7. *Cheng B., Schwing A., Kirillov A.* Per-pixel classification is not all you need for semantic segmentation, *Advances in Neural Information Processing Systems,* 2021, Vol. 34, pp. 17864-17875.
8. *Yang Z., Yang Y.* Decoupling features in hierarchical propagation for video object segmentation, *Advances in Neural Information Processing Systems,* 2022, Vol. 35, pp. 36324-36336.
9. *Yang Z., Wei Y., Yang Y.* Associating objects with transformers for video object segmentation, *Advances in Neural Information Processing Systems*, 2021, Vol. 34, pp. 2491-2502.
10. *Cherti M., et al.* Reproducible scaling laws for contrastive language-image learning, *IEEE/CVF Conference on Computer Vision and Pattern Recognition,* 2023, pp. 2818-2829.
11. *Awadalla A., et al.* Openflamingo: An open-source framework for training large autoregressive vision-language models, *CoRR*, 2023, Vol. abs/2308.01390. Available at: http://arxiv.org/abs/2308.01390.
12. *Li J., Li D., Xiong C., Hoi S.* Blip: Bootstrapping language-image pre-training for unified vision-language understanding and generation, *International Conference on Machine Learning,* 2022, pp. 12888-12900.
13. *Radford A., et al.* Learning transferable visual models from natural language supervision, *International conference on machine learning,* 2021, pp. 8748-8763.
14. *Mueller M., Smith N., Ghanem B.* A benchmark and simulator for uav tracking //Computer Vision–ECCV 2016: 14th European Conference. 2016. – P. 445-461.
15. Github: fbrs_interactive_segmentation. Available at: https://github.com/SamsungLabs/fbrs_interactive_segmentation.
16. *Sofiiuk K., Petrov I., Barinova O., Konushin A*. F-BRS: Rethinking Backpropagating Refinement for Interactive Segmentation, *IEEE/CVF Conference on Computer Vision and Pattern Recognition,* 2020, pp. 8623-8632.
17. *Fomin I., Arhipov A.* Selection of Neural Network Algorithms for the Semantic Analysis of Local Industrial Area, *International Russian Automation Conference,* 2021, pp. 380-385.
18. *Miao J., et al.* VSPW: A Large-scale Dataset for Video Scene Parsing in the Wild, *IEEE/CVF Conference on Computer Vision and Pattern Recognition,* 2021, pp. 4133-4143.
19. *Zhang C., et al.* Faster Segment Anything: Towards Lightweight SAM for Mobile Applications, *CoRR*, 2023, Vol. abs/2306.14289. Available at: http://arxiv.org/abs/2306.14289.
20. *Wang A., et al*. RepViT-SAM: Towards Real-Time Segmenting Anything, *CoRR*, 2023, Vol. abs/2312.05760 Available at: http://arxiv.org/abs/2312.05760.

Статью рекомендовал к опубликованию к.т.н. Л.А. Станкевич.

**Архипов Андрей Евгеньевич** – Государственный научный центр РФ – Федеральное государственное автономное научное учреждение «Центральный научно-исследовательский и опытно-конструкторский институт робототехники и технической кибернетики»; e-mail: a.arkhipov@rtc.ru; г. Санкт-Петербург, Россия; тел.: +78125523351; м.н.с.

**Фомин Иван Сергеевич** – e-mail: i.fomin@rtc.ru; м.н.с.

**Матвеев Виктор Дмитриевич** – e-mail: v.matveev@rtc.ru; инженер.

**Arkhipov Andrey Evgenievich** – Russian State Scientific Center for Robotics and Technical Cybernetics (RTC); e-mail: a.arkhipov@rtc.ru; Saint-Petersburg, Russia; phone: +78125523351; junior researcher.

**Fomin Ivan Sergeevich** – e-mail: i.fomin@rtc.ru; junior researcher.

**Matveev Victor Dmitrievich** – e-mail: v.matveev@rtc.ru; engineer.

УДК 004.383 DOI 10.18522/2311-3103-2024-1-257-267

**Н.А. Бочаров, И.Н. Бычков, П.В. Коренев, Н.Б. Парамонов**

## ЖИВУЧЕСТЬ БОРТОВЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ НАЗЕМНЫХ РОБОТОТЕХНИЧЕСКИХ КОМПЛЕКСОВ

*Исследования в области создания специализированных вычислительных комплексов для робототехнических комплексов (РТК) ведутся во многих мировых научных центрах и в том числе в нашей стране. Развитие возможностей сенсорных систем, систем глобальной нави-*

