Обеспечение устойчивости функционирования облачных платформ на основе кибериммунитета

А. А. Балябин

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

treven.wt@yandex.ru

Аннотация. **В работе рассмотрена проблема обеспечения устойчивости функционирования облачных платформ в условиях информационно-технических воздействий. Предложено использовать принципы кибериммунитета, позволяющие наделить информационно-вычислительные системы способностью обнаруживать как известные, так и ранее неизвестные вредоносные воздействия, противодействовать им и осуществлять самовосстановление в реальном времени по аналогии с иммунной системой живого организма. Определены показатель, метрика и мера устойчивости функционирования облачных платформ. Предложена модель облачной платформы с кибериммунитетом, позволяющая обеспечить требуемую устойчивость ее функционирования, на примере облачной платформы Российской Федерации «ГосТех».**

Ключевые слова: модель; облачные вычисления; информационно-технические воздействия; кибератаки; устойчивость; обеспечение устойчивости; кибериммунитет.

I. Введение

Современные информационно-вычислительные системы развиваются стремительными темпами, все чаще применяются облачные, туманные и пограничные вычисления, внедряются технологии интернета вещей и иные технологии SmartGrid [1]. Растет и сложность программно-аппаратного обеспечения. Так, например, программное обеспечение (ПО), функционирующее на базе облачных платформ, часто обладает сложной, многоуровневой, распределенный архитектурой (2/3/N-Tier), что может затруднять обеспечение информационной безопасности облачных платформ [2, 3].

Усложнение ПО повышает риски возникновения программных ошибок, приводящих к уязвимостям. Общее количество уязвимостей, выявленных в различном ПО за 2023 год, превысило 29 тысяч, что на 16% больше показателя за 2022 год [4]. Также наблюдается постоянный рост количества и сложности кибератак. По данным [5] общемировое количество кибератак с применением вредоносного ПО за 2023 год увеличилось на 11% и превысило 6 миллиардов. Современные компьютерные атаки все чаще носят организованный и целенаправленный характер (Advanced Persistent Threats, APT) [6, 7]. Наиболее опасными являются атаки, связанные с эксплуатацией ранее неизвестных уязвимостей «нулевого дня» (0-day), поскольку они не могут быть своевременно обнаружены и предотвращены классическими средствами защиты [8, 9]. Среди векторов атаки одним из распространенных является проникновение в облачные среды [10].

Современные информационные технологии внедряются на различных объектах информатизации. Так, например, в Российской Федерации ведутся работы по созданию облачной платформы «ГосТех» [11]. Очевидно, что к таким платформам предъявляются повышенные требования в части устойчивости их функционирования. С другой стороны, использование заимствованного аппаратного и программного обеспечения, потенциально содержащего уязвимости и недекларированные возможности, в условиях разнородных информационно-технических воздействий (ИТВ) создает угрозу устойчивости функционирования облачных платформ, а применяемые классические методы и средства защиты не способны в полной мере предотвратить катастрофические последствия в случае реализации таких угроз [12]. Данное противоречие характеризует проблемную ситуацию, разрешение которой является актуальной научной задачей.

Целью исследования является обеспечение устойчивости функционирования облачных платформ в условиях ИТВ на примере облачной платформы Российской Федерации «ГосТех».

II. Анализ источников

Проблеме обеспечения устойчивости функционирования различных информационно-вычислительных систем посвящено множество научных работ. Например, в работе [13] исследуется повышение устойчивости функционирования автоматизированных систем за счет совершенствования системы обнаружения ИТВ. В работе [14] исследуются ИТВ в автоматизированных системах специального назначения. В работе [15] устойчивость систем предлагается обеспечивать за счет синтеза упреждающего поведения систем кибербезопасности. Общим недостатком таких подходов является невозможность противодействия новым, ранее неизвестным кибератакам и восстановления штатного функционирования.

Принципиально иной подход на основе биологической метафоры кибериммунитета предлагается в работах зарубежных [16-19] и отечественных [20-24] ученых. Применение аналогии иммунной системы живого организма позволяет выявлять как известные, так и ранее неизвестные информационно-технические воздействия. Однако, большинство работ также посвящено решению задачи обнаружения воздействий,

оставляя за рамками вопросы восстановления штатного функционирования информационно-вычислительных систем.

Таким образом, проблема обеспечения устойчивости функционирования облачных платформ на основе кибериммунитета с учетом самовосстановления ранее не рассматривалась.

