.2023.3333242.
12. Nand K., Zhang Z., Hu J. A Comprehensive Survey on the Usage of Machine Learning to Detect False Data Injection Attacks in Smart Grids. IEEE Open Journal of the Computer Society. 2025. vol. 6. pp. 1121–1132. DOI: 10.1109/OJCS.2025.3585248.
13. Hao W., Yang T., Yang Q. Hybrid Statistical-Machine Learning for Real-Time Anomaly Detection in Industrial Cyber–Physical Systems. IEEE Transactions on Automation Science and Engineering. 2023. vol. 20. no. 1. pp. 32–46. DOI: 10.1109/TASE.2021.3073396.
14. Ozdogan E. A Comprehensive Analysis of the Machine Learning Algorithms in IoT IDS Systems. IEEE Access. 2024. vol. 12. pp. 46785–46811. DOI: 10.1109/ACCESS.2024.3382539.
15. Novikova E.S., Kotenko I.V., Meleshko A.V., Izrailov K.E. [Federated Learning Based Intrusion Detection: System Architecture and Experiments]. Voprosy kiberbezopasnosti – Cybersecurity issues. 2023. no. 6(58). pp. 50–66. DOI: 10.21681/2311-3456-2023-6-50-66. (In Russ.).
16. Aljuaid W.H., Alshamrani S.S. A deep learning approach for intrusion detection systems in cloud computing environments. Applied sciences. 2024. vol. 14. no. 13. DOI: 10.3390/app14135381.

17. Alrayes F.S., Zakariah M., Amin S.U., Iqbal Khan Z., Helal M. Intrusion Detection in IoT Systems Using Denoising Autoencoder. IEEE Access. 2024. vol. 12. pp. 122401–122425. DOI: 10.1109/ACCESS.2024.3451726.
18. Liu X., Xie L., Wang Y., Zou J., Xiong J., Ying Z. Privacy and Security Issues in Deep Learning: A Survey. IEEE Access. 2021. vol. 9. pp. 4566–4593. DOI: 10.1109/ACCESS.2020.3045078.
19. Burlakov M.E., Ivkin A.N. [Intrusion Detection System Based on the Artificial Immune System]. Vestnik Permskogo natsional'nogo issledovatel'skogo politekhnicheskogo universiteta. Elektrotekhnika, informatsionnye tekhnologii, sistemy upravleniya – Bulletin of Perm National Research Polytechnic University. Electrical Engineering, Information Technologies, and Control Systems. 2019. no. 29. pp. 209–224. (In Russ.).
20. Shamsutdinov R.R., Vasil'ev V.I., Vul'fin A.M. [Intelligent System for Monitoring Information Security of the Industrial Internet of Things using Artificial Immune Systems Mechanisms]. Sistemnaya inzheneriya i informatsionnye tekhnologii – Systems engineering and information technologies. 2024. vol. 6. no. 4(19). pp. 14–31. DOI: 10.54708/2658-5014-SIIT-2024-no4-p14. (In Russ.).
21. Branitskiy A.A., Kotenko I.V. [Network Attack Detection Based on Combination of Neural, Immune and Neuro-Fuzzy Classifiers]. Informatsionno-upravlyayushchie sistemy – Information and control systems. 2015. no. 4(77). pp. 69–77. DOI: 10.15217/issn1684-8853.2015.4.69. (In Russ.).
22. Dutt I., Borah S., Maitra I.K. Immune System Based Intrusion Detection System (IS-IDS): A Proposed Model. IEEE Access. 2020. vol. 8. pp. 34929–34941. DOI: 10.1109/ACCESS.2020.2973608.
23. Aldhaheri S., Alghazzawi D., Cheng L., Alzahrani B., Al-Barakati A. DeepDCA: Novel Network-Based Detection of IoT Attacks Using Artificial Immune System. Appl. Sci. 2020. vol. 10(6). DOI: 10.3390/app10061909.
24. Gijsen B., Montalto R., Panneman J., Falconieri F., Wiper P., Zuraniewski P. Self-Healing for Cyber-Security. Sixth International Conference on Fog and Mobile Edge Computing (FMEC). 2021. pp. 1–7. DOI: 10.1109/FMEC54266.2021.9732575.
25. Pinto C., Pinto R., Gonçalves G. Towards Bio-Inspired Anomaly Detection Using the Cursory Dendritic Cell Algorithm. Algorithms. 2022. vol. 15(1). DOI: 10.3390/a15010001.
26. Bereta M. Negative selection algorithm for unsupervised anomaly detection. Applied sciences. 2024. vol. 14. no. 23. DOI: 10.3390/app142311040.
27. Jerbi M., Dagdia Z.C., Bechikh S., Said L.B. Immune-based system to enhance malware detection. IEEE congress on evolutionary computation (CEC). 2023. pp. 1–8. DOI: 10.1109/CEC53210.2023.10254159.
28. Voevodin V.A. [On the formulation of the task of assessing the stability of the functioning of critical information infrastructure facilities]. Voprosy kiberbezopasnosti – Cybersecurity issues. 2025. no. 1(65). pp. 41–49. DOI: 10.21681/2311-3456-2025-1-41-49. (In Russ.).
29. Balyabin A.A., Petrenko S.A. [A self-healing model for cyber-physical systems of the Russian Federation's critical information infrastructure under cyberattacks based on cyber-immunity]. Sb. tr. IX Mezhdunar. nauchn.-tekhn. konf. (CDE'25) [The 2025 Symposium on Cybersecurity of the Digital Economy (CDE'25): Collected papers]. 2025. pp. 76–91. (In Russ.).
30. Petrenko S.A. Kiberimmunologiya: nauchnaya monografiya [Cyber Immunology]. Saint Petersburg: Izdatel'skiy dom «Afina». 2021. 239 p. (In Russ.).
31. Petrenko S.A. Kiberustoychivost' industrii 4.0 [Cyber Resilience Industry 4.0]. Saint Petersburg: Izdatel'skiy dom «Afina». 2020. 256 p. (In Russ.).

