ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ КАЗАХСТАН
MINISTRY OF SCIENCE AND HIGHER EDUCATION OF THE REPUBLIC OF KAZAKHSTAN

ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

2024 (19) 3

шілде - қыркүйек

ISSN 2708–2032 (print)
ISSN 2708–2040 (online)

БАС РЕДАКТОР:

Исахов Асылбек Абдиашимович — басқарма төрағасы, Халықаралық ақпараттық технологиялар универси тетінің ректоры, есептеу теориясы саласындағы математика бойынша PhD докторы, "Компьютерлік ғылымдар және информатика"бағыты бойынша қауымдастырылған профессор (Қазақстан)

БАС РЕДАКТОРДЫҢ ОРЫНБАСАРЫ:

Колесникова Катерина Викторовна — техника ғылымдарының докторы, Халықаралық ақпараттық технологиялар университеті, «Ақпараттық жүйелер» кафедрасының проректоры (Қазақстан)

ҒАЛЫМ ХАТШЫ:

Ипалакова Мадина Тулегеновна — техника ғылымдарының кандидаты, қауымдастырылған профессор, «Халықаралық ақпараттық технологиялар университеті» АҚ, Ғылыми-зерттеу жұмыс департаментінің директоры (Қазақстан)

РЕДАКЦИЯЛЫҚ АЛҚА:

Разак Абдул — PhD, Халықаралық ақпараттық технологиялар университетінің профессоры (Қазақстан)

Лучио Томмазо де Паолис — Саленто университетінің (Италия) инновациялар және технологиялық инженерия департаменті AVR зертханасының зерттеу және әзірлеу бөлімінің директоры

Лиз Бэкон — профессор, Абертей университеті вице-канцлердің орынбасары (Ұлыбритания)

Микеле Пагано — PhD, Пиза университетінің профессоры (Италия)

Отелбаев Мухтарбай Отелбаевич — физика-математика ғылымдарының докторы, ҚР ҰҒА академигі, Халықаралық ақпараттық технологиялар университеті, «Математикалық және компьютерлік модельдеу» кафедрасының профессоры (Қазақстан)

Рысбайұлы Болатбек — физика-математика ғылымдарының докторы, Халықаралық ақпараттық технологиялар университеті, «Математикалық және компьютерлік модельдеу» кафедрасының профессоры (Қазақстан)

Дайнеко Евгения Александровна — PhD, қауымдастырылған профессор, Халықаралық ақпараттық технологиялар университетінің Жаһандық серіктестік және қосымша білім беру жөніндегі проректоры (Қазақстан)

Дузбаев Нуржан Токкужаевич — PhD, Халықаралық ақпараттық технологиялар университетінің Цифрландыру және инновациялар жөніндегі проректоры (Қазақстан)

Сынчев Бахтгерей Куспанович — техника ғылымдарының докторы, Халықаралық ақпараттық технологиялар университетінің «Ақпараттық жүйелер» кафедрасының профессоры (Қазақстан)

Сейлова Нұргүл Абдуллаевна — техника ғылымдарының кандидаты, Халықаралық ақпараттық технологиялар университетінің «Компьютерлік технологиялар және киберқауіпсіздік» факультетінің деканы (Қазақстан)

Мухамедиева Ардақ Габитовна — экономика ғылымдарының кандидаты, Халықаралық ақпараттық технологиялар университетінің «Цифрлық трансформациялар» факультетінің деканы (Қазақстан)

Ыдырыс Айжан Жұмабайқызы — PhD, Халықаралық ақпараттық технологиялар университетінің «Математикалық және компьютерлік модельдеу» кафедрасының меңгерушісі (Қазақстан)

Шильдибеков Ерлан Жаржанович — PhD, Халықаралық ақпараттық технологиялар университетінің «Экономика және бизнес» кафедрасының меңгерушісі (Қазақстан)

Аманжолова Сауле Токсановна — техника ғылымдарының кандидаты, Халықаралық ақпараттық технологиялар университетінің «Киберқауіпсіздік» кафедрасының меңгерушісі (Қазақстан)

Ниязгулова Айгүл Аскарбековна — филология ғылымдарының кандидаты, Халықаралық ақпараттық технологиялар университетінің «Медиакоммуникациялар және Қазақстан тарихы» кафедрасының меңгерушісі (Қазақстан)

Айтмагамбетов Алтай Зуфарович — техника ғылымдарының кандидаты, Халықаралық ақпараттық технологиялар университетінің «Радиотехника, электроника және телекоммуникация» кафедрасының профессоры (Қазақстан)

Алмисреб Али Абд — PhD, Халықаралық ақпараттық технологиялар университетінің қауымдастырылған профессоры (Қазақстан)

Мохамед Ахмед Хамада — PhD, Халықаралық ақпараттық технологиялар университетінің «Ақпараттық жүйелер» кафедрасының қауымдастырылған профессоры (Қазақстан)

Янг Им Чу — PhD, Гачон университетінің профессоры (Оңтүстік Корея)

Тадеуш Валлас — PhD, Адам Мицкевич атындағы университеттің проректоры (Польша)

Мамырбаев Өркен Жұмажанұлы — Ақпараттық жүйелер саласындағы техника ғылымдарының (PhD) докторы, ҚР БҒМ ҚҰО ақпараттық және есептеу технологиялары институты директорының ғылым жөніндегі орынбасары (Қазақстан)

Бушуев Сергей Дмитриевич — техника ғылымдарының докторы, профессор, Украинаның «УКРНЕТ» жобаларды басқару қауымдастығының директоры, Киев ұлттық құрылыс және сәулет университетінің «Жобаларды басқару» кафедрасының меңгерушісі (Украина)

Белощицкая Светлана Васильевна — техника ғылымдарының докторы, доцент, Астана IT университетінің деректер жөніндегі есептеу және ғылым кафедрасының профессоры (Қазақстан)

ЖАУАПТЫ РЕДАКТОР:

Мрзабаева Раушан Жәлиқызы — «Халықаралық ақпараттық технологиялар университеті» АҚ (Қазақстан)

Халықаралық ақпараттық және коммуникациялық технологиялар журналы
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Меншіктенуші: «Халықаралық ақпараттық технологиялар университеті» АҚ (Алматы қ.).
Қазақстан Республикасы Ақпарат және әлеуметтік даму министрлігінің Ақпарат комитетінде – **20.02.2020** жылы берілген.
№ KZ82VPY00020475 мерзімдік басылым тіркеуіне қойылу туралы куәлік.
Тақырыптық бағыты: ақпараттық технологиялар, әлеуметтік-экономикалық жүйелерді дамытудағы цифрлық технологиялар, ақпараттық қауіпсіздік және коммуникациялық технологияларға арналған.
Мерзімділігі: жылына 4 рет.
Тиражы: 100 дана
Редакцияның мекенжайы: 050040, Алматы қ-сы, Манас к-сі, 34/1, 709-кабинет, тел: +7 (727) 244-51-09.
E-mail: ijict@iitu.edu.kz Журнал сайты: https://journal.iitu.edu.kz
© Халықаралық ақпараттық технологиялар университеті АҚ, 2024
© Авторлар ұжымы, 2024

ГЛАВНЫЙ РЕДАКТОР:

Исахов Асылбек Абдиашимович — кдоктор PhD по математике в области теории вычислимости, ассоциированный профессор по направлению "Компьютерные науки и информатика", Председатель Правления – Ректор АО «Международный университет информационных технологий» (Казахстан)

ЗАМЕСТИТЕЛЬ ГЛАВНОГО РЕДАКТОРА:

Колесникова Катерина Викторовна — доктор технических наук, профессор, проректор по научно-исследо ва тель-ской деятельности Международного университета информационных технологий (Казахстан)

УЧЕНЫЙ СЕКРЕТАРЬ:

Ипалакова Мадина Тулегеновна — кандидат технических наук, ассоциированный профессор, директор департа мента по научно-исследовательской деятельности Международного университета информационных технологий (Казахстан)

РЕДАКЦИОННАЯ КОЛЛЕГИЯ:

Разак Абдул — PhD, профессор кафедры кибербезопасности Международного университета информационных тех нологий (Казахстан)

Лучио Томмазо де Паолис — директор отдела исследований и разработок лаборатории AVR департамента инноваций и технологического инжиниринга Университета Саленто (Италия)

Лиз Бэкон — профессор, заместитель вице-канцлера Университета Абертей (Великобритания)

Микеле Пагано — PhD, профессор Университета Пизы (Италия)

Отелбаев Мухтарбай Отелбайулы — доктор физико-математических наук, профессор, академик НАН РК, профессор кафедры математического и компьютерного моделирования Международного университета информационных технологий (Казахстан)

Рысбайулы Болатбек — доктор физико-математических наук, профессор, профессор кафедры математического и компьютерного моделирования Международного университета информационных технологий (Казахстан)

Дайнеко Евгения Александровна — PhD, ассоциированный профессор, проректор по глобальному партнерству и дополнительному образованию Международного университета информационных технологий (Казахстан)

Дузбаев Нуржан Токкужаевич — PhD, ассоциированный профессор, проректор по цифровизации и инновациям Международного университета информационных технологий (Казахстан)

Синчев Бахтгерей Куспанович — доктор технических наук, профессор, профессор кафедры информационных систем Международного университета информационных технологий (Казахстан)

Сейлова Нургуль Абадуллаевна — кандидат технических наук, декан факультета компьютерных технологий и кибербезопасности Международного университета информационных технологий (Казахстан)

Мухамедиева Ардак Габитовна — кандидат экономических наук, декан факультета цифровых трансформаций Международного университета информационных технологий (Казахстан)

Ыдырыс Айжан Жумабаевна — PhD, ассистент профессор, заведующая кафедрой математического и компьютерного моделирования Международного университета информационных технологий (Казахстан)

Шилдибеков Ерлан Жаржанович — PhD, заведующий кафедрой экономики и бизнеса Международного университета информационных технологий (Казахстан)

Аманжолова Сауле Токсановна — кандидат технических наук, заведующая кафедрой кибербезопасности Международного университета информационных технологий (Казахстан)

Ниязгулова Айгуль Аскарбековна — кандидат филологических наук, доцент, заведующая кафедрой медиакоммуникаций и истории Казахстана Международного университета информационных технологий (Казахстан)

Айтмагамбетов Алтай Зуфарович — кандидат технических наук, профессор кафедры радиотехники, электроники и телекоммуникаций Международного университета информационных технологий (Казахстан)

Алмисреб Али Абд — PhD, ассоциированный профессор кафедры кибербезопасности Международного университета информационных технологий (Казахстан)

Мохамед Ахмед Хамада — PhD, ассоциированный профессор кафедры информационных систем Международного университета информационных технологий (Казахстан)

Янг Им Чу — PhD, профессор университета Гачон (Южная Корея)

Тадеуш Валлас – PhD, проректор университета имен Адама Мицкевича (Польша)

Мамырбаев Оркен Жумажанович — PhD, заместитель директора по науке РГП Института информационных и вычислительных технологий Комитета науки МНВО РК (Казахстан)

Бушуев Сергей Дмитриевич — доктор технических наук, профессор, директор Украинской ассоциации управления проектами «УКРНЕТ», заведующий кафедрой управления проектами Киевского национального университета строительства и архитектуры (Украина)

Белощицкая Светлана Васильевна — доктор технических наук, доцент, профессор кафедры вычислений и науки о данных Astana IT University (Казахстан)

ОТВЕТСТВЕННЫЙ РЕДАКТОР:

Мрзабаева Раушан Жалиевна — АО «Международный университет информационных технологий» (Казахстан).

Международный журнал информационных и коммуникационных технологий
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Собственник: АО «Международный университет информационных технологий» (г. Алматы).
Свидетельство о постановке на учет периодического печатного издания в Министерство информации и общественного развития Республики Казахстан **№ KZ82VPY00020475,** выданное от **20.02.2020 г.**
Тематическая направленность: информационные технологии, информационная безопасность и коммуникационные технологии, цифровые технологии в развитии социо-экономических систем**.**
Периодичность: 4 раза в год.
Тираж: 100 экземпляров.
Адрес редакции: 050040 г. Алматы, ул. Манаса 34/1, каб. 709, тел: +7 (727) 244-51-09.
E-mail: ijict@iitu.edu.kz Сайт журнала: https://journal.iitu.edu.kz
© АО Международный университет информационных технологий, 2024
© Коллектив авторов, 2024

EDITOR-IN-CHIEF:

Isakhov Asylbek Abdiashimovich — PhD in Mathematics specializing in Computability Theory and Associate Professor in Computer Science and Informatics, Chairman of the Board, Rector of International Information Technology University (Kazakhstan)

DEPUTY CHIEF DIRECTOR:

Kolesnikova Katerina Viktorovna — Doctor of Technical Sciences, Vice-Rector of Information Systems Department, International Information Technology University (Kazakhstan)

SCIENTIFIC SECRETARY:

Ipalakova Madina Tulegenovna — Candidate of Technical Sciences, Associate Professor, Director of the Research Department, International University of Information Technologies (Kazakhstan)

EDITORIAL BOARD:

Razaq Abdul — PhD, Professor of International Information Technology University (Kazakhstan)

Lucio Tommaso de Paolis — Director of Research and Development, AVR Laboratory, Department of Innovation and Process Engineering, University of Salento (Italy)

Liz Bacon — Professor, Deputy Director, and Deputy Vice-Chancellor of the University of Abertay. (Great Britain)

Michele Pagano — Ph.D., Professor, University of Pisa (Italy)

Otelbaev Mukhtarbay Otelbayuly – Doctor of Physical and Mathematical Sciences, Academician of the National Academy of Sciences of the Republic of Kazakhstan, Professor of the Department of Mathematical and Computer Modeling of International Information Technology University (Kazakhstan)

Rysbayuly Bolatbek — Doctor of Physical and Mathematical Sciences, Professor of the Department of Mathematical and Computer Modeling, International Information Technology University (Kazakhstan)

Daineko Yevgeniya Alexandrovna — PhD, Associate Professor, Vice-Rector for Global Partnership and Continuing Education, International Information Technology University (Kazakhstan)

Duzbaev Nurzhan Tokkuzhaevich — Candidate of Technical Sciences, Vice-Rector for Digitalization and Innovations, International Information Technology University (Kazakhstan)

Sinchev Bakhtgerey Kuspanuly — Doctor of Technical Sciences, Professor of the Department of Information Systems, International Information Technology University (Kazakhstan)

Seilova Nurgul Abdullaevna — Candidate of Technical Sciences, Dean of the Faculty of Computer Technologies and Cybersecurity, International Information Technology University (Kazakhstan)

Mukhamedieva Ardak Gabitovna – Candidate of Economic Sciences, Dean of the Faculty of Digital Transformations, International Information Technology University (Kazakhstan)

Idyrys Aizhan Zhumabaevna — PhD, Head of the Department of Mathematical and Computer Modeling, International Information Technology University (Kazakhstan)

Shildibekov Yerlan Zharzhanuly — PhD, Head of the Department of Economics and Business, International Information Technology University (Kazakhstan)

Amanzholova Saule Toksanovna — Candidate of Technical Sciences, Head of the Department of Cyber Security, International Information Technology University (Kazakhstan)

Niyazgulova Aigul Askarbekovna — Candidate of Philology, Head of the Department of Media Communications and History of Kazakhstan, International Information Technology University (Kazakhstan)

Aitmagambetov Altai Zufarovich — Candidate of Technical Sciences, Professor of the Department of Radioengineering, Electronics and Telecommunication, International Information Technology University (Kazakhstan)

Almisreb Ali Abd — PhD, Associate Professor, International Information Technology University (Kazakhstan)

Mohamed Ahmed Hamada — PhD, Associate Professor, Department of Information systems, International Information Technology University (Kazakhstan)

Young Im Choo — PhD, Professor, Gachon University (South Korea)

Tadeusz Wallas — PhD, University of Dr. Litt Adam Miskevich in Poznan (Poland)

Mamyrbayev Orken Zhumazhanovich — PhD in Information Systems, Deputy Director for Science, Institute of Information and Computing Technologies CS MSHE RK (Kazakhstan)

Bushuyev Sergey Dmitriyevich — Doctor of Technical Sciences, Professor, Director of Uдоктор технических наук, профессор, директор Ukrainian Association of Project Management UKRNET, Head of Project Management Department, Kyiv National University of Construction and Architecture (Ukraine)

Beloshitskaya Svetlana Vasilyevna — Doctor of Technical Sciences, Associate Professor, Professor of the Department of Computing and Data Science, Astana IT University (Kazakhstan)

EXECUTIVE EDITOR

Mrzabayeva Raushan Zhalievna — International Information Technology University (Kazakhstan)

«International Journal of Information and Communication Technologies»
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Owner: International Information Technology University JSC (Almaty).
The certificate of registration of a periodical printed publication in the Ministry of Information and Social Development of the Republic of Kazakhstan, Information Committee No. KZ82VPY00020475, issued on 20.02.2020.
Thematic focus: information technology, digital technologies in the development of socio-economic systems, information security and communication technologies
Periodicity: 4 times a year.
Circulation: 100 copies.
Editorial address: 050040. Manas st. 34/1, Almaty. +7 (727) 244-51-09. E-mail: ijict@iitu.edu.kz
Journal website: https://journal.iitu.edu.kz
© International Information Technology University JSC, 2024
© Group of authors, 2024

МАЗМҰНЫ

АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР

АҚПАРАТТЫҚ ҚАУІПСІЗДІК ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАРҒА АРНАЛҒАН

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

INFORMATION TECHNOLOGY

INFORMATION SECURITY AND COMMUNICATION TECHNOLOGIES

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

INFORMATION TECHNOLOGY

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Vol. 5. Is. 3. Number 19 (2024). Pp. 8–22
Journal homepage: https://journal.iitu.edu.kz
https://doi.org/10.54309/IJICT.2024.19.3.001
УДК 004.413.2

SOFTWARE DEVELOPMENT PROJECT MANAGEMENT: METRICS AND QUALITY MANAGEMENT IN PROJECTS

G.T. Alin
International Information Technology University, Almaty, Kazakhstan.
E-mail: g.alin@iitu.edu.kz

Alin Galymzada Temirtasovich — candidate of technical sciences, assistant professor, Department of Computer Engineering and Information Security, International Information Technology University, Almaty, 050063, Zhetysu-2, 28
E-mail: g.alin@iitu.edu.kz, https://orcid.org/0000-0003-1028-5452.

© G.T. Alin, 2024

Abstract. This article continues the discussion of the general characteristics and main management technologies in software development projects: determining the necessary metrics, developing models of acceptable limits related to ensuring the achievement of the project goal. The general existing approaches to managing the metrics of a software development project, the roles and tasks of the project manager and his team in the context of metrics management are highlighted. The article discusses the need for a quantitative assessment of the metrics and status of the project, i.e. the development of necessary and sufficient tests of all key requirements which were put forward by the customer for software development.

Keywords: IT projects, project risk management, analysis, accounting and development of a plan to mitigate the risks of a software development project

For citation: *G.T. Alin. SOFTWARE DEVELOPMENT PROJECT MANAGEMENT: CONFIGURATION MANAGEMENT, VERSION CONTROL AND SOFTWARE PRODUCT RELEASES//INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES. 2024. Vol. 5. No. 19. Pp. 08–22 (In Rus.). https://doi.org/10.54309/IJICT.2024.19.3.001.*

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

БАҒДАРЛАМАЛЫҚ ҚҰРАМДЫ ЖАСАУ ЖОБАСЫН БАСҚАРУ: ЖОБАДА МЕТРИКА ЖӘНЕ САПА БАСҚАРУ

Г.Т. Алин
Халықаралық ақпараттық технологиялар университеті, Алматы, Қазақстан.
E-mail: g.alin@iitu.edu.kz

Алин Ғалымзада Теміртасович — техника ғылымдарының кандидаты, Халықаралық ақпараттық технологиялар университетінің Компьютерлік инженерия және ақпараттық қауіпсіздік кафедрасының ассистенті профессоры. ҚР, Алматы қ., 050063 Жетісу-2, 28, 13 пәтер

E-mail: g.alin@iitu.edu.kz; https://orcid.org/0000-0003-1028-5452.

© Г.Т. Алин, 2024

Аннотация. Бұл мақалада бағдарламалық қамтамасыз етуді әзірлеу жобаларындағы жалпы сипаттамалар мен негізгі басқару технологияларын талқылау жалғасады: қажетті көрсеткіштерді анықтау, жобаның мақсатына жетуді қамтамасыз етуге байланысты рұқсат етілген шектердің үлгілерін әзірлеу. Бағдарламалық жасақтаманы әзірлеу жобасының метрикасын басқарудың жалпы қолданыстағы тәсілдері, метриканы басқару контекстіндегі жоба менеджері мен оның командасының рөлдері мен тапсырмалары бөлектелген. Мақалада жобаның өлшемдері мен мәртебесін сандық бағалау қажеттілігі талқыланады, яғни бағдарламалық қамтамасыз етуді әзірлеу үшін тапсырыс беруші қойған барлық негізгі талаптардың қажетті және жеткілікті сынақтарын әзірлеу.

Түйін сөздер: IT-жобалар, жобалық тәуекелдерді басқару, талдау, есепке алу және бағдарламалық жасақтама жобасының тәуекелдерін азайту жоспарын құру

Дәйексөздер үшін: *Г.Т. Алин. БАҒДАРЛАМАЛЫҚ ЖАСАҚТАМАНЫ ӘЗІРЛЕУ ЖОБАЛАРЫН БАСҚАРУ: КОНФИГУРАЦИЯНЫ БАСҚАРУ, БАҒДАРЛАМАЛЫҚ ӨНІМНІҢ НҰСҚАЛАРЫ МЕН ШЫҒАРЫЛЫМДАРЫН БАСҚАРУ//ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ. 2024. Т. 5. No. 19. 08–22 бет. (орыс тілінде). https://doi.org/10.54309/IJICT.2024.19.3.001.*

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

УПРАВЛЕНИЕ ПРОЕКТАМИ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ: УПРАВЛЕНИЕ КОНФИГУРАЦИЯМИ, КОНТРОЛЬ ВЕРСИЙ И РЕЛИЗОВ ПРОГРАММНОГО ПРОДУКТА

Г.Т. Алин
Международный университет информационных технологий, Алматы, Казахстан.
E-mail: g.alin@iitu.edu.kz

Алин Галымзада Темиртасович — кандидат технических наук, ассистент профессор кафедры компьютерной инженерии и информационной безопасности Международного университета информационных технологий. РК, г. Алматы, 050063 Жетысу-2, 28

E-mail: g.alin@iitu.edu.kz, https://orcid.org/0000-0003-1028-5452.

© Г.Т. Алин, 2024

Аннотация. В данной статье продолжается обсуждение основных необходимых технологий управления в проектах разработки программного обеспечения: управление конфигурациями программного продукта, применение систем контроля версий и релизов, направленных на достижение конечных целей проекта. Выделены общие существующие подходы к управлению изменениями артефактов проекта программной разработки, роли и задачи разработчиков проекта и его менеджмента в контексте управления изменениями. В статье рассматривается необходимость построения процесса строгого контроля изменений артефактов проекта, т. е. выбор и использование необходимых и достаточных инструментов для внесения изменений, распределение ролей в данном процессе и его основные компоненты.

Ключевые слова: IT-проекты, оптимизация планирования, управление конфигурациями программного обеспечения, система контроля версий, изменений в процессе разработки программного обеспечения

Для цитирования: *Г.Т. Алин. УПРАВЛЕНИЕ ПРОЕКТАМИ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ: УПРАВЛЕНИЕ КОНФИГУРАЦИЯМИ, КОНТРОЛЬ ВЕРСИЙ И РЕЛИЗОВ ПРОГРАММНОГО ПРОДУКТА//МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ. 2024. Т. 5. No. 19. Стр. 08–22. (На русс.). https://doi.org/10.54309/IJICT.2024.19.3.001.*

Введение

Процесс разработки программного обеспечения (ПО) формально можно представить, как поэтапный (дискретный) процесс внесения изменений в основные документы кода и другие необходимые артефакты: графические схемы алгоритмов и интерфейсов, диаграммы процессов обработки данных и т.п. с целью реализации требований, описанных в документе технической спецификации ПО (Чарльз и др., 2008). Основная проблема, связанная с контролем данного процесса, заключается в том, что над артефактами работают несколько разработчиков в конкурентном режиме, т. е. параллельно. В (Том Демарко, 2018: 352) утверждается, что для устранения возможных проблем и конфликтов, а также для достижения требуемой эффективности внесения изменений необходимо:

1) Понимание принципа работы, структуры и составляющих компонент процесса внесения изменений;2) Правильное распределение ролей между исполнителями и

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

разрешение конфликтов;

3) Применение автоматизированной системы контроля версий артефактов и релизов проекта.

В целом, это означает строгое следование парадигмам и идеологии процесса управления изменениями. С другой стороны, данное требование порождает наем необходимого количества дополнительного персонала, который будет заниматься только вопросами контроля внесения изменений (Ванита и др., 2014).

Как же правильно соблюсти баланс, связанный с процессом управления изменениями в разработке ПО? Начинать необходимо с выбора базовых методов разработки ПО (Институт управления проектами, справочник. Руководство к своду знаний по управлению проектами. 19073-3299: 309), т.е. выбрать между методами разработки по последовательной технологии (Waterfall) и гибкой технологии (Agile). В последнее время большое внимание уделяется гибкой технологии разработки ПО и связанных с ней практических рекомендаций для процесса управления изменениями программных разработок.

Материалы и методы

Основные концепции процесса управления изменениями, его причины и цель

Как уже было сказано выше процесс разработки ПО можно представить, как дискретную цепь переходов из одного состояния в последующее более соответствующее требованиям и ожиданиям клиента до тех пор, пока не будет достигнуто приемлемое финальное состояние (Норман и др., 2000). “SCM is the control of the evolution of complex systems, for the purpose to contribute to satisfying quality and delay constraints.” – Jacky Estublier.

Таким образом, управление изменениями является неизбежным в процессе разработки ПО, и его разработчики во главе с менеджментом должны фокусироваться на том, чтобы обеспечить контроль качества управления процесса изменений (УПИ), где необходимость проведения изменений обусловлены следующими причинами:

– Новые рыночные условия диктуют необходимость изменений к требованиям продукта или правил ведения бизнеса;

– Новые потребности клиента требуют изменения данных, функционала или сервиса;

– Бизнес реорганизации вызывают изменения в проектных приоритетах или структуре команды разработчиков;

– Бюджетные или временные ограничения также могут потребовать пересмотр процесса.Что еще важно помнить в УПИ: это в первую очередь то, что УПИ гораздо больше, чем система контроля версий; второе, УПИ не только занимается контролем изменений кода и работает не только в фазе разработки ПО; третье, но не последнее – выбор инструментов разработки очень важен, но выбор дизайна и строгое следование процессу УПИ гораздо важнее.

Давайте рассмотрим самые простые примеры, когда необходимо УПИ:

- Разработчик А живет в Нью Дели, Индия, а разработчик В живет Бостоне, США они хотят работать на одним HelloWorld.java вместе;

- В последнем релизе была найдена серьезная проблема и менеджер С хочет проследить какие изменения ее вызвали, кто сделал эти изменения;

- Менеджер С хочет получить репорт о текущем прогрессе проекта чтобы решить нужно ли ей нанять больше разработчиков и задержать alpha релиз.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

Описание основных составляющих УПИ

В процессе УПИ выделяют следующие компоненты ((Институт управления проектами, справочник. Руководство к своду знаний по управлению проектами. 19073-3299: 124):

- Процесс контроля изменений
- Статус учета изменений
- Аудит конфигураций
- Управление релизами
- Планирование управления изменениями

Ключевым компонентом является процесс контроля изменений.

С точки зрения разработчика ПО сам процесс контроля изменений можно представить в виде следующей последовательности:

- Проблема обнаружена;- Проблема отрапортована команде по контролю конфигурации;- Команда обсуждает проблему:

- Является проблема ошибкой?

- Является ли проблема необходимостью расширения функционала?

- Кому следует платить за ее решение (клиенту или команде разработчиков)?

- Назначить проблеме приоритет или уровень сложности, и назначить персонал для ее устранения;- Разработчик или аналитик определяет ресурсы для устранения проблемы и что необходимо сделать;

- Разработчик работает вместе с держателем библиотек с целью контроля процесса установки изменений в операционную систему и документацию;- Разработчик записывает в файлы рапорта изменения, документируя все сделанные изменения.

Но лучше его представить в более общем виде, отраженном на диаграмме:

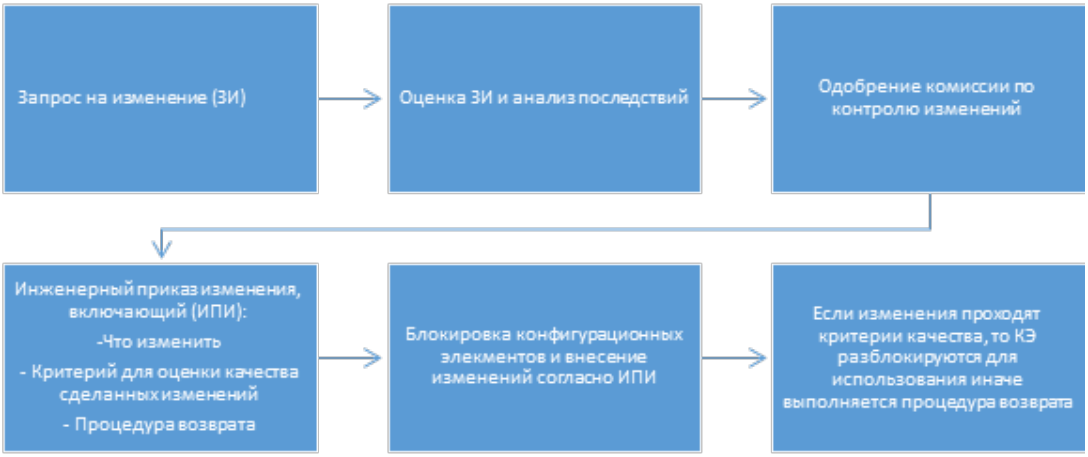


Рис. *1*. Диаграмма процесса контроля изменений

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

Здесь конфигурационный элемент (КЭ) — это утвержденный и одобренный результат изменения, который необходимо провести посредством формальной процедуры.

В данной диаграмме запрос на изменение может быть инициирован пользователем ПО, клиентом или менеджером. Запросы на изменение следует тщательно анализировать как часть процесса изменения, прежде чем проводить имплементацию. Некоторые запросы требуют срочного исполнения ввиду своей природы: необходимость устранения проблема, срочные запросы от бизнеса, изменения рабочей среды ПО.

В состав команды по управлению изменениями как правило входят аналитики, разработчики и контроллеры программных библиотек, в то время как в состав комиссии по контролю изменениями входят представители клиента и члены команды управления изменениями.

