Угрозы устойчивости функционирования облачных платформ

А. А. Балябин

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

treven.wt@yandex.ru

Аннотация. **В работе определены актуальные угрозы устойчивости функционирования облачных платформ в соответствии с международной базой знаний о компьютерных атаках MITRE ATT&CK. Определены показатель, метрика и мера устойчивости, проведена оценка влияния информационно-технических воздействий на устойчивость функционирования облачных платформ на примере облачной платформы Российской Федерации «ГосТех».**

Ключевые слова: облачные вычисления; устойчивость; угрозы устойчивости; информационно-технические воздействия; кибератаки.

I. Введение

Современные информационно-вычислительные системы развиваются в направлении внедрения распределенных облачных, туманных, пограничных вычислений и интернета вещей (IoT) [1, 2]. Такое развитие обусловлено ростом требований к вычислительным ресурсам, производительности, а также большими объемами обрабатываемых данных. Вместе с этим растет и сложность программного обеспечения. Так программное обеспечение, функционирующее в облачных средах, зачастую имеет распределенный и многоуровневый характер, сложную 2-, 3- или многозвенную архитектуру [2–4].

Общемировой тенденцией является рост количества кибератак, а также усложнение ландшафта киберугроз в целом. Современные кибератаки все чаще носят организованный и целенаправленный характер (Advanced Persistent Threats, APT), отличаются высокой интенсивностью и большим количеством задействованных ресурсов [5, 6]. Наибольшую опасность среди них представляют атаки, связанные с эксплуатацией уязвимостей «нулевого дня» (0-day), поскольку они не могут быть своевременно обнаружены и предотвращены применяемыми сегодня традиционными средствами защиты [7, 8]. В качестве среды распространения киберугроз все чаще используются облачные платформы. С середины 2021 года количество фишинговых атак в облачной среде увеличилось в 10 раз [9].

В случае Российской Федерации отдельное внимание следует уделить объектам информатизации, на базе которых создаются облачные платформы [10]. Аппаратно-программное обеспечение облачных платформ характеризуется высокой структурно-функциональной сложностью, что затрудняет обеспечение их информационной безопасности. Кроме того, серьезную угрозу представляет использование заимствованных технологий, потенциально содержащих уязвимости и недекларированные возможности [11].

Очевидно, что в современных условиях к информационным инфраструктурам предъявляются повышенные требования в части информационной безопасности и устойчивости, а непрерывный рост количества и сложности кибератак создает угрозу устойчивости их функционирования. Это характеризует проблемную ситуацию, разрешение которой является актуальной научной задачей.

Целью настоящей работы является определение актуальных угроз устойчивости функционирования облачных платформ на примере облачной платформы Российской Федерации «ГосТех».

II. Краткая характеристика объекта исследования

Объектом исследования в настоящей работе является облачная платформа «ГосТех» [10]. Принципы построения таких платформ и применяемые технологии универсальны, поэтому угрозы, характерные для данной платформы, могут быть присущи и другим облачным платформам. Укрупненная архитектура типовой облачной платформы представлена на рис. 1.

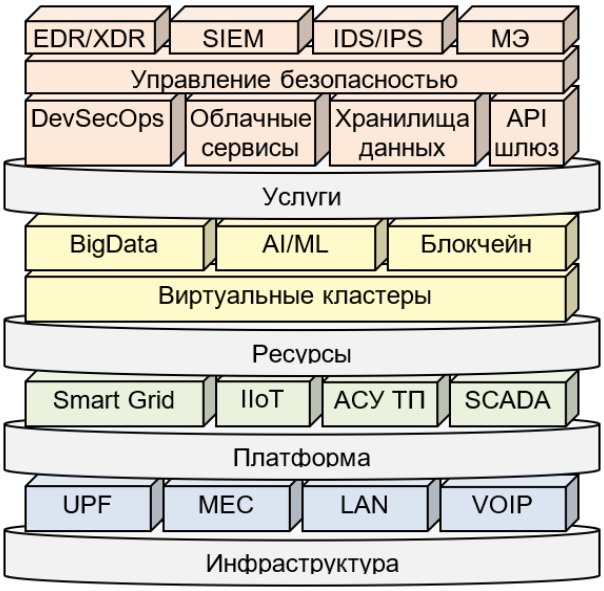

Рис. 1. Укрупненная архитектура типовой облачной платформы

Типовая облачная платформа имеет ряд ключевых особенностей, характеризующих ее как:

- информационно-вычислительную систему;
- многоуровневую иерархическую систему;
- динамическую систему с обратной связью;
- систему с повышенными требованиями к устойчивости;
- систему в условиях кибератак.

