Технологии информационного общества

АРХИТЕКТУРА И АЛГОРИТМ РАБОТЫ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОНОМНЫХ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ И КОМПЛЕКСОВ

Статья рекомендована к публикации членом редакционного совета А. А. Стрельцовым 25.06.2024.

Бжихатлов Кантемир Чамалович

Кандидат физико-математических наук
ФГБНУ «ФНЦ Кабардино-Балкарский научный центр РАН», лаборатория «Нейрокогнитивные автономные интеллектуальные системы», заведующий лабораторией
Нальчик, Российская Федерация
haosit13@mail.ru

Пшенокова Инна Ауесовна

Кандидат физико-математических наук
Институт информатики и проблем регионального управления Кабардино-Балкарского научного центра РАН, лаборатория «Интеллектуальные среды обитания», заведующий лабораторией
Нальчик, Российская Федерация
pshenokova_inna@mail.ru

Заммоев Аслан Узеирович

Кандидат технических наук
Институт информатики и проблем регионального управления Кабардино-Балкарского научного центра РАН, лаборатория «Бионаноробототехника», заведующий лабораторией
Нальчик, Российская Федерация
zammoev@mail.ru

Аннотация

В статье представлена концепция системы кибербезопасности для автономного робототехнического комплекса на примере робота-ритейлера, предназначенного для выкладки товаров в крупных магазинах. Проанализированы виды угроз, определена архитектура системы безопасности и алгоритмы ее работы. В качестве интеллектуальной системы управления робота используется система на основе мультиагентных нейрокогнитивных архитектур. Система безопасности робота разделена на систему защиты от физических воздействий и систему информационной защиты. В первом случае сенсоры робота отслеживают попытки перемещения, вскрытия и нарушения работы системы управления. Во втором случае используются защищенные протоколы обмена информацией при работе в сети Интернет.

Ключевые слова

киберфизические системы; информационная безопасность; автономный робот; интеллектуальная система управления; робот-ритейлер

Введение

Обеспечение безопасности при работе автономных роботов связано с радом сложностей, среди которых и необходимость обеспечения информационной защиты системы управления [1, 2]. При этом стоит понимать, что в отличие от классических угроз, связанных с недостаточной надежностью защиты информационных ресурсов, взлом роботов (как и других киберфизических систем) несет более широкий спектр угроз, часть из которых связана с возможностью влияния на внешний мир, то есть взлом робота может привести не только к потере данных, но и к физическим разрушениям.

https://doi.org/10.52605/16059921_2025_01_118

Можно выделить дополнительные особенности киберфизических систем с точки зрения обеспечения безопасности: наличие возможности сбора данных с помощью сенсоров непосредственно из внешней среды, возможность воздействия на реальный мир за счет эффекторов, возможность разрушения узлов робота при отправке неправильных сигналов на эффекторы (перегрузка системы энергообеспечения, заклинивание двигателей и т.д.), доступ к обработке большого объема личных данных, постоянное подключение к сети Интернет и работа с множеством облачных сервисов, использование нейросетевых систем прогнозирования в принятии решений, представляющих «черный ящик», а также возможность распознавания и имитации эмоций для манипулирования пользователем. Кроме того, в работе [1] отмечается несовершенство существующих подходов к нормативно-правовой базе, регламентирующей безопасность применения роботов. При этом, подобные проблемы, связанные со стремительным развитием робототехники, наблюдаются не только в Европе.

Стоит отметить, что роботы уже давно внедряются в сферы деятельности человека, где последствия сбоя или взлома могут нести значительную угрозу. Например, широкое распространение медицинских роботов хирургов [3] предполагает, что от надежности работы алгоритма управления зависит жизнь пациента. Не менее важной областью медицинской робототехники является роботы для сопровождения диагностики пациентов, что стало еще более актуально во время пандемии COVID-19 [4]. При этом несмотря на неоспоримые преимущества автоматизированной работы с инфицированными больными, возможность взлома и нарушения работоспособности подобных роботов несет угрозу другим пациентами и персоналу медицинских учреждений.