На данном этапе должны быть определены ответы на следующие вопросы:

- ✓ Синхронизация (Когда требуется провести изменение?)
- ✓ Идентификация (Кто будет проводить изменение?)
- ✓ Название (Что будет менять в процессе изменения?)
- ✓ Аутентификация (Как проверить, что изменение сделано правильно?)
- ✓ Авторизация (Кто будет одобрять это изменение?)
- ✓ Маршрутизация (Кто должен быть информирован?)
- ✓ Отмена (Кто может отменить это изменение?)
- ✓ Делегация (Вопросы делегирования, если ответственные лица отсутствуют)
- ✓ Оценка (Вопросы приоритета, если есть несколько запросов)

Статус учета изменений

Статус учета изменений – администрирование отслеживания и репорта конфигурационных элементов в системе управления изменениями

Примерами могут являться:

- ✓ Статус предложенных изменений;
- ✓ Статус одобренных изменений;
- ✓ Прогресс текущей версии ПО: в соответствии, с опережением или с опозданием;
- ✓ Оценка ресурсов, необходимых для завершения задач;
- ✓ Проблемы, определенные в процессе аудита конфигурации.

Конфигурационный аудит

Независимые обследование или оценка факта соответствия продукта или процесса заявленным спецификациям, стандартам, контрактным соглашениям или другим критериям

Примерами могут являться:

- ✓ Верификация факта, что конфигурационные элементы протестированы на соответствие функциональным требованиям;
- ✓ Верификация факта, что текущая одобренная версия содержит необходимые и корректные версии конфигурационных элементов;
- ✓ Проверка факта, что изменения, сделанные в текущей одобренной версии, находятся в соответствии с репортом о статусе конфигурации.

На данном этапе обычно обращается внимание на следующие моменты:

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

- ✓ Были ли изменения сделаны без отклонений от одобренных спецификаций?
- ✓ Было ли проведено функционально-техническое обследование для оценки технической корректности?
- ✓ Был ли соблюден одобренный процесс разработки ПО и применялись ли стандарты программной разработки?
- ✓ Отражают ли атрибуты конфигурации объекта заявленное изменение?
- ✓ Были ли соблюдены стандарты записи и репорта при проведении изменений?
- ✓ Все ли необходимые конфигурационные элементы были правильно обновлены?

Управление релизами

Под управлением релизами понимается создание и доступность новых версий ПО для клиентов.

Основные атрибутами релиза являются его:

Формат:

- ✓ Исходный код плюс скрипт построения(компиляции) плюс инструкции;
- ✓ Исполняемые пакеты для определенных платформ;
- ✓ Другие компактные форматы: Java Web среда, плагины;
- ✓ Патчи и обновления: автоматические, ручные;

И содержание:

- ✓ Исходные файлы и/или бинарные;файлы данных;
- ✓ установочные скрипты;
- ✓ библиотеки;
- ✓ документация пользователя и/или разработчика;
- ✓ программы сбора отзывов, т.д.

Планирование управления конфигурациями

Планирование управления конфигурациями производится в соответствии со стандартами IEEE Std 828-2012 (SCM Plans), ANSI-IEEE Std 1042 (SCM), и др.

Чтобы спланировать управление конфигурациями необходимо ответить на следующие вопросы:

- ✓ Чем мы будем управлять? (список и организация КЭ)
- ✓ Кто будет ответственным и за какие операции? (роли и задачи)
- ✓ Как сделать те или иные операции? (дизайн процессов для управления изменениями, задачи диспетчеризации, мониторинга, тестирования, релиза, и др.)
- ✓ Какие записи необходимо сохранять? (логи, заметки, конфигурации, измерения, и др.)
- ✓ Какие ресурсы нужны и как много? (инструменты, деньги, люди, и др.)
- ✓ Какие метрики нужны для измерения прогресса и успеха?
- ✓ **Результаты и обсуждение**

Основные термины системы контроля изменений ПО

К основным терминам систем контроля изменений относят (Институт управления проектами, справочник. Руководство к своду знаний по управлению проектами. 19073-3299: 235):

- ✓ Конфигурационный элемент (КЭ);
- ✓ Версия, вариант и ревизия;

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

- ✓ Конфигурация;
- ✓ Базовый порог (промежуточный результат);
- ✓ Рабочее место.

Конфигурационный элемент (КЭ)Под КЭ поднимается одобренный и принятый результат, достижение которого должно быть сделано в строгом соответствии с формальной процедурой, иначе любой артефакт проекта, чей статус необходимо строго контролировать и проводить его изменения в соответствии с одобрением определенных участников проекта

Примерами являются: план управления проектом, список требований, спецификация дизайна, исходный код и исполняемый код, спецификация тестов, формат данных, записи, информация лога, пользовательская документация, библиотеки и сопровождающие программы, репорты ошибок и т.д.

Наиболее популярными КЭ в среде разработчиков ПО являются:

- ✓ Компьютерные программы: исходные коды, исполняемые коды;
- ✓ Документация: техническая, пользовательская;
- ✓ Данные: внутренние, т.е. содержащиеся в программах и внешние (т.е. файлы и базы данных).

Версии, варианты и ревизии

- – Под версией понимается КЭ в определенной точке его разработки, включая Ревизии и Варианты;Под ревизией понимается КЭ связанный с другой версией КЭ посредством ревизии отношений в упорядоченном порядке во времени;
- – Под вариантом понимаются функционально эквивалентные версии, но разработанные с различными настройками, например, для различных программно-аппаратных платформ;
- – Под веткой понимается последовательность Версий, распределённых во времени.

Сохраняются Версии следующим способом:

Полная копия каждой версии плюс дельта (разница между двумя версиями)

Выделяют три вида дельт:

- Нарастающая дельта:

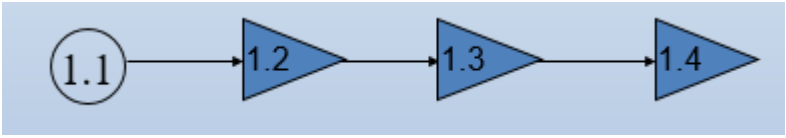


Рис. *2.* Контроль версий: нарастающая дельта

- Убывающая дельта:

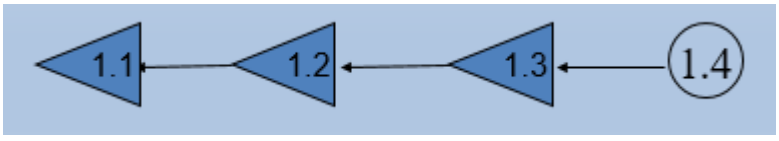


Рис.*3.* Контроль версий: убывающая дельта

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

- Смешанная дельта представляет смесь нарастающей и убывающей.

Система контроля версий, также называется системой контроля ревизий и исходного кода, это способ управления изменениями набора файлов с целью сохранения истории изменений.

Выгодами системы контроля являются: возможность эффективной совместной работы; отчетность и прозрачность; работа в изолированной среде; безопасность и возможность работы из любого места (из офиса, из дома, из отеля и т.д.)

Выделяют три основных типа систем контроля версии:

- ✓ Локальная
- ✓ Централизованная
- ✓ Распределенная (пример Git)

Систему Git мы рассмотрим ниже в разделе 4.

Конфигурация

Под конфигурацией понимается набор функциональных КЭ в соответствии с их природой, версиями и другими характеристиками

Конфигурация гарантирует создание ПО с заданными уровнем качества и функционала

Часто конфигурация нуждается в записи деталей среды окружения, т. е. версии компилятора, библиотек, аппаратной платформы и др.

Простые примеры: Ant buildfile, Makefile

Базовый порог – это коллекция элементов версии, которая была формально рассмотрена и одобрена в качестве версии конфигурации

Базовая порог соответствует определенной стадии проекта (майл стоун) и служит как база для дальнейшей разработки. Базовый порог — это определенная стадия в процессе разработки ПО, отмеченная доставкой одного или более КЭ. Он может быть изменен только после формализованного процесса изменения (Как только базовый порог достигнут, каждый запрос на изменение должен быть оценен и верифицирован, прежде чем допущен для исполнения.)

Базовый порог плюс запрос на изменение создает новый базовый порог

Рабочее место

Под рабочим местом понимается изолированное рабочая среда, где разработчик может работать (редактировать, изменять, собирать, тестировать) не мешая другим разработчикам

Примеры таких рабочих мест: локальная директора системы контроля версий; приватная (домашняя) директория на сервере.

Наиболее общие операции, которые совершаются на рабочем месте: Импорт или загрузка последней информации из системы контроля версий в локальный репозиторий; Обновление или получение последних обновлений версии из ветки репозитория; Блокировка КЭ для внесения изменений; Разблокировка КЭ для разрешения внесения изменений

Примеры инструментов, необходимых разработчику:

- ✓ Для системы контроля версий применяются следующие инструменты:

RCS, CVS, Subversion, Visual Source Safe (Team Foundation Server), Rational ClearCase, Bazaar, GIT

- ✓ Для нахождения ошибок и проблем в коде:

Bugzilla, Mantis Bugtracker, Rational ClearQuest

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

✓ Для построения исполняемого кода:

GNU Make and many variants, Ant

✓ В целом для управления проектом:

Sourceforge.net, freshmeat.net, GForge, Basecamp

Системы контроля версий и ***GitHub как наиболее популярная система контроля версий***

Системы контроля версий (VCS) являются важными инструментами в разработке программного обеспечения, которые помогают управлять изменениями в исходном коде с течением времени. Они обеспечивают основу для отслеживания изменений, совместной работы членов команды и эффективного управления несколькими версиями кода. Системы контроля версий делятся на два основных типа (Ватаре и др., 2019):

- Централизованные системы контроля версий (CVCS): эти системы используют центральный сервер для хранения всех версий проекта. Разработчики извлекают файлы из центрального репозитория, вносят изменения, а затем фиксируют изменения обратно на сервере. Примерами являются Subversion (SVN) и Perforce;- Распределенные системы контроля версий (DVCS): в этих системах каждый разработчик имеет локальную копию всего репозитория, включая его историю. Это позволяет работать в автономном режиме и более гибко ветвиться и объединять. Примерами являются Git, Mercurial и Bazaar.

Система контроля версий	Доля на рынке	Статистика пользования	Причина популярности
Subversion (SVN)	2–4 %	Редко для старых и корпоративных проектов	Простота модели и централизованный подход, который некоторые организации предпочитают из-за простоты контроля доступа и надзора. Отрасли со строгими требованиями соответствия иногда отдают предпочтение SVN из-за его единой точки контроля.
Mercurial	<1 %	Очень редко для старых проектов	Простота и производительность. Некоторые проекты, такие как оригинальные репозитории для Python и Mozilla Firefox, использовали Mercurial до перехода на Git.
Git (GitHub, GitLab)	90–95 %	~93 %	Распределенная база, скорость, возможность ветвления и широкое распространение на таких крупных платформах, как GitHub, GitLab и Bitbucket. Гибкость Git позволяет ему обрабатывать проекты любого размера, что делает его фаворитом как среди небольших команд, так и среди крупных предприятий.
Perforce	1–2 %	Корпоративная специфика	Высокая производительность и надежная обработка больших наборов данных, широко используется в разработке игр, цифровых медиа и корпоративных средах.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

Bazaar	<1 %	Очень редко	Несмотря на то, что изначально Bazaar пользовался популярностью за удобство использования и децентрализованный характер, он не получил существенных обновлений, что привело к его упадку.

Таблица 1. Сравнительная характеристика систем контроля версий (2023 Developer Survey)

Распределенная система контроля версий (DVCS)

DVCS — это одно ранговая модель.

Репозиторий может храниться в клиентской системе, но обычно он хранится в службе хостинга репозитория.

В DVCS каждый человек может одновременно работать с любым файлом, поскольку в рабочей копии изменяется локальный файл. Следовательно, блокировка не требуется.

Когда разработчик внес изменения, он отправляет файл в основной репозиторий, который находится в службе размещения репозитория, и система контроля версий обнаруживает любые конфликты между изменениями файлов. на рисунке 4 (Дорри и др., 2015):

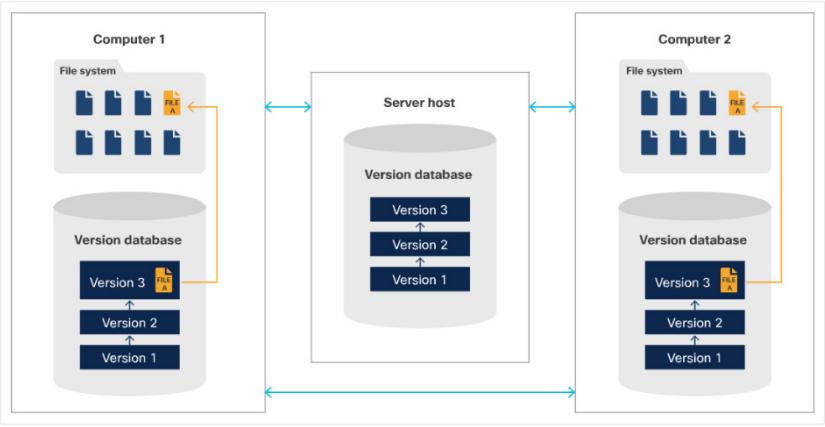


Рис. *4.* Распределенная система контроля версий (DVCS)

Git — это реализация распределенной системы контроля версий с открытым исходным кодом, которая на данный момент является последней тенденцией в разработке программного обеспечения.

Клиент Git должен быть установлен на клиентском компьютере. Он доступен для MacOS, Windows и Linux/Unix.

Одним из ключевых отличий между Git и другими системами контроля версий является то, что Git хранит данные в виде снимков, а не дельт (разницы между текущим файлом и предыдущей версией).

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

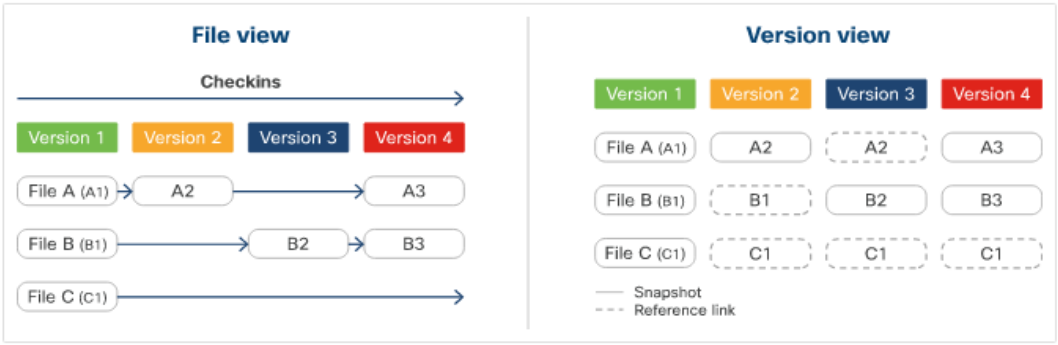


Рис. *5.* Особенность системы контроля версий Git

Если файл не изменяется, Git использует ссылку на последний снимок в системе вместо создания нового и идентичного снимка.

Git организован по принципу три этапа и три состояния.

Три этапа:

- ✓ Репозиторий (каталог.git)Рабочий каталог
- ✓ Промежуточный каталог

Три состояния:

- ✓ Переданный
- ✓ Модифицированный
- ✓ Промежуточный

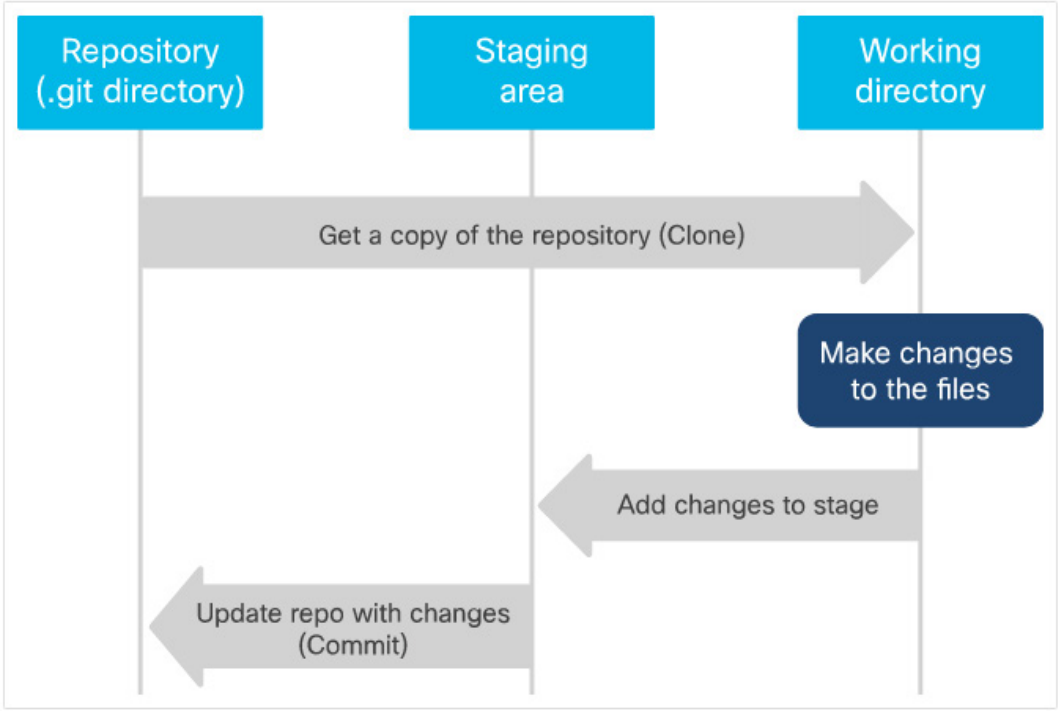


Рис. *6.* Рабочие состояния системы Git

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

Локальные и удаленные репозитории

Git имеет два типа репозиториев: локальные и удаленные.

✓ Локальный репозиторий хранится в файловой системе клиентского компьютера, на котором выполняются команды git;Удаленный репозиторий хранится не на клиентском компьютере, обычно на сервере или в службе размещения репозитория;Удаленный репозиторий с Git остается DVCS, поскольку удаленный репозиторий будет содержать полный репозиторий, включающий код и историю файлов;Когда клиентский компьютер клонирует репозиторий, он получает полный репозиторий без необходимости его блокировки, как в CVCS (центральной системе контроля версий).

После клонирования локального репозитория из удаленного репозитория или создания удаленного репозитория из локального репозитория два репозитория независимы друг от друга до тех пор, пока изменения содержимого не будут применены к другой ветке посредством выполнения команды Git вручную.

Преимущества GitGit допускает сложные стратегии ветвления и слияния, что делает его подходящим для крупномасштабных проектов и нескольких команд;Git имеет обширное сообщество, которое вносит свой вклад в его постоянное совершенствование и обширную документацию;Интеграция с популярными платформами и инструментами CI/CD делает Git выбором номер один для современной разработки программного обеспечения.

ПроблемыМощные функции Git требуют обучения. Новым пользователям команды и рабочие процессы Git могут показаться сложными.

Хотя существуют такие инструменты, как Git LFS (большое файловое хранилище), обработка больших двоичных файлов не является основной сильной стороной Git, поэтому в некоторых сценариях предпочтительнее использовать Perforce.

Тенденции использования и аналитика

Наблюдается растущее внедрение распределенных систем управления версиями (DVCS), так как переход к DVCS, возглавляемый Git, обусловлен потребностью в более тесном сотрудничестве, улучшенных возможностях ветвления и слияния, а также автономной работе (Ватаре и др., 2019). DVCS предлагает большую гибкость и более устойчив к отдельным точкам отказа по сравнению с централизованными системами и предлагает легкую интеграцию с DevOps и конвейерами CI/CD.

Системы управления версиями являются неотъемлемой частью практик DevOps и конвейеров CI/CD. Большинство современных инструментов CI/CD, таких как Jenkins, CircleCI и GitLab CI, предлагают встроенную интеграцию с Git, что еще больше расширяет его внедрение (Стерман и др., 2022: 1–25).

Такие облачные платформы, как GitHub, GitLab, Bitbucket и Azure DevOps, еще больше увеличили популярность Git (Ватаре и др., 2019). Эти платформы предоставляют дополнительные сервисы, такие как отслеживание проблем, обзор кода и функции совместной работы, что делает их незаменимыми в современных рабочих процессах разработки.

Платформа GitHub имеет более 100 миллионов разработчиков и более 330 миллионов репозиториев (по состоянию на 2023 год 2023 Developer Survey), что подчеркивает доминирующее положение Git и его экосистемы.

Платформа GitLab также очень популярна благодаря своей универсальной платформе DevOps, она предлагает схожие с GitHub функции с интегрированным CI/

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

CD и имеет растущую базу пользователей.

Предприятия все чаще отдают предпочтение Git из-за его масштабируемости и совместимости с agile- и DevOps-методологиями (2023 Developer Survey). Крупные организации, включая таких технологических гигантов, как Google, Facebook и Microsoft, стандартизировали Git (Диипа и др., 2020: 1–9).

Заключение

В заключении отметим, что УПИ достаточно сложный и ответственный процесс, определяющий поступательную эффективность в достижении поставленной цели. В УПИ необходимо выделить следующие типовые задачи:

Идентификация – отражение изменений в много ступенчатой системе версии КЭ;

Контроль версий – контролирование изменений до и после релизов клиенту;

Контроль изменения – авторизация одобрений на изменения и контроль приоритетов если одновременно поступило несколько запросов на изменение;

Аудит конфигураций – проверка соблюдения выполнения всех необходимых шагов процесса;

Выдача рапортов – информирование всех необходимых участников что изменение сделано. При выполнении задачи подготовки рапортов необходимо ответить на следующие вопросы: Что происходит? Кто это сделал? Когда это произошло? Что еще будет затронуто данным изменением?

Для оптимизации УПИ всегда необходимо задуматься над минимизацией количества изменений (Кэрол и др., 2009):

- ✓ Для прогноза количества изменений требуется понимать взаимоотношения между системой и ее окружающей средой;
- ✓ Жестко связанные системы требуют изменения при любом изменении окружающей среды.

Факторы, влияющие на отношения систем-среда:

- ✓ Число и сложность интерфейсов системы;
- ✓ Число и волатильность требований системы;
- ✓ Бизнес-процессы, где используется система.

ЛИТЕРАТУРА:

Ванита Бхула, S.B. Hiremath, Дебасис Маллик (2014). Оценка стратегий реагирования на риски, применяемые в проектах программного обеспечения. Австралазийский журнал информационных систем. — Том 18. — № 3, 2014 г.

Ватаре А.С. и Адкар П. (2019). Обзорная статья о централизованной и распределенной системе контроля версий.

Н. Диипа, Б. Прабадеви, Л.Б. Критика и Б. Диипа (2020). Анализ систем контроля версий. Международная конференция 2020 года по новым тенденциям в области информационных технологий и инженерии (ic-ETITE). — 1–9. https://doi.org/10.1109/ic-ETITE47903.2020.39.

Дорри, Норберт и Сибли, Мартина (2015). Монетизация рисков и снижение рисков. — Журнал морских инженеров. 127. — 35–46.

Кэрол Л. Гувер, Мел Россо-Ллопарт, Гил Таран (2009). Оценка решений по проекту: примеры из практики SE. Опубликовано 27 октября 2009г. — издательством Addison-Wesley Professional.

Майкл Килинг (2010). Размышления о программной инженерии: порог успеха. — Опубликовано 15 января 2010 г. — Издатель: Neverletdown

Норман Эллиотт Фентон, Мартин Нил (2000). Метрики программного обеспечения: дорожная карта. — 12 с. — Сентябрь 2000 г. DOI: 10.1145/336512.336588

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

Институт управления проектами, справочник. Руководство к своду знаний по управлению проектами. 14 Campus Boulevard Newtown Square, Пенсильвания. — 19073-3299. —США.

Том Демарко (2018). Крайний срок: роман об управлении проектами. — 1-е издание для США, 2-е издание Автор: 352 стр. ISBN-13. —2018. 978-0932633392

Стерман С., Николас М. и Паулос Э. (2022). На пути к творческому контролю версий. Труды ACM по взаимодействию человека и компьютера. — 6. — 1–25. https://doi.org/10.1145/3555756.

Чарльз В.Л. Хилл, Стивен Л. Мак Шейн (2008). Принципы управления Опубликовано McGraw-Hill/Irwin, авторское право. — 2008 г. принадлежит McGraw-Hill Companies, Inc.

2023 Developer Survey [сайт]. URL.: https://survey.stackoverflow.co/2023/#overview

REFERENCES:

Charles W.L. Hill, Steven L. McShane (2008). Principles of management Published by McGraw-Hill/Irwin, Copyright. — 2008 by The McGraw-Hill Companies, Inc.

Carol L. Hoover, Mel Rosso-Llopart, Gil Taran (2009). Evaluating Project Decisions: Case Studies in SE. Published Oct 27. — 2009 by Addison-Wesley Professional.

Doerry Norbert & Sibley Martina. (2015). Monetizing Risk and Risk Mitigation. Naval Engineers Journal. — 127. — 35–46.

N. Deepa, B. Prabadevi, L.B. Krithika and B. Deepa (2020). "An analysis on Version Control Systems," 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), Vellore. — India, 2020. — Pp. 1–9. DOI: 10.1109/ic-ETITE47903.2020.39.

Michael Keeling (2010). Reflections on Software Engineering: Threshold of Success. — Neverletdown, published on January 15. — 2010

Vanita Bhoola, S.B. Hiremath, Debasis Mallik (2014). An Assessment of Risk Response Strategies Practiced in Software Projects. Australasian Journal of Information Systems. — Volume 18. — Number 3. — 2014

Project Management Institute (2013). A Guide to the Project Management Body of Knowledge. Inc. 14 Campus Boulevard Newtown Square, Pennsylvania. — 19073-3299. — USA

Tom DeMarco (2018). The Deadline: A Novel About Project Management. 1st U.S. Edition, 2nd Printing. — 352 p. 2018. ISBN-13: 978-0932633392

Software Metrics (2000). Roadmap. Authors: Norman Elliott Fenton, Martin Neil. — 12c. September 2000 DOI:10.1145/336512.336588

Sterman S., Nicholas M. & Paulos E. (2022). Towards Creative Version Control. Proceedings of the ACM on Human-Computer Interaction. — 6. — 1–25. https://doi.org/10.1145/3555756.

Vatare A.S. & Adkar P. (2019). Review Paper on Centralized and Distributed Version Control System.

2023 Developer Survey [site]. — URL: https://survey.stackoverflow.co/2023/#overview

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Vol. 5. Is. 3. Number 19 (2024). Pp. 23–31
Journal homepage: https://journal.iitu.edu.kz
https://doi.org/10.54309/IJICT.2024.19.3.002

AUDIOSIGNAL BASED EVENT DETECTION USING DEEP LEARNING TECHNIQUES

Zh. Dosbayev[1,2*], L. Ilipbayeva[2], A. Suliman[3]

[1]U.A. Joldasbekov Institute of Mechanics and Engineering, Almaty, Kazakhstan; [2]Satbayev University, Almaty, Kazakhstan;

[3]INTI International University, Putra Nilai, Malaysia.
E-mail: zh.dosbayev@satbayev.university

Zhandos Dosbayev — PhD, researcher, [1]U.A. Joldasbekov Institute of Mechanics and Engineering, Almaty, Kazakhstan
E-mail: zh.dosbayev@satbayev.university, https://orcid.org/0000-0003-1673-4036;
Lyazzat Ilipbayeva — Satbayev University, associate professor, Almaty, Kazakhstan
E-mail: l.ilipbayeva@iitu.edu.kz, https://orcid.org/0000-0002-4380-7344;
Azizah Suliman — Associate professor, INTI University, Putra Nilai, Malaysia.
E-mail: azizah@uniten.edy.my, https://orcid.org/0000-0001-8486-3230.

© Zh. Dosbayev, L. Ilipbayeva, A. Suliman, 2024

Abstract. Deep learning has garnered significant interest from researchers for performing pattern recognition tasks. In particular, the detection of events based on audio signals and the recognition of natural sounds in the environment stand out. The DCASE challenge – Detection and Classification of Acoustic Scenes and Events – has further highlighted the efficiency of deep learning in accomplishing these tasks. This paper reviews the works of other researchers that applied various deep learning techniques to detect emergency events based on audio signals. It focuses on the complexity and specific challenges of recognizing polyphonic sound-based events. The use and structures of neural networks are presented, with an emphasis on the application of CNN and RNN for event detection based on audio signals. Evaluation metrics and an overview of datasets are also provided.

Keywords: Audio classification, deep learning, audio signals, neural networks, CNN, RNN

For citation: *Zh. Dosbayev, L. Ilipbayeva, A. Suliman. AUDIOSIGNAL BASED EVENT DETECTION USING DEEP LEARNING TECHNIQUES//INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES. 2024. Vol. 5. No. 19. Pp. 23–31 (In Eng.). https://doi.org/10.54309/IJICT.2024.19.3.002.*

Funding. *The research was funded by the Scientific Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (grant IRN AP14971555 Design and Implementation of Real-Time Safety Ensuring System in the Indoor Environment by Applying Machine Learning Techniques).*

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

ОҚИҒАЛАРДЫ АУДИОСИГНАЛДАР НЕГІЗІНДЕ ТЕРЕҢ ОҚЫТУ ӘДІСТЕРІ НЕГІЗІНДЕ АНЫҚТАУ

Ж. Досбаев[1,2*], Л. Илипбаева[2], А. Сулиман[3]

[1]Ө.А. Жолдасбеков атындағы механика және машинатану институты, Алматы, Қазақстан;

[2]Қ.И. Сәтбаев атындағы ҚазҰТЗУ, Алматы, Қазақстан;

[3]Халықаралық INTI университеті, Путра Нилаи, Малайзия.
E-mail: zh.dosbayev@satbayev.university

Жандос Досбаев — PhD, Зерттеуші, Satbayev университеті, Алматы, Қазақстан
E-mail: zh.dosbayev@satbayev.university, https://orcid.org/0000-0003-1673-4036;
Ляззат Илипбаева — Техника ғылымдарының кандидаты, Сәтбаев Университеті, доцент, Алматы, Қазақстан
E-mail: l.ilipbayeva@iitu.edu.kz, https://orcid.org/0000-0002-4380-7344;
Азиза Сулиман — Қауымдастырылған профессор, Халықаралық INTI университеті, Путра Нилаи, Малайзия
E-mail: azizah@uniten.edy.my, https://orcid.org/0000-0001-8486-3230.

© Ж. Досбаев, Л. Илипбаева, А. Сулиман, 2024

Аннотация. Терең оқыту (deep learning) үлгілерді тану тапсырамаларын орындауда зерттеушілердің үлкен қызығушылық ие болып отыр. Соның ішінде, оқиғаларды аудиосигналдар негізінде анықтау және қоршаған ортадағы табиғи дыбыстарды тануды ерекше атап өтуге болады. DCASE challenge – Detection and Classification of Acoustic Scenes and Events шарасы терең оқытудың бұл тапсырмаларды орындауда тиімділігін айқындай түсті. Бұл жұмыста аудиосигналдар негізінде төтенше оқиғаларды анықтау, ол үшін түрлі терең оқыту әдістерін қолданған өзге зерттеушілердің жұмыстарына шолу жасалды. Әсіресе, полифониялық дыбыс негізіндегі оқиғаларды тану тапсырмасының күрделігі мен тапсырманы шешу ерекшеліктері қарастырылады. Нейрондық желілерді қолдану мен құрылымдары келтіріліп, аудиосигналдар негізінде оқиғаларды анықтау үшін CNN және RNN қолдану назарға алынады. Бағалау метрикалар мен мәліметтер дерекқорларға шолу жасалды.