*гации, рост вычислительной мощности и совершенствование алгоритмов позволяют создавать бортовые вычислительные комплексы, обладающие широкими интеллектуальными возможностями. Важной, но нерешенной проблемой остается оснащение таких вычислительных комплексов микропроцессорами отечественного производства. Актуальным направлением развития перспективных систем управления РТК является разработка производительных бортовых вычислительных систем (БВС), обладающих свойством живучести. Существенным, но нерешенным вопросом остается оснащение таких БВС средствами вычислительной техники отечественной разработки. Появление современных отечественных микропроцессоров Эльбрус-2С3 и Эльбрус-8СВ открывает новые возможности перед разработчиками РТК. Появление таких аппаратных технологий, как сторожевой таймер и модуль привязки времени, позволяет создавать БВС, обладающие высокой живучестью в условиях боевых действий. Для РТК специального назначения, можно разделить период нормальной эксплуатации робота на сегменты по аналогии со степенями боевой готовности вооруженных сил, для каждого из которых РТК будет работать в специальном режиме. Режимы характеризуются согласно сложившейся обстановке и соответствующим потоком отказов. В работе представлена модель угроз для самого жесткого из режимов работы. В данной работе представлен метод обеспечения живучести БВС РТК за счет использования адаптивного резервирования. Метод заключается в переключении между схемами резервирования для обеспечения высокой производительности при сохранении достаточной надежности в зависимости от текущего уровня потока отказов. С использованием разработанной авторами модели проведено экспериментальное исследование по оценке эффективности разработанного метода при работе на отечественном БВС на базе микропроцессора «Эльбрус». Использование разработанного метода позволило увеличить среднюю функциональность РТК на 23-43% по сравнению с режимом с постоянным резервированием.*

*Бортовые вычислители; бортовые вычислительные системы; робототехника; живучесть; адаптивное резервирование; Эльбрус.*

**N.A. Bocharov, I.N. Bychkov, P.V. Korenev, N.B. Paramonov**

## SURVIVABILITY OF ONBOARD COMPUTERS OF GROUND ROBOTS

*Research in the field of creating specialized computing systems for robots is conducted in many world scientific centers, including our country. The development of capabilities of sensor systems, global navigation systems, growth of computing power and improvement of algorithms allow creating onboard computing systems with broad intellectual capabilities. An important, but unsolved problem remains in the equipping of such computing systems with domestically produced microprocessors. An urgent direction in the development of prospective robot control systems is the development of high-performance on-board computers with the property of survivability. A significant but unresolved issue remains in the equipping of such computers with computer equipment of domestic development. The appearance of modern domestic microprocessors Elbrus-2S3 and Elbrus-8SV opens up new opportunities for robot developers. The emergence of hardware technologies such as a watchdog timer and a time-binding module makes it possible to create robots with high survivability in combat conditions. For special purpose robots, it is possible to divide the period of normal operation of the robot into modes by analogy with the degrees of combat readiness of the armed forces, for each of which the robot will operate in a special mode. The modes are characterized according to the prevailing situation and the corresponding failure rate. The paper presents a threat model for the harshest of the operating modes. This paper presents a method for ensuring the survivability of onboard robot computers by using adaptive redundancy to ensure the survivability of on-board computers. The method consists in switching between redundancy schemes to ensure high performance while maintaining sufficient reliability, depending on the current level of failure flow. Using the model developed by the authors, an experimental study was conducted to evaluate the effectiveness of the developed method when working with a domestic onboard computer based on the Elbrus microprocessor. Using the developed method made it possible to increase the average functionality of the robot by 23-43% compared to the mode with constant redundancy.*

*Onboard computers; robotics; survivability; adaptive redundancy; Elbrus.*

**Введение.** Управление современными автономными робототехническими комплексами (РТК) осуществляются с помощью специализированных бортовых вычислительных систем [1]. Развитие возможностей сенсорных систем, систем

глобальной навигации, рост вычислительной мощности и совершенствование алгоритмов позволяют создавать бортовые вычислительные системы, обладающие широкими интеллектуальными возможностями. В процессе перевооружения Вооруженных сил Российской Федерации все большее внимание уделяется оснащение РТК различного функционального назначения.

Такие РТК требуют наличия развитых систем управления с распределенной архитектурой, включающих уровни планирования и управления движением, управления подсистемами обработки и комплексирования сенсорной информации, исполнительными механизмами, управления энергообеспечением, управления полезной нагрузкой, средствами безопасности. В этой связи актуальным направлением развития перспективных систем управления РТК является разработка производительных бортовых вычислительных систем (БВС), обладающих свойством живучести.

Появление современных отечественных микропроцессоров Эльбрус-2С3 [2, 3] Эльбрус-8СВ [4] открывает новые возможности перед разработчиками РТК. Появление таких аппаратных технологий, как сторожевой таймер и модуль привязки времени позволяет создавать БВС [5-7], обладающих высокой живучестью в условиях боевых действий.

В данной работе представлен метод обеспечения живучести БВС РТК за счет использования адаптивного резервирования для обеспечения живучести бортовых вычислителей. Приведены результаты моделирования разработанного метода на отечественных БВС РТК на базе отечественных микропроцессоров Эльбрус.

**Особенности работы РТК.** При решении задачи обеспечения живучести в условиях рассматриваемой модели необходимо учитывать, что помимо основного (естественного) потока отказов, которые являются следствием ошибок, сбоев и т.д., есть поток отказов, вызванный целенаправленными попытками нанести повреждения роботу. Такие отказы могут быть, например, результатом выстрела в робота или тарана. Будем называть этот поток – потоком преднамеренных отказов. В дальнейшем будем обозначать $\lambda_1$ – интенсивность потока естественных отказов, а $\lambda_2$ – интенсивность потока преднамеренных отказов. Таким образом, общий поток отказов для робота и, в частности, бортового вычислительного комплекса будет определяться суммой этих двух потоков:

$$\lambda=\lambda_1+\lambda_2.$$

Интенсивность потока естественных отказов $\lambda_1$ определяется техническими условиями на изделие, в рамках данной работы для определенности примем, что средняя наработка на отказ робота составляет 1000 часов, интенсивность потока естественных отказов составляет $\lambda_1 \in [10^{(-7)}; 10^{(-5)};]$ 1/час, а $\lambda_2$ зависит от режима работы робота.