Не менее важной областью применения киберфизических систем является автотранспорт. Учитывая распространение систем автопилотирования или поддержки водителя на основе систем искусственного интеллекта, надежность обеспечения информационной безопасности системы управления транспортным средством связана с жизнью и здоровьем всех участников дорожного движения. При этом стоит понимать, что причиной аварии могут стать как недочеты в работе самих систем автопилота [5], так и взлом и перехват управления транспортным средством [6]. Для беспилотных летательных аппаратов вопросы кибербезопасности еще более актуальны [7].

Отдельно стоит упомянуть применение роботов в промышленности, связанной с высоким уровнем ответственности. Например, применение робототехники и искусственного интеллекта в атомной энергетике позволяет заметно снизить стоимость и опасность обслуживания реактора, но при этом минимальная возможность сбоя работы подобной системы может привести к катастрофе [8]. Даже незначительные нарушения работы системы энергообеспечения могут нарушить работы важных узлов инфраструктуры города [9].

Учитывая широкий спектр опасностей, связанных с надежностью информационной системы робота, задача разработки системы безопасности становится обязательной при создании автономных коллаборативных роботов. Целью данного исследования является разработка архитектуры системы информационной безопасности для автономных роботов, работающих в условиях реальной среды. Реализация подобной системы позволит обеспечить безопасность и надежную защиту автономных робототехнических и программных комплексов, окружающих людей и имущество, а также данных пользователей, хранящихся в базе знаний программной или робототехнической системы.

1 Архитектура системы информационной безопасности для интеллектуального автономного робота

В рамках проектирования автономных роботов-ритейлеров [10, 11] стоит задача разработки комплексной системы обеспечения информационной безопасности. Робот предназначен для выкладки товаров в крупных магазинах и представляет собой транспортную платформу с узлом, соответствующим торсу человека и имеющим два манипулятора с антропоморфными кистями. На рис. 1 показан внешний вид робота.

Рис. 1. Внешний вид робота-ритейлера в процессе сборки

Вычислительная система робота представлена бортовой ЭВМ, занимающейся сбором и хранением данных с сенсорной подсети, управлением эффекторами и моделированием процесса принятия решений. Связь с сенсорами и эффекторами обеспечивает внутренняя проводная сеть микроконтроллеров UpioNet, построенная на базе UDP/IP и I2C протоколов. Для связи с внешними устройствами, в том числе с сервером и пользователями, установлен роутер, позволяющий использовать проводную сеть (в случае ремонта) или WiFi соединение. В случае отсутствия доступа к WiFi-сигналу за связь с сервером отвечает встроенный 3G модем. Структурная схема организации сети роботов приведена на рис. 2.