III. Постановка задачи исследования

Определим модель облачной платформы как вычислительную модель машины Тьюринга (МТ) T:

$$T = \langle Q, \Sigma, \Gamma, \delta, q_0, q_F \rangle, \quad (1)$$

где Q – конечное множество состояний; Γ – конечное множество символов ленты, включая пробел B; $\Sigma \subseteq \Gamma$ – множество входных символов; δ – функция переходов; q_0 – начальное состояние; q_F – конечное состояние.

Язык входных данных МТ (1) определим как:

$$L = \left\{ w \mid w \in \Sigma^*, (q_0, \alpha, 0) \mapsto_T^* (q_F, \alpha, i) \right\},$$

где запись (q, α, i) обозначает конфигурацию МТ.

Вычислительный процесс (ВП), порождаемый запуском МТ с определенными входными данными, определим как:

$$P = \langle X, S, A, Y \rangle, \quad (2)$$

где X – множество входных данных; S – множество абстрактных семантических состояний; A – множество переходов между семантическими состояниями; Y – множество выходных данных.

Запуск МТ с заданными входными данными порождает ВП (2). Отображение B запуска МТ обозначим как:

$$B : T \times L_{вх} \to P,$$

где T – множество МТ; $L_{вх}$ – язык входных данных.

Задачей исследования является разработка модели облачной платформы с кибериммунитетом для обеспечения устойчивости функционирования облачных платформ в условиях ИТВ. Математически задачу можно сформулировать как поиск системы Ω обеспечения устойчивого функционирования облачных платформ в условиях ИТВ:

$$\Omega = \langle C, D, R, K, I, J \rangle,$$

где C – оператор трансляции исходных программ в программы с кибериммунитетом; D – оператор обнаружения нарушений семантики вычислений; R – оператор синтеза микропрограмм восстановления; K – оператор восстановления штатного функционирования; I – оператор проверки входных данных; J – оператор формирования приобретаемого кибериммунитета.

Частные задачи исследования:

- формализация понятий кибериммунитета;
- разработка математической модели облачной платформы с кибериммунитетом;
- определение показателя, метрики и меры устойчивости функционирования облачных платформ с кибериммунитетом;
- оценка устойчивости функционирования облачных платформ с кибериммунитетом в условиях ИТВ.

Гипотеза исследования: учет свойства самовосстановления позволяет обеспечить требуемую устойчивость функционирования облачных платформ с кибериммунитетом в условиях ИТВ.

IV. Моделирование облачной платформы с кибериммунитетом в условиях ИТВ

A. Формализация понятий кибериммунитета

Определение 1. Будем считать, что программа, реализуемая МТ T_2 семантически эквивалентна программе, реализуемой МТ T_1, тогда и только тогда, когда:

$$\forall x \in L_{вх}\ g(x) = f(x); g(x), f(x) \in L_{вых},$$

где $L_{вх}$ и $L_{вых}$ языки входных и выходных данных, а f и g – функции, реализуемые МТ T_1 и T_2 соответственно.

В иных случаях будем считать, что программа, реализуемая МТ T_2, содержит ошибки семантики. Приведем без доказательства теорему и следствие из нее.

Теорема 1. Пусть T_1 – спецификация МТ, а T_2 – ее реализация, $L_{вх}$ – язык входных данных, принимаемых T_1 и T_2. Если программа, реализуемая МТ T_2 содержит семантическую ошибку, то $L_{вх} = L_{вх}^{+} \cup L_{вх}^{-}, L_{вх}^{-} \neq \varnothing$, где $L_{вх}^{+} = \left\{ w \mid w \in \Sigma^*, f(w) = g(w) \right\}$, а $L_{вх}^{-} = \left\{ w \mid w \in \Sigma^*, f(w) \neq g(w) \right\}$.

Следствие 1.1. Если программа T_2 содержит семантическую ошибку, то существует грамматика $G_{вх}^{-}$, порождающая язык входных данных $L_{вх}^{-}$.

Значит с точки зрения атакующего необходимо и достаточно найти некоторое слово языка $L_{вх}^{-}$ и передать его в качестве входных данных программе, принимающей этот язык и содержащей семантическую ошибку. Это действие будет являться информационно-техническим воздействием, направленным на снижение устойчивости облачной платформы.

Тогда под кибериммунитетом будем понимать все необходимые и достаточные меры для обеспечения требуемой устойчивости.