Применительно к рассматриваемой предметной области, а именно РТК специального назначения, можно разделить период нормальной эксплуатации робота на сегменты по аналогии со степенями боевой готовности вооруженных сил, для каждого из которых РТК будет работать в специальном режим. Режимы характеризуются согласно сложившейся обстановке и соответствующим потоком отказов. В рамках данной работы выделим три режима, в которых могут функционировать РТК:

- Режим подготовки. Робот движется к назначенной цели, ведет активную работу с системами технического зрения, строит подробные карты проходимости и т.д. В этом режиме поток преднамеренных отказов находится на практически нулевом уровне, т.е. $\lambda_2 \approx 0$, а поток естественных отказов находится на обычном уровне. Риск получения физического урона или несанкционированного доступа в систему управления минимален. Обеспечение живучести в таком режиме работы тривиально.
- Режим повышенной боевой готовности. Робот находится близко к зоне боевых действий и должен быть готов к переходу в режим боевых действий. В этом режиме уровень потока преднамеренных отказов растет, поэтому должны быть применены соответствующие методы, обеспечивающие своевременное переключение в режим боевых действий при возросшей угрозе возникновения предна-

меренных отказов. Риск получить физический урон минимален, риск несанкционированного доступа в систему управления возрастает, по сравнению с режимом подготовки. Будем считать, что в таком режиме $\lambda_2 \in [1*10^{(-5)};1*10^{(-1)}]$1/час

- Режим боевых действий. Роботу непосредственно угрожает противоборствующие элементы, велик риск получения серьезного физического урона или несанкционированного доступа в систему управления. В данном режиме показатель потока преднамеренных отказов $\lambda_2$ возрастает до своего максимального значения и становится много больше потока естественных отказов $\lambda_2 \gg \lambda_1$). Будем считать, что в таком режиме $\lambda_2 \in [1*10^{(-1)};5*10^{(-1)}]$ 1/час

**Модель угроз БВС РТК.** К характеристикам БВС РТК, обусловливающим возникновение угроз безопасности можно отнести категорию и объем обрабатываемых в системе данных, структуру системы, наличие подключений системы к сетям связи, местонахождение и условия размещения технических средств системы.

Свойства среды (пути) распространения информативных сигналов, содержащих защищаемую информацию, характеризуются видом физической среды, в которой распространяются данные, и определяются при оценке возможности реализации угроз безопасности данным.

Возникновение угрозы безопасности вычислительной системы является следствием наличия определенных уязвимостей в системе [8]. Уязвимости могут возникать еще на этапе проектирования, например, из-за принятых ограничений функционирования, особенностей архитектуры, выбранных протоколов передачи данных и интерфейсов, используемого в системе программного обеспечения, условий эксплуатации и пр. Поскольку угрозы безопасности и причины их возникновения (уязвимости) неразрывны, каждой угрозе можно сопоставить множество уязвимостей.

Модель угроз расширяется в зависимости от режима работы робота и достигает полноты для самого жесткого режима – режима боевых действий. При работе этом режиме модель угроз расширяется рядом преднамеренных внешних угроз, заключающихся в основном в том, что становится вероятным физическое воздействие на робота и его компоненты:

- Преднамеренные угрозы
  - Внешние угрозы
    - Электромагнитное воздействие по сетям питания, проводным линиям связи, эфиру [9–11];
    - Информационные разрушающие воздействия, проникающие через каналы данных[12–15];
    - Физическое воздействие на компоненты РТК;
    - Порча СВТ и вспомогательного оборудования.
- Непреднамеренные угрозы
  - Внутренние угрозы
    - Ошибки в данных (входных, управляющих, выходных);
    - Отказ ПО [16];
    - Отказ средств обработки данных;
    - Отказ вспомогательного оборудования;
    - Отказ сетей связи [17].
  - Внешние угрозы
    - Аварийные ситуации;
    - Ошибочные действия оператора;
    - Воздействия окружающей среды.

Последствиями перечисленных угроз для вычислительного комплекса РТК могут быть:

- Потеря связи между вычислительными машинами;
- Выход из строя одной или нескольких вычислительных машин;
- Сбой в работе одной или нескольких вычислительных машин;

- Потеря связи в РТК;
- Выход из строя внешних датчиков или потеря связи с ними.

**Резервирование для обеспечения живучести.** Одним из основных методов обеспечения дополнительной надежности объекта является резервирование. Метод реализуется благодаря использованию дополнительных средств и возможностей, которые являются избыточными к минимально необходимым для выполнения требуемых функций. Наиболее частой реализацией метода резервирования является включение параллельно объекту резервирования дополнительных средств, которые полностью или частично дублируют его функции, и способны взять на себя его задачи при возникновении отказа.

В БВС РТК могут применяться следующие основные виды резервирования:

- аппаратное (схемное, структурное);
- временное;
- информационное;
- функциональное;
- нагрузочное.