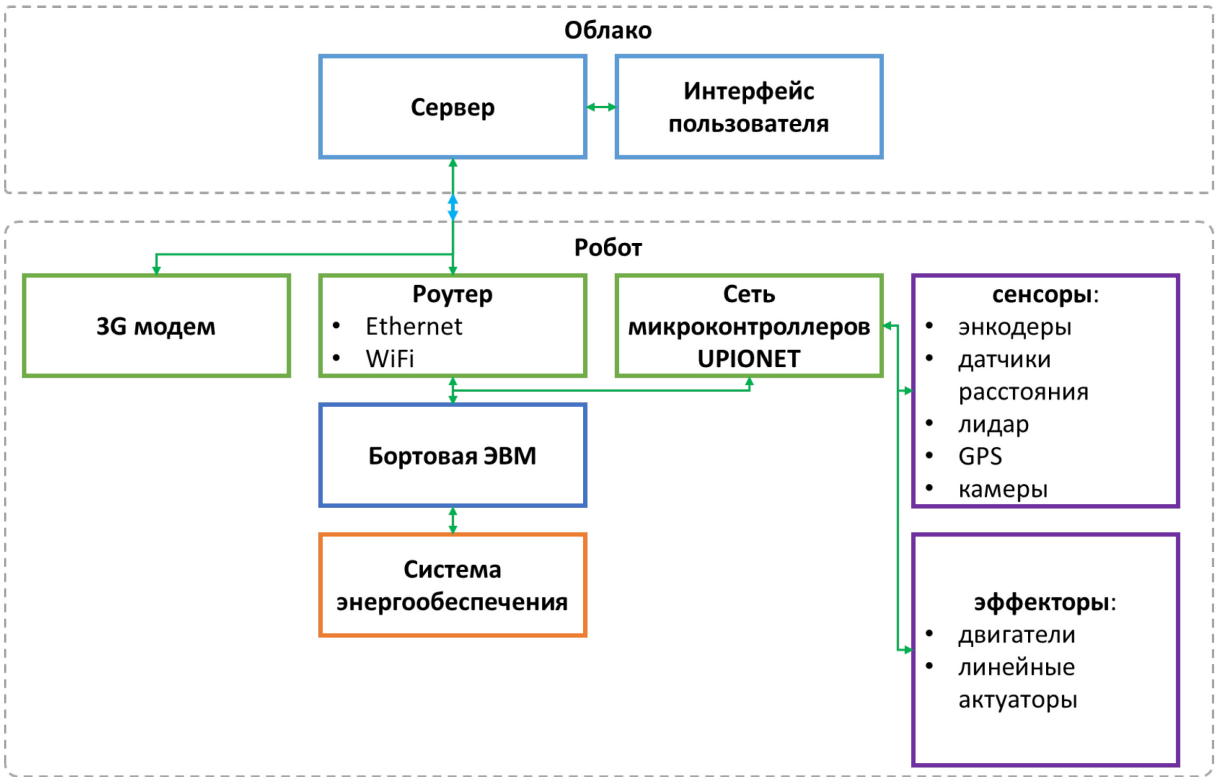

Рис. 2. Структурная схема организации сети для роботов-ритейлеров

Под сервером в этой системе понимается система управления группой роботов и взаимодействия с пользователями. Например, для обеспечения работы в магазине сервер собирает данные по заказам, заполнению полок с товарами и остаткам на складе, а также формирует задания для роботов, обслуживающих торговую зону и склад. При этом система принятия решений, развернутая на сервере основана на самоорганизации мультиагентных нейрокогнитивных архитектур. Подробное описание интеллектуальных систем на основе мультиагентных нейрокогнитивных архитектур можно найти в [12].

В подобной системе управления необходимо учитывать угрозы, связанные как с несанкционированным доступом к данным, так и с перехватом управления роботом (рис. 3). Доступ к данным может привести к потере и утечке информации, собранной роботами, в том числе личным данным клиентов и товарообороте магазина. Доступ к управлению может не только остановить работу робота, но и привести к его поломкам, а также к нанесению вреда окружающим людям и предметам, находящимся в магазине. При этом нарушение работы системы может быть связано не только с информационной безопасностью, но и физическим доступом к элементам управления роботом, вплоть до вскрытия робота и извлечения бортового ЭВМ или нарушения работы сенсоров.

Рис. 3. Виды угроз взлома робототехнического комплекса и их последствия

Для обеспечения физической защиты робота предлагается использовать дополнительный набор датчиков и эффекторов, алгоритм работы которых не зависит от внешних команд или принятых интеллектуальных решений. Схема системы обеспечения безопасности автономного робота-ритейлера приведена на рис. 4. Для обеспечения защиты робота от попытки переноса, переворота или механических ударов используются уже доступные датчики системы навигации: GPS (или RTK) приемник и 9-осевой IMU сенсор (гироскоп, акселерометр, магнетометр). Эти сенсоры позволят определить любое незапланированное перемещение робота и оповестить оператора за счет сети интернет. Для определения попыток вскрытия корпуса необходимо использование датчиков целостности (герконов или датчиков касания) на каждом крепежном элементе робота. Несмотря на их значительное количество (например, для робота-ритейлера таких датчиков нужно около 160 шт.), невысокая стоимость и простота работы с ними позволят обойтись без заметного удорожания конечной стоимости робота.

Независимо от работы системы навигации и ориентации робота, работает система избегания столкновений, которая собирает данные со всех датчиков расстояния (ультразвуковые и ИК датчики расстояния, акселерометр, лидар) и при возникновении опасности блокирует перемещение робота (и его манипуляторов), тем самым обеспечивая безопасность людей вокруг. Надежность энергосистемы обеспечивается несколькими аккумуляторами, напряжение и ток через которые отслеживаются соответствующими датчиками, а контакт при необходимости отключается с помощью реле. Отдельно реализована система отслеживания радиопомех, которая при необходимости включает резервную систему передачи информации на сервер и соседних роботов. При обнаружение любой из указанных проблем робот сигнализирует об этом аудиосообщением, через систему эффекторов робота.