B. Модель облачной платформы с кибериммунитетом в условиях ИТВ

Введем ряд взаимосвязанных отображений, необходимых для построения модели.

- $C: T \to T$ – отображение трансляции с кибериммунитетом, сопоставляющее каждой МТ соответствующую ей МТ с кибериммунитетом;
- $\mu: T \to M$ – отображение из множества МТ T в множество семантических моделей M;
- $B: T \times L_{вх} \to P$ – отображение запуска вычислительного процесса P путем передачи МТ слова из языка входных данных;
- $D: M \times S \to \{0,1\}$ – отображение обнаружения нарушения семантики вычислений, где S – множество семантических состояний;
- $R: M \times S \to A$ – отображение генерации микропрограмм восстановления семантики вычислений, где A – множество переходов между семантическими состояниями;
- $K: S \times A \to S$ – отображение восстановления семантики вычислений;
- $I: L_{вх} \times U \to \{0,1\}$ – отображение проверки входных данных, где $U = \{x \mid x \in L_{вх}^{-}\}$;
- $J: U \times L_{вх} \to U$ – отображение формирования иммунной памяти.

Тогда общая схема модели будет выглядеть как показано на рис. 1.

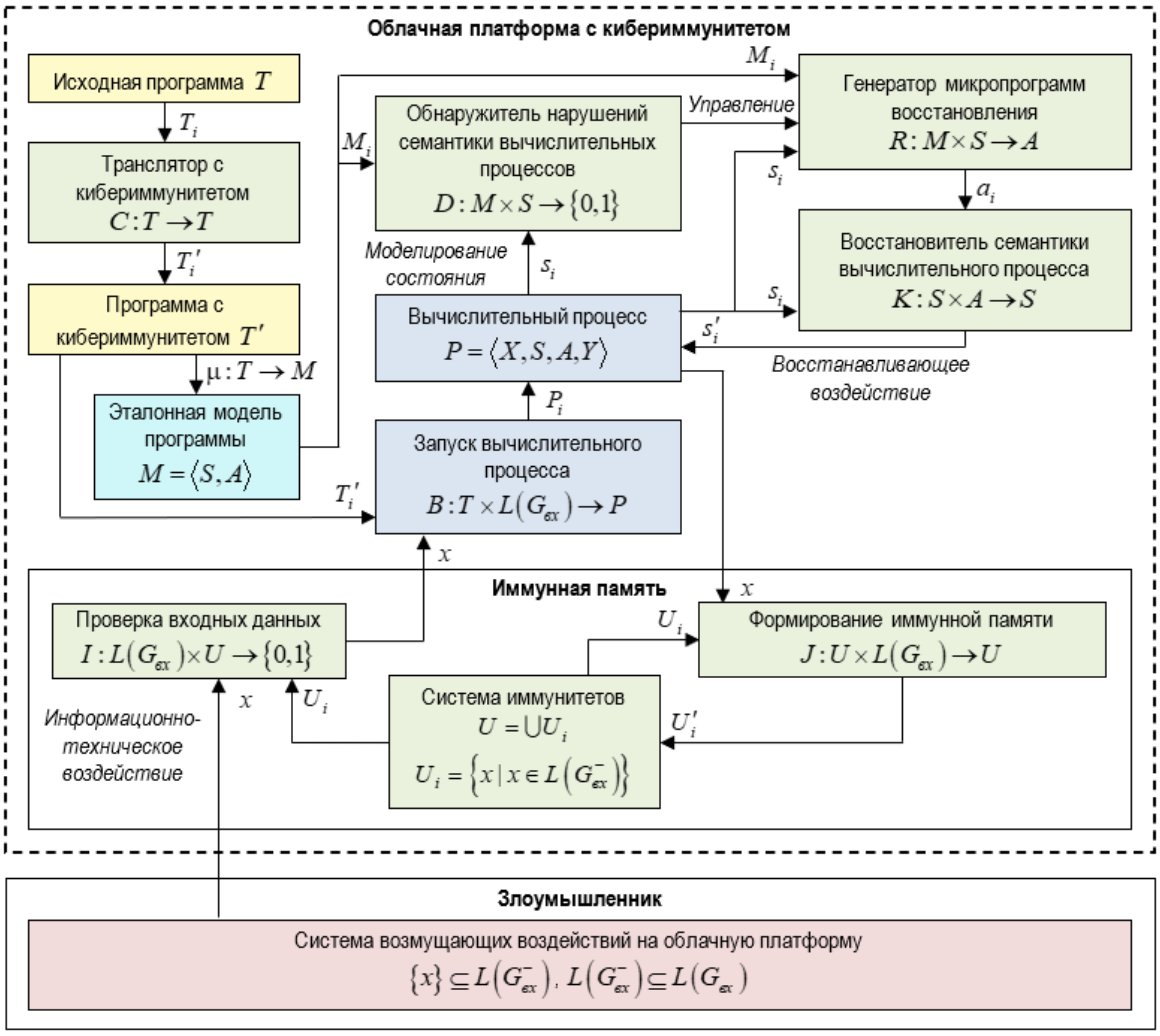

Рис. 1. Схема модели облачной платформы с кибериммунитетом в условиях ИТВ

V. Квалиметрия модели

Для оценки качества модели были доказаны утверждения относительно ее разрешимости, полноты и непротиворечивости. Приведем их здесь без доказательства.

Утверждение 1. Математическая модель облачной платформы с кибериммунитетом в условиях ИТВ разрешима:

$$\forall x \in L_{вх}\ \exists y \in L_{вых} : f(x) = y.$$

Утверждение 2. Математическая модель облачной платформы с кибериммунитетом в условиях ИТВ полна:

$$\forall T_1 \in T\ \exists T_2 \in T, g: T \times L_{вх} \to L_{вых},$$

так, что:

$$\forall x \in L_{вх}\ g(T_1, x) = f(x).$$

Утверждение 3. Математическая модель облачной платформы с кибериммунитетом в условиях ИТВ непротиворечива:

$$\forall x_1, x_2 \in L_{вх}\ x_1 = x_2 \Rightarrow f(x_1) = f(x_2).$$

VI. Оценка устойчивости функционирования облачных платформ с кибериммунитетом в условиях ИТВ

A. *Показатель, метрика и мера устойчивости*