При реализации аппаратного резервирования предполагается применение резервных элементов вычислительного комплекса, в виде отдельных блоков или целой дублирующей вычислительной машины, которые включаются в процесс управления робототехническим комплексом автоматически или вручную, при возникновении отказа в основной управляющей вычислительной машине, и способны поддерживать функционирование робототехнического комплекса. При этом операция замены отказавшего элемента на резервный не прерывает функционирования совсем или прерывает его на незначительный период времени, необходимый для определения отказа и переключения на резервные элементы.

Реализация временного резервирования предполагает использование резерва времени при работе устройства. Для робототехнического комплекса это связано с добавлением избытка времени выполнения вычислений в бортовом вычислительном комплексе.

При использовании информационного резервирования повышение надежности процесса управления робототехническим комплексом происходит за счет применения избытка бортовых аппаратных, вычислительных и программных средств для решения взаимосвязанных задач.

Функциональное резервирование может повысить надежность системы в случае, если элементы системы могут решать дополнительные задачи, помимо выполнения основной функции при нормальной эксплуатации. Например, использование высокоэнергетической линии связи для отправки управляющих команд в случае отказа в энергоскрытной системе связи, или использование системы стереозрения для определения расстояния до препятствий при отказе в системе дальномеров.

Повышение надежности системы с использованием нагрузочного резервирования происходит благодаря способности системы воспринимать дополнительные нагрузки. Источником резерва в данном случае является запас вычислительной мощности или электрической прочности в радиотехнических элементах или устройствах.

Одновременное применение двух и более видов резервирования является предпочтительным, так как обеспечивает больший эффект в повышении надежности. Но основной вклад сохраняет за собой аппаратное резервирование, и оно должно реализовываться в первую очередь.

При реализованном резервировании отказ системы управления робототехнического комплекса в целом наступает только после отказа в основной вычислительной машине и во всех резервных. Основной вычислительной машиной при этом считается та машина, которая необходима для выполнения требуемых функций без использования резерва.

**Адаптивное резервирование.** Использование адаптивного резервирования для вычислительных машин предполагает смену схемы резервирования в зависимости от режима функционирования робота. Режим функционирования робота определяется интенсивностью потока преднамеренных отказов и характеризуется решаемыми задачами и временем реакции на отказ. Таким образом выбор схемы резервирования можно описать функцией r, зависящей от режима функционирования робота m.

$$r(m) = \{\dots\}.$$

Работа в режиме подготовки предполагает низкий уровень потока отказов, сравнимый с естественным уровнем, то есть отказ вычислительных машин маловероятен. Также, работа в режиме подготовки характеризуется активной работой сенсоров робота, связанной с накоплением информации. Активно функционирует система стереозрения, проводится сканирование пространства с лидара и дальномеров. Такой высокий поток данных приводит к необходимости использования всех имеющихся вычислительных ресурсов. Поскольку риск отказа вычислительных машин минимален, можно использовать все резервные вычислительные машины в качестве дополнительных устройств для вычислений, а задаче резервирования основной вычислительной машины поставить минимальный приоритет. Резервирование данных проводится регулярно, но с меньшей частотой по сравнению с другими режимами, для сохранения полученных результатов. В случае отказа основной вычислительной машины переключение на резервный произойдет не моментально, но оно в любом случае произойдет с восстановлением данных с контрольной точки. Таким образом можно использовать схему с теплым резервом без ограничений по времени.

Работа в режиме повышенной боевой готовности характеризуется повышением уровня потока преднамеренных отказов, вследствие чего повышается вероятность выхода из строя вычислительных машин. Также, критически важным моментом работы в данном режиме является скорость реакции на возникновение риска угроз и переключения в режим боевых действий. Этой задаче отдается большое количество вычислительных ресурсов, распределяемых между основной и резервными вычислительными машинами. Репликации данных дается более высокий приоритет, она проводится с большей частотой. Переключение на резервную вычислительную машину в случае отказа основной будет являться наиболее приоритетной задачей и должно осуществляться в режиме реального времени. Время реакции устанавливается ТУ на устройство. Из вышеперечисленного видим, что для данного режима необходимо использовать схему с теплым резервом с ограничениями по времени.

Работа в режиме боевых действий характеризуется чрезвычайно высоким уровнем потока отказов. Критически важной задачей становится сохранение работоспособности робота при возникновении преднамеренного отказа в любых его компонентах. Репликация данных проводится максимально часто. Переключение на резервную вычислительную машину при возникновении отказа в основной должно происходить максимально быстро. Поскольку активного накопления данных в данном режиме не происходит, свободные вычислительные ресурсы пускаются на сохранение данных и максимально быстрое переключение при отказе основного элемента. Согласно проведенным исследованиям, достаточным для РТК специального назначения является время обнаружения отказа не более 0.1 секунды. Ввиду вышесказанного для данного режима подходит схема с горячим резервом с ограничениями по времени.