Түйін сөздер: Аудиоклассификация, терең оқыту, аудиосигналдар, нейрондық желілер, CNN, RNN

Дәйексөз үшін: *Ж. Досбаев, Л. Илипбаева, А. Сулиман. ОҚИҒАЛАРДЫ АУДИОСИГНАЛДАР НЕГІЗІНДЕ ТЕРЕҢ ОҚЫТУ ӘДІСТЕРІ НЕГІЗІНДЕ АНЫҚТАУ// ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ. 2024. Т. 5. No. 19. 23–31 бет. (ағылшын тілінде). https://doi.org/10.54309/IJICT.2024.19.3.002.*

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

ОБНАРУЖЕНИЕ СОБЫТИЙ НА ОСНОВЕ АУДИОСИГНАЛОВ С ПРИМЕНЕНИЕМ ГЛУБОКОГО ОБУЧЕНИЯ

Ж. Досбаев[1,2*], Л. Илипбаева[2], А. Сулиман[3]

[1]Институт механики и машиноведения имени академика У.А. Джолдасбекова, Алматы, Казахстан;

[2]КазНИТУ им. К.И. Сатпаева, г. Алматы, Казахстан;
Международный INTI университет, Путра Нилаи, Малайзия.
E-mail: zh.dosbayev@satbayev.university

Жандос Досбаев — PhD, исследователь, Институт механики и машиноведения имени академика У.А. Джолдасбекова, Алматы, Казахстан
E-mail: zh.dosbayev@satbayev.university, https://orcid.org/0000-0003-1673-4036;
Ляззат Илипбаева — кандидат технических наук, Университет имени Сатпаева, Алматы, Казахстан
E-mail: l.ilipbayeva@iitu.edu.kz, https://orcid.org/0000-0002-4380-7344;
Азиза Сулиман — ассоцированный профессор, Международный INTI университет, Путра Нилаи, Малайзия
E-mail: azizah@uniten.edy.my, https://orcid.org/0000-0001-8486-3230.

© Ж. Досбаев, Л. Илипбаева, А. Сулиман, 2024

Аннотация. Глубокое обучение вызывает большой интерес у исследователей при выполнении задач распознавания образов. В частности, стоит отметить выявление событий на основе аудиосигналов и распознавание природных звуков окружающей среды. Мероприятие DCASE challenge — Detection and Classification of Acoustic Scenes and Events — продемонстрировало эффективность глубокого обучения в выполнении этих задач. В данной работе проводится обзор исследований других авторов, которые применяли различные методы глубокого обучения для определения чрезвычайных событий на основе аудиосигналов. Особое внимание уделяется сложности задачи распознавания событий на основе полифонических звуков и особенностям решения этой задачи. Рассматривается применение и структура нейронных сетей, а также использование CNN и RNN для обнаружения событий на основе аудиосигналов. Приведен обзор метрик оценки и баз данных.

Ключевые слова: аудиоклассификация, глубокое обучение, аудиосигналы, нейронные сети, CNN, RNN

Для цитирования: *Ж. Досбаев, Л. Илипбаева, А. Сулиман. ОБНАРУЖЕНИЕ СОБЫТИЙ НА ОСНОВЕ АУДИОСИГНАЛОВ С ПРИМЕНЕНИЕМ ГЛУБОКОГО ОБУЧЕНИЯ//МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ. 2024. Т. 5. No. 19. Стр. 23–31. (На анг.). https://doi.org/10.54309/IJICT.2024.19.3.002.*

Introduction

Deep learning is being advanced based on performing complex tasks such as recognizing images, sounds, and speech text in various languages (Mohmmad et al., 2024: 1–43; Jiang Y. et al., 2024: 1–16; Li, 2022: 994–999; Zhang et al., – 2021: 107760). Deep learning refers to artificial neural networks with multiple levels of abstraction and several learning layers in data representation. It enhances efficiency in learning complex structures in large datasets by using backpropagation, determining how to adjust internal parameters to obtain

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

the expected signal in the output.

The task of audio signal based event detection (ASED) involves classification and recognition based on audio sounds in the natural environment, such as a baby crying, a person walking, or a dog barking. In other words, the main goal of sound-based event detection is to measure the start and end times of each event and provide a textual description alongside the audio recording. ASED consists of two main tasks: monophonic and polyphonic sound event detection. Monophonic sound event detection focuses on identifying the most prominent sound event at any given time, while polyphonic sound event detection identifies overlapping sound events occurring simultaneously with the primary sound event (Mesaros et al., 2016). Compared to monophonic ASED, polyphonic ASED is a more complex task due to the necessity of detecting all events happening at once and the presence of overlapping sounds. Figure 1 illustrates the polyphonic ASED task.

Currently, various methods are used to solve the ASED task. For instance, several ASED systems employ non-negative matrix factorization and Gaussian mixture models with hidden Markov models for polyphonic sound detection (He et al., 2021: 4160–4170; Wang, 2019; Heitola et al., 2013: 1–13). In recent years, many deep learning methods have been proposed for performing ASED tasks, establishing themselves as advanced techniques. In the work by Annamaria M. and other authors, a deep neural network architecture is utilized, achieving high accuracy (Mesaros et al., 2015: 151–155). However, while this architecture consists of several intermediate hidden layers, it is not particularly effective for processing input temporal sequences like video and audio due to its reliance on short time windows and instantaneous information.

To address this task more effectively, powerful neural networks such as convolutional neural networks (CNN) and recurrent neural networks (RNN) have been employed (Mesaros et al., 2015: 151–155; Jeong et al., 2017; Smailov, 2023; Al Dabel, 2024: 173–183; Al Dabel, 2024: 173–183; Momynkulov et al., 2024: 284–289; Lan et al., 2022). These have demonstrated very high efficiency in solving the ASED task in subsequent research works. Moreover, models trained using a combination of CNNs and RNNs have achieved outstanding results.

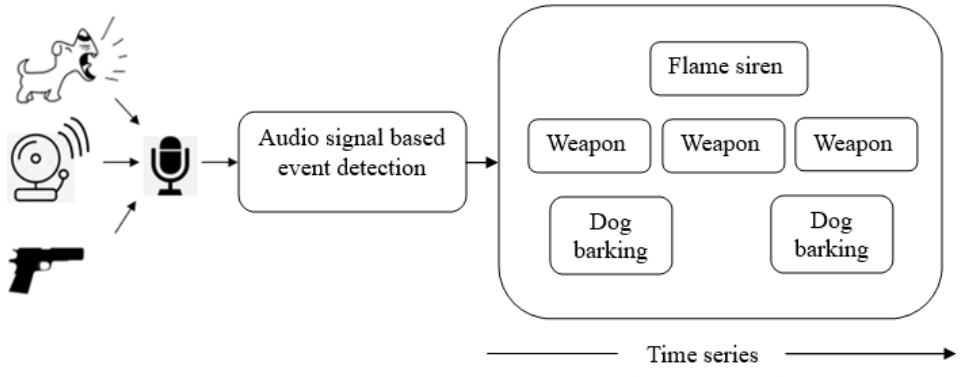


Fig. 1. Task of identifying polyphonic sound events

In this work, we will review the studies of other authors on the application of deep learning to solve the task of sound event detection (SED).

Deep learning

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

In this section, we describe deep learning, neural networks, convolutional neural networks (CNN), and recurrent neural networks (RNN).

Neural Networks

The fundamental structure of neural networks is organized in layers, forming artificial neural networks. The layers consist of neurons with internal connections that constitute the activation function. In turn, the connections between neurons have corresponding weights. Each neuron receives inputs that are multiplied by the connection weights and then calculated through a mathematical function. The mathematical function used determines the activation of the neuron.

In simple neural networks, neurons within a single layer do not connect to each other, but neurons in two adjacent layers are fully interconnected. Such layers are called fully connected layers. In many applications, at least three types of standard layers are required: the input layer, hidden layers, and the output layer. The input layer consists of D neurons, which is equal to the dimensionality of the input data. The hidden layer, positioned between the input layer and the output layer, performs intermediate computations for the network. A neural network is only called a deep neural network when it consists of multiple stacked hidden layers. As the number of hidden layers increases, the depth of the network also increases. To train neural networks, a backpropagation algorithm is used to optimize the effectiveness of neurons by adjusting the weights.

Although neural networks are found in many systems, they also exhibit drawbacks when applied to spatial and temporal structured data, such as text, images, video, audio, and sound text. Firstly, the structure of neural networks consists of fully connected layers with multiple parameters, and the number of parameters rapidly increases during training. This slows down the learning speed for spatial and temporal structured data. Secondly, each pair of neurons between two adjacent layers of a neural network has its own parameters, which hinders the ability to exploit the correlations in multi-dimensional spatial and temporal contexts. In contrast, CNNs and RNNs allow for the distribution of parameters among neurons, which helps overcome this limitation.

CNN

CNNs are a type of neural network architecture designed to address the shortcomings of neural networks when working with spatially structured data (LeCun, 1989). A CNN consists of three basic components: convolutional layers, pooling layers, and fully connected layers.

The convolutional layer performs convolution operations to obtain a set of linear activations. Each linear activation is then transformed into a nonlinear activation using functions like ReLU or tanh. In convolutional networks, local connections are used to take advantage of spatial-local correlations between neurons in adjacent layers. The size of these connections is controlled by hyperparameters known as the receptive field. The receptive field is a tensor with dimensions [w × h × depth] (w - width; h - height; depth - depth) that uses the same parameters applied to previous layers. The shared parameters in convolutional layers reduce the overall number of parameters in the network and improve computational efficiency.

Pooling layers are used after each convolutional layer to reduce the computational complexity of estimating the proposed size of the convolutional output. The pooling function divides its input data into sets of rectangles, with each piece providing the collective statistical value of neighboring input data. Using pooling is very effective for extracting the most informative data in a segment. There are several types of pooling functions: max pooling, L2

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

norm pooling, average pooling, and weighted average pooling. Among these, max pooling is the most commonly used in pooling layers.

Following the CNN, several convolutional and pooling layers are succeeded by fully connected layers. These layers in a CNN resemble the layers in standard neural networks, where neurons in adjacent layers are fully interconnected, while neurons within the same layer do not connect to each other.

RNN

Recurrent neural networks (RNNs) are neural networks used for processing sequential and temporal data. While the strength of CNNs lies in their ability to efficiently work with large spatially structured data with width and height, RNNs excel at handling very long sequences. In recurrent neural networks, interconnected hidden layers act like memory, gathering information from input sequences over time. Many recurrent networks can work with sequences of variable lengths.

Given an input vector sequence $x=(x_1, x_2, \ldots, x_n)$, a standard recurrent neural network computes a sequence of hidden activations $h=(h_1,h_2,\ldots,h_n)$ and a task vector $\hat{y}=(\hat{y}_1, \hat{y}_2,\ldots, \hat{y}_n)$:

$$h_s = f(W_{xh}h_t + W_{hh}h_{t-1} + b_h) \quad (1)$$

$$\hat{y}_t = g(W_{h\hat{y}}h_t + b_{\hat{y}}) \quad (2)$$

where: s=1,2,…, n represents time steps;;

, , - are weight matrices for the connections between layers (input and hidden layer; hidden to hidden layer; hidden and output layer);

, – are bias terms;

f and g are activation functions.

n deep recurrent neural networks consisting of multiple hidden layers, the first hidden layer takes the input vectors as its input, while each subsequent hidden layer takes the output of the previous layer as its input.

The recurrent connections between hidden blocks in standard recurrent neural networks allow the network to retain information from previous time steps. Therefore, recurrent neural networks are very suitable for accepting input sequences. However, the complexity of training recurrent neural networks to capture long-term dependencies arises from the tendency of gradients to vanish or explode across many layers. Exploding gradients can be easily managed by clipping the gradients element-wise before updating parameters in a mini-batch. In contrast, vanishing gradients are difficult to handle due to the long-term dependencies problem.

Methods such as LSTM (Long Short-Term Memory) and GRU (Gated Recurrent Unit) have been developed to address the vanishing gradient problem. LSTM and GRU architectures extend standard recurrent neural networks by replacing simple interconnected neurons with memory blocks that accumulate information. These memory blocks are better at capturing long-term dependencies in data consisting of time sequences.

Materials and methods

This section discusses the metrics used to evaluate the effectiveness of ASED systems. Additionally, we will compare the effectiveness of deep learning models used to solve ASED tasks and draw conclusions based on the methods. A brief description of the dataset

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

provided by the DCASE challenge will also be given.

Metrics

In ASED tasks, evaluations such as segment-based error rate and segment-based F1-score are used. The segment-based error rate is measured based on the number of errors in insertions (I), deletions (D), and substitutions (S) during the specified periods. A substitution is determined when an event in the given segment is detected but an incorrect label is provided. Once the number of substitutions in the segment is counted, the insertions are considered false positives in the system output, while deletions are treated as false negatives. Furthermore, the number of active true events in the segment is determined. The overall error rate is calculated as follows:

$$\mathrm{ERROR} = \frac{\sum_{k=1}^{K} S(k) + \sum_{k=1}^{K} D(k) + \sum_{k=1}^{K} I(k)}{\sum_{k=1}^{K} N(k)} \quad (3)$$

The second evaluation metric, the segment-based F1-score, is calculated based on three statistics: false positives, false negatives, and true positives. A false positive occurs when an event in the given segment is detected, but it does not exist in the corresponding segment of the labeled data; a false negative occurs when an event in the given segment is not detected, but it exists in the corresponding segment of the labeled data; and a true positive occurs when an event in the given segment is detected and it exists in the corresponding segment of the labeled data. These statistics are collected through the test data. Based on the collected statistics, precision (P-precision) and recall (R-recall) are calculated using the following equations::

$$\mathrm{Precision} = \frac{TP}{TP + FP}; \quad (4)$$

$$\mathrm{Recall} = \frac{TP}{TP + FN}; \quad (5)$$

$$F1 = \frac{2PR}{P + R} \quad (6)$$

Discussion and results

Dataset

In recent years, the TAU Urban Acoustic Scenes 2020 Mobile, Development dataset (Heittola et al., 2020) and the TAU Urban Acoustic Scenes 2020 3Class, Development dataset (Heittola et al., 2020), introduced by Tampere University at the DCASE challenge 2020 event, have been widely used for ASED tasks. Additionally, the list of datasets is updated and enhanced with new datasets every year.

The TAU Urban Acoustic Scenes 2020 Mobile, Development dataset contains data collected in twelve cities across Europe, within ten different acoustic environments, using four different devices. Based on the original recordings, synthetic data for eleven mobile devices was created. The recordings were captured using four main devices: Soundman OKM II Classic/studio A3, an electret binaural microphone, and a Zoom F8 audio recorder with 24-bit capacity and a 48 kHz sampling rate. Additionally, commonly available devices such as the Samsung Galaxy S7, iPhone SE, and GoPro Hero5 Session were used. The total duration of

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

the dataset is 64 hours, comprising 23,040 segments, with 13,965 segments used for training and 2,970 segments for testing.

Deep Neural Networks:

In (Mesaros et al., 2015: 151–155), the authors explore a multi-label feedback deep neural network for polyphonic ASED (Direction of Arrival) tasks. The study considers three different features: log mel-band energies, mel-band energies, and MFCC. The deep neural network consists of two hidden layers and eight hundred classifier blocks. The model is evaluated using natural environmental sounds, achieving an accuracy of 63.8 %, demonstrating a 20 % higher efficiency compared to (Wang, 2019).

CNN

1. In (Heitola et al., 2013: 1–13), the researchers apply convolutional neural networks (CNN) for the ASED task. Long-term and short-term audio signals are used as input features in the study. They employ a one-dimensional layer with sixty-four filters. The model shows excellent results in terms of error rate and F1-score.

RNN

Several studies have been conducted to solve the ASED task using recurrent neural networks (RNN) (Smailov, 2023; Al Dabel, 2024: 173–183; Al Dabel, 2024: 173–183; Momynkulov et al., 2024: 284–289; Lan et al., 2022).). Almost all of them employ bidirectional LSTM and GRU architectures. These architectures are powerful methods for reducing overfitting and capturing long-term dependencies. Compared to deep neural networks and convolutional neural network architectures, recurrent neural networks show a clear advantage when working with sequential input data.

CRNN

For the ASED task, audio signals are sequential data over time. Recurrent neural networks (RNNs) are based on processing time series data. They can relate information from previous time windows and, by moving backward through time, offer unlimited information. However, audio input features are known to be represented in both time and frequency. While RNNs perform well along the time dimension, CNNs can apply linear convolutional filters across both time and frequency. To leverage the advantages of both architectures, a combination of convolutional and recurrent neural networks (CRNN) is used (Heittola et al., 2020). As a result, CRNN demonstrates higher efficiency compared to all previously mentioned methods.

Conclusion

This work reviewed deep learning methods used to perform the ASED task. In recent years, deep learning methods have been widely adopted for this task due to their ability to achieve high accuracy. The features of standard neural networks, as well as CNN and RNN architectures, commonly used for solving considered task. The main steps of deep learning and the structural characteristics of neural networks were described by analyzing the works of other researchers. The advantages, disadvantages and challenges of the methods were discussed in the context of the ASED task. Evaluation metrics for the results obtained using these methods were presented, along with their equations. A brief description of the datasets presented at the DCASE challenge event in 2020, aimed at solving the ASED task, was provided. Additionally, the results achieved by researchers for each method were presented. The CRNN architecture, which combines recurrent and convolutional neural networks, was identified as the most effective method for solving the ASED task.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

REFERENCES

M. Al Dabel M. Diffusion-Based (2024). Convolutional Recurrent Neural Network for Improving Sound Event Detection //International Congress on Information and Communication Technology. — Singapore: Springer Nature Singapore, 2024. — Pp. 173–183.

Heittola Toni, Mesaros Annamaria & Virtanen Tuomas (2020). TAU Urban Acoustic Scenes 2020 Mobile, Evaluation dataset [Data set]. — Zenodo. https://doi.org/10.5281/zenodo.3685828

Heittola Toni, Mesaros Annamaria & Virtanen Tuomas (2020). TAU Urban Acoustic Scenes 2020. — 3Class. Development dataset [Data set]. — Zenodo. https://doi.org/10.5281/zenodo.3670185

He Y., Trigoni N., Markham A. (2021). SoundDet: Polyphonic moving sound event detection and localization from raw waveform //International Conference on Machine Learning. — PMLR, 2021. — Pp. 4160–4170.

T. Heitola, A. Mesaros, A.J. Eronen, T. Virtanen (2013). Context — dependent sound event detection. EURASIP J. Audio, Speech, Music Process. — Vol. 1. — Pp. 1–13.2013

Lan C., Zhang L., Zhang Y. et al. (2022). Attention mechanism combined with residual recurrent neural network for sound event detection and localization. J AUDIO SPEECH MUSIC PROC. **2022**. — 29. https://doi.org/10.1186/s13636-022-00263-6

Li Y. (2022). Research and application of deep learning in image recognition //2022 IEEE 2nd international conference on power, electronics and computer applications (ICPECA). — IEEE, 2022. — Pp. 994–999.

Mohmmad S., Sanampudi S.K. (2024). Exploring current research trends in sound event detection: a systematic literature review //Multimedia Tools and Applications. — 2024. — Pp. 1–43.

Mesaros A., Heittola T., Virtanen T. (2016). Metrics for Polyphonic Sound Event Detection. Applied Sciences. 2016. — 6(6). —162. https://doi.org/10.3390/app6060162

A. Mesaros, T. Heittola, O. Dikmen and T. Virtanen (2015). “Sound event detection in real life recordings using coupled matrix factorization of spectral representations and class activity annotations,” 2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). — South Brisbane, QLD, Australia, 2015. — Pp. 151–155. DOI: 10.1109/ICASSP.2015.7177950.

Momynkulov Z., Omarov N., Altayeva A. (2024). CNN-RNN Hybrid Model for Dangerous Sound Detection in Urban Area //2024 IEEE 4th International Conference on Smart Information Systems and Technologies (SIST). — IEEE, 2024. — Pp. 284–289.

Jiang Y. et al. (2024). Sound event detection in traffic scenes based on graph convolutional network to obtain multi-modal information //Complex & Intelligent Systems. — 2024. — Pp. 1–16.

Jeong I., Lee S., Han Y. & Lee K. (2017). Audio Event Detection Using Multiple-Input Convolutional Neural. —Network. Workshop on Detection and Classification of Acoustic Scenes and Events.

Smailov N. et al. (2023). A novel deep CNN-RNN approach for real-time impulsive sound detection to detect dangerous events //International Journal of Advanced Computer Science and Applications. — 2023. — V. 14. — №. 4.

Zhang X., Wang L., Su Y. (2021). Visual place recognition: A survey from deep learning perspective //Pattern Recognition. — 2021. — T. 113. — P. 107760.

Wang D., Wang X., Lv S. (2019). An Overview of End-to-End Automatic Speech Recognition. Symmetry. 2019. —11(8). —1018. https://doi.org/10.3390/sym11081018

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Vol. 5. Is. 3. Number 19 (2024). Pp. 32–48
Journal homepage: https://journal.iitu.edu.kz
https://doi.org/10.54309/IJICT.2024.19.3.003
УДК: 004.85, 004.

MATHEMATICAL APPROACH OF THE BACKPROPAGATION METHOD FOR CONSTRUCTING ARTIFICIAL NEURAL NETWORKS

A.B. Yemberdiyeva[1]*, I.C. Young[2], S.Ye. Mamanova[1], S.B. Mukhanov[1]
[1]International Information Technology University, Almaty, Kazakhstan;
[2]Gachon University Seoul, Republic of Korea.
E-mail: s.mukhanov@edu.iitu.kz

Aknur Yemberdiyeva — Master in CSSE, lecturer, Computer Engineering, International Information Technology University
E-mail:a.yemberdiyeva@iitu.edu.kz;
Young I. Cho — PhD Computer Science, Professor, Gachon University, Seoul, the Republic of Korea
E-mail: yicho@gachon.ac.kr
Symbat Mamanova — Doctoral (PhD) student Computer Engineering, senior-lecturer, International Information Technology University
E-mail: s.mukhanov@edu.iitu.kz,
Samat B. Mukhanov — PhD CSSE, assistant-professor, Computer Engineering, International Infor-mation Technology University
E-mail: s.mamanova@iitu.edu.kz

© A.B. Yemberdiyeva, I.C. Young, S.Ye. Mamanova, S.B. Mukhanov, 2024

Abstract. Backpropagation isthe core part of a neural network. This method is used to efficiently train a network using a chain rule that allows differentiation of complex functions. In other words, after each pass through the network, the backpropagation method performs a backward pass to adjust the model parameters, such as weights and biases. This article highlights the importance of using the backpropagation method from the point of view of mathematical formulas for neural networks. The importance of using the backpropaga-tion learning algorithm to calculate the gradient (gradient descent) and the need to use the activation function to minimize the loss function is mathematically described and calculated by formulas, and also proven by calculating the matrix products of vectors for each layer of parameters - weights and biases and applying complex differential equations.

Keywords: backpropagation method; loss function; ANN (artificial neural network); gradient descent, activation function; weights; biases; parameters

For citation: *A.B. Yemberdiyeva, I.C. Young, S.Ye. Mamanova, S.B. Mukhanov. MATHEMATICAL APPROACH OF THE BACKPROPAGATION METHOD FOR CONSTRUCTING ARTIFICIAL NEURAL NETWORKS//INTERNATIONAL JOUR-NAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES. 2024. Vol. 5. No. 19. Pp. 32–48 (In Eng.). https://doi.org/10.54309/IJICT.2024.19.3.003.*

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

ЖАСАНДЫ НЕЙРОНДЫҚ ЖЕЛІЛЕРДІ ҚҰРУ ҮШІН КЕРІ ТАРАЛУ ӘДІСІНІҢ МАТЕМАТИКАЛЫҚ ТӘСІЛІ

А.Б. Ембердіева[1]*, I.C. Young[2], С.Е. Маманова[1], С.Б. Муханов[1]
[1]International Information Technology University, Almaty, Kazakhstan;
[2]Gachon University Seoul, Republic of Korea.
E-mail: s.mukhanov@edu.iitu.kz

Ақнұр Ембердиева — Магистр, Халықаралық ақпараттық технологиялар университетінің ком-пьютерлік инженерия кафедрасының оқытушысы
E-mail: a.yemberdiyeva@iitu.edu.kz;
I.C. Young — «Информатика» Ғылымдарының Кандидаты, Профессор, Гачон Университеті, Сеул, Корея Республикасы
E-mail: yicho@gachon.ac.kr;
Сымбат Маманова — «Есептеу техникасы» мамандығы бойынша докторант (PhD), халықара-лық Ақпараттық Технологиялар Университетінің аға оқытушысы
E-mail: s.mukhanov@edu.iitu.kz;
Самат Б. Мұханов — ОӘК PhD Докторы, халықаралық ақпараттық технологиялар универси-тетінің есептеу техникасы кафедрасының доценті
E-mail: s.mamanova@iitu.edu.kz

© А.Б. Ембердіева, I.C. Young, С.Е. Маманова, С.Б. Муханов, 2024

Аннотация. Кері таралу нейрондық желінің негізгі бөлігі болуы мүмкін. Бұл әдіс күрделі мүмкіндіктерді ажырата алатын тізбекті ережені пайдаланып желіні тиімді оқыту үшін қолданылады. Басқаша айтқанда, желі арқылы әрбір өтуден кейін кері таралу әдісі салмақтар мен ауытқулар сияқты модель параметрлерін реттеу үшін кері өтуді орындайды. Бұл мақала нейрондық желілер үшін математикалық формулалар тұрғысынан кері таралу әдісін қолданудың маңыздылығын көрсетеді. Математикалық сипатталған және формулалармен есептелген, сонымен қатар параметрлердің әрбір қабаты үшін векторлардың матрицалық туындыларын есептеу арқылы дәлелденген — салмақтар мен қиғаштықтар және күрделі дифференциалданған теңдеулерді қолдану) градиентті (градиенттің төмендеуі) және есептеу үшін кері таралуды оқыту алгоритмін пайдаланудың маңыздылығы. функцияның жоғалуын азайту үшін белсендіру функциясын пайдалану қажет.

Түйін сөздер: кері таралу әдісі; жоғалту функциясы; ANN (Жасанды нейрондық желі); градиенттің түсуі, белсендіру функциясы; салмақ; ығысулар; параметрлері

Дәйексөз үшін: *А.Б. Ембердіева, I.C. Young, С.Е. Маманова, С.Б. Муханов. ЖАСАНДЫ НЕЙРОНДЫҚ ЖЕЛІЛЕРДІ ҚҰРУ ҮШІН КЕРІ ТАРАЛУ ӘДІСІНІҢ МАТЕМАТИКАЛЫҚ ТӘСІЛІ//ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ. 2024. Т. 5. No. 19. 32–48 бет. (ағылшын тілінде). https://doi.org/10.54309/IJICT.2024.19.3.003.*

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

МАТЕМАТИЧЕСКИЙ ПОДХОД МЕТОДА ОБРАТНОГО РАСПРОСТРАНЕНИЯ ДЛЯ ПОСТРОЕНИЯ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

А.Б. Ембердиева[1]*, I.C. Young[2], С.Е. Маманова[1], С.Б. Муханов[1]
[1]International Information Technology University, Almaty, Kazakhstan;
[2]Gachon University Seoul, Korea.
E-mail: s.mukhanov@edu.iitu.kz

Акнур Ембердиева — магистр CASE, преподаватель кафедры компьютерной инженерии Международного университета информационных технологий
E-mail: a.yemberdiyeva@iitu.edu. kz;
I.C. Young — доктор философии по специальности «Компьютерные науки», профессор Университета Гачон, Сеул, Республика Корея
E-mail: yicho@gachon.ac.kr
Сымбат Маманова — докторант по специальности «Компьютерная инженерия», старший преподаватель Международного университета информационных технологий
E-mail: s.mukhanov@edu.iitu.kz;
Самат Б. Муханов — доктор PhD, ассистент-профессор кафедры компьютерной инженерии Международного университета информационных технологий
E-mail: s.mamanova@iitu.edu.kz

© А.Б. Ембердиева, I.C.Young, С.Е. Маманова, С.Б. Муханов, 2024

Аннотация. Метод обратного распространения ошибки, вероятно, является основной частью нейронной сети. Этот метод применяется для эффективного обучения сети, используя цепное правило, которое позволяет дифференцировать сложные функции. Другими словами, после каждого прохода через сеть метод обратного распространения выполняет обратный проход, чтобы скорректировать параметры модели, такие как веса и смещения. В данной статье освящается важность применения метода обратного распространения ошибки с точки зрения математических формул для нейронных сетей. Математически описана и доказана расчетами матричных произведений векторов для каждого слоя параметров важность применения алгоритма обучения метода обратного распространения ошибок для вычисления градиента (gradient descent) и необходимость применения функции активаций для минимизации функции потерь.

Ключевые слова: метод обратного распространения; loss function; ANN (Artificial neural network); градиентный спуск, функция активации; веса; смещения; параметры

Для цитирования: *А.Б. Ембердиева, И.Чо. Янг, С.Е. Маманова, С.Б. Муханов. МАТЕМАТИЧЕСКИЙ ПОДХОД МЕТОДА ОБРАТНОГО РАСПРОСТРАНЕНИЯ ДЛЯ ПОСТРОЕНИЯ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ//МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ. 2024. Т. 5. No. 19. Стр. 32–48. (На анг). https://doi.org/10.54309/IJICT.2024.19.3.003.*

Introduction

Backpropagation is one of the well-known methods used for deep learning of feedforward neural networks, also called multilayer perceptrons. This method is related to supervised learning, which requires setting target values in training examples. In this article, we will consider what backpropagation is, how it is implemented, and its pros and cons (Mukhanov et al., 2020: 31–37).

Modern feedforward neural networks are used to solve many complex problems. In

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

training such networks using the backpropagation method, two types of passes are used: forward and backward. During the forward pass, the input vector is fed to the input layer of the network, after which the signals are propagated through the layers of the network, forming a set of output signals, which are the network's response to a given input image (Mukhanov et al., 2023: 16–27).

At this stage, all synaptic weights are fixed. The backward pass involves adjusting the synaptic weights according to error correction rules: the difference between the actual and desired outputs is calculated and an error signal is formed. This signal is then propagated back through the network, in the direction opposite to the direction of the synaptic connections. That is why this method is called the backpropagation algorithm. The weights are adjusted so that the network output signals are as close as possible to the desired values (Mukhanov et al., 2023: 15–27).