32. Balyabin A.A. Threats to the Resilience of Cloud Platforms. XXVII International Conference on Soft Computing and Measurements (SCM). 2024. pp. 246–249. DOI: 10.1109/SCM62608.2024.10554080.
33. Balyabin A.A. Ensuring the Resilience of Cloud Platforms Based on Cyber Immunity. XXVII International Conference on Soft Computing and Measurements (SCM). 2024. pp. 233–237. DOI: 10.1109/SCM62608.2024.10554277.
34. Balyabin A.A. [Model of the Cloud Platform of Critical IT Infrastructure of the Russian Federation Under the Conditions of Information Technology Impacts]. Zaŝita informacii. Inside – Information protection. Inside. 2024. no. 5(119). pp. 35–44. (In Russ.).
35. Kharzhevskaya A., Lomako A., Petrenko S. [Representing programs with similarity invariants for monitoring tampering with calculations]. Voprosy kiberbezopasnosti – Cybersecurity issues. 2017. no. 2(20). pp. 9–20. DOI: 10.21581/2311-3456-2017-2-9-20. (In Russ.).

Balyabin Artyom — Junior researcher, Scientific center for information technologies and artificial intelligence, Sirius University of Science and Technology. Research interests: software security research, formal verification, reverse engineering of software systems, organization of self-healing computations, cyber immunology, artificial intelligence, blockchain, quantum computing. The number of publications — 112. balyabin.aa@talantiuspeh.ru; 1, Olympiysky Av., 354340, Federal Territory "Sirius", Russia; office phone: +7(911)260-0620.

Petrenko Sergei — Ph.D., Dr.Sci., Professor, Leader of the group, Scientific center for information technologies and artificial intelligence, Sirius University of Science and Technology. Research interests: quantum informatics and information security, information technology and artificial intelligence. The number of publications — 560. petrenko.sa@talantiuspeh.ru; 1, Olympiysky Av., 354340, Federal Territory "Sirius", Russia; office phone: +7(903)742-8543.

Acknowledgements. This research is supported by the Russian Science Foundation (project № 25-11-20037, https://www.rscf.ru/project/25-11-20037/).