Систематизируя вышесказанное, опишем выбор схемы резервирования следующими уравнениями:

r(m1) → ($\lambda = \lambda_{min}$; $V = V_{max}$) = теплый резерв, $t_п >> 0$;

r(m2) → ($\lambda_{min} < \lambda < \lambda_{max}$; $V < V_{max}$) = горячий резерв, $t_п < 1$с;

r(m3) → ($\lambda = \lambda_{max}$; $V = V_{max}/n$) = горячий резерв, $t_п < 0.1$с;

где m1 – режим подготовки, m2 – режим повышенной боевой готовности, m3 – режим боевых действий, $t_п$ – время на переключение с основной вычислительной машины на резервную, V – объем используемых вычислительных ресурсов на работу с датчиками, $V_{max}$ – максимальный доступный объем вычислительных ресурсов на всех вычислительных машинах, n – количество вычислительных машин.

Блок схема общего алгоритма переключения между режимами представлена на рис. 1.

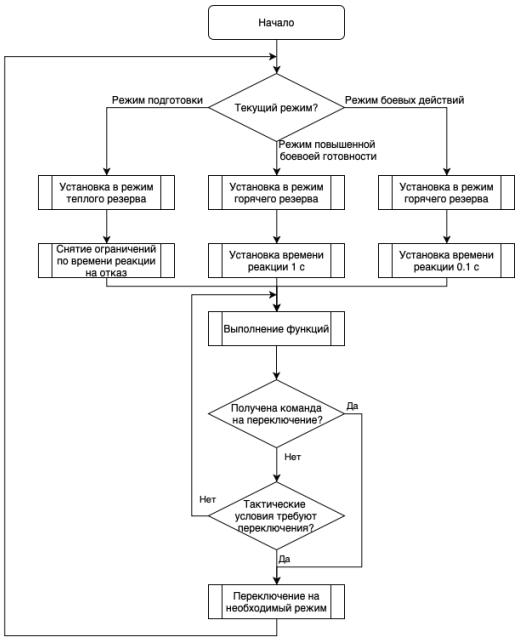


*Рис. 1. Общий алгоритм переключения между режимами*

Поскольку параметр потока интенсивности преднамеренных отказов не поддается контролю, то параметры вычислительных ресурсов и времени реакции на отказ являются ключевыми для реализации метода адаптивного резервирования. Программно-аппаратное обеспечение РТК должно иметь возможности по установке указанных выше параметров. Переключение между схемами резервирования происходит либо по сигналу оператора, либо в результате изменения значения оценочной функции, которая определяет на основе тактических данных наиболее подходящий режим работы

**Моделирование работы адаптивного резервирования.** Для оценки разработанного метода разработаны программы на языке Java с использованием средств ОПО и СПО «Эльбрус», объединенные в программную модель, в которой есть возможности для проведения экспериментов по оценке функциональности РТК по критерию функциональности [8, 9]. В качестве протокола обмена сообщениями «я живой» между вычислительными машинами программой использовались средства Socket API и аппаратное устройство МПВ. С использованием данной программы могут быть решены следующие задачи:

♦ моделирование многомашинного вычислительного комплекса, работающего по схеме Ведущий-Ведомый;

- работа с устройством МПВ;
- оценка времени реакции на одиночные отказы.

Программа для реализации метода реконфигурации вычислительных комплексов РТК использует сторожевой таймер ОС «Эльбрус», который производит попытку перезапуска отказавшей вычислительной машины. При невозможности перезапуска задачи отказавшей вычислительной машины распределяются по другим вычислительным машинам в комплексе.

Для моделирования уровней загрузки вычислительных машин в вычислительных комплексах РТК использовались разработанные модели системы стереозрения, поиска пути роботом и поиска пути группой роботов [10].

На рис. 2 представлен скриншот окна программы с результатами эксперимента.

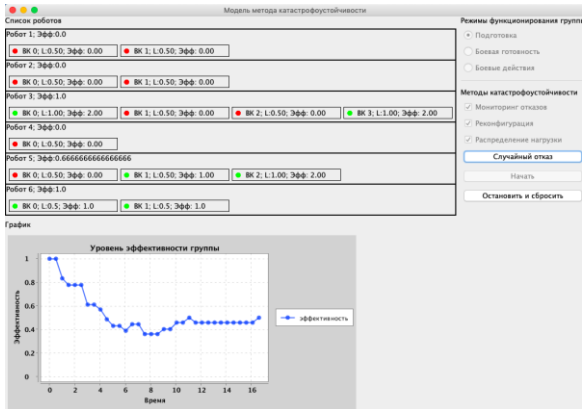


*Рис. 2. Окно программы*

С использованием разработанной модели проведено экспериментальное исследование по оценке функциональности РТК в зависимости от использования разработанного метода адаптивного резервирования БВС РТК. Исследованием показало повышение средней функциональности на 23-43% по сравнению с режимом работы с постоянным резервированием.

**Заключение.** В статье представлен метод адаптивного резервирования БВС РТК для повышения живучести. Метод заключается в переключении между схемами резервирования для обеспечения высокой производительности при сохранении достаточной надежности в зависимости от текущего уровня потока отказов.