Указанные особенности необходимо учитывать при построении моделей и методов обеспечения устойчивого функционирования облачных платформ.

III. Анализ источников и постановка задачи исследования

A. *Анализ источников*

Существует ряд научных работ отечественных и зарубежных ученых, посвященных угрозам, характерным для облачных информационно-вычислительных систем. Например, в работах [6, 12] рассматриваются угрозы информационной безопасности и атаки, характерные для облачной модели вычислений в целом. В работе [13] приводится классификация информационно-технических воздействий (ИТВ) на автоматизированные системы специального назначения. В работах [14, 15] рассматриваются подходы к оценке устойчивости критических информационных инфраструктур в целом, однако, не учитываются особенности облачных вычислений. Отдельные вопросы устойчивости функционирования автоматизированных систем в условиях ИТВ рассматриваются в работе [16]. В работе [17] устойчивость информационной системы в условиях информационного конфликта предлагается обеспечивать за счет синтеза упреждающего поведения систем кибербезопасности.

Таким образом, актуальные угрозы устойчивости функционирования облачных платформ с учетом формализованного описания причин возникновения уязвимостей и недекларированных возможностей (НДВ) ранее не рассматривались, а количественная оценка устойчивости функционирования облачных платформ в условиях ИТВ – не проводилась.

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

Тогда L, язык входных данных МТ (1), определим как множество слов w, принимаемых ею:

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

Задачей исследования является формирование перечня актуальных угроз и количественная оценка устойчивости облачных платформ в условиях ИТВ.

Частные задачи исследования:

- определение перечня актуальных угроз устойчивости функционирования облачных платформ;
- определение показателя, метрики и меры устойчивости функционирования облачных платформ;
- количественная оценка устойчивости облачных платформ в условиях ИТВ.

Гипотеза исследования: целенаправленные ИТВ снижают устойчивость функционирования облачных платформ.

IV. Актуальные угрозы устойчивости функционирования облачных платформ

A. *Причины возникновения уязвимостей и недекларированных возможностей*

Одними из самых серьезных угроз являются угрозы, связанные с эксплуатацией уязвимостей «нулевого дня» и недекларированных возможностей. Уязвимости являются следствием программных ошибок, меняющих поведение программы [18].

Выступая как автомат-преобразователь, МТ (1) реализует функцию над строками $f : X \to Y$, где $X \in L_{вх}$ – множество строк языка входных данных $L_{вх}$; $Y \in L_{вых}$ – множество строк языка выходных данных $L_{вых}$. Поскольку МТ реализует заданный алгоритм и обладает свойством детерминированности, изменить результат ее выполнения возможно лишь путем изменения входных данных. Таким образом, МТ T_1 (спецификация) семантически эквивалентна МТ T_2 (реализация, не содержит ошибок семантики), тогда и только тогда, когда:

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

где f и g – функции, реализуемые МТ T_1 и T_2 соответственно. В противном случае для одних и тех же входных данных результаты выполнения МТ могут быть различными, как показано на рис. 2.

В общем случае при отсутствии семантической эквивалентности возможно 25 различных вариантов соотношения входных и выходных языков. На рис. 3 представлена сокращенная интерпретация из 5 возможных нарушений семантики с точки зрения языков входных данных МТ. Таким образом, если программа содержит семантическую ошибку, то принимаемый ею язык входных данных содержит непустое подмножество слов, результат преобразования которых отличается от ожидаемого в соответствии со спецификацией.