Под устойчивостью обычно понимают способность системы сохранять значения параметров ее функционирования в заданных пределах в условиях дестабилизирующих воздействий [25]. Применительно к объекту исследования деструктивными воздействиями являются информационно-технические воздействий.

Будем оценивать устойчивость облачных платформ с кибериммунитетом по показателю вероятности P работоспособности восстанавливаемой системы в зависимости от времени t [26]:

$$P(t) = \frac{\mu}{\lambda + \mu}\left(1 + \frac{\lambda}{\mu} e^{-(\lambda+\mu)t}\right), \qquad (3)$$

где λ – интенсивность потока нарушений; μ – интенсивность потока восстановлений.

Допустим, что потоки искажений и восстановлений являются простейшими. Также допустим, что вредоносные входные данные не запоминаются. Это необходимо для соблюдения условия простейшего потока нарушений, в противном случае его интенсивность снижалась бы со временем. Данное допущение лишь ужесточает условия проверки.

Интенсивность потока искажений:

$$\lambda \approx \frac{P_{иск}}{t_{вып}} = \frac{\left|L_{вх}^{-}\right|}{\left|L_{вх}\right|} \cdot \frac{1}{t_{вып}},$$

где $t_{вып}$ – время выполнения программы.

Интенсивность потока восстановлений:

$$\mu \approx \frac{P_{восст}}{t_{восст}},$$

где $P_{восст}$ – вероятность восстановления; $t_{восст}$ – время восстановления.

Мерой устойчивости будет число в отрезке $[0;1]$, где 0 обозначает абсолютно неустойчивую, а 1 – абсолютно устойчивую системы.

B. *Результаты оценки устойчивости функционирования облачных платформ с кибериммунитетом в условиях ИТВ*

Пусть требуется обеспечить вероятность работоспособности облачной платформы $P(t) \geq 0{,}85$ в течение времени $t = 10000$ ед. Время выполнения программы $t_{вып} = 1000$ ед. Вероятность искажения $P_{иск} = 0{,}5$. Вероятность восстановления $P_{восст} = 0{,}5$. В этих условиях решение будет зависеть от времени, затрачиваемого на восстановление $t_{восст}$.

Результаты оценки устойчивости функционирования облачной платформы с кибериммунитетом в условиях ИТВ по показателю вероятности работоспособности в зависимости от времени функционирования при различных значениях $t_{восст}$ приведены на рис. 2.