С использованием разработанной авторами модели проведено экспериментальное исследование по оценке эффективности разработанного метода при работе на отечественной БВС на базе микропроцессора «Эльбрус». Использование разработанного метода позволило увеличить среднюю функциональность РТК на 23-43% по сравнению с режимом с постоянным резервированием.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Романов А.М.* Обзор аппаратно-программного обеспечения систем управления роботов различного масштаба и назначения. Ч. 3. Экстремальная робототехника // Российский технологический журнал. – 2020. – Т. 8, № 3 (35). – С. 14-32. – DOI: 10.32362/2500-316X-2020-8-3-14-32.
2. *Чучко П.А., Бычков И.Н., Панченко Е.Г.* Проблема унификации модулей на основе процессора "Эльбрус-2С3" // Наноиндустрия. – 2021. – Т. 14, № S7(107). – С. 96-97. – DOI: 10.22184/1993-8578.2021.14.7s.96.97.
3. *Nedbailo Y.A., Bychkov I.N., Slesarev M.V. [et al.].* Elbrus-2C3: A Dual-Core VLIW Processor with Integrated Graphics // 2021 International Conference Engineering and Telecommunication, En and T 2021, Dolgoprudny, 24–25 ноября 2021 года. – Dolgoprudny: Institute of Electrical and Electronics Engineers Inc., 2022. – DOI: 10.1109/EnT50460.2021.9681771.

4. *Дружинина О.В., Корепанов Э.Р., Белоусов В.В. [и др.].* Развитие инструментального обеспечения отечественной вычислительной платформы "Эльбрус 801-РС" в задачах нейросетевого моделирования нелинейных динамических систем // Нелинейный мир. – 2021. – Т. 19, № 1. – С. 15-28. – DOI: 10.18127/j20700970-202101-02.
5. *Бычков И.Н., Лобанов И.Н., Молчанов И.А.* Решения по включению средств защиты информации в вычислительные комплексы на основе платформы "Эльбрус" // Наноиндустрия. – 2020. – Т. 13, № S4 (99). – С. 103-104. – DOI: 10.22184/1993-8578.2020.13.4s.103.104.
6. *Фельдман В.М., Зуев А.Г., Дорофеев А.И. [и др.].* Особенности конструирования переносных вычислительных устройств в защищенном исполнении // Приборы. – 2023. – № 5 (275). – С. 24-33.
7. *Тачков А.А., Козов А.В., Вуколов А.Ю.* Особенности портирования Robot Operating System на программно-аппаратную платформу "Эльбрус" // Программные продукты и системы. – 2019. – № 4. – С. 655-664. – EDN TVJSXJ.
8. *Абрамов Н.С., Фраленко В.П.* Угрозы безопасности вычислительных комплексов: классификация, источники возникновения и методы противодействия // Программные системы: теория и приложения. – 2015. – № 2 (25). – С. 63-83.
9. *Sands T.* Countering the Deleterious Effects of Electromagnetic Pulse // Frontiers in Electronics. – 2021. – Vol. 2. – P. 727994.
10. *Kim S., Jeong I.* Vulnerability assessment of Korean electric power systems to late-time (E3) high-altitude electromagnetic pulses // Energies. – 2019. – Vol. 12, No. 17. – P. 3335.
11. *Dayanikli G.Y.* Electromagnetic Interference Attacks on Cyber-Physical Systems: Theory, Demonstration, and Defense: дисс. – Virginia Tech, 2021.
12. *Mayoral-Vilches V.* Robot cybersecurity, a review // International Journal of Cyber Forensics and Advanced Threat Investigations. – 2022.
13. *Yaacoub J.P. A. et al.* Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations // International Journal of Information Security. – 2022. – P. 1-44.
14. *Zhu Q. et al.* Cybersecurity in robotics: Challenges, quantitative modeling, and practice // Foundations and Trends® in Robotics. – 2021. – Vol. 9, No. 1. – P. 1-129.
15. *Theron P. et al.* Reference architecture of an autonomous agent for cyber defense of complex military systems // Adaptive autonomous secure cyber systems. – 2020. – P. 1-21.
16. *Afzal A. et al.* A study on challenges of testing robotic systems // 2020 IEEE 13th International Conference on Software Testing, Validation and Verification (ICST). – IEEE, 2020. – P. 96-107.
17. *Huang H. et al.* Disturbance observer-based fault-tolerant control for robotic systems with guaranteed prescribed performance // IEEE transactions on cybernetics. – 2020. – Vol. 52, No. 2. – P. 772-783.
18. *Бочаров Н.А.* Моделирование алгоритмов катастрофоустойчивости групп роботов на программно-аппаратной платформе "Эльбрус" // Радиопромышленность. – 2019. – № 3. – С. 8-14. – DOI: 10.21778/2413-9599-2019-29-3-8-14.
19. *Бочаров Н.А.* Модель обеспечения катастрофоустойчивости бортовых вычислительных комплексов на базе аппаратно-программной платформы «Эльбрус». Свидетельство о государственной регистрации программы для ЭВМ №2019616256 от 30.04.2019.
20. *Бочаров Н.А., Парамонов Н.Б., Сапачев И.Д.* Реализация алгоритмов группового управления на языке Java в среде ОС «Эльбрус» // Современные информационные технологии и ИТ-образование. – 2016. – № 1. – С. 108-115.