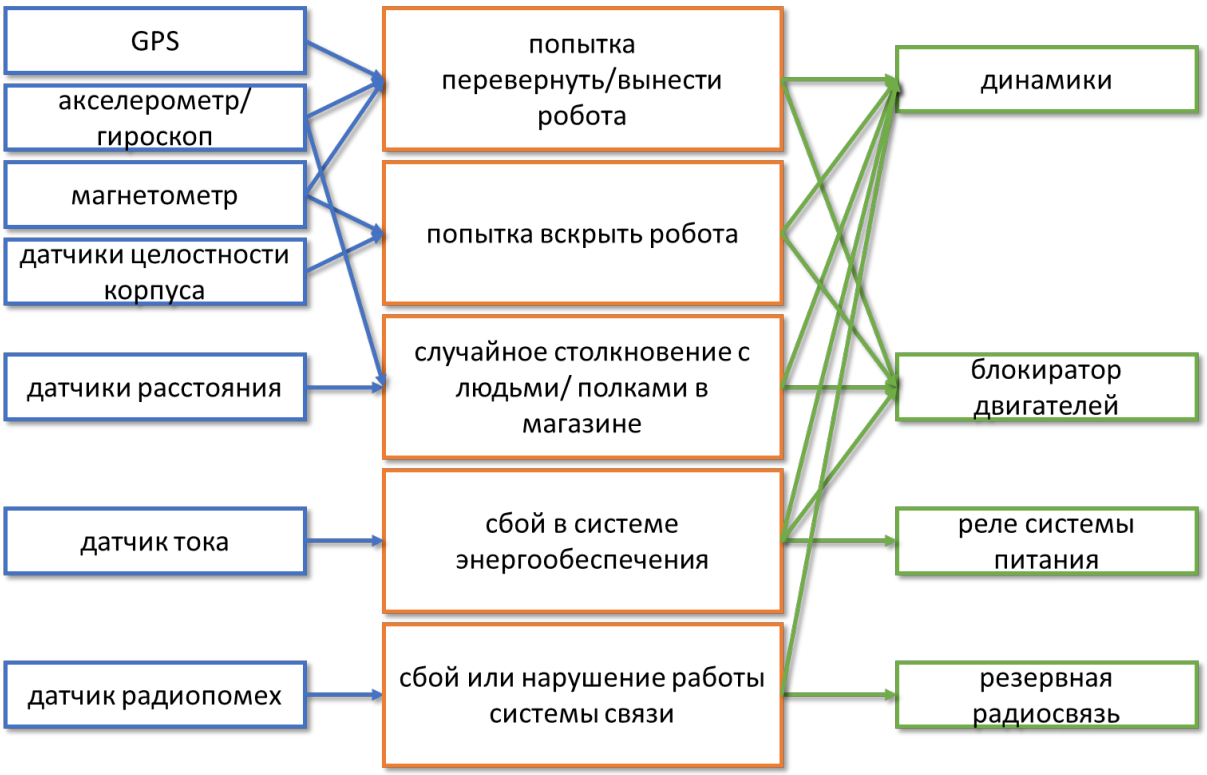

Рис. 4. Схема системы обеспечения безопасности автономного робота-ритейлера

Стоит отметить, что описанная система позволит минимизировать риски, вызванные взломом системы управления или механического воздействия на робота. Но представленные меры защиты не исключают необходимости обеспечения информационной безопасности сети робота. Информация между узлами робота передается по внутренней локальной сети, без доступа к «внешнему» интернету. Вся информация на этом уровне обрабатывается в отдельном защищенном потоке и не уходит на внешний сервер, поэтому дополнительных мер защиты данной сети не требуется. Кроме того, учитывая большой объем передаваемых данных в локальной сети робота и низкую производительность контроллеров конечных устройств (микроконтроллеров, управляющих сенсорами и эффекторами), применение более высокоуровневого протокола TCP/IP и шифрование данных на этом уровне негативно скажется на производительности всей системы управления.