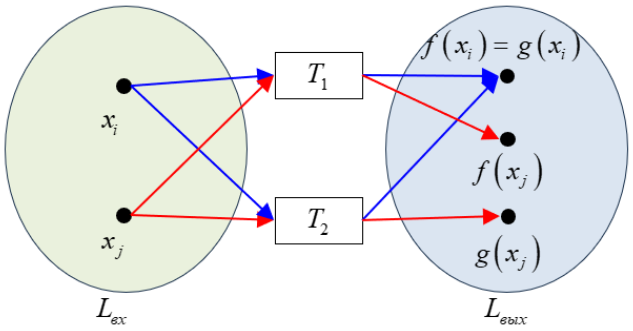

Рис. 2. Нарушение семантики вычислений при совпадении принимаемых языков

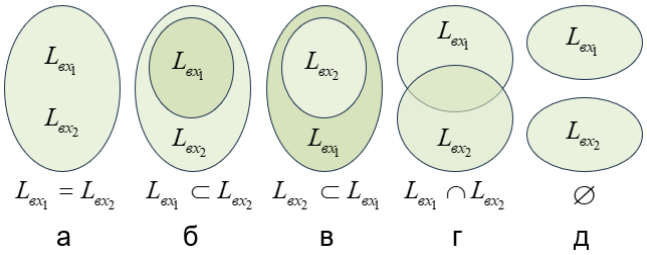

Рис. 3. Виды нарушений семантики с точки зрения языков входных данных: а – языки совпадают; б – расширение; в – сужение; г – пересечение; д – несовпадение

При $L_{вх_1} = L_{вх_2}$ нарушение семантики происходит, если для одних и тех же входных данных результаты выполнения МТ различны. При $L_{вх_1} \subset L_{вх_2}$ МТ кроме всех слов входного языка спецификации принимает некоторое непустое множество слов, не заданных спецификацией, что является потенциально опасным. При $L_{вх_2} \subset L_{вх_1}$, наоборот, МТ не принимает некоторое непустое подмножество слов входного языка спецификации, что также может приводить к программным ошибкам. При $L_{вх_1} \cap L_{вх_2}$ языки входных данных спецификации и реализации пересекаются, то есть МТ принимает некоторые слова, принадлежащие входному языку спецификации, и некоторые слова, не принадлежащие ему. Наконец, при $L_{вх_1} \cap L_{вх_2} = \varnothing$ считаем, что МТ, соответствующие спецификации и реализации, полностью не совпадают и вычисляют различные функции.

B. Угрозы устойчивости функционирования облачных платформ

Запущенная с некоторыми входными данными МТ порождает вычислительный процесс (ВП), характеризующийся последовательной сменой состояний памяти под воздействием инструкций и входных данных:

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

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

Зная все возможные семантические состояния вычислительного процесса, возможно построить эталонную абстрактную семантическую модель программы:

$$M = \langle S, A \rangle. \qquad (3)$$

Тогда с учетом определения нарушений семантики вычислений с точки зрения языков входных данных под информационно-техническим воздействием, направленным на нарушение устойчивости облачной платформы будем понимать реализацию угрозы запуска ВП (2) на МТ с такими входными данными, которые приводят его в состояние, не удовлетворяющее его эталонной семантической модели (3).

Возможны два типа нарушений семантики ВП с точки зрения его эталонной семантической модели: нарушение состояния и нарушение перехода. Графическая интерпретация этих нарушений приведена на рис. 4.

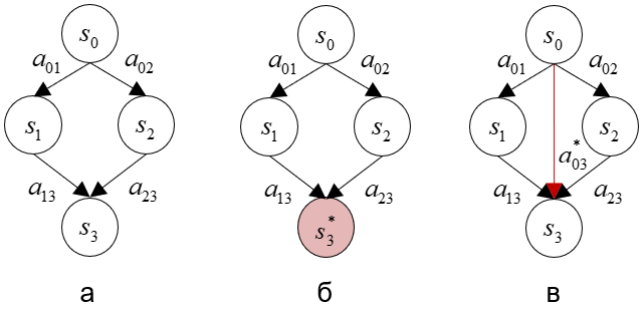

Рис. 4. Типы нарушений семантики вычислительного процесса: а – нет нарушений; б – нарушение состояния; в – нарушение перехода

Таким образом, возможно сформировать перечень угроз устойчивости облачных платформ с учетом международной базы знаний MITRE ATT&CK [19], разделив их на группы, как показано в табл. 1.