REFERENCES

1. *Romanov A.M.* Obzor apparatno-programmnogo obespecheniya sistem upravleniya robotov razlichnogo masshtaba i naznacheniya. Ch. 3. Ekstremal'naya robototekhnika [A review on control systems hardware and software for robots of various scale and purpose. Part 3. Extreme robotics], *Rossiyskiy tekhnologicheskiy zhurnal* [Russian Technological Journal], 2020, Vol. 8, No. 3 (35), pp. 14-32. DOI: 10.32362/2500-316X-2020-8-3-14-32.
2. *Chuchko P.A., Bychkov I.N., Panchenko E.G.* Problema unifikatsii moduley na osnove protsessora "El'brus-2S3" [The problem of unification of modules based on the processor "Elbrus-2C3"], *Nanoindustriya* [Nanoindustry], 2021, Vol. 14, No. S7(107), pp. 96-97. DOI: 10.22184/1993-8578.2021.14.7s.96.97.
3. *Nedbailo Y.A., Bychkov I.N., Slesarev M.V. [et al.].* Elbrus-2C3: A Dual-Core VLIW Processor with Integrated Graphics, *2021 International Conference Engineering and Telecommunication, En and T 2021, Dolgoprudny, 24–25 ноября 2021 года*. Dolgoprudny: Institute of Electrical and Electronics Engineers Inc., 2022. DOI: 10.1109/EnT50460.2021.9681771.

4. *Druzhinina O.V., Korepanov E.R., Belousov V.V. [i dr.]*. Razvitie instrumental'nogo obespecheniya otechestvennoy vychislitel'noy platformy "El'brus 801-PC" v zadachakh neyrosetevogo modelirovaniya nelineynykh dinamicheskikh sistem [Development of instrumental support for the domestic computing platform "Elbrus 801-PC" in problems of neural network modeling of nonlinear dynamic systems], *Nelineynyy mir* [Nonlinear World], 2021, Vol. 19, No. 1, pp. 15-28. DOI: 10.18127/j20700970-202101-02.
5. *Bychkov I.N., Lobanov I.N., Molchanov I.A.* Resheniya po vklyucheniyu sredstv zashchity informatsii v vychislitel'nye kompleksy na osnove platformy "El'brus" [Solutions for the inclusion of information security tools in computing systems based on the Elbrus platform], *Nanoindustriya* [Nanoindustry], 2020, Vol. 13, No. S4 (99), pp. 103-104. DOI: 10.22184/1993-8578.2020.13.4s.103.104.
6. *Fel'dman V.M., Zuev A.G., Dorofeev A.I. [i dr.]*. Osobennosti konstruirovaniya perenosnykh vychislitel'nykh ustroystv v zashchishchennom ispolnenii [Features of the design of portable computing devices in a protected design], *Pribory* [Devices], 2023, No. 5 (275), pp. 24-33.
7. *Tachkov A.A., Kozov A.V., Vukolov A.Yu*. Osobennosti portirovaniya Robot Operating System na programmno-apparatnuyu platformu "El'brus" [Features of porting the Robot Operating System to the Elbrus software and hardware platform], *Programmnye produkty i sistemy* [Software products and systems], 2019, No. 4, pp. 655-664. EDN TVJSXJ.
8. *Abramov N.S., Fralenko V.P.* Ugrozy bezopasnosti vychislitel'nykh kompleksov: klassifikatsiya, istochniki vozniknoveniya i metody protivodeystviya [Threats to the security of computing systems: classification, sources of occurrence and countermeasures], *Programmnye sistemy: teoriya i prilozheniya* [Software systems: theory and applications], 2015, No. 2 (25), pp. 63-83.
9. *Sands T.* Countering the Deleterious Effects of Electromagnetic Pulse, *Frontiers in Electronics,* 2021, Vol. 2, pp. 727994.
10. *Kim S., Jeong I.* Vulnerability assessment of Korean electric power systems to late-time (E3) high-altitude electromagnetic pulses, *Energies,* 2019, Vol. 12, No. 17, pp. 3335.
11. *Dayanikli G.Y.* Electromagnetic Interference Attacks on Cyber-Physical Systems: Theory, Demonstration, and Defense: дисс. Virginia Tech, 2021.
12. *Mayoral-Vilches V.* Robot cybersecurity, a review, *International Journal of Cyber Forensics and Advanced Threat Investigations,* 2022.
13. *Yaacoub J.P. A. et al.* Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations, *International Journal of Information Security,* 2022, pp. 1-44.
14. *Zhu Q. et al.* Cybersecurity in robotics: Challenges, quantitative modeling, and practice, *Foundations and Trends® in Robotics,* 2021, Vol. 9, No. 1, pp. 1-129.
15. *Theron P. et al.* Reference architecture of an autonomous agent for cyber defense of complex military systems, *Adaptive autonomous secure cyber systems,* 2020, pp. 1-21.
16. *Afzal A. et al.* A study on challenges of testing robotic systems, *2020 IEEE 13th International Conference on Software Testing, Validation and Verification (ICST)*. IEEE, 2020, pp. 96-107.
17. *Huang H. et al.* Disturbance observer-based fault-tolerant control for robotic systems with guaranteed prescribed performance, *IEEE transactions on cybernetics,* 2020, Vol. 52, No. 2, pp. 772-783.
18. *Bocharov N.A.* Modelirovanie algoritmov katastrofoustoychivosti grupp robotov na programmno-apparatnoy platforme "El'brus" [Modeling algorithms for disaster resistance of groups of robots on the Elbrus software and hardware platform], *Radiopromyshlennost'* [Radio industry], 2019, No. 3, pp. 8-14. DOI: 10.21778/2413-9599-2019-29-3-8-14.
19. *Bocharov N.A.* Model' obespecheniya katastrofoustoychivosti bortovykh vychislitel'nykh kompleksov na baze apparatno-programmnoy platformy «El'brus». Svidetel'stvo o gosudarstvennoy registratsii programmy dlya EVM №2019616256 ot 30.04.2019 [A model for ensuring disaster resistance of on-board computing systems based on the Elbrus hardware and software platform. Certificate of state registration of a computer program No. 2019616256 dated 04/30/2019].
20. *Bocharov N.A., Paramonov N.B., Sapachev I.D.* Realizatsiya algoritmov gruppovogo upravleniya na yazyke Java v srede OS «El'brus» [Implementation of group control algorithms in Java in the Elbrus OS environment], *Sovremennye informatsionnye tekhnologii i IT-obrazovanie* [Modern information technologies and IT education], 2016, No. 1, pp. 108-115.