Problem, relevance

There are several issues and relevance aspects to consider with backpropagation:

Issues of backpropagation:

Vanishing gradient problem:

In deep neural networks, gradients can decrease exponentially during backpropagation, especially in layers closer to the input. This makes it difficult to train these layers and can lead to insufficient weight updates, which slows down or stops training (Kenshimov et al., 2021: 44–54).

Exploding gradient problem:

In some cases, gradients can increase too quickly, which can lead to instability in training and large fluctuations in weight values.

Dependence on hyperparameter selection:

The effectiveness of the method depends on the correct choice of hyperparameters, such as learning rate, regularization, and initialization of weights. Incorrectly setting these parameters can significantly worsen training results.

Time and computational resources:

Training deep neural networks using backpropagation is computationally expensive and time-consuming, especially when working with large amounts of data and complex models.

Local Minima:

The loss function may have many local minima, and backpropagation may get stuck in these local minima instead of finding the global minimum, resulting in suboptimal solutions (Uskenbayeva et al., 2020: 1–6; Bazarevsky et al., 2019; Vidyanova, 2022).

Relevance of Backpropagation:

A Foundational Method for Deep Learning:

Despite its limitations, backpropagation remains a fundamental and widely used method for training deep neural networks. Its efficiency and ease of implementation have made it a standard in the field of machine learning.

Support for Modern Architectures:

Backpropagation is the basis for many modern deep learning architectures, such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), and transformers.

Development of new methods and improvements:

The problems associated with backpropagation have inspired the development of new methods and improvements, such as optimizers (e.g., Adam, RMSprop), improved

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

weight initialization methods, and architectural innovations such as layer-wise normalization and dropout (Wang et al., 2020; Lee et al., 2020).

Importance to Practical Applications:

Backpropagation remains relevant due to its importance in practical applications of deep learning, including image processing, speech recognition, and natural language recognition, making it a key tool in modern AI systems (Bilgin et al., 2019; Kudubaeva et al., 2016; Liukai et al., 2022: 103364).

Thus, backpropagation plays a central role in training neural networks despite its existing problems and remains relevant and in demand in modern research and applications (Yuanguo et al., 2023: 103688; Baiju et al., 2023: 119042).

Materials and methods

A key stage in training neural networks involves using backpropagation algorithm, which correct errors through a process known as backpropagation. This technique applies gradient descent in multilayer feedforward networks. Its central idea is to efficiently compute the partial derivatives of the network function F (w, x) with respect to each element of the weight vector W, based on a given input vector X. The algorithm's goal is to determine the error gradient for all parameters in the model (Guoxiang et al., 2023: 118912; Laura-Bianca et al., 2023: 84–90; Yeo et al., 2013).

We will focus on standard fully connected networks for the classification task. However, many of these principles are also relevant to other types of neural networks and to any differentiable computational graphs in general. When computing within a single fully connected layer, let us first consider working with row-oriented vectors instead of column-oriented ones:

$$x = [x_1 \;\; x_2], \tag{1}$$

$$h = [h_1 \;\; h_2 \;\; h_3], \tag{2}$$

$$b = [b_1 \;\; b_2 \;\; b_3], \tag{3}$$

Thus, the output vector h is calculated using the nonlinear activation function:

$$h = F(xW + b), \tag{4}$$

To calculate, for example, first component (element) of the vector h_1, you need to perform the following steps:

x_1 and x_2 for w_{11} and w_{21} from the matrix:

$$W = \begin{bmatrix} w_{11} & w_{12} & w_{13} \\ w_{21} & w_{22} & w_{23} \end{bmatrix}, \tag{5}$$

We get

$$h_1 = F(x_1 w_{11} + x_2 w_{21} + b_1), \tag{6}$$

In the same way, h_2 and h_3 are calculated.

Let us split the calculations of one layer into two stages: linear and nonlinear. Let us

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

assume that after the linear part we get a vector t. Then the nonlinear function applied to each element transforms it into the final vector h then, $t = xW + b$ $h = F(t)$. Let us break this down into components for one element:

$$t_1 = x_1 w_{11} + x_2 w_{21} + b_1, \quad (7)$$

$$h_1 = F(t_1), \quad (8)$$

In our case, it is important to realize that fully connected layers of a neural network are just special cases of computational graphs. Let us look at an example of a graph visualization for a fully connected layer in question. This will help us later understand how we navigate the graph during backpropagation.

The computation graph for a fully connected layer look like this. Nodes with data x, t and h, and to compute node t we need nodes with parameters w and b.

To optimize the parameters of a neural network using an optimization algorithm, we need the error gradient vector for all trainable parameters of our model:

$$\frac{\partial E}{\partial \Omega} = \left\{\frac{\partial E}{\partial w_1}, \frac{\partial E}{\partial w_2}, \frac{\partial E}{\partial w_2}, \dots\right\}, \quad (9)$$

The number of elements in the gradient corresponds to the number of trainable parameters, and for convenience we can divide the gradient into groups corresponding to different unions of parameters. For example, if we have a weight matrix W, we can consider it as a separate object with its own set of parameters, and therefore it is necessary to have a part of the gradient of the same size for it. Let us denote it as $\frac{\partial E}{\partial W}$ that is, as the partial derivative of the error E with respect to the matrix W for our current layer. Similarly, for a vector b, the corresponding part of the gradient is $\frac{\partial E}{\partial b}$. For each layer and for each object, we train them with parameters: for b_1 it will be $\frac{\partial E}{\partial b_1}$, for W_2 it will be $\frac{\partial E}{\partial w_2}$, for b_2 it will be $\frac{\partial E}{\partial b_2}$. Thus, it is a scalar, a vector, a matrix, or a tensor.

It is important to realize that in most cases the learning algorithm, such as Stochastic Gradient Descent, and the gradient computation algorithm (BACKPROP) can be completely independent. The learning algorithm wants to get the gradient, and it does not care how it was computed. In the process of computing the gradient, we do not care how it will be used during training. So, Let us focus on computing the gradient. Suppose that this layer is part of a certain model that we are training, and we need to find $\frac{\partial E}{\partial W}$ and $\frac{\partial E}{\partial b}$. For this layer, we use the Chain Rule from calculus and work backwards. Let us assume that we are already given $\frac{\partial E}{\partial h}$

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

in numerical form. That is, given the input to the network with given weights, we got $\frac{\partial E}{\partial h}$. Its dimension is the same as the vector h, that is, it is a row vector of three elements:

$$\left[\frac{\partial E}{\partial h_1} \quad \frac{\partial E}{\partial h_2} \quad \frac{\partial E}{\partial h_3}\right], \tag{10}$$

Then we can calculate $\frac{\partial E}{\partial t}$. This will also be a vector of three elements, like the vector t. Now, understanding $\frac{\partial E}{\partial t}$, we can calculate $\frac{\partial E}{\partial w}$ and $\frac{\partial E}{\partial b}$, the quantities we need. These will have the same dimensions as the original matrices and vectors. $\frac{\partial E}{\partial w}$ – will be 2x3 matrix, $\frac{\partial E}{\partial b}$ –will be a vector of three elements. Additionally, we can also compute the gradient with respect to the input, $\frac{\partial E}{\partial x}$.

This is necessary to propagate the gradient back to the previous layer and preform similar computations for its parameters. Here, vector x is the input to our layer, and h is the output from the previous layer. In this example, $\frac{\partial E}{\partial x}$ consists of two-elements vectors.

Now, we need to compute and output these gradients in sequence.

Let us start with $\frac{\partial E}{\partial t}$, given that $\frac{\partial E}{\partial h}$ is available. The most accurate approach is to track the individual components of the gradient vector. For instance, consider $\frac{\partial E}{\partial t_1}$, which represents the partial derivative of the error function E with respect to t_1. We will utilize the fact that the error function E depends on h_1, and h_1 depends on t_1. Therefore, applying the chain rule:

$$\frac{\partial E}{\partial t_1} = \frac{\partial E}{\partial h_1} \cdot \frac{\partial h_1}{\partial t_1}, \tag{11}$$

It all comes down to numerical calculations. It would be beneficial to fully write out the derivative using the rule for differentiating a complex function with multiple variables, considering the intermediate variables that link t_1 with the error E. However, from the diagram, it is evident that this connection is only through h_1, while h_2 and h_3 are independent of t_1.Therefore, no additional explanation is needed. Now, Let us examine the results we have obtained:

$$\frac{\partial E}{\partial t_1} = \frac{\partial E}{\partial h_1} \cdot \frac{\partial h_1}{\partial t_1} = \frac{\partial E}{\partial h_1}, \tag{12}$$

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

What does $\frac{\partial h_1}{\partial t_1}$. As shown, $\frac{\partial h_1}{\partial t_1}$ is connected through the scalar function $h_1 = F(t_1)$. This means that $\frac{\partial h_1}{\partial t_1}$ is simply the derivative of the function F evaluated at t_1:

$$\frac{\partial E}{\partial t_1} = \frac{\partial E}{\partial h_1} \cdot \frac{\partial h_1}{\partial t_1} = \frac{\partial E}{\partial h_1} \cdot F'(t_1), \quad (13)$$

subsequently, in a similar manner

$$\frac{\partial E}{\partial t_2} = \frac{\partial E}{\partial h_2} \cdot F'(t_2) \quad \text{и} \quad \frac{\partial E}{\partial t_3} = \frac{\partial E}{\partial h_3} \cdot F'(t_3), \quad (14)$$

This is sufficient for calculating the vector $\frac{\partial E}{\partial t}$. However, this expression can be represented in a more compact form. In this case, we perform element-wise multiplication of the two vectors.

$$\frac{\partial E}{\partial h} = \left[\frac{\partial E}{\partial h_1} \quad \frac{\partial E}{\partial h_2} \quad \frac{\partial E}{\partial h_3}\right], \quad (15)$$

on a vector consisting of derivatives of the function at different points:

$$F'(t_1) = [F(t_1)' \quad F(t_2) \quad 'F(t_3)')], \quad (16)$$

This is equivalent to applying the function $F'(t)$ elementwise to the vector t. The resulting final vector then has the following gorm:

$$\frac{\partial E}{\partial t} = \frac{\partial E}{\partial h} \odot F'(t) \quad (17)$$

This vector also has three elements. Such an element-wise multiplication is often referred to as the Hadamard product. Thus, we have derived an expression for computing the vector $\frac{\partial E}{\partial t}$.

Next, Let us examine the gradient with respect to the matrix W.Similarly, we track the individual elements of the matrix and apply the chain rule of differentiation. We start with $\frac{\partial E}{\partial w_{11}}$. The weight w_{11} connects the input x_1 to the output t_1. Therefore, it does not contribute to t_2 or t_3. Consequently:

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

$$\frac{\partial E}{\partial w_{11}} = \frac{\partial E}{\partial t_1} \cdot \frac{\partial t_1}{\partial w_{11}}, \quad (18)$$

What is $\frac{\partial t_1}{\partial w_{11}}$. This represents the differential of t_1:

$$\frac{\partial E}{\partial w_{11}} = \frac{\partial E}{\partial t_1} \cdot \frac{\partial t_1}{\partial w_{11}} = \frac{\partial E}{\partial t_1} \cdot x_1, \quad (19)$$

Let us consider the derivative for another matrix element. We will start by changing the first index, which means we will move downwards:

$$\frac{\partial E}{\partial w_{21}} = \frac{\partial E}{\partial t_1} \cdot \frac{\partial t_1}{\partial w_{21}} = \frac{\partial E}{\partial t_1} \cdot x_2, \quad (20)$$

If we move along the columns and increase the second index, this weight now connects the input to the output t_2. Therefore, this derivative will be equal to:

$$\frac{\partial E}{\partial w_{12}} = \frac{\partial E}{\partial t_2} \cdot \frac{\partial t_2}{\partial w_{12}} = \frac{\partial E}{\partial t_2} \cdot x_1, \quad (21)$$

Similarly, we can apply the same approach to all other elements of the gradient $\frac{\partial E}{\partial w}$. It is important to note that there is a correlation between the weight index w and the indices x and t. The first index corresponds to the x index, while the second index corresponds to the t index. This process closely resembles matrix multiplication. In fact, we can compactly represent the final matrix $\frac{\partial E}{\partial w}$ using matrix multiplication. Let us consider:

$$x^T = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \quad (22)$$

$$\frac{\partial E}{\partial t} = \begin{bmatrix} \frac{\partial E}{\partial t_1} & \frac{\partial E}{\partial t_2} & \frac{\partial E}{\partial t_3} \end{bmatrix}, \quad (23)$$

then

$$\frac{\partial E}{\partial W} = x^T \cdot \frac{\partial E}{\partial t}, \quad (24)$$

Now that we have the gradients with respect to the weight matrix, Let us look at the vector $\frac{\partial E}{\partial b}$. The contribution to the first element comes solely from the component in t_1:

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

$$\frac{\partial E}{\partial b_1} = \frac{\partial E}{\partial t_1} \cdot \frac{\partial t_1}{\partial b_1} = \frac{\partial E}{\partial t_1} \cdot 1 \quad (25)$$

Similarly for the other two elements:

$$\frac{\partial E}{\partial b_2} = \frac{\partial E}{\partial t_2} \quad \text{и} \quad \frac{\partial E}{\partial b_3} = \frac{\partial E}{\partial t_3}, \quad (26)$$

then

$$\frac{\partial E}{\partial b} = \frac{\partial E}{\partial t} \quad (27)$$

Both vectors consist of three elements.

Now, the most crucial step: computing the gradient with respect to the input. This process will be more complex. We need to determine $\frac{\partial E}{\partial x}$, a two-element vector, given $\frac{\partial E}{\partial t}$. We start with $\frac{\partial E}{\partial x_1}$, as x_1 contributes to all elements of the vector t.

Next, we must apply the chain rule for differentiating a function of several variables. This will result in a sum over intermediate variables.

$$\frac{\partial E}{\partial x_1} = \frac{\partial E}{\partial t_1} \cdot \frac{\partial t_1}{\partial x_1} + \frac{\partial E}{\partial t_2} \cdot \frac{\partial t_2}{\partial x_1} + \frac{\partial E}{\partial t_3} \cdot \frac{\partial t_3}{\partial x_1}, \quad (28)$$

Note that a sum over all elements has appeared, which includes the contribution from $\frac{\partial E}{\partial x_1}$. By using the same relationships, we can obtain the corresponding weights W:

$$\frac{\partial t_1}{\partial x_1} = w_{11}, \frac{\partial t_2}{\partial x_1} = w_{12}, \frac{\partial t_3}{\partial x_1} = w_{13}, \quad (29)$$

These weights are precisely those that connect x_1 to t_1, t_2 and t_3:

$$\frac{\partial E}{\partial x_1} = \frac{\partial E}{\partial t_1} \cdot w_{11} + \frac{\partial E}{\partial t_2} \cdot w_{12} + \frac{\partial E}{\partial t_3} \cdot w_{13}, \quad (30)$$

Similarly, for x_2 there will already be other weights w:

$$\frac{\partial E}{\partial x_2} = \frac{\partial E}{\partial t_1} \cdot w_{21} + \frac{\partial E}{\partial t_2} \cdot w_{22} + \frac{\partial E}{\partial t_3} \cdot w_{23}, \quad (31)$$

Let us also note the hidden matrix multiplication here and express everything in a

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

compact form:

$$\frac{\partial E}{\partial x} = \frac{\partial E}{\partial t} \cdot W^T \quad . \qquad (32)$$

Now we understand how to find gradients for the parameters of a fully connected layer and, furthermore, how to propagate the gradients to the previous layer to perform similar computations for its parameters, etc. To do this, we calculated $\frac{\partial E}{\partial x}$. However, it is not clear what assumptions we have made about knowing $\frac{\partial E}{\partial h}$. If we have $\frac{\partial E}{\partial h}$ for the final layer, we can sequentially compute all gradients for the preceding layers. So, how do we obtain $\frac{\partial E}{\partial h}$, from which we need to start? Since this is the last layer, its output is related to the final error E. We need to compute the corresponding derivative. In the final layer, we do not use an activation function, so our task reduces to finding $\frac{\partial E}{\partial t}$, and we will proceed from there. To do this, we need to understand how the final t is related to the error E. After performing certain operations, we should obtain a one-dimensional array(scalar) E, the error, which always represents a single number, regardless of other factors. To start, Let us compute the final predictions of our model:

$$Z = \text{Softmax}(t) = S(t) = \left\{\frac{e^{t_i}}{\sum_j e^{t_i}}\right\} \quad , (33)$$

We applied the exponential function to each element of the vector, mapping them monotonically to the range from zero to positive infinity. We then divided by the sum to ensure that the final probabilities sum to one. Now that we have the probabilities provided by the neural network as its output, we can calculate the prediction error. For this, we also need the known correct answer, which we will denote as y. Recall that y is a vector of zeros with one in the position corresponding to the index of the correct class (in this case, 0,1 or 2). This represents the true distribution we aim to match with the given neural network input. The error can then be calculated as follows:

$$E = \text{CrossEntropy}(z,y) = -\sum_i y_i \ln z_i \quad , \qquad (34)$$

y – is the correct answer, z – is the output from Softmax.

Thus, we have a combination of Softmax and CrossEntropy in this case we can substitude one into the other, simplify, and the differentiation process will be simplified:

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

$$E = \text{CrossEntropy}(S(t), y) = -\sum_i y_i \ln \frac{e^{t_i}}{\sum_j e^{t_j}} = -\sum_i y_i \left(t_i - \ln \sum_j e^{t_j}\right) = -\sum_i y_i t_i + \sum_i y_i \ln \sum_j e^{t_j} =$$

$$-\sum_i y_i t_i + \ln \sum_j e^{t_j}$$

, (35)

We derived a straightforward relationship between E and t:

$$E = \text{CrossEntropy}(S(t), y) = -\sum_i y_i t_i + \ln \sum_j e^{t_j}$$

, (36)

We can calculate the required vector $\frac{\partial E}{\partial t}$. Let us express one of its elements:

$$\frac{\partial E}{\partial t_k} = -y_k + \frac{1}{\sum_j e^{t_k}} \cdot e^{t_k}$$

, (37)

If we examine closely, this corresponds to one of the Softmax elements:

$$\frac{\partial E}{\partial t_k} = -y_k + \frac{1}{\sum_j e^{t_k}} \cdot e^{t_k} = S(t)_k - y_k$$

, (38)

Now Let us express this for the entire vector:

$$\frac{\partial E}{\partial t} = S(t) - y = Z - y$$

, (39)

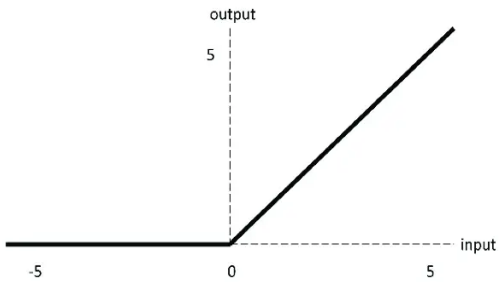
Activation Function: We will use one of the simplest and most popular functions, ReLU:

$$F(t) = \text{ReLU}(t) = \max(o, t)$$

, (40)

$$F'(t) = \begin{cases} 1, t \geq 0 \\ 0, t < 0 \end{cases}$$

, (41)



Picture 1 – Activation Function ReLU

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

Now that we have all the necessary information, we can put it together. Consider a neural network with two fully connected layers. It there are more layers, the process would be similar. Let us create a computational graph for this neural network- a feedforward graph. The input to the network is x, which is transformed into t_1. For this transformation, we need a matrix W_1 and a vector b_1:

$$t_1 = xW_1 + b_1, \tag{42}$$

In this context, the index refers to the layer number rather then element number as before. t_1 is transformed into h_1, which is the output of the first layer. This output is then fed into the second layer and transformed into t_2 using the matrix W_2 and the bias vector b_2:

$$h_1 = F(t_1), \tag{43}$$

$$t_2 = h_1 W_2 + b_2 \tag{44}$$

In the final layer, no activation function is applied. Instead, we directly obtain the probabilities Z using the $\mathrm{Softmax}$ function. We then compute the error using $\mathrm{CrossEntropy}$:

$$Z = S(t_2), \tag{45}$$

$$E = CE(z,y). \tag{46}$$

After computing the error, we proceed by calculating gradients in the reverse direction along the computational graph, which is the essence of the backpropagation algorithm.

We know how to determine $\frac{\partial E}{\partial t_2}$, t_2 – is the final vector t in the last layer. Given $\frac{\partial E}{\partial w_2}$, we can compute $\frac{\partial E}{\partial b_2}$, the two parameters of the second layer. We can also calculate $\frac{\partial E}{\partial h_1}$, the gradients at the output of the first layer, which allows us to find $\frac{\partial E}{\partial t_1}$. From we can then determine $\frac{\partial E}{\partial w_1}$ and $\frac{\partial E}{\partial b_1}$.

There is no need to compute $\frac{\partial E}{\partial x}$ since it is not propagated further. Now, Let us summarize everything we have derived so far:

$$\frac{\partial E}{\partial w_2} = S(t_2) - y = Z - y \tag{47}$$

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

$$\frac{\partial E}{\partial w_2} = h_1^T \cdot \frac{\partial E}{\partial t_2} \tag{48}$$

The next step is to calculate the derivative of the vector for the second layer:

$$\frac{\partial E}{\partial b_2} = \frac{\partial E}{\partial t_2} \tag{49}$$

Next, we calculate the derivative by multiplying by the weights for the first layer:

$$\frac{\partial E}{\partial h_1} = \frac{\partial E}{\partial t_2} \cdot W_2^T \tag{50}$$

Next, we calculate the derivative with the Hadamard product for the derivative of the vector function t of the first layer:

$$\frac{\partial E}{\partial h_1} = \frac{\partial E}{\partial h_1} \odot F'(t_1) \tag{51}$$

Then, we calculate x transposed by the derivative for the second layer:

$$\frac{\partial E}{\partial w_2} = x^T \cdot \frac{\partial E}{\partial t_2} \tag{52}$$

Finally, we complete the last step with derivatives for the second layer:

$$\frac{\partial E}{\partial b_1} = \frac{\partial E}{\partial t_1} \tag{53}$$

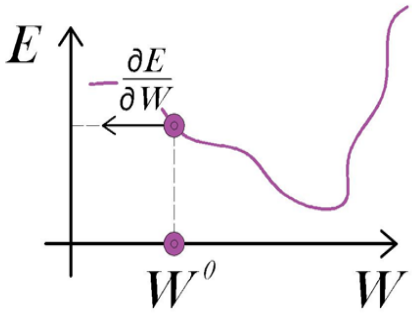
We have performed the calculations to determine the gradients using partial differential equations and the chain rule for complex functions, which involve computing gradients for matrices and vectors. This intricate and extensive process is part of the backpropagation algorithm. The upcoming chapters will cover the technical implementation of this algorithm in Python using machine learning libraries, including for convolutional and recurrent neural networks.

Next, we will visualize the results through graphs, starting with a depiction of the loss function (Picture 2).

Picture 2 – Loss function in the structure of neural networks

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

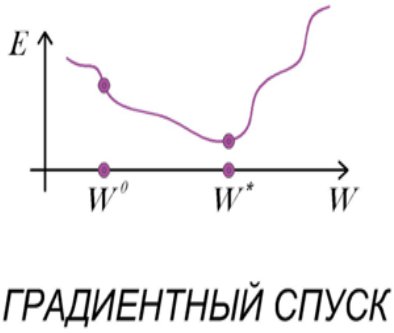
The following graph shows the error function being found:



Picture 3 – Error function in gradient

E – is the error function (cross-entropy), w – weight.

Then we calculate the gradients descent using the following 3.61.



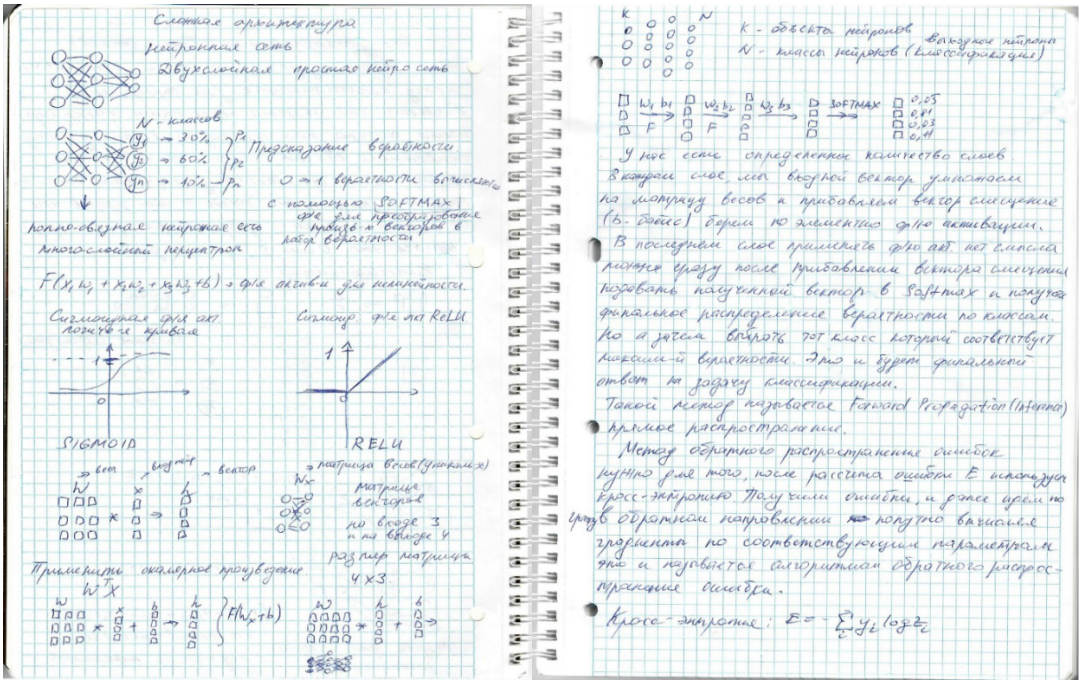
Picture 4 – Gradient descent

$$W^{t+1} = W^t - \alpha * \frac{\partial E}{\partial w} \cdot (W^t) \quad (54)$$

Where W – weights, α – is the learning rate, $\frac{\partial E}{\partial w}$ – is the gradient of the error, t – is a vector.

Below are records of the mathematical calculations, equation formulas, and concepts studied from textbooks on linear algebra, analytical geometry, mathematical analysis, statistics, mathematical logic, and algorithm theory, all of which are applied in neural networks.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License



Picture 5 – Calculations of complex architecture in layers of neural networks

In conclusion, all the mathematical calculations performed for each layer of neural networks have been visualized. The theoretical and analytical studies conducted will be further tested through experimental validation. Additionally, software for implementing recognition tasks will be developed.

Conclusion

The advantages of the method include its ease of implementation and resistance to outliers and anomalies in the data. However, there are also disadvantages:

- long training time;
- the possibility of “network paralysis”, when at large values the activation function falls into the sigmoid saturation region, and its derivative tends to zero, which slows down the weight update and slows down the learning process;
- a tendency to get stuck in local minima of the error function.

The introduction of this algorithm was an important step in the development of neural networks, as it is an effective method for training multilayer perceptrons from the point of view of computational processes. However, it would be a mistake to think that the algorithm offers an ideal solution to all possible problems.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

REFERENCES

Anna Vidyanova (2022). “In the USA, they are interested in the development of Kazakhs for the deaf”. — Capital. — 2022. https://kapital.kz/business/105455/v-ssha-zainteresovalis-razrabotkoykazakhstantsev-dlya-glukhikh.html.

Bazarevsky V., Fan Zh. (2019). On-device, real-time hand tracking with mediapipe. Google AI Blog. — Available at: https:// ai.googleblog.com/2019/08/on-device-real-time-hand-tracking-with.html.

Baiju Yan, Peng Wang, Lidong Du, Xianxiang Chen, Zhen Fang, YirongWu (2023). “mmGesture: Semi-supervised gesture recognition system using mmWave radar”. — 2023. — Vol. 213. — P. B. — P. 119042.

Bilgin M. & Mutludogan K. (2019). American Sign Language character recognition with capsule networks. Proceedings of the 3 rd International Symposium on Multidisciplinary Studies and Innovative Technologies. — Ankara, Turkey. https://doi.org/10.1109/ismsit.2019.8932829.

Guoxiang Tong, Yueyang Li, Haoyu Zhang, Naixue Xiong (2023). A Fine-grained Channel State Information-based Deep Learning System for Dynamic Gesture Recognition // Information Sciences. — 2023. — Vol. 636. — P. 118912.

Kenshimov C., Mukhanov S., Merembayev T., Yedilkhan D. (2021). A Comparison of Convolutional Neural Networks for Kazakh Sign Language Recognition Eastern-European // Journal of Enterprise Technologies. — 2021. — Vol. 5. — № 2. —113. — Pp. 44–54.

Kudubaeva S.A., Ryumin D.A. and Kalzhanov M.U. (2016). Support vector machine for sign speech recognition using the KINECT sensor. —Volume 91. — No. 3. (2016): Bulletin of KazNU. Series “Mathematics, mechanics, computer science”. https://bm.kaznu.kz/index.php/kaznu/article/view/541.

Lee A.R., Cho Y., Jin S. & Kim N. (2020). Enhancement of surgical hand gesture recognition using a capsule network for a contactless interface in the operating room. Computer methods and programs in biomedicine. — 190. — 105385. https://doi.org/10.1016/j.cmpb.2020.105385.

Liukai Xu, Keqin Zhang, Genke Yang, Jian Chu (2022). Gesture recognition using dual-stream CNN based on fusion of sEMG energy kernel phase portrait and IMU amplitude image // Biomedical Signal Processing and Control. — 2022. — Vol. 73. — P. 103364.

Laura-Bianca Bilius, Ştefan-Gheorghe Pentiuc, Radu-Daniel Vatavu (2023). TIGER: A Tucker-based instrument for gesture recognition with inertial sensors // Pattern Recognition Letters. — 2023. — Vol. 165. — Pp. 84–90.

Mukhanov S.B., Uskenbayeva R.K. (2020). Pattern Recognition with Using Effective Algorithms and Methods of Computer Vision Library // Advances in Intelligent Systems and Computing. — 2020. — №1. — Pp. 31–37.

Mukhanov Samat, Uskenbayeva Raissa, Im Cho Young, Dauren Kabyl, Les Nurzhan, Amangeldi Maqsat (2023). Gesture Recognition of Machine Learning and Convolutional Neural Network Methods for Kazakh Sign Language // — *Вестник Scientific Journal of Astana IT Univers ity.* — 2023. — Vol. 15. — Pp. 16–27.

Mukhanov S.B., Lee A.S., Zheksenov D.B., Yevdokimov D.D., Amirgaliev E.N., Kalzhigitov N.K., Kenshimov Sh. (2023). Comparative analysis of neural network models for gesture recognition methods hands // Bulletin of NIA RK. Information and communication technologies. — 2023. — No. 2(88). — Pp. 15–27.

Uskenbayeva R.K. & Mukhanov S.B. (2020). Contour analysis of external images. Proceedings of the 6th International Conference on Engineering & MIS 2020. — 1–6. https://doi.org/10.1145/3410352.3410811.