ТАБЛИЦА I. ПЕРЕЧЕНЬ АКТУАЛЬНЫХ УГРОЗ УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ ОБЛАЧНЫХ ПЛАТФОРМ

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

Угрозы, связанные с эксплуатацией уязвимостей вынесены в отдельную группу, поскольку они могут влиять как на сами семантические состояния ВП, так и на переходы между ними.

C. Пример реализации угрозы

Рассмотрим реализацию угрозы устойчивости функционирования облачных платформ на примере

атаки переполнения буфера с перехватом потока управления (T1574).

Пусть машина Тьюринга T осуществляет копирование подстроки и принимает в качестве входных данных слово, состоящее из числа n, обозначающего длину строки, копируемой подстроки A^n и подстроки B^n, в которую осуществляется копирование. Предположим, в реализации язык входных данных был расширен таким образом, что $L_{вх} = \{n\varepsilon A^n \varepsilon B^n \varepsilon; n \in [1;9]\}$ – язык входных данных спецификации, а $L^*_{вх} = \{n\varepsilon A^m \varepsilon B^n \varepsilon; m,n \in [1;9]\}$ – язык входных данных реализации. Код уязвимой машины Тьюринга приведен на рис. 5.

$$
\begin{aligned}
&q_0 i \to q_i iR, i = \overline{1..9}\\
&q_i \varepsilon \to q_{10+i} \varepsilon R, i = \overline{1..9}\\
&q_{10+i} A \to q_{10+i} AR, i = \overline{1..9}\\
&q_{10+i} \varepsilon \to q_{20+i} \varepsilon R, i = \overline{1..9}\\
&q_{20+i} B \to q_{20+i-1} BR, i = \overline{1..9}\\
&q_{20} \varepsilon \to q_{30} \varepsilon L\\
&q_{30} \{A,B,\varepsilon\} \to q_{30} \{A,B,\varepsilon\} L\\
&q_{30} i \to q_{40} iR, i = 1..9\\
&q_{40} \varepsilon \to q_{40} \varepsilon R\\
&q_{40+j} A \to q_{40+j+1} AR, j = \overline{0..8}\\
&q_{40+i} \varepsilon \to q_{50+i} \varepsilon R, i = \overline{1..9}\\
&q_{50+i} \forall \to q_{50+i-1} AR, i = \overline{1..9}\\
&q_{50} \forall \to q_F \forall N
\end{aligned}
$$

Рис. 5. Код уязвимой машины Тьюринга

Результаты выполнения МТ без нарушения и с нарушением приведены в табл. 2.

ТАБЛИЦА II. РЕЗУЛЬТАТЫ ВЫПОЛНЕНИЯ МТ

Пример	Начальное состояние ленты	Конечное состояние ленты
Без нарушения	3εAAAεBBBε###...	3εAAAεAAAε###...
С нарушением	3εAAAAAεBBBε###...	3εAAAAAεAAAAA##...

В случае с нарушением завершающий строку символ «ε» и следующая за ним пустая ячейка были перезаписаны символами «A». Если бы сразу за завершающим символом «ε» на ленте был расположен адрес возврата, то после выполнения МТ он оказался бы перезаписан данными, переданными в качестве входной строки, после чего управление было бы передано по новому адресу. Такое поведение является примером успешной реализации атаки перехвата потока управления.

V. ОЦЕНКА УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ ОБЛАЧНЫХ ПЛАТФОРМ В УСЛОВИЯХ ИТВ

A. *Показатель, метрика и мера устойчивости*

Поскольку облачные платформы являются динамическими системами, сформируем показатель устойчивости на основе аналогии с техническими системами. В качестве показателя будем оценивать вероятность P работоспособности облачной платформы в зависимости от времени t [20]:

$$P(t) = e^{-\lambda t},$$

где λ – интенсивность потока искажений.

Примем допущение, что поток искажений является простейшим. Интенсивность потока искажений постоянна и зависит от вероятности искажения, которая в свою очередь зависит от языка $L^-_{вх}$ входных данных, приводящих к нарушению, и языка $L^+_{вх}$ входных данных, не приводящих к нарушению, при этом $L_{вх} = L^-_{вх} \cup L^+_{вх}$:

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

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

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

B. *Результаты оценки устойчивости облачных платформ в условиях ИТВ*

Результаты оценки устойчивости функционирования типовой облачной платформы в условиях ИТВ по показателю вероятности работоспособности в зависимости от времени при различных значениях вероятности искажения приведены на рис. 6.