Статью рекомендовал к опубликованию д.т.н., профессор В.М. Фельдман.

**Бочаров Никита Алексеевич** – ПАО «ИНЭУМ им. И.С. Брука»; e-mail: bocharov.na@phystech.edu; г. Москва, Россия, тел.: +79167346437; к.т.н.; зам. руководителя управления; г.н.с.

**Бычков Игнат Николаевич** – e-mail: ignat_b@ineum.ru, тел.: +74991353321; д.т.н.; зам. генерального директора.

**Коренев Павел Валерьевич** – e-mail: ineum@ineum.ru; тел.: +74991353321; соискатель.

**Парамонов Николай Борисович** – e-mail: paramonov_n_b@mail.ru; тел.: +74991355336; д.т.н.; профессор; руководитель управления; г.н.с.

**Bocharov Nikita Alexeevich** – JSC «INEUM»; e-mail: bocharov.na@phystech.edu; Moscow, Russia; phone: +79167346437;cand. of eng. sc.; deputy head of department; chief scientific officer.

**Bychkov Ignat Nikolaevich** – e-mail: ignat_b@ineum.ru; phone: +74991353321; dr. of eng. sc.; deputy general director.

**Korenev Pavel Valerievich** – e-mail: ineum@ineum.ru; phone: +74991353321; candidate.

**Paramonov Nikolay Borisovich** – e-mail: paramonov_n_b@mail.ru; phone: +74991355336; dr. of eng. sc.; head of department; chief scientific officer.

УДК 004.89 DOI 10.18522/2311-3103-2024-1-267-276

**В.В. Ковалев, Н.Е. Сергеев**

# РАСШИРЕНИЕ ПРИЗНАКОВОГО ПРОСТРАНСТВА В ЗАДАЧЕ ПОИСКА И РАСПОЗНАВАНИЯ МАЛОРАЗМЕРНЫХ ОБЪЕКТОВ НА ИЗОБРАЖЕНИЯХ

*Одним из актуальных направлений при создании систем раннего обнаружения объектов является разработка алгоритмов поиска и распознавания малоразмерных объектов на изображениях. В задаче раннего обнаружения приходится распознавать объекты на дальних расстояниях от места их фиксации камерой. Образ на изображении таких объектов представлен малой компактной группой пикселей, которая претерпевает пространственные и яркостные изменения от кадра к кадру. Для успешного решения этой задачи целевые объекты реального мира должны иметь большие физические размеры. Кроме физических размеров объекта на образ объекта на изображении влияют большое количество факторов: разрешение матрицы камеры, фокусное расстояние объектива, светочувствительность матрицы и др. Вектор решения такой задачи направлен в сторону сверточных нейронных сетей. Однако, даже у передовых архитектур сверточных нейронных сетей поиск и распознавание малоразмерных объектов на изображениях вызывает трудности. Эта проблема напрямую связана с эффектом переобучения модели нейронной сети. Переобучение модели нейронной сети можно оценить на основе анализа кривых обучения. Для снижения вероятности переобучения применяют специальные методы, которые объединяет термин регуляризация. Однако, в распознавании малоразмерных объектов существующих методов регуляризации бывает недостаточно. В работе произведено исследование разработанного алгоритма предварительной обработки последовательности видеокадров, увеличивающего исходное пространство признаков новым независимым признаком движения в кадре. Алгоритм предварительной обработки основан на пространственно-временной фильтрации последовательности видеокадров, применение которого распространяется на широкий спектр архитектур сверточных нейронных сетей. Для исследования характеристик точности и распознавания сверточных нейронных сетей сформированы датасеты изображений в градациях серого и изображений с признаком движения на основе среды разработки 3D графики Unreal Engine 5. В работе приведен критерий малоразмерности объектов на изображениях. Произведено обучение и оценка характеристик точности тестовой модели сверточной нейронной сети и анализ динамики кривых обучения тестовой модели. Показано положительное влияние предложенного алгоритма предварительной обработки последовательности видеокадров на интегральную точность обнаружения малоразмерных объектов.*

*Обнаружение малоразмерных объектов; сверточные нейронные сети; подвижные объекты; переобучение нейронных сетей.*