Однако, обмен информацией между группой роботов и между роботом и основным сервером требует полноценной системы защиты и шифрования. Не менее важной задачей является обеспечение безопасности работы мультиагентной нейрокогнитивной системы принятия решений, используемой для задач распознавания товаров на полке и складе, построение маршрута перемещения, управления манипуляторами и обеспечения естественно-языкового интерфейса взаимодействия с посетителями и сотрудниками магазина [13]. Все передаваемые между роботами и сервером данные используют защищенные протоколы HTTPS (HyperText Transfer Protocol Secure) [14] и WSS (WebSockets Secure) и представлены в виде JSON объектов. Для обеспечения защиты этих сообщений используется также двусторонняя аутентификация (клиент у сервера и сервер у клиента), система контроля доверенности серверу и шифрование всех переданных данных. Кроме того, операционная система бортовой ЭВМ проверяет надежность источников, из которых получает обновления программного обеспечения робота. Основной алгоритм работы системы защиты информации показан на рис. 5.

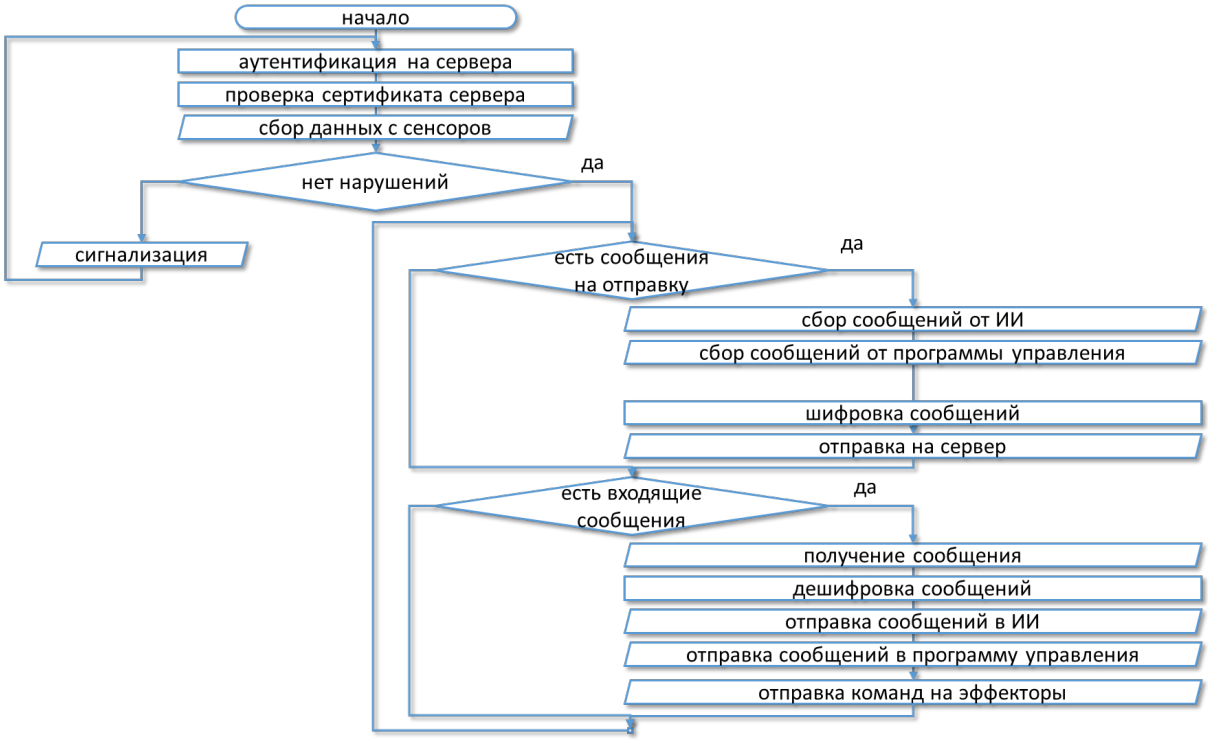

Рис. 5. Алгоритм работы системы защиты информации

На данном этапе разработки, описанных методов защиты достаточно для обеспечения безопасности при угрозе утечки информации или перехвата управления роботом. Следует отметить, что шифрование и расшифровка информации происходят на производительной бортовой ЭВМ робота и незначительно влияют на скорость работы системы управления.