Wang Y., Wang H. & He X. (2020). Sign language recognition based on deep convolutional neural network”. — IEEE Access. — 8. — 64990–64999. 2020. https://doi.org/10.3390/electronics12040786.

Yuanguo Zhou, Shan Shui, Yijun Cai, Chengying Chen, Yingshi Chen, Reza Abdi-Ghaleh (2023). An improved all-optical diffractive deep neural network with less parameters for gesture recognition // — *Journal of Visual Communication and Image Representation.* — 2023. — Vol. 90. — P. 103688.

Yeo H.S., Lee B.G., Lim H. (2013). Hand tracking and gesture recognition system for human-computer interaction using low-cost hardware // Multimed. Tools Appl. — 2013. https://link.springer.com/article/10.1007/s11042-013-1501-1 01.11.2022.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Vol. 5. Is. 3. Number 19 (2024). Pp. 49–59
Journal homepage: https://journal.iitu.edu.kz
https://doi.org/10.54309/IJICT.2024.19.3.004

ANALYSIS OF ENERGY COSUMPTION IN THE NETWORK USING IOT SOLUTIONS

R. Lisnevskyi[1]*, M. Gladka[1], S. Biloshchytska[2]
[1]Taras Shevchenko National University of Kyiv;
[2]Astana IT University.
E-mail: lisa1304400@gmail.com

Lisnevskyi Rostyslav — PhD, professor Taras Shevchenko National University of Kyiv
E-mail: lisa1304400@gmail.com, https://orcid.org/0000-0002-9006-6366;
Gladka Myroslava — PhD, professor Taras Shevchenko National University of Kyiv
E-mail: miragla-dka@gmail.com, https://orcid.org/0000-0001-5233-2021;
Biloshchytska Svitlana — Doctor of Sciences, professor, professor Astana IT University
E-mail: bs-vetlana2007@gmail.com, https://orcid.org/0000-0002-0856-5474.

© R. Lisnevskyi , M. Gladka, S. Biloshchytska, 2024

Abstract. The article explores the importance of implementing IoT systems to analyze energy conditions in current locations. The designed system architecture ensures scalability and flexibility, which allows to effectively collect, save and analyze data. The research results confirm the hypothesis about the value of reduced control and optimization of energy consumption due to automated monitoring and compensation of reactive energy. A practical solution is being developed to automate the monitoring and balance of phase pressures, which promotes energy supply and reduces energy costs.

Keywords: sensors, energy management**,** IoT - internet of things, CEM - energy management system, API - application programming interface, CRUD – (create, read, update, delete), IDE - integrated development environment, ISO 50001 - international standard for energy efficiency management system, MDM - Meter Data Management

For citation: *R. Lisnevskyi, M. Gladka, S. Biloshchytska. ANALYSIS OF ENERGY COSUMPTION IN THE NETWORK USING IOT SOLUTIONS // INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES. 2024. Vol. 5. No. 19. Pp. 49–59 (In Eng.). https://doi.org/10.54309/IJICT.2024.19.3.004.*

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

IOT ШЕШІМДЕРІН ҚОЛДАНА ОТЫРЫП, ЖЕЛІДЕГІ ЭНЕРГИЯ ШЫҒЫНЫН ТАЛДАУ

Р. Лисневский[1]*, М. Гладка[1], С. Билощицкая[2]

[1]Тарас Шевченко Атындағы Киев Ұлттық Университеті;
[2]Астана IT Университеті.
E-mail: lisa1304400@gmail.com

Лисневский Ростислав — PhD, Профессор. Тарас Шевченко Атындағы Киев Ұлттық Университеті
E-mail: lisa1304400@gmail.com, https://orcid.org/0000-0002-9006-6366;
Гладка Мирослава — PhD, Профессор Тарас Шевченко Атындағы Киев Ұлттық Университеті
E-mail: miragladka@gmail.com, https://orcid.org/0000-0001-5233-2021;
Билощицкая Светлана — Ғылым Докторы, Профессор, Профессор Астана IT Университеті
E-mail: bsvetlana2007@gmail.com, https://orcid.org/0000-0002-0856-5474.

© Р. Лесневский, М. Гладка, С. Билощицкая, 2024

Аннотация. Мақалада Ағымдағы орындардағы энергия жағдайларын талдау үшін IoT жүйелерін енгізудің маңыздылығы қарастырылады. Жобаланған жүйенің архитектурасы деректерді тиімді жинауға, сақтауға және талдауға мүмкіндік беретін ауқымдылық пен икемділікті қамтамасыз етеді. Зерттеу нәтижелері реактивті энергияның автоматтандырылған мониторингі мен өтемақысы есебінен энергия тұтынуды төмендетілген бақылау мен оңтайландырудың мәні туралы гипотезаны растайды. Фазалық қысымның мониторингі мен тепе-теңдігін автоматтандыруға арналған практикалық шешім әзірленуде, бұл энергиямен жабдықтауға ықпал етеді және энергия шығындарын азайтады.

Түйін сөздер: Сенсорлар, Энергияны басқару, Заттар Интернеті IoT, CEM - энергияны басқару жүйесі, API - Қолданбалы Бағдарламалау Интерфейсі, CRUD - (Жасау, Оқу, Жаңарту, Жою), IDE – Интеграцияланған Даму Ортасы, ISO 50001 - энергия тиімділігін басқарудың халықаралық стандарты.жүйе, MDM - Есептегіш Деректерін Басқару

Дәйексөз үшін: *Р. Лесневский, М. Гладка, С. Билощицкая. IOT ШЕШІМДЕРІН ҚОЛДАНА ОТЫРЫП, ЖЕЛІДЕГІ ЭНЕРГИЯ ШЫҒЫНЫН ТАЛДАУ// ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ. 2024. Т. 5. No. 19. 49–59 бет. (ағылшын тілінде). https://doi.org/10.54309/IJICT.2024.19.3.004.*

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

АНАЛИЗ ЭНЕРГОПОТРЕБЛЕНИЯ В СЕТИ С ИСПОЛЬЗОВАНИЕМ IOT-РЕШЕНИЙ

Р. Лисневский [1]*, М. Гладка [1], С. Билощицкая[2]
[1]Киевский национальный университет имени Тараса Шевченко;
[2]Астанинский университет информационных технологий.
E-mail: lisa1304400@gmail.com

Лисневский Ростислав — кандидат технических наук, профессор Киевского национального университета имени Тараса Шевченко
E-mail: lisa1304400@gmail.com, https://orcid.org/0000-0002-9006-6366;
Гладка Мирослава — доктор философии, профессор Киевского национального университета имени Тараса Шевченко
E-mail: miragladka@gmail.com, https://orcid.org/0000-0001-5233-2021;
Билощицкая Светлана — доктор технических наук, профессор, профессор Astana IT University
E-mail: bsvetlana2007@gmail.com, https://orcid.org/0000-0002-0856-5474.

© Р. Лесневский, М. Гладка, С. Билощицка, 2024

Аннотация. В статье рассматривается важность внедрения систем интернета вещей для анализа состояния энергоснабжения в текущих местах. Разработанная архитектура системы обеспечивает масштабируемость и гибкость, что позволяет эффективно собирать, сохранять и анализировать данные. Результаты исследований подтверждают гипотезу о ценности снижения контроля и оптимизации энергопотребления за счет автоматизированного мониторинга и компенсации реактивной энергии. В настоящее время разрабатывается практическое решение для автоматизации мониторинга и балансировки фазных давлений, которое способствует энергоснабжению и снижает затраты на электроэнергию.

Ключевые слова: датчики, управление энергопотреблением, IoT - интернет вещей, CEM - система управления энергопотреблением, API - интерфейс прикладного программирования, CRUD – (создание, чтение, обновление, удаление), IDE - интегрированная среда разработки, ISO 50001 - международный стандарт для систем управления энергоэффективностью, MDM - управление данными счетчиков

Для цитирования: *Р. Лесневский, М. Гладка, С. Билощицка. АНАЛИЗ ЭНЕРГОПОТРЕБЛЕНИЯ В СЕТИ С ИСПОЛЬЗОВАНИЕМ IOT-РЕШЕНИЙ // МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ. 2024. Т. 5. No. 19. Стр. 49–59. (На анг.). https://doi.org/10.54309/IJICT.2024.19.3.004.*

Introduction

The new solution to IoT in the context of monitoring and managing energy consumption opens new horizons of possibilities for the place of their management. These technologies will ensure the automation of the processes of collecting data on stored energy, analyzing it, and promoting approaches to its effective recovery. Sensors and intelligent healers, located at various points in the energy infrastructure of a place, collect a large amount of data in real time. This data includes information about the energy generated by residential buildings, commercial facilities, and municipal installations, as well as energy management parameters. Analytical platforms that collaborate with IoT allow you to collect data, see trends, identify anomalies, and optimize the distribution and distribution of energy resources. Such in-depth analysis encourages the development and promotion of innovative methods of energy saving,

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

for example, adaptive control of street lighting, optimization of thermal measures, or automated control of energy consumption in households.

The stagnation of the Internet not only reduces energy consumption and saves money on the local budget, but also has a positive impact on the quality of life of the population. Through effective management of energy resources, the stability of energy supply will be ensured, tariffs for terminal residents will be reduced and the comfort of living in the middle class will be improved. In addition, the reduction in the vicinity of fossil fuels and the optimization of energy consumption result in a decrease in greenhouse gas emissions, which is a crucial step towards environmental safety and development.

Material and methods

Energy management is a vital component of the integrated management system at enterprises of any city and aims to optimize the use of energy resources. It covers the necessary tools, structural organization, and strategies to implement energy saving in accordance with corporate policy. The implementation of energy management systems at local enterprises will help increase control over energy consumption and reduce its costs within the framework of production cycles. Considering energy management as a set of management practices aimed at improving energy efficiency is different from other approaches, such as engineering or technical solutions. It is important to realize that the division into managerial and technical measures is conditional.

Effective use of energy resources at the enterprise can be achieved only under the condition of the interaction of management and technical measures, selected specifically for the needs of each specific case. Engineering innovations and technical improvements will certainly contribute to a more rational use of energy, but their integration into a structured management system at the enterprise will ensure the long-term effectiveness of the energy efficiency improvement process and the overall stability of the company's work.

In the traditional approach, energy management includes a set of functions that ensure the collection of important data about the main energy consumers, the efficiency of the use of resources in various processes and production lines, as well as about the possibilities of reducing energy consumption. Modern methods of managing energy consumption at enterprises often turn out to be insufficiently effective and require optimization. The key role in this process is played by the chief energy department, which, however, usually faces limitations in the resources and organizational structure necessary for in-depth analysis and control of energy consumption at all stages of production.

There is also a noticeable lack of technical means for comprehensive monitoring and evaluation of the efficiency of energy use at production sites. The current system of energy consumption management is characterized by the centralization of responsibility on one person - the chief energy engineer, who, without proper tools and support, is unable to effectively manage and optimize energy consumption processes. This emphasizes the need to develop and implement a new, more efficient energy resource management system, based on modern principles and technologies, capable of providing an organized and responsible approach to energy consumption.

First, it is necessary to determine the basis for the development of an energy consumption management system, to assess the current state of control over the use of energy in cities, to identify weak points in the existing energy accounting system and to propose ways to improve them. Energy consumption management includes the following steps:

- fixation of important parameters;

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

- comparison of received data with target indicators;
- determination of actions to correct the situation.

This technique is also applicable in the field of energy management, as shown in the practice of managing and regulating energy consumption at the global level (Voloshyn et al., 2023).

This management approach demonstrates high efficiency and can be adapted for energy management at any type of enterprise. The main concept of building these systems is based on the individual responsibility of department heads for the level of energy efficiency in their departments. The development of the system, considering the unique features of a particular enterprise, allows to achieve significant results in energy saving.

The fact that energy audits do not lead to significant improvements can be explained by the fact that the review of energy consumption only provides a snapshot of the situation and does not ensure long-term preservation of high energy efficiency. Practice shows that only some of the recommended measures are implemented after the energy audit. Usually, these are the initiatives that have a solid foundation and are the basis for the business of energy service companies (ESCOs), while other proposals lose their relevance over time and are forgotten (Brych et al., 2023).

Changes in technologies, the introduction of energy-saving initiatives and the use of more efficient equipment should lead to a decrease in specific energy consumption in CHPs. Accordingly, it is necessary to adjust the planned indicators, considering these changes, toto establish new target indicators that will reflect the actual situation in the management objects (Dreshpak et al., 2023).

The management system is characterized by a closed loop, where the interaction between the adopted measures for improvement and the object of management is ensured through effective feedback. The development of effective mechanisms to provide this feedback is critical to the functioning of the system, and its absence can lead to its inefficiency. The system involves the active interaction of personnel involved in its work, and not just automated management.

The success of the implementation of the energy management system depends on the support of the company's management, where active participation and initiative determine the direction of further actions, whether it will be the continuation of reforms or the limitation of only formal documentation. However, the key role in this process is played by the energy manager - the person responsible for managing and optimizing energy efficiency at the enterprise (Oryshchyn et al., 2016).

Energy consumption monitoring allows you to promptly track changes in energy supply and assess the energy efficiency of production processes for accurate assessment of achieved results. The transfer of responsibility for energy consumption to the level of the company's subdivisions strengthens control and expands its functions, contributes to timely detection and correction of problems. The highest, fifth, level of control is achieved when implementing full-fledged energy management, which is based on the principles of system control and regulation of energy consumption, thereby realizing all its advantages (Logutova et al., 2011).

The essence of the ISO 50001 international standard is to assist organizations in creating structured systems and procedures aimed at improving the efficiency of using energy resources. This includes considering the intensity of energy consumption and the amount of energy used. The use of this standard aims not only to reduce greenhouse emissions, but also

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

to optimize energy consumption through a systematic approach to energy management. It enables companies equipped with the necessary information about their energy consumption to set goals, develop effective strategies and plans to optimize energy use, while considering current legislation (Denisyuk et al., 2015).

In accordance with the requirements of the DSTU ISO 50001 standard, first of all, it is necessary to identify all the main energy-consuming departments, processes, equipment and mechanisms, and then to determine the energy base, which will be formed on the basis of key energy and production indicators for the base period. The energy consumption management system (EMS) should include documented confirmation of the process of developing such an energy base (Danilkova et al., 2015).

To analyze the efficiency of energy use and the degree of achievement of the set goals, it is necessary to establish energy efficiency indicators. These indicators should be regularly updated and compared with previous indicators of energy consumption.

One of the effective approaches to energy consumption management is the use of the target energy monitoring (TEM) method, which is widely implemented in large industrial facilities in Western Europe and the USA and is part of their overall management structure. According to the estimates of the British Energy Efficiency Agency, the implementation of the CEM method can reduce energy costs by 10-20% without the need for additional investments in modernization. Implementation of CEM is often recommended as a primary step in comprehensive energy efficiency improvement programs.

The relevance of research and deployment of energy consumption analysis systems based on IoT technologies in modern cities is explained by a number of key factors. First, global energy challenges require a focus on reducing the carbon emissions of human activity. This applies not only to industrial production, but also to the everyday life of city dwellers. Climate change and its consequences force us to reconsider approaches to the use of energy resources, emphasizing the need for more efficient use of them.

The next factor that emphasizes the relevance of this issue is the growing need to optimize the use of available energy resources. Every year, the demand for energy in cities is growing, which requires city administrations and their residents to implement innovative methods to ensure energy efficiency. Innovative solutions, such as IoT, pave the way for smart energy consumption management, allowing not only to monitor, but also to adapt energy consumption to actual needs.

Another important aspect is the modern development of technologies, which provides unique opportunities for the creation of efficient and scalable energy consumption analysis and management systems. These technologies allow not only to collect data on energy consumption, but also to analyze them in real time, identify places of irrational use of resources and take measures to optimize them. The implementation of such systems is of great importance for the urban economy, ensuring its efficiency and sustainability, as well as improving the quality of life of residents.

Considering the above aspects, the importance of research and analysis of energy consumption systems using IoT solutions for modern cities is indisputable. This will not only increase energy efficiency, but also contribute to the sustainable development of urban areas, ensuring a balance between the needs of the present and the future requirements.

Discussion and results

In the process of system development, the key is the selection of technologies that best meet the needs of the project, guaranteeing its efficiency and adequacy. Such selection

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

involves an in-depth review of the existing range of technologies, analyzing their functionality, limitations, and degree of compliance with the unique requirements and goals of the project. Consideration should be given to aspects such as the scalability and flexibility of the system, the efficiency of data processing, the intuitiveness of the interface, and the level of personalization that the system can provide. In addition to technical parameters, the economic feasibility of the chosen solution, its compatibility with existing systems and ease of integration should also be evaluated. Attention to these criteria is a guarantee of high quality and the ability of the product to compete in the information technology market.

The choice of programming language is a critical decision at the initial stage of development of any project in the field of information technology. Each language has its own unique features that make it ideal for certain types of tasks. This overview examines Python, Java, and C#, focusing on their key features and applications. The choice of C# as the main programming language for our research justifies itself due to its performance and ability to work on different platforms with active support from Microsoft. This language is characterized by the ability to easily modulate and scale, which is key to developing programs that can be reliably adapted to changing requirements. In addition, the extensive library of resources and frameworks within the C# ecosystem provides greater efficiency in the development of complex control systems.

Among software development tools, integrated development environments (IDEs) play a key role in simplifying and optimizing the process of creating applications. They provide developers with powerful tools for coding, debugging, and testing applications, which greatly improves the productivity and quality of the final products. Among the most popular IDEs today are Microsoft Visual Studio, Visual Studio Code, and JetBrains Rider, each of which has its own unique features and advantages.

The choice of Visual Studio as the main integrated development environment for research was determined by its high adaptability and an expanded arsenal of tools that greatly facilitate the process of creating a software product. With a large number of project templates available, Visual Studio helps you get started and develop quickly, and code completion features help improve programming productivity. Its comprehensive debugging and testing capabilities help detect and eliminate errors in a timely manner, ensuring the high reliability of the developed applications. Graphic design tools that allow you to intuitively create user interfaces adapted to the specifics of construction and repair management are of particular value in Visual Studio.

Choosing a database management system (DBMS) is a key decision for any research that requires data storage, processing, and analysis. Each DBMS has its own characteristics, advantages, and limitations that should be considered in the context of specific research requirements. MS SQL Server, MySQL, and Oracle are three widely used DBMS that support a variety of applications from simple websites to complex enterprise systems. In this study, it was decided to use MS SQL Server as the key DBMS, due to its affiliation with Microsoft, a leading company in the field of software development. The choice in favor of MS SQL Server is due to its close integration with other Microsoft products, including Microsoft Office and SharePoint, which is an important aspect for companies that have already implemented these solutions in their business processes. In addition, MS SQL Server offers wide support for various programming languages, high security standards and reliability, thereby ensuring the stability of the system and protection against possible threats.

The Smart-MAIC sensor is a modern high-precision device designed to measure

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

various parameters of energy consumption. The sensor can conduct constant monitoring of energy consumption, which allows detecting anomalies and optimizing the use of energy resources. IoT Integration: Smart-MAIC easily integrates with other IoT devices and systems, making it an ideal solution for building comprehensive energy management systems.

In the research process, the three-level architecture in Fig. 1 was used, which is known for its high efficiency and adaptability in the distribution of various system functions. This approach was chosen to provide the system with a harmonious balance between ease of management, scalability, and performance.

The architecture divides the functionality of the system into three main levels: presentation, business logic and data access, where each level is responsible for its specific area of work in the system. The presentation layer creates a user-friendly interface that allows users to efficiently interact with the system while providing security by isolating user access from direct interaction with the database.

The business logic level focuses on processing and analytical work with data, using modern technologies and algorithms for analysis, which contributes to making informed decisions. Thanks to its modular structure, this level allows flexible modification and updating of algorithms without affecting the stability of the system.

At the data access level, the system's interaction with databases and other sources of information is managed, ensuring effective data collection, storage, and processing.

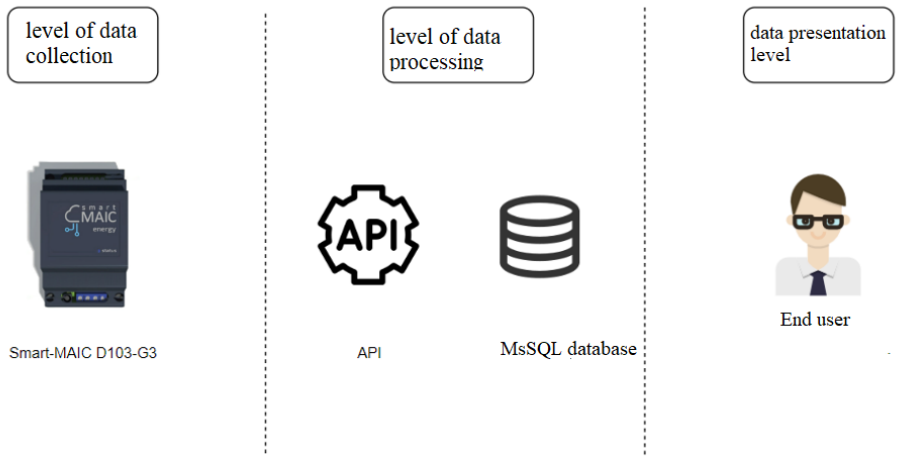


Fig. 1 - Architecture of the energy consumption analysis system

The control scheme of the energy consumption analysis system consists of the following components:

- database. A central repository for storing all data received from the monitoring system and the controller. The database serves as a basis for analysis, processing, and long-term storage of energy consumption information;

- monitoring system. Responsible for collecting energy consumption data from the electricity meter. The system analyzes the received data and sends it to the database for storage. Also provides communication with a personal computer for management and monitoring and cloud storage for data backup;

- controller (Smart-MAIC D103-G3). Receives information from the monitoring

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

system and performs system control and analysis. Can accept commands to perform certain actions based on data analysis. Also, it has direct access to the database to collect or update information;

- electricity meter. It measures the amount of electricity consumed and sends this information via Ethernet to the controller. Next, consumption data is forwarded to the monitoring system;

- a personal computer. It is used to manage and monitor the energy consumption analysis system. Provides a user interface allowing viewing of reports, system settings, and command execution;

The proposed research architecture demonstrates how system components interact with each other to collect, analyze, store, and manage energy consumption data, providing effective control and optimization of electricity use (Voronina et al., 2015).

Management of energy consumption analysis systems plays a key role in today's energy industry, helping to reduce costs and improve resource efficiency. In the context of growing demands for economy and environmental friendliness, as well as the constant growth of energy prices, accurate monitoring and management of energy consumption is becoming a decisive factor for businesses, residential complexes, educational institutions, and other institutions. Traditional approaches to measuring and analyzing energy consumption are often not flexible enough and do not provide the required granularity of data or agility in responding to changes.

Using the developed system for researching the analysis of energy consumption in the network, we obtain the data shown in Fig. 2.

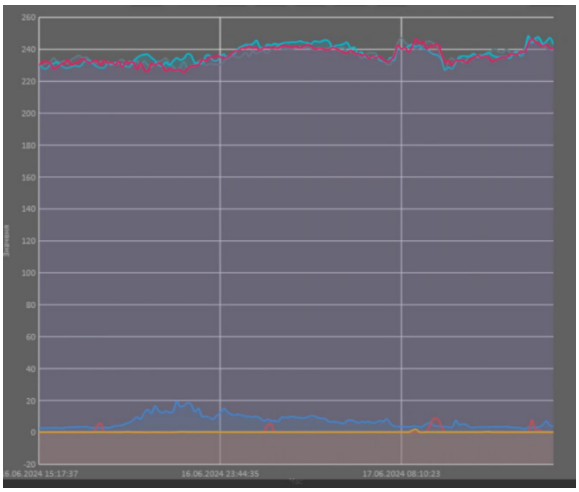


Fig.2 - Current and voltage graph for three phases

Based on the analysis of the graph, it can be concluded that the voltage in the system remains stable throughout the monitoring period, without significant deviations. The current shows several peaks, indicating a short-term increase in power consumption, due to the start of powerful devices or equipment. In general, the power supply system works reliably, with a normal level of voltage stability, but possible fluctuations in current consumption require additional control to prevent overloads. Such analyzes can be useful for monitoring the elec-

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

trical system to identify potential problems or to determine when and why system loads are increasing. Let us also examine the data from Fig. 3.

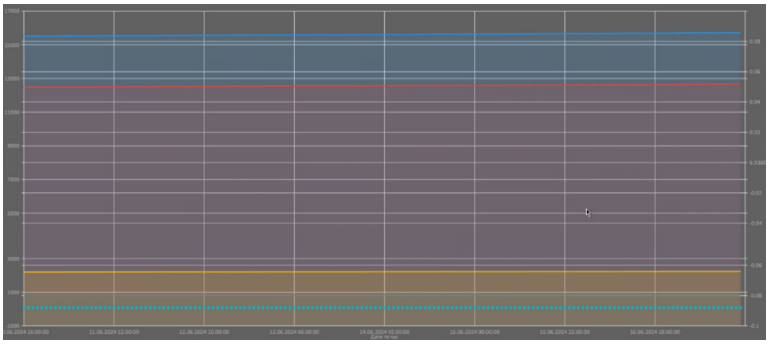


Fig. 3 - Graph with active and reactive energy in three phases

Fig. 3 shows the distribution of active energy between phases, with the largest load on phase L1. This indicates the unevenness of the phase loads, which can lead to inefficient operation of the power grid and possible overloads on individual components. Reactive energy has a relatively small value, but even such indicators can affect the overall efficiency of the system. Optimizing the system through phase balancing and reactive power correction will help improve performance and reduce losses. It is recommended to review the load distribution between phases and, if necessary, to implement reactive energy compensation measures to achieve better energy efficiency.

To increase the efficiency of energy consumption and reduce losses in the system, it is necessary to balance the load between phases, by redistributing the load and installing automatic balancers to avoid overloads and uneven energy consumption. Let us offer a general assessment of the efficiency of the energy system:

$E_{overall}$ — overall efficiency of the energy system.

E_{load} — load balancing efficiency.

E_{comp} — effectiveness of reactive energy compensation

$E_{monitoring}$ — effectiveness of monitoring and control systems.

Assume that all these factors have the same weighting factor (can be adjusted depending on importance). Overall efficiency can be calculated as an arithmetic mean:

$$E_{overall} = \frac{E_{load}+E_{comp}+E_{monitoring}}{3} \quad (1)$$

The proposed model will provide a comprehensive assessment of the impact of various measures on the overall efficiency of the energy system. Depending on specific needs, you can modify the model by adding additional factors or changing weighting factors. Implement measures to compensate for reactive energy, through the installation of capacitor banks or other compensating devices, which will increase the power factor and reduce losses. systems. These actions will help to optimize the operation of the electricity grid, reduce electricity costs, and ensure the stability of its supply.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

Conclusion

The study highlights the importance of implementing IoT systems to analyze energy consumption in modern cities, given the global energy challenges and growing ener-gy demand. The proposed architecture of the energy consumption analysis system provides scalability and flexibility, which allows efficient collection, storage, and analysis of data. The results confirmed the hypothesis that the use of IoT systems significantly improves the management and optimization of energy consumption. Data analysis demonstrated voltage stability, but also revealed current consumption peaks and phase load unevenness, highlight-ing the need for automated reactive energy monitoring and compensation to improve energy efficiency. This confirms that such systems contribute to more precise control and optimization of energy use in accordance with modern requirements. The practical contribution of the work consists in the development of specific solutions for the automation of monitoring, bal-ancing of phase loads and compensation of reactive energy, which contributes to improving the quality of energy supply and reducing energy costs.

Further research

For further research, it is recommended to study in detail the impact of different types of IoT sensors and data processing algorithms on the efficiency of energy management systems, and to explore integration with other smart city systems, such as smart lighting and transportation. The development of advanced energy management systems using IoT, cloud computing and artificial intelligence can make a significant difference by automating the collection, analysis, and monitoring of real-time data to quickly respond to problems and optimize energy consumption.

REFERENCES

Brych V., Fedirko M., Franchuk L., Mykytyuk V. (2017). Development of the energy service market: world experience and Ukrainian realities. —и2017. — 16 p.

N.S. Dreshpak, S.I. Vypanasenko, Dreshpak O.S. (2020). Accounting of electrical energy in systems for con-trolling the effectiveness of its use. Electrotechnical and information systems, —и2020. — 20 p.

Denisyuk S.P. (2015). ISO 50001: Objectives of the standard and prospects for its implementation in Ukraine. — K.: UNIDO, 2015. — 104 p.

Danilkova A.Yu. (2015). Peculiarities of implementation of energy efficiency benchmarking, as a toolkit of DSTU ISO 50001: 2014. — at industrial enterprises of Ukraine. ScienceRise. — 2015. — 28 p.

Logutova T.G., Poltoratska O.V. (2011). Some aspects of the development and formation of energy manage-ment in Ukraine. Bulletin of the Azov State Technical University. Ser.: Economic Sciences. — 2011. — 22 p.

Oryshchyn T.M. (2016). Optimization of energy resource management: methodological aspect. Scientific Bulletin of Ivano-Frankivsk National Technical University of Oil and Gas (Series: Economics and Management in the Oil and Gas Industry). — 2016. — 108 p.

Voronina O.S. (2015). Energy saving management system at housing and communal enterprises. Internet-con-ferences of XNUMX named after OM Beketova, — 2015. — 8 p.

Voloshyn M.M., Voloshyn S.M. (2013). System of energy consumption management and monitoring of energy resource costs. Collection of scientific works of Podilsk State Agrarian and Technical University. — 2013.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Vol. 5. Is. 3. Number 19 (2024). Pp. 60–70
Journal homepage: https://journal.iitu.edu.kz
https://doi.org/10.54309/IJICT.2024.19.3.005

MATHEMATICAL MODELS IN MEDICINE: MODERN APPROACHES TO DIAGNOSTIC PROCESS AUTOMATION

A. Myrzakerimova*, A.K. Khikmetov
Astana IT University, Astana, Kazakhstan.
E-mail: alua.myrzakerimova@astanait.edu.kz

Alua Myrzakerimova — Master of Technical Sciences, senior-Lecturer of the Department of Comput-er Engineering. Astana IT University, Astana, Kazakhstan
E-mail: alua.myrzakerimova@astanait.edu.kz; orcid. org/0000-0002-8500-1672;
Askar K. Khikmetov — Candidate of Physical and Mathematical Sciences, Rector, Astana IT Univer-sity, Astana, Kazakhstan
E-mail: akhikmetov@iitu.edu.kz, https://orcid.org/0000-0002-3045-7592.