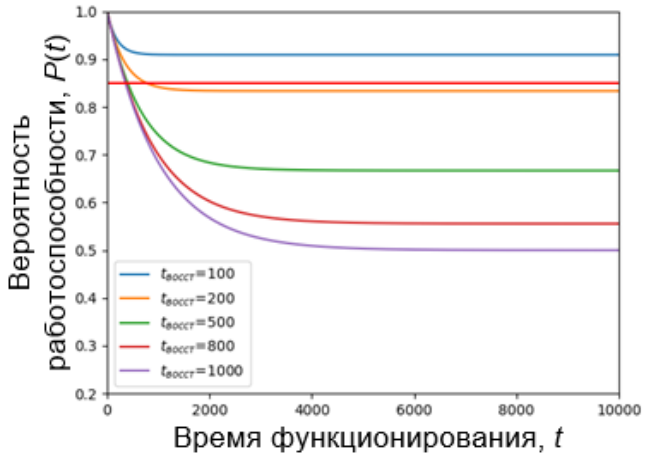

Рис. 2. Результаты оценки вероятности работоспособности облачной платформы с кибериммунитетом в условиях ИТВ

В результате эксперимента требуемая устойчивость в соответствии с заданными условиями обеспечивается только в случае $t_{восст} = 100$ ед. Однако, если решить уравнение (3) относительно $t_{восст}$ при заданных параметрах, возможно найти максимальное допустимое время восстановления, равное для данных условий $t_{восст} \approx 176{,}47$ ед. Полученные результаты позволяют подтвердить выдвинутую гипотезу исследования.

VII. Заключение

В исследовании была выдвинута научная гипотеза о возможности обеспечения требуемой устойчивости функционирования облачных платформ с кибериммунитетом в условиях ИТВ при учете свойства самовосстановления. В ходе исследования был решен ряд частных научных задач. Формализованы понятия кибериммунитета. Разработана модель облачной платформы с кибериммунитетом в условиях ИТВ на примере облачной платформы Российской Федерации «ГосТех». Определен показатель, метрика и мера устойчивости, проведена количественная оценка устойчивости функционирования облачных платформ с кибериммунитетом в условиях ИТВ по показателю вероятности работоспособности в зависимости от времени $P(t)$. Результаты эксперимента показали, что учет свойства самовосстановления позволяет обеспечить выполнение требований к устойчивости функционирования облачных платформ, что подтверждает выдвинутую гипотезу.

В дальнейшем результаты работы предполагается использовать для построения методов и методик защиты облачных платформ на основе свойств

кибериммунитета. Результаты исследования также применимы для разработки методов и средств защиты иных информационно-вычислительных систем и обеспечения устойчивости вычислительных процессов в них.

Благодарность

Автор выражает благодарность своему научному руководителю, доктору технических наук, профессору Петренко Сергею Анатольевичу за ценные замечания, позволившие повысить качество настоящей работы.

Список литературы

[1] X. Yu and Y. Xue, "Smart Grids: A Cyber–Physical Systems Perspective," in *Proceedings of the IEEE*, vol. 104, no. 5, pp. 1058-1070, May 2016, doi: 10.1109/JPROC.2015.2503119.

[2] Petrenko S. Big Data Technologies for Monitoring of Computer Security: A Case Study of the Russian Federation. Cham, Switzerland: Springer International Publishing, 2018. 249 p. DOI: 10.1007/978-3-319-79036-7.

[3] K. Cao, Y. Liu, G. Meng and Q. Sun, "An Overview on Edge Computing Research," in *IEEE Access*, vol. 8, pp. 85714-85728, 2020, doi: 10.1109/ACCESS.2020.2991734.

[4] Common Vulnerability Database: Published CVE Records. URL: https://www.cve.org (дата обращения: 09.03.2024).

[5] SonicWall Cyber Threat Report 2024. URL: https://www.sonicwall.com/medialibrary/en/white-paper/2024-cyber-threat-report.pdf (дата обращения: 09.03.2024).

[6] Y. Li, Q. Liu. «A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments», Energy Reports, vol. 7, pp. 8176-8186, 2021, DOI 10.1016/j.egyr.2021.08.126.

[7] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami and M. Ayaz, "A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies," in *IEEE Access*, vol. 9, pp. 57792-57807, 2021, doi: 10.1109/ACCESS.2021.3073203.