Представленная система кибербезопасности может использоваться для обеспечения защиты автономных коллаборативных роботов, например для упомянутых выше роботов RetailMultiBot, предназначенных для выкладки товаров и сбора заказов в крупных сетевых магазинах и пунктах выдачи маркетплейсов. Важность системы кибербезопасности для подобного робота обусловлена функцией обработки онлайн заказов, которая влечет за собой необходимость постоянного подключения к сети Интернет и доступа к личным данным покупателей. После апробации системы кибербезопасности планируется ее внедрение и в другие робототехнические комплексы, разрабатываемые в КБНЦ РАН, например для обеспечения защиты автономного робота по уходу за посевами [15], робототехнической системы мониторинга археологических раскопок [16] и ряда других проектов.

Заключение

В статье представлена концепция и алгоритм работы системы кибербезопасности для автономного интеллектуального робототехнического комплекса на примере робота для выкладки товаров в крупных магазинах. Система безопасности разделена на два уровня: система защиты от физических воздействий и система информационной защиты. В первом случае, на роботе развернута система сенсоров и эффекторов, отвечающих за контроль состояния функциональных узлов и сигнализацию при попытке вскрытия корпуса. Система защиты данных, в том числе и сообщений интеллектуальной системы принятия решений, представлена стандартными средствами авторизации и шифрования, используемыми при работе с HTTPS и WSS протоколами. Стоит отметить, что вопросы отслеживания возможных ошибок работы системы распознавания или принятия решений, связанные с ошибочным определением препятствия, неправильно простроенным маршрутом перемещения или неверно распознанными товарами, требует дальнейшей доработки. В текущей реализации единственной защитой в этом случае является система избегания столкновений.

Литература

1. Fosch-Villaronga E., Mahler T. Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots // Computer Law & Security Review. 2021. V. 41. P. 105528. DOI: 10.1016/j.clsr.2021.105528.
2. Ivanov G. O., Kamenskikh A. N., Yuzhakov A. A. The Problem of Ensuring the Information Security of Robots in the Implementation of the Laws of Robotics // Seminar on Information Computing and Processing (ICP). IEEE. 2023. P. 86-88. DOI: 10.1109/ICP60417.2023.10397124
3. Dupont P. E., Simaan N., Choset H., Rucker D. C. Continuum Robots for Medical Interventions // Proceedings of the IEEE. 2022. V. 110. №. 7. P. 847-870. DOI: 10.1109/jproc.2022.3141338.
4. Di Lallo A., Murphy R., Axel Krieger A. K., Zhu J., TAYLOR R. H., Su H. Medical Robots for Infectious Diseases: Lessons and Challenges from the COVID-19 Pandemic // IEEE Robotics and Automation Magazine. 2021. V. 28. №. 1. P. 18-27. DOI: 10.1109/mra.2020.3045671.
5. Sinha A., Chand S., Vu V., Huang C., Dixit V. Crash and disengagement data of autonomous vehicles on public roads in California // Scientific data. 2021. V. 8. №. 1. P. 298. DOI: 10.1038/s41597-021-01083-7.
6. Khan S. K., Shiwakoti N., Stasinopoulos P., Chen Y. Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions // Accident Analysis and Prevention. 2020. V. 148. P. 105837. DOI: 10.1016/j.aap.2020.105837.
7. Аменитский М. В. Анализ потенциальных угроз системы управления беспилотных летательных аппаратов средних и тяжелых классов //Труды МАИ. 2017. №. 94. С. 16-16.
8. Suman S. Artificial intelligence in nuclear industry: Chimera or solution? // Journal of Cleaner Production. 2021. V. 278. P. 124022. DOI: 10.1016/j.jclepro.2020.124022.
9. Su Q., Wang H., Sun C., Li B., Li J. Cyber-attacks against cyber-physical power systems security: State estimation, attacks reconstruction and defense strategy // Applied Mathematics and Computation. 2022. V. 413. P. 126639. DOI: 10.1016/j.amc.2021.126639.
10. Бжихатлов, К. Ч., Пшенокова, И. А., Абазоков, М. А. Оценка вычислительной нагрузки различных вариантов группового управления роботами на основе мультиагентных нейрокогнитивных архитектур // Информационное общество. 2024. Т. 2. С. 134-148. DOI: 10.52605/16059921_2024_02_134.
11. Retail MultiBot. Мультиагентный робототехнический комплекс для замещения персонала в торговых залах универсамов и гипермаркетов // Официальный сайт ФГБНУ «ФНЦ Кабардино-Балкарский центр РАН» kbncran.ru. URL: http://projects.kbncran.ru/?page_id=539 (дата обращения: 27.05.2024).
12. Нагоев З.В. Интеллектика, или мышление в живых и искусственных системах // Нальчик: Издательство КБНЦ РАН, 2013. 211 с.
13. Nagoev Z. V., Nagoeva O., Anchokov M., Bzhikhatlov K. C., Kankulov S. A., Enes A. The symbol grounding problem in the system of general artificial intelligence based on multi-agent neurocognitive architecture // Cognitive Systems Research. 2023. V. 79. P. 71-84. DOI: 10.1016/j.cogsys.2023.01.002.
14. HTTP Over TLS // Интернет-ресурс. URL: https://datatracker.ietf.org/doc/html/rfc2818 (дата обращения: 27.05.2024).
15. Bzhikhatlov K., Pshenokova I. Intelligent Spraying System of Autonomous Mobile Agricultural Robot. In: Ronzhin, A., Kostyaev, A. (eds) Agriculture Digitalization and Organic Production. ADOP 2023. Smart Innovation, Systems and Technologies. 2023. V. 362. Springer, Singapore. DOI: 10.1007/978-981-99-4165-0_25.
16. Бжихатлов К.Ч., Пшенокова И.А., Заммоев А.У., Кокова Л.Б. Автономный робот для мониторинга наземных археологических раскопок // Известия ЮФУ. Технические науки. 2023. № 1. С. 100-109. DOI: 10.18522/2311-3103-2023-1-100-109.