© A. Myrzakerimova, A.K. Khikmetov, 2024

Abstract. Technology is becoming vital in improving diagnostic accuracy in modern medical field. The diagnostic process, like a production chain, consists of databases (resourc-es), the diagnostic activities (production), and the ultimate diagnosis (outcome). However, the intricacy of medical diagnostics has evolved due to the swift proliferation of medical knowledge and immense amount of patient data. Physicians encounter the complexity of handling huge volumes of clinical data,. To address these issues, the work examines the use of automated diagnostic systems supported by sophisticated mathematical models. The aim of the project is to investigate novel mathematical methods for disease detection and predic-tion, with a specific emphasis on fuzzy set theory. Particularly when dealing with imprecise or confusing initial data, such as medical histories and laboratory results, these techniques are indispensable. The authors investigate the function of expert systems and machine learning in the diagnosis of diseases such as gallstone formation and the detection of the diseases like sclerosis using medical imaging algorithms. These systems are specifically developed to as-sist medical professionals in making sound judgments, thereby presenting a very promising prospect for medical diagnostics through the integration of knowledge from several academic fields. The use of such technology will enhance clinical procedures, optimizing both the pre-cision and effectiveness of diagnoses while increasing healthcare accessibility .

Keywords: medical diagnostics, fuzzy set theory, automated systems, artificial neu-ral networks, expert systems, clinical decision-making

For citation: *A. Myrzakerimova, A.K. Khikmetov. MATHEMATICAL MODELS IN MEDICINE: MODERN APPROACHES TO DIAGNOSTIC PROCESS AUTOMA-TION // INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES. 2024. Vol. 5. No. 19. Pp. 60–70 (In Eng.). https://doi.org/10.54309/IJICT.2024.19.3.005.*

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

МЕДИЦИНАДАҒЫ МАТЕМАТИКАЛЫҚ МОДЕЛЬДЕР: ДИАГНОСТИКА ПРОЦЕСІН АВТОМАТТАНУДАҒЫ ЗАМАНАУ ТӘСІЛДЕР

А. Мырзакерімова*, А. Хикметов
Astana IT University, Астана, Казахстан.
E-mail: alua.myrzakerimova@astanait.edu.kz

Алуа Мырзакерімова — техника ғылымдарының магистрі, старший преподаватель департамента компьютерной инженерии. Astana IT University, Астана, Казахстан
E-mail: alua.myrzakeri-mova@astanait.edu.kz, https://orcid.org/0000-0002-8500-1672;
Аскар Хикметов — кандидат физико-математических наук, ректор Astana IT University, Астана, Казахстан
E-mail: akhikmetov@iitu.edu.kz, https://orcid.org/0000-0002-3045-7592.

© А. Мырзакерімова, А. Хикметов, 2024

Аннотация. Информатика технологиясы қазіргі заманғы медицина саласында диагностикалық дәлдікті арттыру үшін маңыздырақ болып келеді. Өндіріс тізбегіне ұқсас диагностикалық процесс мәліметтер қорынан (ресурстардан), диагностикалық әрекеттерден (өндіріс) және соңғы диагностикадан (нәтижеден) тұрады. Осыған қарамастан, медициналық диагностиканың күрделілігі медициналық білімнің жылдам таралуымен және пациенттер туралы деректердің үлкен көлемімен қатар дамыды. Дәрігерлер үлкен көлемдегі клиникалық деректермен жұмыс істеудің күрделілігіне тап болады, бұл қателіктер мен кемшіліктердің алдын алуда қиындық тудырады. Осы мәселелерді шешу үшін бұл жұмыс күрделі математикалық модельдермен қамтамасыз етілген автоматтандырылған диагностикалық жүйелерді пайдалануды зерттейді. Жобаның негізгі мақсаты анық емес жиындар теориясына ерекше назар аудара отырып, ауруларды анықтау және болжау үшін жаңа математикалық әдістерді зерттеу болып табылады. Әсіресе, клиникалық тарих және зертханалық нәтижелер сияқты дәл емес немесе шатастыратын бастапқы деректермен жұмыс істегенде, бұл әдістер өте қажет. Бұл жұмыс өт тастарының пайда болуы және медициналық бейнелеу алгоритмдері арқылы склероз сияқты ауруларды анықтау сияқты ауруларды диагностикалауда сараптамалық жүйелер мен машиналық оқытудың қызметін зерттеуге бағытталған. Бұл жүйелер медициналық мамандарға жақсы ақпараттандырылған пайымдаулар жасауға көмектесу үшін арнайы әзірленген, осылайша бірнеше академиялық пәндердегі білімдерді біріктіру арқылы медициналық диагностиканың өте перспективалы болашағын ұсынады. Мұндай технологияны қолдану клиникалық процедураларды жақсартуға, диагноздың дәлдігі мен тиімділігін оңтайландыруға және денсаулық сақтаудың қолжетімділігін арттыруға мүмкіндік береді.

Түйін сөздер: медициналық диагностика, анық емес жиындар теориясы, автоматтандырылған жүйелер, жасанды нейрондық желілер, сараптамалық жүйелер, клиникалық шешім қабылдау

Дәйексөз үшін: *А. Мырзакерімова, А. Хикметов. МЕДИЦИНАДАҒЫ МАТЕМАТИКАЛЫҚ МОДЕЛЬДЕР: ДИАГНОСТИКА ПРОЦЕСІН АВТОМАТТАНУДАҒЫ ЗАМАНАУ ТӘСІЛДЕР//ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ. 2024. Т. 5. No. 19.60–70 бет. (ағылшын тілінде). https://doi.org/10.54309/IJICT.2024.19.3.005.*

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

МАТЕМАТИЧЕСКИЕ МОДЕЛИ В МЕДИЦИНЕ: СОВРЕМЕННЫЕ ПОДХОДЫ К АВТОМАТИЗАЦИИ ДИАГНОСТИЧЕСКОГО ПРОЦЕССА

А. Мырзакерімова*, А. Хикметов
Astana IT University, Астана, Казахстан.
E-mail: alua.myrzakerimova@astanait.edu.kz

Алуа Мырзакерімова — магистр технических наук, старший преподаватель департамента компьютерной инженерии. Astana IT University, Астана, Казахстан
E-mail: alua.myrzakerimova@astanait. edu.kz, https://orcid.org/0000-0002-8500-1672;
Аскар Хикметов — кандидат физико-математических наук, ректор Astana IT University, Астана, Казахстан
E-mail: akhikmetov@iitu.edu.kz, https://orcid.org/0000-0002-3045-7592.

© А. Мырзакерімова, А. Хикметов, 2024

Аннотация. Информатика становится все более важной для повышения точности диагностики в современной медицинской сфере. Диагностический процесс, подобно производственной цепочке, состоит из баз данных (ресурсов), диагностических мероприятий (производства) и окончательного диагноза (результата). Тем не менее, сложность медицинской диагностики развивалась вместе с быстрым распространением медицинских знаний и огромным количеством данных о пациентах. Врачи сталкиваются со сложностью обработки огромных объемов клинических данных, что затрудняет предотвращение ошибок. Чтобы решить эти проблемы, в работе рассматривается использование автоматизированных диагностических систем, поддерживаемых сложными математическими моделями. Ключевой целью проекта является исследование новых математических методов обнаружения и прогнозирования заболеваний с особым акцентом на теорию нечетких множеств. Эти методы незаменимы, особенно при работе с неточными или запутанными исходными данными, такими как истории болезни и результаты лабораторных исследований. Авторы исследуют функции экспертных систем и машинного обучения в диагностике таких заболеваний, как образование желчных камней, и обнаружении таких недугов, как склероз, с использованием алгоритмов медицинской визуализации. Эти системы специально разработаны для того, чтобы помочь медицинским специалистам принимать обоснованные решения, тем самым представляя весьма многообещающую перспективу для медицинской диагностики посредством интеграции знаний из нескольких академических дисциплин. Использование такой технологии имеет возможность улучшить клинические процедуры, оптимизируя как точность, так и эффективность диагностики, одновременно увеличивая доступность здравоохранения.

Ключевые слова: медицинская диагностика, теория нечетких множеств, автоматизированные системы, искусственные нейронные сети, экспертные системы, принятие клинических решений

Для цитирования: *А. Мырзакерімова, А. Хикметов. МАТЕМАТИЧЕСКИЕ МОДЕЛИ В МЕДИЦИНЕ: СОВРЕМЕННЫЕ ПОДХОДЫ К АВТОМАТИЗАЦИИ ДИАГНОСТИЧЕСКОГО ПРОЦЕССА//МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ. 2024. Т. 5. No. 19. Стр. 60–70. (На анг.). https://doi.org/10.54309/IJICT.2024.19.3.005.*

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

Introduction

Nowadays information technology plays a vital part in a wide range of fields, including medicine, where it is becoming an essential instrument for enhancing the accuracy of diagnostic procedures. Modern medical profession is confronted with the difficulties that come with the processing of enormous amount of information, which results in an increased risk of making mistakes or overlooking crucial information. When faced with a situation like this, automated systems that are based on mathematical models save the day. By analyzing medical data and aiding physicians in the process of diagnosis, these systems are intended to dramatically decrease the amount of work while simultaneously improving the precision of conclusions.

The study explores innovative mathematical techniques for diagnosing and forecasting diseases. The newly devised mathematical diagnostic methods aim to support medical professionals in making sound decisions. Particularly, when faced with decision-making challenges involving uncertain initial data, such as medical information (clinical history, lab results, etc.), the use of fuzzy set theory appears to be the most suitable approach.

Materials and methods

Reviewed medical expert systems represent specialized software designed to assist healthcare professionals in making decisions. These systems empower doctors to validate their diagnostic hypotheses and to seek computer-based advice when faced with intricate diagnostic scenarios. Typically, the development of expert systems involves collaboration of a proficient medical expert, a mathematician, and a programmer. The primary responsibility for crafting such systems lies with the medical expert, as they have domain-specific knowledge and insight into the process. Expert systems allow making early preclinical diagnostics, and assessing the body's resistance and predisposition to diseases, including cancer.

Self-learning intelligent systems: Among expert medical systems, a special place belongs to so-called self-learning intelligent systems (SIS). They are based on methods for automatic classification of practical situations or learning by example. The most striking example of SIS is artificial neural networks.

An Artificial Neural Network (ANN) is a computational framework designed to process cognitive information by simulating the operations of the human brain. The basis of every Artificial Neural Network (ANN) is a simple structure, mostly consisting of identical components, like brain cells or neurons. Every individual neuron has a unique current state, like the excitatory or inhibitory states of neurons in the brain (Soheila et al., 2020: 23–47). A predictive approach for evaluating the probability of gallstone disease formation in persons with obesity was developed by P.L. Liew (Soheila et al., 2020: 23–47). The researchers performed a retrospective analysis that included anthropometric measures, medical histories, clinical evaluations, and laboratory findings from 117 individuals who had undergone surgery due to obesity. The artificial neural network (ANN) was built and trained using the backpropagation technique. The input dataset consisted of thirty variables comprising a range of clinical parameters including gender, age, body mass index, prior health problems, laboratory measurements, and histology. The objective of this strategy was to use artificial neural networks (ANNs) to systematically analyze complex patterns in the gathered data and finally forecast the likelihood of gallstone disease in overweight persons.

In medical imaging Dohler F. and his colleagues utilized a neural network to classify MRI images to automate the detection of hippocampal sclerosis (Döhler et al., 2008: 324–331). Using a dataset of 144 example images, the neural network was trained to identify

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

changes in brain tissue that suggest the existence of sclerotic degenerations.

Juan G. and his colleagues devised an artificial neural network (ANN) to automate the identification of bone structures. They evaluated the effectiveness of this approach in contrast to traditional methodologies (Juan et al., 2023:163–174). The Artificial Neural Network (ANN) demonstrated superior efficiency by achieving circa ten times faster segmentation of bone features compared to conventional methods. These findings emphasize the ability of neural networks to completely transform the effectiveness and accuracy of medical imaging analysis and diagnoses.

In neurology Tzallas A.T. and his colleagues utilized a neural network to predict epileptic episodes through the analysis of electroencephalograms (EEGs) (Tzallas et al., 2009: 703–710). This novel methodology demonstrated high precision, ranging from 98 % to 100 %.

Contemporary technological advancements enable a paradigm shift in representing the progression of diseases, particularly through the utilization of automated expert technologies. These expert computer-based medical systems empower physicians to validate their diagnostic hypotheses and seek guidance from computers, particularly in intricate diagnostic scenarios. This synergy between medical expertise and computer technology may enhance the accuracy and efficiency of disease prediction and diagnosis.

Diagnosing a disease is the process of finding out what is causing someone's medical symptoms. It is like solving a puzzle, where the doctor must gather information and put the pieces together to have a complete picture (Coffin, 2015: 537–545).

There are several ways doctors can diagnose a disease, including:

- Physical examination: doctor will check your body for any signs of the disease, such as rashes, lumps, or swelling;Medical history: doctor will ask about your symptoms, when they started, and if you have any other medical conditions;Laboratory tests: doctor may take samples of blood, urine, or other bodily fluids to be tested in a lab for any signs of the disease;Imaging tests: doctor may use X-rays, CT scans, or MRI scans to see inside your body and look for any abnormal structures or conditions;Biopsy: doctor may take a small piece of tissue from your body to be examined under a microscope to confirm the presence of a disease.

Once all this information has been gathered, the doctor will use it to make a diagnosis and recommend the best treatment plan. It is important to remember that getting a proper diagnosis is a crucial step in treating a disease, so it is important to be open and honest with the doctor about your symptoms and medical history.

Discussion and results

Mathematical models that are utilized in the field of medicine offer a variety of significant benefits. However, in contrast to models that are based on biological, physical, or chemical processes, these models are realistic and can be technically realized on computers by making use of contemporary algorithms and software. This enables the processing of enormous amounts of data, the execution of complex computations, and the analysis of the findings while taking into consideration a wide range of factors, which eventually leads to an improvement in the quality of diagnostic measurements. In addition, these kinds of systems can include knowledge from a variety of medical specialties by employing artificial intelligence, machine learning, and fuzzy set theory to develop adaptive models (Pi et al., 2021: 203–219). These models can learn from new data and continuously improve, which makes them vital in a medicine that is currently undergoing rapid change. Automated diagnostic sys-

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

tems can assess quantitative data and analyze qualitative information. This enables the building of complicated medical models that consider the unique characteristics of each patient.

Therefore, the implementation of mathematical models and automated systems in medicine contributes to the enhancement of diagnostic accuracy and helps to optimize procedures in clinical practice, thereby rendering them more efficient and accessible to patients.

The structural model allows to trace the process of database transformation in a system that is structured in a certain way and represents a matrix:

$$U = \begin{Vmatrix} u_1 & \dots & u_{1n} \\ u_2 & \dots & u_{2n} \\ & \dots & \\ u_{m1} & \dots & u_m \end{Vmatrix}$$

$$\tilde{U}_j = \bigcup_k \mu_{u_{ij}}(u_k)/u_k \ , \ u_k = \mu \sim (x_k),$$

Where

Diagnosis is conducted using various diagnostic models and the patient's existing symptom complex:

$$X = \bigcup \mu(X_k)/X_k$$

where $X_k \in X$ and $\mu(X_i)$ - degree of membership X_i for symptom set X

The process of diagnosis is the selection of the most probable disease (the result):

$$A^* = \mu_{\tilde{A}_o}(a_o) = \max \mu_{\tilde{A}_o}(a_i)$$

where $\mu_{A_o} \sim (a_i) = \max \mu_{\tilde{u}_{io}}(u_k)$

The implementation of automated systems for illness diagnosis enables the automation of the decision-making process during patient examination, diagnosis, and treatment prescription, therefore enhancing the degree of qualification. Practically, the implementation of automated systems has demonstrated a substantial enhancement in the quality of patient diagnosis and treatment. Medical automated systems enable doctors to verify their own assumptions and assist in problem-solving for challenging diagnostic scenarios. This information system does not replace a doctor, but functions as a "competent partner" – a proficient advisor in a certain field of expertise (Frank, et al., 2014: 105). Furthermore, they amass the expertise and information of exceptionally skilled professionals. Hence, it is necessary for automated systems to be able to adaptably define tasks, be applicable to all domains of medicine, possess substantial information capacity and noise immunity, and rapidly process medical data.

At present the professional capacities of doctors are being enhanced using sever-

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

al automated diagnostic methods that rely on advanced computer technology. Employing computer-based information systems for diverse research enables access to local and remote resources, technologies, and databases, resulting in a decrease in material, energy, and financial expenses. The evolution of this diagnostic technique is essential for medical educational institutions. Undoubtedly, there is a growing interest in medical issues today. The aspiration to discover the fundamental principles of operation of these systems and to comprehend the nature of life has become heightened. Development and application of mathematical diagnostic models are key components of future medicine (Naizagarayeva et al., 2023: 6673). The automation of disease diagnosis involves several steps to ensure efficient and accurate outcomes, illustrated in figure 1.

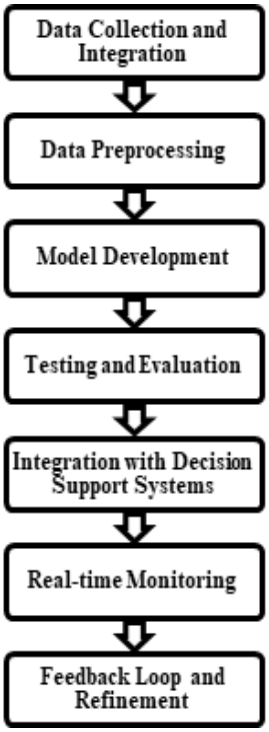


Fig. 1. Key steps for disease diagnosis automation

The first stage in figure 1 involves gathering and combining various medical data sources, such as patient case history, laboratory tests, and medical imaging. Finally, these data are combined to provide a complete patient profile. Feature extraction is used to identify pertinent characteristics that are strongly associated with diseases, such as symptoms and biomarkers. The acquired data is subsequently subjected to preprocessing techniques to guarantee uniformity and dependability, which include cleansing and normalization methods.

At the heart of automation is the creation of predictive models, employing sophisticated algorithms such as machine learning and statistical methods. These models are designed to provide precise illness forecasts using extant data. The selection of the most relevant features is crucial to improve the accuracy of these models. The primary objective of this feature selection procedure is to enhance the performance of the model. The models undergo comprehensive training and validation stages, during which they are trained on the data and evaluated using validation sets to determine their ability to make accurate predictions. A

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

thorough evaluation of the models is conducted using new data and diverse performance measures to guarantee their resilience and efficacy. The incorporation of these models into clinical decision support systems facilitates their practical implementation, offering healthcare practitioners prompt and well-informed diagnostic findings. The implementation of systems for real-time analysis of fresh data enables the timely detection of any changes in health state, therefore facilitating continuous monitoring of patient health.

An essential component of this procedure entails the integration of a feedback loop. The loop facilitates the continuous improvement of the system by incorporating new data and insights obtained from clinical practice. Ensuring ethical, privacy, and regulatory considerations is import for the deployment of automated diagnostic systems. Complying with healthcare regulations guarantees the conscientious utilization of sensitive patient information.

Finally, the process of clinical validation, conducted in partnership with medical experts, guarantees the precision and efficiency of the automated system in actual clinical situations.

Addressing Diagnostic Uncertainty

The field of medicine encounters the formidable burden of diagnosing many diseases using intricate and frequently imprecise data. The diagnostic process entails the integration and analysis of data of the patient, encompassing clinical observations, medical history, laboratory test findings, imaging investigations, and other pertinent information. These datasets may include potential uncertainties, variances, and ambiguity, therefore increasing the complexity of the diagnostic procedure.

Thus, the utilization of fuzzy sets theory and the concepts of decision-making relying on fuzzy information has emerged as a significant and urgent concern in the field of medicine. The mathematical framework of fuzzy sets theory, invented by Lotfi A. Zadeh in the 1960s, is designed to effectively manage imprecise and uncertain information (Smith et al., 2017: 155–166). The notion of fuzzy sets provides a useful tool for reasoning and decision-making in medical diagnostics, where data typically contains vagueness and ambiguity. The development of the automated system is expected to bring substantial improvements to the work of medical professionals in diagnosing and predicting diseases affecting internal organs. By utilizing the newly created information mathematical models, the system will empower doctors with advanced tools and insights, enhancing their diagnostic accuracy and predictive capabilities. The goal of the research is to deliver a highly efficient information system based on these sophisticated models. By doing so, the system aims to address and reduce subjectivity that can occur during the initial checkup process. This reduction in subjectivity will lead to more reliable and objective medical assessments, ensuring that patients receive accurate diagnoses and appropriate treatment plans promptly (Wiharto, 2018).

Benefits and drawbacks of the presented automated system

The analysis of advantages and disadvantages of the system can be conducted to automate and better diagnose the diseases of internal organs.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

Table 1. Analysis of advantages and disadvantages of the proposed system

Benefits	Drawbacks
Automated system improves the decision quality	Errors in the knowledge base can lead to wrong decision
Cuts the expense of consulting doctors for diagnosing	The maintenance cost of the system is too expensive
It provides fast and efficient solutions in detecting disease	There is no flexibility and ability to adapt to changing environments
Offers consistent answer for the repetitive process during	Unable to work in an extraordinary situation
Automated Systems can work gradually without getting emotional, tensed, or exhausted like human	Approbation of developed system is too long, to be sure that everything works correctly

The process of differential diagnosis can be divided into three interrelated steps: making a primary diagnosis (preliminary hypothesis), building a differential diagnostic series (proposing additional hypotheses), and final diagnosis (substantiating the final hypothesis) (fig 2).

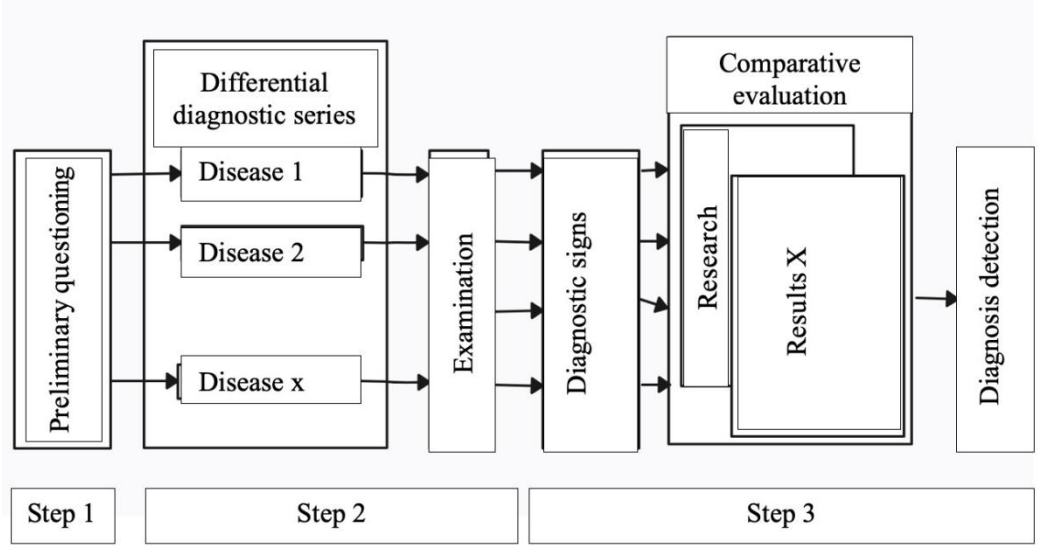


Fig. 2. Steps in Differential Diagnosis.

At the initial step, following a logical inference approach, the doctor acts based on patient complaints, an evaluation of historical data (including the inception of initial disease symptoms), and observed pathological indications to formulate a preliminary (primary) diagnosis. When formulating a hypothesis, potential underlying conditions are considered, where symptoms could distort the presentation of the core ailment (Lin et al., 2016: 1152–116). This process is automated through tests and questionnaires administered to the patient during their initial clinic visit. The test outcomes are then conveyed either to the doctor or a machine for analysis.

At the second step, the argumentation "for" is conducted, which ensures the involvement of additional diagnostic hypotheses. A differential diagnostic series is being formed,

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

i.e., a range of diseases in which there are signs determined by the patient and for which similar initial manifestations may be characteristic. In other words, the potentially diagnostic sequence is expanded for the subsequent adoption of the final one: the decision (Mardani et al., 2019: 202–231). At this step, the doctor chooses examination methods: to confirm the hypotheses (diseases). It is important at this step to optimize the choice and sequencing of laboratory and functional examinations in terms of maximizing: increasing: probability and speed, establishing a final diagnosis in conditions of minimizing cost.

Conclusion

The automated system is an interactive and reliable computer-based decision-making system which helps doctors to diagnose efficiently. There are key components of an automated system: user interface, inference engine, and knowledge base, which form a system shell. And some key participants in systems development: doctor, knowledge engineer, programming engineer, end user. Better decision qualities, reliability, consistency, speed of diagnosing are key benefits of an automated system. An automated system cannot give creative solutions during extraordinary situations and can be costly to maintain.

Diagnosis rises from the doctor's intricate and imaginative grasp of the pathological process, involving a holistic comprehension of the patient's circumstances precisely expressed. It is crucial to strictly adhere to the principles governing the structure of the diagnosis. In practical terms, the doctor establishes a series of inferences regarding the correlation of observed symptoms with a particular diagnosis. However, it is conceivable that essential characteristics might be overlooked or disregarded in this process. Throughout the proposed examination period, there is a risk of overdiagnosis due to the extensive observation and analysis of incoming data. Ensuring objective and high-quality diagnostics has become a critical priority in the field of healthcare. The challenge lies in striking a balance thorough observation and avoiding the potential pitfalls of over diagnosing, which can have significant implications for patients' well-being and treatment plans. Thus, the developed mathematical methods of diagnostics play a crucial role in addressing the challenges of subjectivity, both during the examination and in clinical practice. These methods offer a more objective approach to medical decision-making, reducing the potential impact of human bias and variability.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

REFERENCES

Coffin D.W. (2015). Some observations towards improved predictive models for box compression strength. — TAPPI J, 2015. — 14. — 537–545.

Döhler F., Mormann F., Weber B., Elger C.E. & Lehnertz K. (2008). A cellular neural network-based method for classification of magnetic resonance images: Towards an automated detection of hippocampal sclerosis. — *Journal of Neuroscience Methods*. — 170(2). — 324–331. https://doi.org/10.1016/j.jneumeth.2008.01.002

Frank B. (2014). Corrugated Box Compression — A Literature Sur-vey. Packaging Technology and Science. — 2014. — 27(2). — 105

L. Lin, P.J.H. Hu and O.R. Liu Sheng (2006). "A decision support system for lower back pain diagnosis: uncertainty management and clinical evaluations, "Decision Support Systems. — Vol. 42. — №. 2. — Pp. 1152–1169. — 2006. DOI: 10.1016/j.dss.2005.10.007

A. Mardani et al. (2019). "Application of decision making and fuzzy sets theory to evaluate the healthcare and medical problems: a review of three decades of research with recent developments," Expert Systems with Applications. —Vol. 137. — Pp. 202–231. —Déc.. 2019. DOI: 10.1016/j.eswa.2019.07.002

A. Naizagarayeva et al. (2023). "Detection of heart pathology using deep learning methods," International Journal of Electrical and Computer Engineering (IJECE). — Vol. 13. — № 6. — P. 6673. — Dec. 2023. DOI: 10.11591/ijece.v13i6.pp6673-6680

Soheila Zarei, Omid Bozorg-Haddad (2020). The basis of artificial neural networks (ANN): Structures, algorithms, and functions. In Artificial Intelligence and Machine Learning. — Pp. 23–47. https://link.springer.com/chapter/10.1007/978-981-19-2519-1_11

Juan Gu, Benjamin Frank, Euihark Lee (2023). A Comparative Analysis of Artificial Neural Network (ANN) Architectures for Box Compression Strength Estimation. — Vol. 29. — No. 3. (2023.12). — Pp. 163–174 https://www.earticle.net/Article/A439339

Tzallas A.T., Tsipouras M.G. & Fotiadis D.I. (2009). Epileptic seizure detection in EEGs using time-frequency analysis. IEEE Transactions on Information Technology in Biomedicine. — 13(5). — Pp. 703–710. https://ieeexplore.ieee.org/document/4801967

Pi Y. (2021). Machine learning in governments: Benefits, challenges, and future directions. — *JeDEMe Journal of eDemocracy and Open Government*. — 2021. — 13(1): 203–219.

I. Razzak, S. Naz, and A. Zaib (2018). "Deep learning for medical image processing: Overview, challenges and the future," Classification in BioApps: Automation of Decision Making. — 2018. — Pp. 323–350. DOI: 10.1007/978-3-319-65981-7_12

E. Gulbandilar, M. Sari and A. Cimbiz (2015). "Prediction of low back pain using a fuzzy logic algorithm. — №. September. — Pp. 1–6. — 2015. DOI: 10.13140/RG.2.1.3929.6486.

M.Y. Smith, J.D. Depue and C. Rini (2007). "Computerized decision-support systems for chronic pain management in primary care,"Pain Medicine. — Vol. 8. — №. SUPPL.3. — Pp. 155–166. — 2007. — DOI: 10.1111/j.1526-4637.2007.00278.x.

W. Wiharto (2018). Clinical decision support systems theory and practice. — Vol. 7. — №. 2. — Springer. — 2018

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Vol. 5. Is. 3. Number 19 (2024). Pp. 71–79
Journal homepage: https://journal.iitu.edu.kz
https://doi.org/10.54309/IJICT.2024.19.3.006

OPTIMIZATION OF MULTITASKING IN ANDROID USING COROUTINES: A COMPARATIVE PERFORMANCE ANALYSIS

A.B. Nurgalykov*, A.M. Akim
International Information Technology University, Almaty, Kazakhstan.

A.B. Nurgalykov — Master student, Software Engineering, the Department of Computer Engineering, International Information Technology University
A.M. Akim — Master of Technical Science, the Department of Computer Engineering, International Information Technology University

© A.B. Nurgalykov, A.M. Akim, 2024

Abstract. This article addresses the issue of multitasking in Android applications and provides a performance analysis of coroutines as a modern tool for asynchronous task handling. A comparative analysis of coroutines with traditional approaches such as AsyncTask, Thread, and Handler is conducted in terms of task execution time, energy consumption, and impact on the main thread. The focus is on how coroutines improve UI responsiveness and simplify asynchronous management through sequential code. The experiments reveal the advantages of coroutines in performance and reducing the load on the main thread. The article also discusses potential issues and limitations of coroutine usage and offers solutions for effective management of the Android component lifecycle.

Keywords: coroutine technologies in Android development, asynchronous programming, comparative performance analysis, thread management in Android, coroutine efficiency

For citation: *A.B. Nurgalykov, A.M. Akim. OPTIMIZATION OF MULTITASKING IN ANDROID USING COROUTINES: A COMPARATIVE PERFORMANCE ANALYSIS // INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES. 2024. Vol. 5. No. 19. Pp. 71–79 (In Russ.). https://doi.org/10.54309/IJICT.2024.19.3.006.*

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

ANDROID ЖҮЙЕСІНДЕ КОРУТИНДЕРДІ ҚОЛДАНУ АРҚЫЛЫ КӨПТАПСЫРМАЛЫЛЫҚТЫ ОҢТАЙЛАНДЫРУ: ӨНІМДІЛІКТІ САЛЫСТЫРМАЛЫ ТАЛДАУ

А.Б. Нургалыков*, А.М. Әкім

Халықаралық ақпараттық технологиялар университеті, Қазақстан, Алматы.