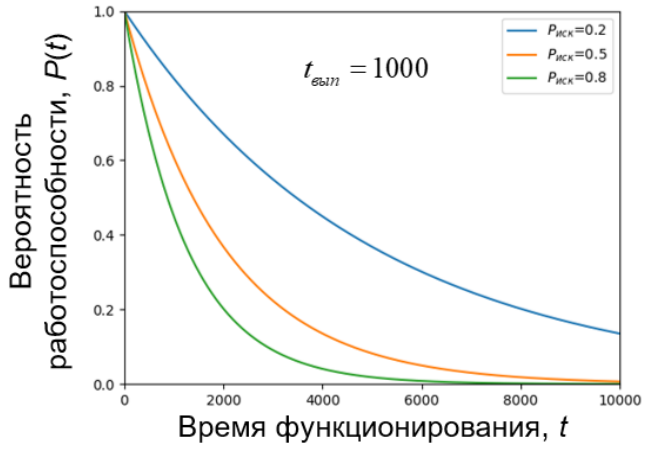

Рис. 6. Результаты оценки вероятности работоспособности типовой облачной платформы в условиях ИТВ

С учетом сделанных допущений результаты эксперимента позволяют сделать вывод, что в условиях ИТВ вероятность работоспособности облачных платформ с течением времени снижается экспоненциально. При уменьшении мощности множества слов языка $L^-_{вх}$, вероятность искажения также уменьшается, а снижение вероятности работоспособности замедляется.

Полученные результаты позволяют подтвердить выдвинутую гипотезу исследования о том, что целенаправленные ИТВ снижают устойчивость функционирования облачных платформ.

VI. ЗАКЛЮЧЕНИЕ

В исследовании была выдвинута научная гипотеза о снижении устойчивости функционирования облачных платформ в условиях целенаправленных ИТВ. В ходе исследования был решен ряд частных научных задач.

Сформирован перечень актуальных угроз устойчивости функционирования облачных платформ на примере облачной платформы Российской Федерации «ГосТех». Определены показатель, метрика и мера устойчивости, проведена количественная оценка устойчивости функционирования облачных платформ в условиях ИТВ по показателю вероятности работоспособности в зависимости от времени $P(t)$. Результаты эксперимента показали, что целенаправленные ИТВ снижают устойчивость функционирования облачных платформ, что позволило подтвердить выдвинутую гипотезу.

В дальнейшем результаты настоящей работы предполагается использовать для построения моделей, методов и методик защиты облачных платформ на основе свойств кибериммунитета с целью обеспечения требуемой их устойчивости. 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. Cyber Resilience / S. Petrenko. Denmark (Gistrup): River Publishers, 2019. 444 p.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] Атаки на российские компании во II квартале 2023 года // РТК-Солар. URL: https://rt-solar.ru/analytics/reports/3610/ (дата обращения: 05.03.2024).

[10] 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.

[11] 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.

[12] Mishra, P., Pilli, E.S., & Joshi, R.C. (2021). Cloud Security: Attacks, Techniques, Tools, and Challenges (1st ed.). Chapman and Hall/CRC. https://doi.org/10.1201/9781003004486.

[13] 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.

[14] Краснов А.Е. Оценивание устойчивости критических информационных инфраструктур к угрозам информационной безопасности / А.Е. Краснов, А.С. Мосолов, Н.А. Феоктистова // Безопасность информационных технологий. 2021. Т. 28, № 1. С. 106-120. DOI 10.26583/bit.2021.1.09.

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

[17] Бирюков Д.Н. Синтез упреждающего поведения систем кибербезопасности в информационном конфликте / Д.Н. Бирюков, А.Г. Ломако // Методы и технические средства обеспечения безопасности информации. 2014. № 23. С. 10-11.

[18] Г. Майерс. Надежность программного обеспечения. М.: Мир, 1980. 360 с.

[19] Globally accessible knowledge base of adversary tactics and techniques MITRE ATT&CK. URL: https://attack.mitre.org/ (дата обращения: 06.03.2024).

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