ARCHITECTURE AND OPERATING ALGORITHM OF THE INFORMATION SECURITY SYSTEM OF AUTONOMOUS INTELLIGENT SYSTEMS AND COMPLEXES

Bzhikhatlov, Kantemir Chamalovich

Candidate of physical-mathematical sciences
Kabardino-Balkarian Scientific Center of the Russian Academy of Sciences, laboratory «Neurocognitive autonomous intelligent systems», head of the laboratory
Nalchik, Russian Federation
haosit13@mail.ru

Pshenokova, Inna Auesovna

Candidate of physical-mathematical sciences
Institute of Computer Science and Problems of Regional Management, Kabardino-Balkarian Scientific Center of the Russian Academy of Sciences, laboratory «Smart living environments», head of the laboratory
Nalchik, Russian Federation
pshenokova_inna@mail.ru

Zammoev, Aslan Uzeyrovich

Candidate of technical sciences
Institute of Computer Science and Problems of Regional Management, Kabardino-Balkarian Scientific Center of the Russian Academy of Sciences, laboratory «Bionanorobotics», head of the laboratory
Nalchik, Russian Federation
zammoev@mail.ru

Abstract

The article presents the concept of a cybersecurity system for an autonomous robotic complex using a retail robot as an example. The robot's security system is divided into a system of protection against physical impacts and an information security system. The types of threats are analyzed, the architecture of the security system and its operating algorithms are defined.

Keywords

cyber-physical systems; information security; autonomous robot; intelligent control system; retail robot