А.Б. Нургалыков — «Компьютерлік Инженерия» кафедрасының, бағдарламалық инженерия мамандығының магистранты, Халықаралық ақпараттық технологиялар университеті

А.М. Әкім — «Компьютерлік Инженерия» кафедрасының, техникалық ғылымдарының магистрі, Халықаралық ақпараттық технологиялар университеті

© А.Б. Нургалыков, А.М. Әкім, 2024

Аннотация. Бұл мақалада Android-қосымшаларындағы көптапсырмалылық мәселесі қарастырылады және корутиндерді асинхронды тапсырмаларды орындау құралы ретінде өнімділігіне талдау ұсынылады. Корутиндер мен дәстүрлі әдістер (мысалы, AsyncTask, Thread және Handler) тапсырмаларды орындау уақыты, энергияны тұтыну және басты ағынға әсері тұрғысынан салыстырмалы талдау жасалған. Негізгі назар корутиндердің интерфейстің жауап беруін қалай жақсартатынына және асинхрондылықты басқаруды дәйекті код арқылы жеңілдетуіне аударылған. Эксперименттер барысында корутиндердің өнімділік тұрғысынан және басты ағынға жүктемені азайтуда артықшылықтары анықталды. Корутиндерді қолданудағы ықтимал мәселелер мен шектеулер талқыланып, Android компоненттерінің өмірлік циклін тиімді басқаруға арналған шешімдер ұсынылады.

Түйін сөздер: Android-қосымшаларындағы корутин технологиялары, Асинхронды бағдарламалау, Өнімділікке салыстырмалы талдау, Android-те ағындарды басқару, Корутиндердің тиімділігі

Дәйексөз үшін: *А.Б. Нургалыков, А.М. Әкім. ANDROID ЖҮЙЕСІНДЕ КОРУТИНДЕРДІ ҚОЛДАНУ АРҚЫЛЫ КӨПТАПСЫРМАЛЫЛЫҚТЫ ОҢТАЙЛАНДЫРУ: ӨНІМДІЛІКТІ САЛЫСТЫРМАЛЫ ТАЛДАУ // ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ. 2024. Т. 5. No. 19. 71–79 бет. (орыс тілінде). https://doi.org/10.54309/IJICT.2024.19.3.006.*

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

ОПТИМИЗАЦИЯ МНОГОЗАДАЧНОСТИ В ANDROID С ПОМОЩЬЮ КОРУТИН: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОИЗВОДИТЕЛЬНОСТИ

А.Б. Нургалыков*, А.М. Аким
Международный Университет Информационных Технологий, Казахстан, Алматы.

А.Б. Нургалыков — магистрант специальности программная инженерия, кафедры «Компьютерная инженерия», Международный университет информационных технологий
А.М. Аким — магистр технических наук, кафедры «Компьютерная инженерия», Международный университет информационных технологий

© А.Б. Нургалыков, А.М. Аким, 2024

Аннотация. В статье рассматривается проблема многозадачности в Android-приложениях и предлагается анализ производительности корутин как современного инструмента для асинхронной обработки задач. Проведен сравнительный анализ корутин с традиционными подходами, такими как AsyncTask, Thread и Handler, с точки зрения времени выполнения задач, энергопотребления и влияния на главный поток. Основное внимание уделено тому, как корутины улучшают отзывчивость интерфейса и упрощают управление асинхронностью благодаря последовательному коду. В ходе экспериментов были выявлены преимущества корутин в плане производительности и снижения нагрузки на главный поток. Обсуждаются возможные проблемы и ограничения использования корутин, а также предлагаются решения для эффективного управления жизненным циклом Android-компонентов.

Ключевые слова: корутинные технологии в Android разработке, асинхронное программирование, сравнительный анализ производительности, управление потоками в Android, эффективность корутин

Для цитирования: *А.Б. Нургалыков, А.М. Аким. ОПТИМИЗАЦИЯ МНОГОЗАДАЧНОСТИ В ANDROID С ПОМОЩЬЮ КОРУТИН: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОИЗВОДИТЕЛЬНОСТИ // МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ. 2024. Т. 5. No. 19. Стр. 71–79. (На русс.). https://doi.org/10.54309/IJICT.2024.19.3.006.*

Введение

В современных Android-приложениях многозадачность является критически важной для обеспечения плавного пользовательского опыта и эффективного использования ресурсов. Традиционные методы, такие как AsyncTask, Thread, и Handler, долгое время использовались для реализации асинхронных операций. Однако с ростом сложности приложений и требованиями к высокой производительности, эти подходы начали демонстрировать свои ограничения, включая трудности в управлении потоками, утечки памяти и значительную нагрузку на главный поток.

В последние годы корутины, внедренные в Kotlin, приобрели популярность как современный инструмент для управления асинхронностью. Корутины обеспечивают упрощенное управление параллелизмом и повышают производительность приложений, позволяя писать асинхронный код в стиле последовательного выполнения. Корутинные технологии позволяют разработчикам эффективно управлять асинхронными задачами и минимизировать блокировки интерфейса, что делает их привлекательным выбором для современных приложений (JetBrains Blog, 2023).

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

Тем не менее, несмотря на очевидные преимущества, использование корутин требует тщательного подхода к управлению жизненным циклом Android-компонентов для предотвращения утечек памяти и других проблем (JetBrains, 2024). В свете этих изменений, важно провести сравнительный анализ производительности корутин и традиционных методов, чтобы оценить их эффективность в современных условиях разработки Android-приложений и выявить потенциальные области для улучшения.

Гипотеза

Целью данного исследования является оценка эффективности корутин в сравнении с традиционными методами асинхронного программирования, такими как использование потоков (Thread), в контексте Android-приложений. Гипотеза исследования заключается в том, что корутины предоставляют значительные преимущества по сравнению с потоками в плане производительности и управления системными ресурсами. Мы сосредоточимся на сравнении времени выполнения задач, а также на оценке влияния каждого метода на производительность и энергопотребление при увеличении количества одновременных задач (Dimiduk и др., 2021; Gray и др., 2020). Конечная цель работы — определить, в какой мере корутины способствуют улучшению отзывчивости интерфейса, снижению энергопотребления и упрощению управления асинхронными задачами в реальных условиях разработки Android-приложений. Это исследование направлено на предоставление количественной оценки преимуществ корутин и выработку рекомендаций для их применения в промышленной разработке.

Материалы и методы исследования

Потоки (Thread) в Java и Kotlin представляют собой один из самых старых и проверенных временем способов выполнения асинхронных задач. Поток можно описать как отдельный путь выполнения программы, который работает параллельно с другими потоками в системе. Это низкоуровневый механизм, который дает разработчику полный контроль над созданием и управлением потоками, обеспечивая возможность выполнять задачи параллельно с другими потоками в фоновом режиме (Bozovic и др., 2021). Когда создается новый поток, он работает независимо от основного потока программы (обычно это главный поток пользовательского интерфейса в Android), что позволяет выполнять операции, которые могут занять много времени, не блокируя основную работу приложения. Это особенно полезно в ситуациях, где необходимо выполнять задачи, такие как сетевые запросы, работа с файлами или вычислительно интенсивные операции. Однако, несмотря на очевидные преимущества, использование потоков влечет за собой ряд существенных недостатков. Время выполнения задачи с использованием потоков можно описать следующей формулой:

$$T_{thread} = T_{base} + p \cdot (T_{create} + T_{context\_swith} + T_{sync}) \quad (1)$$

где: — общее время выполнения задачи с использованием потоков, — базовое время выполнения задачи без учета накладных расходов (время чистых вычислений), — количество потоков, — время, необходимое на создание одного потока, — время, затрачиваемое на переключение контекста между потоками, — время на синхронизацию между потоками при совместном использовании ресурсов.

Каждый поток в операционной системе требует значительных ресурсов для своей работы. Это связано с тем, что каждому потоку выделяется отдельный стек памяти, и операционная система должна следить за их состоянием, планировать выполнение и переключение контекста между ними (Farrell, 2021; Zekovic, 2022). Чем

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

больше потоков создается, тем выше нагрузка на систему. При большом количестве потоков операционная система начинает тратить больше времени на управление ими, что приводит к снижению производительности. Зависимость производительности от количества задач при использовании потоков можно описать следующей формулой:

$$P_{thread} = \frac{C_{total}}{T_{thread} + O_{thread}} \quad (2)$$

где: — общее количество выполненных задач, — накладные расходы на управление потоками.

Создание и уничтожение потоков — это довольно ресурсоемкие операции. При большом количестве потоков время, необходимое для их создания, может существенно замедлить выполнение программы. Кроме того, после завершения работы потоков требуется время на их корректное завершение и очистку ресурсов. Когда количество задач возрастает, и для каждой из них создается отдельный поток, это может привести к значительным накладным расходам. Система начинает тратить больше времени на управление потоками, что снижает общую эффективность работы приложения. Например, при большом количестве одновременно работающих потоков может наблюдаться эффект «thrashing» — ситуация, когда процессор тратит больше времени на переключение между потоками, чем на выполнение самих задач. Это не только увеличивает время выполнения задач, но и вызывает излишнее потребление энергии (Akop и др., 2024).

Мобильных устройствах, таких как смартфоны и планшеты, энергопотребление играет ключевую роль. Каждый новый поток требует ресурсов процессора и памяти, что приводит к увеличению энергозатрат. При интенсивной работе с потоками батарея устройства разряжается быстрее, что снижает общее время работы устройства без подзарядки. В Android-разработке это критичный аспект, так как пользователи ожидают от приложений не только высокой производительности, но и экономного расхода заряда батареи.

Результаты и обсуждение

Управление большим количеством потоков требует высокой точности в синхронизации между ними. Несогласованность доступа к общим ресурсам может привести к ошибкам, таким как состояния гонки, взаимные блокировки и другие проблемы многопоточности, которые сложно обнаружить и исправить. Это делает процесс отладки многопоточных программ более сложным и трудоемким. Приложения, которые интенсивно используют потоки, могут столкнуться с проблемами стабильности, особенно на устройствах с ограниченными ресурсами. Например, на устройствах с низким объемом оперативной памяти или слабым процессором большое количество одновременно работающих потоков может привести к зависанию или даже к аварийному завершению программы.

Таким образом, хотя потоки предоставляют мощный инструмент для асинхронного выполнения задач, их использование связано с множеством ограничений и рисков. Они могут быть полезны для небольшого количества задач, однако, при работе с масштабируемыми системами или задачами, требующими высокой производительности и экономного энергопотребления, применение потоков может быть не самым эффективным решением. Это создает необходимость в более современных подходах к асинхронному программированию, таких как корутины в Kotlin, которые предлагают более легковесную и управляемую альтернативу.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

Корутины в Kotlin представляют собой один из самых современных и эффективных инструментов для работы с асинхронностью и многозадачностью. Они разработаны для решения проблем, которые возникают при использовании потоков, предлагая более легковесный и высокопроизводительный способ управления асинхронными задачами. В отличие от потоков, корутины значительно проще в управлении и потребляют гораздо меньше системных ресурсов.

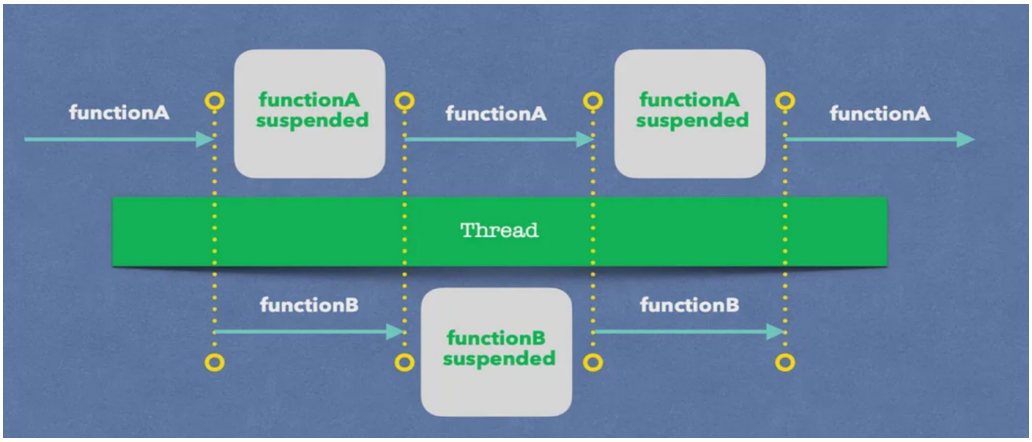


Рис. *1* – «Принцип функционирования Корутин»

Как показано на Рис. 1, каждая корутина, в отличие от потоков, не требует выделения отдельного стека памяти или создания нового системного потока. Корутины работают в рамках одного потока и могут приостанавливать и возобновлять свое выполнение, не создавая дополнительных накладных расходов на управление ими. Это означает, что приложение может запускать тысячи корутин одновременно, без риска перегрузки системы, что делает корутины более масштабируемыми по сравнению с потоками.

Корутины позволяют писать асинхронный код в синхронном стиле, что делает его более читаемым и удобным для понимания. В отличие от потоков, которые блокируют выполнение до завершения задачи, корутины позволяют приостанавливать выполнение задачи и возобновлять его, как только задача завершена, не блокируя основной поток программы. Это особенно важно для Android-приложений, где блокировка главного потока пользовательского интерфейса может привести к замедлению работы приложения и ухудшению пользовательского опыта.

Корутины работают на базе пулов потоков и планировщиков, что позволяет им эффективно распределять задачи между доступными потоками, не создавая излишних накладных расходов. Когда корутина приостанавливается, ее выполнение может быть продолжено на другом потоке, если это необходимо, что позволяет оптимально использовать ресурсы системы. Например, корутина, выполняющая сетевой запрос, может быть приостановлена, пока не получен ответ, и возобновлена на другом потоке для дальнейшей обработки данных. Одним из ключевых преимуществ корутин является то, что они позволяют писать асинхронный код в линейном виде, избегая использования сложных цепочек колбэков и управления потоками. Это упрощает процесс написания кода, делает его более понятным и легко поддерживаемым. Для

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

разработчиков это означает снижение вероятности ошибок и улучшение качества конечного продукта. Время выполнения задачи в корутине можно описать следующим образом:

$$T_{coroutine} = T_{base} + n \cdot T_{suspend\_resume} \quad (3)$$

где: — общее время выполнения корутины, — количество приостановок и возобновлений, — время, затрачиваемое на приостановку и возобновление выполнения корутины.

Когда вы используете корутины в Kotlin, для выполнения длительных операций, таких как сетевые запросы или работа с базой данных, вы можете легко приостанавливать выполнение корутины с помощью функции suspend. Это позволяет избежать блокировки основного потока пользовательского интерфейса и повышает отзывчивость приложения. Например, если нужно выполнить асинхронную задачу, такую как загрузка данных с сервера, корутины позволяют приостановить выполнение до тех пор, пока данные не будут загружены, а затем продолжить выполнение кода. Все это происходит без необходимости создания новых потоков и без накладных расходов, характерных для традиционных потоков.

Корутины оптимизированы для экономии ресурсов, в том числе энергопотребления. Поскольку корутины работают в рамках существующих потоков, они минимизируют количество переключений между потоками и ресурсов, что снижает нагрузку на процессор и батарею устройства. Зависимость производительности от количества задач можно описать следующим образом:

$$P_{coroutine} = \frac{C_{total}}{T_{coroutine}} \quad (4)$$

В отличие от потоков, которые требуют выделения ресурсов для каждого нового потока, корутины работают на базовом уровне и могут выполнять тысячи задач одновременно, практически не влияя на энергопотребление. Для мобильных приложений, где время работы батареи является критическим фактором, использование корутин вместо потоков позволяет значительно сократить энергозатраты. Это особенно важно для приложений с интенсивной обработкой данных, частыми сетевыми запросами и многозадачностью.

Процедура тестирования:

В рамках исследования были проведены тесты, сравнивающие выполнение различных количеств одновременных задач с использованием потоков (Thread) и корутин (Kotlin Coroutines). Каждая задача имитировала продолжительную операцию с задержкой в 100 миллисекунд. Время выполнения измерялось с использованием функции measureTimeMillis, которая фиксировала общее время выполнения всех задач. Эксперименты проводились для 100, 500, 1000, 5000, 10 000, 20 000 и 50 000 задач, что позволило оценить влияние каждого метода на производительность при увеличении нагрузки. Полученные данные были использованы для анализа эффективности управления ресурсами и выявления преимуществ корутин над потоками, особенно в условиях масштабируемых асинхронных операций.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

Таблица 1 – «Результаты экспериментов для метода использования Thread»

Количество задач	Время выполнения (мин)	Время выполнения (макс)
100	121 мс	137 мс
500	135 мс	148 мс
1000	160 мс	171 мс
5000	441 мс	536 мс
10000	888 мс	926 мс
20000	1703 мс	1827 мс
50000	4061 мс	4506мс

При использовании потоков (**таблице 1)** время выполнения задач значительно увеличивается с ростом их количества. Для небольшого числа задач (100–1000) время остается стабильным, но при 5000 задачах оно возрастает до 441–536 мс, а для 50 000 задач достигает 4061–4506 мс. Это демонстрирует ограниченную масштабируемость потоков, где увеличение задач приводит к существенным накладным расходам на создание и управление потоками, что перегружает систему и увеличивает задержки.

Таблица 2 – «Результаты экспериментов для метода использования Корутин»

Количество задач	Время выполнения (мин)	Время выполнения (макс)
100	123 мс	140 мс
500	133 мс	147 мс
1000	146 мс	164 мс
5000	174 мс	185 мс
10000	192 мс	223 мс
20000	234 мс	245 мс
50000	284 мс	305 мс

Корутины демонстрируют стабильное и эффективное выполнение задач, независимо от их количества. Время выполнения задач растет постепенно, начиная от 123–140 мс для 100 задач и достигая 284–305 мс для 50 000 задач. Даже при значительном увеличении числа задач, прирост времени выполнения остается минимальным. Это указывает на высокую эффективность корутин в управлении многозадачностью, где асинхронная обработка задач происходит без существенного увеличения нагрузки на систему.

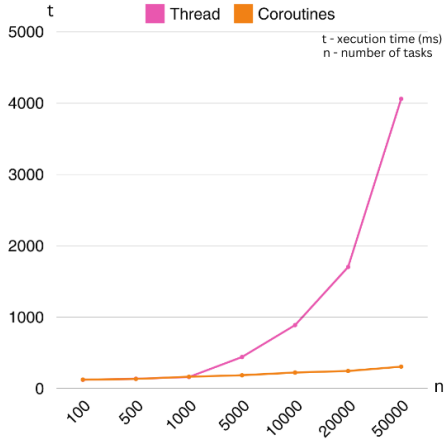


Рис. 2 – «Степень оптимизации задач»

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

Результаты экспериментов показали (*Рисунок 2)*, что корутины значительно превосходят потоки по производительности, особенно при увеличении количества задач. Корутины демонстрируют меньшие накладные расходы на управление задачами, что позволяет им оставаться эффективными даже при выполнении большого количества асинхронных операций. Потоки же становятся менее эффективными при увеличении количества задач, что приводит к значительному увеличению времени выполнения и энергопотребления. Таким образом, для современных Android-приложений использование корутин является более предпочтительным подходом для реализации многозадачности и управления асинхронными операциями.

Выводы

В ходе исследования была подтверждена гипотеза о том, что корутины являются более эффективным инструментом для управления асинхронными задачами по сравнению с потоками. Эксперименты показали, что с увеличением количества задач производительность потоков значительно снижается из-за высоких накладных расходов на создание и управление системными потоками. В то время как корутины демонстрируют линейное увеличение времени выполнения, что свидетельствует о лучшей масштабируемости данного метода. Это делает корутины предпочтительным выбором для задач с большим количеством асинхронных операций. В сравнении с потоками, корутины показали не только лучшее время выполнения, но и более эффективное использование системных ресурсов, что позволяет снизить энергопотребление.

Перспективы дальнейшего развития использования корутин включают их интеграцию с Kotlin Multiplatform, что позволит эффективно использовать асинхронное программирование на различных платформах, таких как iOS и веб-приложения. Также стоит отметить потенциал корутин в сочетании с Jetpack Compose, где они могут улучшить управление асинхронными задачами и состояние пользовательского интерфейса. Эти направления могут значительно повысить производительность приложений и упростить разработку, открывая новые возможности для создания более отзывчивых и масштабируемых решений.

REFERENCES

Jet Brains (2024). «JetBrains Blog on Kotlin Coroutines». — JetBrains Blog. — P. 459

Dimiduk D., Negov V. & Krivoshapka L. (2021). «Kotlin Coroutines by Tutorials». Razeware.

Gray C. & Simon B. (2020). “Kotlin Programming: The Big Nerd Ranch Guide”. Big Nerd Ranch Guides.

Bozovic M., Green D. & Novikov A. (2021). “The Definitive Guide to Kotlin Coroutines”. O’Reilly Media. — Pp. 74–106

Farrell J. (2021). “Android Programming with Kotlin for Beginners”. — Packt Publishing.

Zekovic A. (2022). “Design of Kotlin Coroutines”. — Medium. — P. 536

Akop Vardanian, Alexandr Lenivenko, Anastasiya Zahorskaya (2024). “Android Development UpSkill program” EPAM Learn. — Pp. 104–108

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Vol. 5. Is. 3. Number 19 (2024). Pp. 80–89
Journal homepage: https://journal.iitu.edu.kz
https://doi.org/10.54309/IJICT.2024.19.3.007

COMPUTER VISION METHODS FOR CONDUCTING OSINT INVESTIGATIONS

Y. Sokyran*, T. Babenko, I. Parkhomenko, L. Myrutenko
Taras Shevchenko National University of Kyiv.
E-mail: sokyran@knu.ua

Yurii Sokyran — Master's student, the Department of Cyber Security and Information Protection, Faculty of Information Technologies, Kyiv, Ukraine
E-mail: sokyran@knu.ua, https://orcid.org/0009-0004-7041-2307;
Tetiana Babenko — Doctor of Sciences, professor, the Department of Cyber Security and Information Protection, Faculty of Information Technologies, Kyiv, Ukraine
E-mail: babenkot@ua.fm, https://orcid.org/0000-0003-1184-9483;
Ivan Parkhomenko — Candidate of Technical Science, associate professor, the Department of Cyber Security and Information Protection, Faculty of Information Technologies, Kyiv, UkraineE-mail: parkh08@gmail.com, https://orcid.org/0000-0001-6889-9284;
Larysa Myrutenko — Candidate of Technical Science, associate professor, the Department of Cyber Security and Information Protection, Faculty of Information Technologies, Kyiv, Ukraine
E-mail: myrutenko.lara@gmail.com, https://orcid.org/0000-0003-1686-261X.

© Y. Sokyran, T. Babenko, I. Parkhomenko, L. Myrutenko, 2024

Abstract. This paper researches the application of computer vision techniques in concern with OSINT (Open Source Intelligence) investigations. It explores how state-of-the-art algorithms and models in computer vision can be used to automate and enhance the process of gathering, analyzing, and interpreting visual data from open sources. The research focuses on the critical steps of image scraping, data preprocessing, and embedding generation using advanced deep learning models such as CLIP. Additionally, the study examines the challenges of managing large-scale visual data and implementing efficient search mechanisms through vector databases like Faiss and Weaviate. By applying these technologies, the paper illustrates how investigators can improve the accuracy and efficiency of image-based searches, which are later used for uncovering hidden connections and verifying information in OSINT investigations. The findings contribute to the growing field of computer vision and intelligence gathering, offering practical recommendations for enhancing investigative processes through the integration of computer vision methodologies.

Keywords: intelligence gathering, computer vision, open source intelligence, automated investigations

For citation: *Y. Sokyran, T. Babenko, I. Parkhomenko, L. Myrutenko. COMPUTER VISION METHODS FOR CONDUCTING OSINT INVESTIGATIONS // INTERNATION-AL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES. 2024. Vol. 5. No. 19. Pp. 80–89 (In Eng.). https://doi.org/10.54309/IJICT.2024.19.3.007.*

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

OSINT ЗЕРТТЕУЛЕРІН ЖҮРГІЗУДІҢ КОМПЬЮТЕРЛІК КӨРУ ӘДІСТЕРІ

Ю. Сокыран*, Т. Бабенко, И. Пархоменко, Л. Мирутенко
Тарас Шевченко Атындағы Киев Ұлттық Университеті.
E-mail: sokyran@knu.ua

Юрий Сокыран — Киберқауіпсіздік Және Ақпаратты Қорғау Кафедрасының Магистранты, Ақпараттық Технологиялар Факультеті, Киев, Украина
E-mail: sokyran@knu.ua, https://orcid.org/0009-0004-7041-2307;
Тетиана Бабенко — Ғылым Докторы, Профессор, Киберқауіпсіздік Және Ақпаратты Қорғау Кафедрасы, Ақпараттық Технологиялар Факультеті, Киев, Украина
E-mail: babenkot@ua.fm, https://orcid. org/0000-0003-1184-9483;
Иван Пархоменко — техника Ғылымдарының Кандидаты, Доцент, Киберқауіпсіздік Және Ақпаратты Қорғау Кафедрасы, Ақпараттық Технологиялар Факультеті, Киев, Украина
E-mail: parkh08@ gmail.com, https://orcid.org/0000-0001-6889-9284;
Лариса Мирутенко — техника Ғылымдарының Кандидаты, Доцент, Киберқауіпсіздік Және Ақпаратты Қорғау Кафедрасы, Ақпараттық Технологиялар Факультеті, Киев, Украина
E-mail: myrutenko. lara@gmail.com, https://orcid.org/0000-0003-1686-261X.

© Ю. Сокыран, Т. Бабенко, И. Пархоменко, Л. Мирутенко, 2024

Аннотация. Бұл жұмыста OSINT (Open Source Intelligence) зерттеулерінің бөлігі ретінде компьютерлік көру әдістерін қолдану зерттелген. Ол ашық көздерден көрнекі деректерді жинау, талдау және интерпретациялау процесін автоматтандыру және жақсарту үшін компьютерлік көрудегі заманауи алгоритмдер мен модельдерді қалай пайдалануға болатынын зерттейді. Зерттеу CLIP сияқты тереңдетілген оқытудың озық үлгілерін пайдалана отырып, кескіндерді қиюдың, деректерді алдын ала өңдеудің және ендірудің маңызды кезеңдеріне бағытталған. Сонымен қатар, зерттеу Ауқымды визуалды деректерді басқару және Faiss және Weaviate сияқты векторлық дерекқорлар арқылы тиімді іздеу механизмдерін енгізу мәселелерін зерттейді. Осы технологияларды қолдана отырып, мақалада тергеушілер КЕЙІНІРЕК OSINT тергеулерінде жасырын байланыстарды ашу және ақпаратты тексеру үшін пайдаланылатын кескінге негізделген іздеулердің дәлдігі мен тиімділігін қалай арттыра алатыны суреттелген. Нәтижелер компьютерлік көру әдістемелерін біріктіру арқылы тергеу процестерін жақсарту бойынша практикалық ұсыныстарды ұсына отырып, компьютерлік көру және барлау деректерін жинау саласының өсуіне ықпал етеді.

Түйін сөздер: барлау мәліметтерін жинау, компьютерлік көру, ашық бастапқы барлау, автоматтандырылған тергеу

Дәйексөз үшін: *Ю. Сокыран, Т. Бабенко, И. Пархоменко, Л. Мирутенко. OSINT ЗЕРТТЕУЛЕРІН ЖҮРГІЗУДІҢ КОМПЬЮТЕРЛІК КӨРУ ӘДІСТЕРІ // ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ. 2024. Т. 5. No. 19. 80–89 бет. (ағылшын тілінде). https://doi.org/10.54309/IJICT.2024.19.3.007.*

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

МЕТОДЫ КОМПЬЮТЕРНОГО ЗРЕНИЯ ДЛЯ ПРОВЕДЕНИЯ OSINT-ИССЛЕДОВАНИЙ

Ю. Сокиран*, Т. Бабенко, И. Пархоменко, Л. Мирутенко
Киевский национальный университет имени Тараса Шевченко.
E-mail: sokyran@knu.ua

Юрий Сокиран — магистрант кафедры кибербезопасности и защиты информации Факультета информационных технологий, Киевский национальный университет имени Тараса Шевченко, Киев, Украина
E-mail: sokyran@knu.ua, https://orcid.org/0009-0004-7041-2307;
Татьяна Бабенко — доктор технических наук, профессор кафедры кибербезопасности и защи-ты информации Факультета информационных технологий, Киевский национальный университет имени Тараса Шевченко, Киев, Украина
E-mail: babenkot@ua.fm, https://orcid.org/0000-0003-1184-9483;
Иван Пархоменко — кандидат технических наук, доцент кафедры кибербезопасности и защи-ты информации Факультета информационных технологий, Киевский национальный университет имени Тараса Шевченко, Киев, Украина
E-mail: parkh08@gmail.com, https://orcid.org/0000-0001-6889-9284;
Лариса Мирутенко — кандидат технических наук, доцент кафедры кибербезопасности и защи-ты информации Факультета информационных технологий, Киевский национальный университет имени Тараса Шевченко, Киев, Украина
E-mail: myrutenko.lara@gmail.com, https://orcid.org/0000-0003-1686-261X.

© Ю. Сокиран*, Т. Бабенко, И. Пархоменко, Л. Мирутенко, 2024

Аннотация. В данной статье исследуется применение методов компьютерного зрения в рамках исследований OSINT (Open Source Intelligence). В нем рассказыва-ется о том, как современные алгоритмы и модели компьютерного зрения могут быть использованы для автоматизации и улучшения процесса сбора, анализа и интерпре-тации визуальных данных из открытых источников. Исследование сосредоточено на важнейших этапах очистки изображений, предварительной обработки данных и созда-ния встраиваемых файлов с использованием передовых моделей глубокого обучения, таких как CLIP. Кроме того, в исследовании рассматриваются проблемы управления крупномасштабными визуальными данными и внедрения эффективных механизмов поиска с помощью векторных баз данных, таких как Faiss и Weaviate. В статье показано как с применением этих технологий, исследователи могут повысить точность и эффек-тивность поиска на основе изображений, которые впоследствии используются для вы-явления скрытых связей и проверки информации в расследованиях OSINT. Получен-ные результаты вносят вклад в развитие компьютерного зрения и сбора разведданных, предлагая практические рекомендации по совершенствованию процессов расследова-ния за счет интеграции методологий компьютерного зрения.

Ключевые слова: сбор разведданных, компьютерное зрение, разведданные с открытым исходным кодом, автоматизированные расследования

Для цитирования: *Ю. Сокиран, Т. Бабенко, И. Пархоменко, Л. Мирутен-ко. МЕТОДЫ КОМПЬЮТЕРНОГО ЗРЕНИЯ ДЛЯ ПРОВЕДЕНИЯ OSINT-ИС-СЛЕДОВАНИЙ // МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ. 2024. Т. 5. No. 19. Стр. 80–89. (На анг). https://doi.org/10.54309/IJICT.2024.19.3.007.*

Introduction

Computer vision is a branch of artificial intelligence (AI) that empowers computers and systems to derive meaningful insights from digital images, videos, and other visual in-puts, enabling them to take actions or provide recommendations based on this information.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

Computer vision grants systems the capability to see, observe, comprehend and that allows them to interact with the environment in a more advanced way (Yann et al., 2015).