[8] L. Caviglione *et al*., "Tight Arms Race: Overview of Current Malware Threats and Trends in Their Detection," in *IEEE Access*, vol. 9, pp. 5371-5396, 2021, doi: 10.1109/ACCESS.2020.3048319.

[9] Petrenko S., Khismatullina E. Cyber-resilience concept for Industry 4.0 digital platforms in the face of growing cybersecurity threats. Software Technology: Methods and Tools, 51st International Conference, TOOLS 2019, Innopolis, Russia, October 15–17, 2019, Proceedings. Editors: Mazzara, M., Bruel, J.-M., Meyer, B., Petrenko, A. (Eds.). 420 p. DOI: 10.1007/978-3-030-29852-4.

[10] Атаки на российские компании во II квартале 2023 года // РТК-Солар. URL: https://rt-solar.ru/analytics/reports/3610/ (дата обращения: 09.03.2024).

[11] Об утверждении Концепции создания государственной единой облачной платформы: Распоряжение Правительства РФ от 28.08.2019 г. N 1911-р // Собрание законодательства РФ. 09.09.2019. N 36. ст. 5066.

[12] О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 02.06.2021 г. N 400 // Собрание законодательства РФ. 05.06.2021. N 27 (часть II). ст. 5351.

[13] Рыжов Б.С. Повышение устойчивости функционирования автоматизированной системы за счет совершенствования системы обнаружения информационно-технических воздействий // Нейрокомпьютеры: разработка, применение. 2011. № 7. С. 27-31.

[14] Дубровин А.С. Информационно-технические воздействия в автоматизированных системах специального назначения / А.С. Дубровин, Т.В. Мещерякова, В.И. Арутюнова // Вестник Воронежского института высоких технологий. 2018. № 3(26). С. 28-33.

[15] Фоменко К.Э. Подход к определению устойчивости функционирования элементов критической инфраструктуры в условиях компьютерных атак / К.Э. Фоменко, Т.Р. Сабиров, Д.Н. Бирюков // Методы и технические средства обеспечения безопасности информации. 2019. № 28. С. 4-7.

[16] S. Forrest, A.S. Perelson, L. Allen, and R. Cherukuri. Self-nonself discrimination in a computer. In Proceedings of the 1994 IEEE Symposium on Security and Privacy, page 202. IEEE Computer Society, 1994.

[17] J.O. Kephart. A biologically inspired immune system for computers, in R. A. Brooks and P. Maes, eds., Artificial Life IV. Published in the proceedings of the 4th International Workshop on the Synthesis and Simulation of Living Systems, 130-139. MIT Press, 1994.

[18] Dipankar Dasgupta. 1999. Artificial Immune Systems and Their Applications. Springer Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-642-59901-9.

[19] L.N. de Castro, F.J. Von Zuben. Learning and Optimization Using the Clonal Selection Principle. In the Special Issue on Artificial Immune Systems of the journal IEEE Transactions on Evolutionary Computation, Vol. 6, No. 3, June 2002.

[20] Петренко С.А. Кибериммунология. Санкт-Петербург: Афина, 2021. 239 с.

[21] Tarakanov A.O. Information security with formal immune networks. Lecture Notes in Computer Science, 2001, 2052, pp. 115-126.

[22] Анализ возможностей адаптации общей схемы иммунной системы в системах противодействия вторжениям / С.Ж. Симаворян, А.Р. Симонян, Г.А. Попов, Е.И. Улитина // Вопросы безопасности. 2020. № 4. С. 36-46. DOI: 10.25136/2409-7543.2020.4.33736.

[23] Шелухин О.И. Разработка искусственной иммунной системы на основе отрицательного отбора с применением нейросетевых детекторов для обнаружения компьютерных атак / О.И. Шелухин, Д.А. Пугачев // REDS: Телекоммуникационные устройства и системы. 2020. Т. 10, № 1. С. 3-8.

[24] Браницкий А.А. Обнаружение сетевых атак на основе комплексирования нейронных, иммунных и нейронечетких классификаторов / А.А. Браницкий, И.В. Котенко // Информационно-управляющие системы. 2015. № 4(77). С. 69-77.

[25] Макаренко С.И. Справочник научных терминов и обозначений. Санкт-Петербург: Изд-во «Наукоемкие технологии», 2019. 254 с.

[26] Половко А.М. Основы теории надёжности. М.: Наука, 1964. 446 с.