References

1. Fosch-Villaronga E., Mahler T. Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots // Computer Law & Security Review. 2021. V. 41. P. 105528. DOI: 10.1016/j.clsr.2021.105528.
2. Ivanov G. O., Kamenskikh A. N., Yuzhakov A. A. The Problem of Ensuring the Information Security of Robots in the Implementation of the Laws of Robotics // Seminar on Information Computing and Processing (ICP). IEEE. 2023. P. 86-88. DOI: 10.1109/ICP60417.2023.10397124
3. Dupont P. E., Simaan N., Choset H., Rucker D. C. Continuum Robots for Medical Interventions // Proceedings of the IEEE. 2022. V. 110. №. 7. P. 847-870. DOI: 10.1109/jproc.2022.3141338.
4. Di Lallo A., Murphy R., Axel Krieger A. K., Zhu J., TAYLOR R. H., Su H. Medical Robots for Infectious Diseases: Lessons and Challenges from the COVID-19 Pandemic // IEEE Robotics and Automation Magazine. 2021. V. 28. №. 1. P. 18-27. DOI: 10.1109/mra.2020.3045671.
5. Sinha A., Chand S., Vu V., Huang C., Dixit V. Crash and disengagement data of autonomous vehicles on public roads in California // Scientific data. 2021. V. 8. №. 1. P. 298. DOI: 10.1038/s41597-021-01083-7.
6. Khan S. K., Shiwakoti N., Stasinopoulos P., Chen Y. Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions // Accident Analysis and Prevention. 2020. V. 148. P. 105837. DOI: 10.1016/j.aap.2020.105837.
7. Amenitsky M. V. Analiz potentsial'nykh ugroz sistemy upravleniya bespilotnykh letatel'nykh apparatov srednikh i tyazhelykh klassov [Analysis of potential threats to the control system of

medium and heavy class unmanned aerial vehicles] // Trudy MAI [Proceedings of MAI]. 2017. No. 94. P. 16-16.
8. Suman S. Artificial intelligence in nuclear industry: Chimera or solution? // Journal of Cleaner Production. 2021. V. 278. P. 124022. DOI: 10.1016/j.jclepro.2020.124022.
9. Su Q., Wang H., Sun C., Li B., Li J. Cyber-attacks against cyber-physical power systems security: State estimation, attacks reconstruction and defense strategy // Applied Mathematics and Computation. 2022. V. 413. P. 126639. DOI: 10.1016/j.amc.2021.126639.
10. Bzhikhatlov, K. Ch., Pshenokova, I. A., Abazokov, M. A. Otsenka vychislitel'noy nagruzki razlichnykh variantov gruppovogo upravleniya robotami na osnove mul'tiagentnykh neyrokognitivnykh arkhitektur [Evaluation of the computational load of various options for group control of robots based on multi-agent neurocognitive architectures] // Informatsionnoye obshchestvo [Information Society]. 2024. V. 2. P. 134-148. DOI: 10.52605/16059921_2024_02_134.
11. Retail MultiBot. Multi-agent robotic complex for replacing personnel in the sales areas of supermarkets and hypermarkets // Official website of the Federal State Budgetary Scientific Institution "Federal Scientific Center of the Kabardino-Balkarian Center of the Russian Academy of Sciences" kbncran.ru. URL: http://projects.kbncran.ru/?page_id=539 (accessed on: 27.05.2024).
12. Nagoev Z.V. Intellektika, ili Myshlenie v zhivykh i iskusstvennykh sistemakh [Intellectics, or thinking in natural and artificial systems]. Nal'chik: Izdatel'stvo KBNTS RAN [KBSC RAS Publishing house]. 2013. 211 p.
13. Nagoev Z. V., Nagoeva O., Anchokov M., Bzhikhatlov K. C., Kankulov S. A., Enes A. The symbol grounding problem in the system of general artificial intelligence based on multi-agent neurocognitive architecture // Cognitive Systems Research. 2023. V. 79. P. 71-84. DOI: 10.1016/j.cogsys.2023.01.002.
14. HTTP Over TLS // URL: https://datatracker.ietf.org/doc/html/rfc2818 (accessed on: 27.05.2024).
15. Bzhikhatlov K., Pshenokova I. Intelligent Spraying System of Autonomous Mobile Agricultural Robot. In: Ronzhin, A., Kostyaev, A. (eds) Agriculture Digitalization and Organic Production. ADOP 2023. Smart Innovation, Systems and Technologies. 2023. V. 362. Springer, Singapore. DOI: 10.1007/978-981-99-4165-0_25.
16. Bzhikhatlov K.Ch., Pshenokova I.A., Zammoev A.U., Kokova L.B. Avtonomnyy robot dlya monitoringa nazemnykh arkheologicheskikh raskopok [Autonomous robot for monitoring ground archaeological excavations] // Izvestiya YUFU. Tekhnicheskiye nauki [Bulletin of SFedU. Technical sciences]. 2023. No. 1. P. 100-109. DOI: 10.18522/2311-3103-2023-1-100-109.