Significant advancements in computer vision and multimedia processing over the past decade have allowed many tasks to be performed with human-level accuracy, or even surpassing it. These advancements are attributed to the vast amounts of data available for training, which has enhanced computational capabilities. This processing power is applied in various fields, such as autonomous vehicle navigation, security applications in video surveillance systems, and the analysis of medical images for healthcare diagnostics. A common application is image search, where users directly search for visual content (Radford et al., 2021).

Despite the transformative impact of deep learning on computer vision, current approaches face significant challenges: organizing training datasets with labeled images is both time-consuming and costly, especially when training is focused on a narrow set of visual tasks. Moreover, standard vision models excel at a single task but require substantial effort to adapt to new ones. Models that perform well on benchmarks often show disappointing results in stress tests, raising concerns about the overall deep learning approach in computer vision.

OpenAI's CLIP model seeks to address these challenges by learning from a diverse range of images and their associated textual data, which is abundantly available online. The CLIP model utilizes embeddings, which are numerical representations of data like text and images (Radford et al., 2021). These embeddings are generated using a model trained on image-text pairs, enabling the model to encode the semantic content of images. This approach facilitates the creation of a search engine by following these steps:

1. calculate embeddings for all images in the dataset;generate the text embedding for the user query (e.g., "helmet" or "car");compare the text embeddings with image embeddings to identify relevant matches.

The closer the two embeddings are, the more similar the documents they represent. To measure the similarity between generated vectors, statistical methods such as cosine similarity, Euclidean distance can be used. Cosine similarity is widely used for text similarity.

In the context of modern OSINT investigations, researchers need to gather and process large databases that include both textual and multimedia content—images, videos, and more. An integrated image search system can greatly assist them by enabling searches based on text queries and using embeddings to find images that correspond to a specific query. Additionally, by incorporating a neural network capable of describing images, the system can facilitate searches not only by image embeddings but also by their descriptions (Kermode et al., 2020).

Material and methods

Data collection and preprocessing

Initially, the process involves conducting image scraping, which involves the utilization of web scraping tools such as Scrapy, Selenium, or specialized image scraping libraries to automate the collection of images from various online sources. Common sources for this data include image-hosting websites, social media platforms (such as Instagram and Facebook), messaging services (like Telegram), news sites, forums, and other web resources that contain visual content. During scraping, it is important to follow exclusion rules (such as robots.txt file) and the data usage policies of the respective websites. The collected images are stored in appropriate formats (JPEG, PNG, etc.) in an organized structure on the disk (Walkow et al., 2023: 402–409).

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

Next, along with the collected images, accompanying metadata and textual data is also gathered, such as textual descriptions, titles, tags, user comments, and more. This data can significantly enhance the quality of vector embeddings and search accuracy by providing additional context. At this stage, it is advisable to use various parsers and data scrapers to extract valuable information from web pages, PDF files, documents, and other digital data sources. Depending on the data format, HTML/XML parsing libraries, Regular Expressions, specialized PDF parsers, and others may be used. The obtained textual data is stored together with the images and can be used as additional data to improve and refine search results.

It is essential to conduct thorough data cleansing, which involves the removal of noise, errors, and incorrect data from the set of images and associated metadata (Sohail et al., 2023). This process may include the following steps:

- elimination of exact duplicates and near-duplicates of images with minor variations;
- removal of images that are of very low quality, blurred, or heavily noisy;
- correction or removal of evidently irrelevant tags and textual descriptions;
- filling in missing metadata with synthetic data generated through deep learning models.

Data normalization is also conducted, which involves standardizing images and textual data into a unified format to facilitate further processing.

After data cleansing and normalization, the refined data is utilized to compute vector embeddings. Advanced computer vision deep learning models, such as CLIP, BLIP, and VGG, are applied to calculate vector embeddings for each image in the dataset. These embeddings will be employed for the efficient retrieval of similar images in the subsequent stages of the algorithm (Yann et al., 2015).

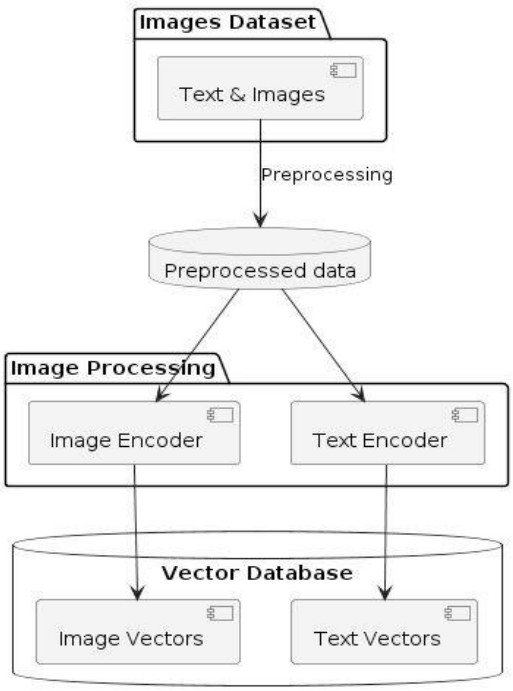


Fig. 1 – "The process of collecting, processing and populating the database"

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

This process is portrayed in figure 1. Next part is selecting a database: The choice of an appropriate vector database is crucial for ensuring efficient search operations based on vector embeddings. Popular options include Faiss, Weaviate, and others (Kukreja et al., 2023: 231–236).

The selection typically depends on the following factors:

- the dimensionality of the vector embeddings (some databases perform better with high or low dimensionality);
- the expected volume of data (certain databases are more efficient for very large datasets);
- supported distance metrics and index types;
- performance requirements for search and data updates;
- scalability, distributed indexing capabilities, and fault tolerance;
- compatibility with selected libraries and frameworks (such as PyTorch, TensorFlow).

Configuring parameters: the vector database is configured with parameters such as vector dimensionality, index type, and distance metric (e.g., cosine similarity, Euclidean distance). The correct selection of these parameters can significantly impact the speed and accuracy of the search, especially when dealing with large volumes of data (Kukreja et al., 2023: 231–236).

Data loading: the calculated image embeddings and associated data are then loaded into the vector database. This allows for efficient storage and indexing of the data for subsequent search operations.

Discussion and results

Application of vector databases in image search

Vector databases have numerous applications in image search and retrieval tasks, making them an essential tool in modern data management. One prominent use case is content-based image search, where vector databases enable the search for visually similar images based on their content, rather than relying solely on textual metadata. This capability allows for more intuitive and accurate search results, particularly in situations where images lack detailed descriptions or where the visual aspect is the primary search criterion (Kukreja et al., 2023: 231–236).

Another significant application is image deduplication. By comparing embedded images, vector databases can efficiently identify and remove duplicates or near-duplicates from large image collections. This is particularly useful in managing extensive datasets, ensuring that storage is optimized and that search results are not cluttered with repetitive images.

Vector databases are also employed in visual product search, especially within e-commerce platforms. These systems allow users to search for visually similar products based on a reference image, providing a more engaging and user-friendly shopping experience. By leveraging visual similarities, these platforms can recommend products that align closely with what the user is seeking, enhancing the overall effectiveness of the search process (Kukreja et al., 2023: 231–236).

Additionally, vector databases are widely used for image clustering and categorization by grouping visually similar images into clusters or categories based on their embedding proximity. This functionality supports the organization of large image datasets, making it easier to manage, analyze, and retrieve images according to their visual characteristics (Kukreja et al., 2023: 231–236).

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

Overall, vector databases, in combination with image embeddings, offer a powerful solution for efficient and accurate image search. By utilizing both semantic and visual information, these databases support rapid and reliable similarity searches across large-scale image collections. As the volume of visual data continues to grow, the importance of vector databases in image search applications is expected to increase, highlighting their critical role in various industries. The primary distinction between vector databases and traditional databases lies in their approach to storing and processing data, as well as the types of queries they are optimized to manage.

Query processing and post-processing

Receiving the query: the user's query may be in the form of an image, text, or a combination of both.

If the user provides a textual description or other accompanying data, the necessary processing and cleaning of this data is performed (Kermode et al., 2020).

The following steps are taken at this stage:

- translation of the text into one of the languages supported by the model, if necessary;

- removal of stop words, punctuation marks, HTML tags, and other "noise" from the text;

- augmentation of the query with synonyms of key words and relevant terms from semantically related topics;

- rephrasing the query to improve its compatibility with the embedding model.

If the user submits a query in the form of an image, deep learning models can be applied to generate an additional description of the provided image.

Next, the query embedding is computed: using the same deep learning model as was used for the image embeddings in the database, we calculate the vector embedding of the user's query.

Then nearest neighbor search is performed: efficient nearest neighbor search algorithms (such as the k-nearest neighbors algorithm) are applied to find the embeddings in the database that are closest to the query embedding.

Displaying results: the query image and the top k nearest images from the database are presented to the user, ordered by decreasing similarity to the query. Alongside each retrieved image, a numerical value representing the distance or similarity metric to the query may be displayed to provide a clearer comparison of relevance. The images can be presented as thumbnails or with an option for full-size viewing.

Displaying metadata: optionally, if available, the system can display accompanying metadata (such as textual descriptions, tags, titles, etc.) for each retrieved image, providing the user with additional context and improving the clarity of the search results.

Navigation and filtering: the user may be provided with the option to view more results through pagination or infinite scrolling. Additionally, filtering results by various criteria such as image size, file type, source, creation date, and more can be implemented. This allows the user to refine search queries and focus on the most relevant results.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

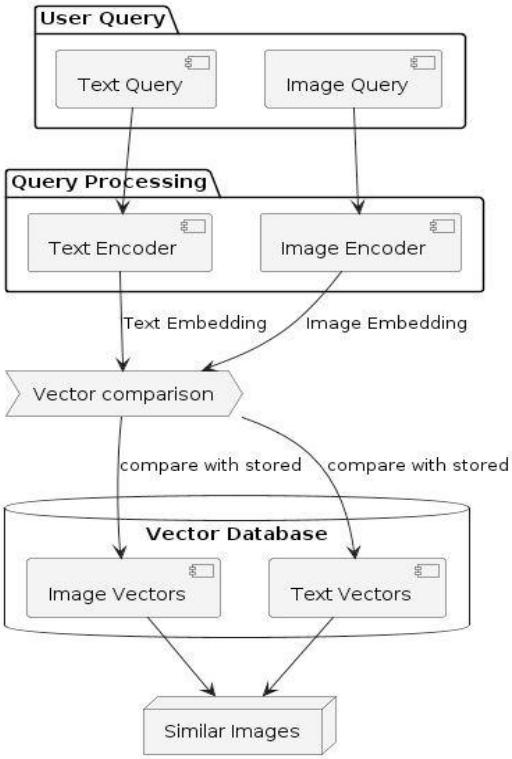


Fig. 2 – "The process of using a user query to find similar images"

Conclusion

In conclusion, the integration of computer vision technologies into OSINT investigations has significantly enhanced the capabilities of analysts and researchers. By employing advanced deep learning models such as CLIP and VGG, it is now possible to automate the process of image analysis and retrieval, providing a more efficient and accurate method for handling vast amounts of visual data. These models enable the extraction of meaningful embeddings from images, which can then be used to find relevant matches within large datasets. This approach not only saves time but also increases the precision of search results, making it an invaluable tool in intelligence gathering and analysis (Sohail et al., 2023).

The meticulous process of data scraping, cleaning, and normalization is crucial in preparing the visual data for effective embedding and retrieval. Ensuring the removal of noise, duplicates, and irrelevant information allows for the creation of high-quality datasets that can be efficiently processed by machine learning models. This preparation stage is essential for achieving accurate embeddings, which are foundational to the success of any image retrieval system. Moreover, the incorporation of metadata and textual information alongside images provides additional layers of context, further refining the search and retrieval process (Walkow et al., 2023: 402–409).

Selecting the appropriate vector database and configuring it with the correct parameters is another critical step in building an effective image retrieval system. The choice of database and its configuration—such as vector dimensionality, indexing methods, and distance metrics—directly impacts the speed and accuracy of search operations. Tuned, these

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

systems can manage large-scale data with ease, enabling rapid and reliable access to relevant visual information, which is essential in high-stakes OSINT operations (Kukreja et al., 2023: 231–236).

The development and implementation of these systems represent a significant advancement in the field of OSINT. By leveraging state-of-the-art computer vision techniques and technologies, analysts are better equipped to manage and interpret complex visual data. This not only enhances their investigative capabilities but also contributes to more informed decision-making processes, thereby strengthening the overall effectiveness of intelligence operations in today's increasingly data-driven world.

Ffurther research

Future research should focus on enhancing the adaptability and accuracy of image search systems based on embeddings, particularly by refining the methods of query refinement and user interaction. One promising area of exploration is the development of more advanced techniques for query enhancement, where users can iteratively refine their searches by adding new images, text, or a combination of both. This would enable a more dynamic and interactive search process, allowing for a gradual narrowing of search scope and yielding more precise results that better align with the user's intentions.

Another critical area for further investigation is the design and optimization of user interfaces that facilitate more intuitive and efficient interaction with the image search system. Research could explore the most effective ways to present search results, including the arrangement of thumbnail galleries, the display of relevant metadata, and the integration of advanced filtering and navigation options. By improving the user experience, researchers can help ensure that users are able to analyze results more effectively and make precise adjustments to their searches, thereby enhancing the overall utility of the system.

Feedback mechanisms also present a significant opportunity for further research. Developing more sophisticated methods for collecting and analyzing user feedback on search relevance can provide valuable insights into the system's performance. This feedback can be used to continuously improve the algorithm by fine-tuning the parameters of embedding models, adjusting similarity metrics, and optimizing search algorithms. Regular updates based on user feedback could lead to more accurate and reliable search outcomes, ensuring that the system remains responsive to the evolving needs of its users.

Finally, research should explore the broader implications of embedding-based image search systems in various domains, such as healthcare, security, and social media. Understanding the specific requirements and challenges of these fields can guide the development of tailored solutions that maximize the impact and effectiveness of image retrieval technologies. By addressing these areas, future research can contribute to the ongoing advancement of computer vision applications and their integration into critical real-world contexts.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

REFERENCES

S. Kukreja, T. Kumar, V. Bharate, A. Purohit, A. Dasgupta and D. Guha (2023). "Vector Databases and Vector Embeddings-Review," 2023 International Workshop on Artificial Intelligence and Image Processing (IWAIIP). — Yogyakarta, Indonesia, 2023. — Pp. 231–236. https://www.doi.org/10.1109/IWAIIP58158.2023.10462847.

Kermode L., Freyberg J., Akturk A., Trafford R., Kochetkov D., Pardinas R., Weizman E., Cornebise J. (2020). Objects of violence: synthetic data for practical ML in human rights investigations. https://doi.org/10.48550/arXiv.2004.01030

Radford A., Kim J.W., Hallacy C., Ramesh A., Goh G., Agarwal S., Sastry G., Askell A., Mishkin P., Clark J., Krueger G., Sutskever I. (2021). Learning Transferable Visual Models From Natural Language Supervision. https://doi.org/10.48550/arXiv.2103.00020.

Sohail Ahmed Khan, Jan Gunnar Furuly, Henrik Brattli Vold, Rano Tahseen, and Duc-Tien Dang-Nguyen (2023). Online multimedia verification with computational tools and OSINT: — Russia-Ukraine conflict case studies. — 2023. https://doi.org/10.48550/arXiv.2310.01978.

Yann LeCun, Yoshua Bengio, and Geoffrey Hinton (2015). Deep learning. Nature. — 521(7553):436. — 2015. https://doi.org/10.1038/nature14539.

Walkow M. and Pöhn D. (2023). Systematically Searching for Identity-Related Information in the Internet with OSINT Tools. In Proceedings of the 9th International Conference on Information Systems Security and Privacy. — SciTePress. — Pp. 402–409. https://doi.org/10.48550/arXiv.2407.16251

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Vol. 5. Is. 3. Number 19 (2024). Pp. 90–98
Journal homepage: https://journal.iitu.edu.kz
https://doi.org/10.54309/IJICT.2024.19.3.008

A COMPARATIVE STUDY OF SOFTWARE-DEFINED RADIO (SDR) AND SMART ACOUSTIC SENSOR PERFORMANCE FOR UAV DETECTION

D. Utebayeva*, L. Ilipbayeva
Satbayev University, Almaty, Kazakhstan.
E-mail: d.utebayeva@satbayev.university

Dana Utebayeva — PhD, researcher, Satbayev University, Almaty, Kazakhstan
E-mail: d.utebayeva@ satbayev.university, https://orcid.org/0000-0002-5535-9200;
Lyazzat Ilipbayeva — associate professor, Satbayev University, Almaty, Kazakhstan
E-mail: l.ilipbaye-va@iitu.edu.kz, https://orcid.org/0000-0002-4380-7344.

© D. Utebayeva, L. Ilipbayeva, 2024

Abstract. Unmanned aerial vehicles (UAVs) pose significant security challenges, especially in sensitive areas such as government buildings, schools, kindergartens, and borders. Effective detection and identification of UAVs are critical to protect sensitive areas from unauthorized access or hostile use. In terms of the ability to effectively detect the activity of suspected UAVs in these critical areas, there are two frequency-based detection technologies: acoustic sensors and program-defined radio (SDR). This study presents a comparative analysis of these technologies and evaluates their effectiveness in UAV identification. By analyzing UAV acoustic signatures and radio frequency (RF) emissions, the authors attempted to evaluate the strengths, limitations, and practical applications of each system. The findings indicate that although both technologies are effective, the choice between them depends on environmental conditions, UAV characteristics, and specific use cases. The researchers also attempted to analyze their effective performance sides to combine both for reliable recognition.

Keywords: drone detection, software-defined radio (SDR), acoustic sensors, unmanned aerial vehicles (UAVs), signal processing, RF emissions, and UAV recognition

For citation: *D. Utebayeva, L. Ilipbayeva. A COMPARATIVE STUDY OF SOFTWARE-DEFINED RADIO (SDR) AND SMART ACOUSTIC SENSOR PERFORMANCE FOR UAV DETECTION. // INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES. 2024. Vol. 5. No. 19. Pp. 90–98 (In Eng.). https://doi.org/10.54309/IJICT.2024.19.3.008.*

Funding. *The research was funded by the Committee of Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan (grant IRN AP14971907, "Development of a robust frequency-based detection system for suspicious UAVs using SDR and acoustic signatures").*

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

БАҒДАРЛАМАМЕН АНЫҚТАЛАТЫН РАДИО-ЖҮЙЕНІҢ (SDR) ЖӘНЕ ИНТЕЛЛЕКТУАЛДЫ АКУСТИКАЛЫҚ СЕНСОРДЫҢ ОРЫНДАУ ҚАБІЛЕТТЕРІН ҰШҚЫШСЫЗ ҰШУ АППАРАТТАРЫН ТАНУҒА САЛЫСТЫРМАЛЫ ЗЕРТТЕУ

Д. Утебаева*, Л. Илипбаева
Satbayev университеті, Алматы, Қазақстан.
E-mail: d.utebayeva@satbayev.university

Дана Утебаева— PhD, Зерттеуші, Satbayev университеті, Алматы, Қазақстан
E-mail: d.utebaye-va@satbayev.university, https://orcid.org/0000-0002-5535-9200;
Ляззат Илипбаева— Техника ғылымдарының кандидаты, Satbayev университеті, Алматы, Қазақстан
E-mail: l.ilipbayeva@iitu.edu.kz, https://orcid.org/0000-0002-4380-7344.

© Д. Утебаева, Л. Илипбаева, 2024

Аннотация. Ұшқышсыз ұшу аппараттары (ҰҰА) әсіресе үкіметтік ғимараттар, мектептер, балабақшалар және шекаралар сияқты сезімтал аймақтарда маңызды қауіпсіздік мәселелерін тудырады. ҰАА-н тиімді анықтау және сәйкестендіру сезімтал аймақтардағы рұқсатсыз кіруден немесе дұшпандық пайдаланудан қорғау үшін өте маңызды болып табылады. Осы маңызды салаларда күдікті ҰҰА-ның әрекетін тиімді анықтау қабілеті тұрғысынан жиілікке негізделген екі анықтау технологиялары бар: акустикалық сенсорлар және бағдарламамен анықталатын радио-жүйе (SDR). Бұл зерттеу осы технологиялардың салыстырмалы талдауын ұсынады және олардың ұшқышсыз ұшу аппараттарын анықтаудағы тиімділігін бағалайды. ҰҰА-ның акустикалық белгілері мен радиожиілік (РЖ) сәулеленулерін талдау арқылы әрбір жүйенің артықшылықтарын, шектеулерін және практикалық қолдануларын бағалауға тырыстық. Біздің қорытындыларымыз негізінде екі технология да тиімді болғанымен, олардың арасындағы таңдау қоршаған орта жағдайларына, ҰҰА-ның өнімділігіне және нақты пайдалану жағдайларына байланысты. Сонымен қатар, сенімді тану үшін екі жүйені біріктіруге олардың тиімді өнімділік жақтарын талдауға тырыстық.

Түйін сөздер: Дронды анықтау, бағдарламамен анықталатын радио-жүйе (SDR), акустикалық сенсорлар, ұшқышсыз ұшу аппараттары (ҰҰА), сигналдарды өңдеу, РЖ сәулелену және ҰҰА тану

Дәйексөз үшін: *Д. Утебаева, Л. Илипбаева. БАҒДАРЛАМАМЕН АНЫҚТАЛАТЫН РАДИО-ЖҮЙЕНІҢ (SDR) ЖӘНЕ ИНТЕЛЛЕКТУАЛДЫ АКУСТИКАЛЫҚ СЕНСОРДЫҢ ОРЫНДАУ ҚАБІЛЕТТЕРІН ҰШҚЫШСЫЗ ҰШУ АППАРАТТАРЫН ТАНУҒА САЛЫСТЫРМАЛЫ ЗЕРТТЕУ. // ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ. 2024. Т. 5. No. 19. 90–98 бет. (ағылшын тілінде). https://doi.org/10.54309/IJICT.2024.19.3.008.*

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

СРАВНИТЕЛЬНОЕ ИССЛЕДОВАНИЕ ХАРАКТЕРИСТИК ПРОГРАММНО-КОНФИГУРИРУЕМОЙ РАДИОСИСТЕМЫ (SDR) И ИНТЕЛЛЕКТУАЛЬНЫХ АКУСТИЧЕСКИХ ДАТЧИКОВ ДЛЯ ОБНАРУЖЕНИЯ БПЛА

Д. Утебаева*, Л. Илипбаева
Satbayev университет, Алматы, Казахстан.
E-mail: d.utebayeva@satbayev.university

Дана Утебаева— PhD, исследователь, Satbayev университет, Алматы, Казахстан
E-mail: d.ute-bayeva@satbayev.university, https://orcid.org/0000-0002-5535-9200;
Ляззат Илипбаева— кандидат технических наук, Satbayev университет, Алматы, Казахстан
E-mail: l.ilipbayeva@iitu.edu.kz, https://orcid.org/0000-0002-4380-7344.

© Д. Утебаева, Л. Илипбаева, 2024

Аннотация. Беспилотные летательные аппараты (БПЛА) представляют собой существенные проблемы безопасности, особенно в таких чувствительных зонах, как правительственные здания, школы, детские сады и границы. Эффективное обнаружение и идентификация БПЛА имеют решающее значение для защиты чувствительных зон от несанкционированного доступа или враждебного использования. С точки зрения способности эффективно обнаруживать активность подозрительных БПЛА в этих критически важных областях, существуют две технологии частотного обнаружения: акустические датчики и программно-определяемая радиосвязь (SDR). В этом ис-следовании проводится сравнительный анализ этих технологий и оценивается их эффективность в идентификации БПЛА. Анализируя акустические сигнатуры БПЛА и радиочастотные (РЧ) излучения, мы попытались оценить сильные стороны, ограничения и практическое применение каждой системы. Наши выводы показывают, что, хотя обе технологии эффективны, выбор между ними зависит от условий окружающей среды, характеристик БПЛА и конкретных вариантов использования. Кроме того, мы попытались проанализировать их эффективные стороны производительности для объединения обеих для надежного распознавания.

Ключевые слова: обнаружение дронов, программно-определяемая радиосистема (SDR), акустические датчики, беспилотные летательные аппараты (БПЛА), обработка сигналов, радиочастотное излучение и распознавание БПЛА

Для цитирования: *Д. Утебаева, Л. Илипбаева. СРАВНИТЕЛЬНОЕ ИССЛЕДОВАНИЕ ХАРАКТЕРИСТИК ПРОГРАММНО-КОНФИГУРИРУЕМОЙ РАДИОСВЯЗИ (SDR) И АКУСТИЧЕСКИХ ДАТЧИКОВ ДЛЯ ОБНАРУЖЕНИЯ БПЛА. // МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ. 2024. Т. 5. No. 19. Стр. 90–98. (На анг.). https://doi.org/10.54309/IJICT.2024.19.3.008.*

Introduction

Unmanned aerial vehicles, sometimes called drones, are becoming increasingly com-mon as they can be used in many different aspects of our daily lives. But even with these benefits, there are many risks and challenges associated with using UAVs, especially when it comes to safety (Seidaliyeva et al., 2020; Taha et al., 2019). Unauthorized UAV use can have serious consequences when it occurs close to highly sensitive locations like airports, power plants, government buildings, and other vital infrastructures (Seidaliyeva et al., 2024). It can also occur in populated areas like kindergartens, universities, and schools. Cases of airspace

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

incidents in critical facilities, including drone malfunctions, have increased in frequency in recent years (Utebayeva et al., 2023; Seidaliyeva et al., 2024). In this regard, there is an urgent need to create and develop effective UAV detection and identification systems. To ensure a timely response to any threats, modern UAV detection systems aim to solve the problem of early warning and detection of drones. It is essential to identify drones and accurately classify, categorize, and track them based on their type, flight path and range (Samaras et al., 2019; Taha et al., 2019). When building such systems, it is necessary to use several strategies and technologies that guarantee accurate, fast detection with a small number of false positives. Smart acoustic sensors (Kashyap et al., 2023; Utebayeva et al., 2023) and software-defined radios (SDR) (Chiper et al., 2023) are two prominent options among several UAV detection methods based on frequency characteristics. Each of these two methods offers unique features, advantages, and disadvantages in addition to different operating principles.

Intelligent acoustic sensors use the ability of microphones and neural networks to recognize UAV sounds. Each model, their actions and UAV states have a unique sound signature, which depends on the rotation speed of the propellers, the number of engines and aerodynamic characteristics. Using digital signal processing techniques such as Fast Fourier Transform (FFT) and their time-frequency processing, these acoustic signatures can be extracted and the sound source can be identified as a UAV (Utebayeva et al., 2023). The advantage of this approach is its passive nature: acoustic sensors do not emit any signals, which makes them less noticeable to a potential intruder. In addition, acoustic sensors are inexpensive and easy to install, which makes them available for widespread use. However, despite the obvious advantages, intelligent acoustic systems also have several significant limitations. First, their operation is highly dependent on the environment. In conditions of strong wind, rain or in noisy urban areas, the effectiveness of acoustic sensors is significantly reduced due to interference from extraneous sounds. In addition, acoustic sensors have a limited range, which cannot offer their use in large open spaces or requires the repetition of installation of several points. There is also a risk of false alarms, when the system can mistakenly identify other sound sources, such as helicopters, motorcycles, or construction equipment, if these sounds are not sufficiently trained in those systems.

UAVs produce radio frequency (RF) signals (Tian et al., 2024) that can be captured and analyzed by software-defined radios (SDRs), which are adaptive systems. Radio transmissions are used by most drones for GPS (global positioning system), as well as for control and data transmission (Bisio et al., 2024; Chiper et al., 2023). By tuning the receiver to different frequencies and communication protocols, SDRs can detect signals emitted by unmanned aerial vehicles (UAVs) and then analyze them to find out various data points, such as the type of device, the frequency of transmission, and the signal strength. The extended detection range of the SDR is one of its key advantages. Since radio signals can be detected at a greater distance than sound sensors, the SDR is especially useful in open areas and situations where drone detection must occur early. Additionally, the SDR can operate over a wide frequency range, allowing it to monitor more complex, encrypted, or frequency-hopping data transmissions in addition to regular UAV control signals. But SDRs also face some challenges. Primarily we would like to consider the issue of radio spectrum congestion, especially in urban environments where multiple devices (such as Wi-Fi, cell phones, and radios) generate increased levels of radio noise that can interfere with the detection of UAV signals. Additionally, drones can be difficult to identify using SDRs due to their use of secure communications channels or frequency manipulation (Chiper et al., 2023; Gelman et al., 2019). There is also

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

the fact that SDR systems can be more expensive to install and maintain than acoustic sensors due to their greater need for complex and expensive hardware.

The aim of this study is to conduct a thorough analysis and comparison of two UAV detection technologies: software-defined radios (SDR) and intelligent acoustic sensors. The objectives of the study are to comparatively study their main advantages, disadvantages, and areas of application. The results of the study will be useful in identifying the best circumstances for using each technology and in suggesting which one to use based on the specifics of the task, such as border control, airport security, or urban safety.

Material and methods

Regarding drone recognition, intelligent acoustic and SDR sensors are complementary in their own ways. The following will discuss the general operations and steps of these two sensors individually:

Smart Acoustic Sensors

Intelligent acoustic sensors can recognize and analyze specific sound signatures generated by unmanned aerial vehicles (UAVs) using neural networks, complex signal processing, and microphones. Propeller rotation and moving activity are the main sources of sound produced by UAVs. The type of UAV, its flight speed, altitude, load, distance from the microphone, and ambient noise can all affect these sound signatures. That is, to detect unmanned aerial vehicles (UAVs) using acoustic sensors, various approaches to capturing, filtering, and analyzing sound data are integrated to accurately detect and identify UAVs in real operating conditions.

The development of intelligent acoustic sensor system consists of the following components: Selection and placement of acoustic sensor microphones, Capture and pre-processing of audio data, Extraction of acoustic features, Classification based on machine and deep learning, and Performance evaluation and testing in real-world conditions (Utebayeva et al., 2023; Dumitrescu et al., 2020; Shi et al., 2018; Sonain et al., 2020).

a) Selection and placement of acoustic sensor microphones: to record the UAV audio signals, various microphones were used, including those built into laptops, which could capture sounds in a wide range of frequencies (from 20 Hz to 20 kHz). This allows recording sounds emitted by the drones' engines and rotating propellers, which have distinctive acoustic properties. The placement of sensors considers the environmental conditions. To reduce the impact of background noise and obstacles on the sound wave, microphones are located either on the ground or at a height of approximately two to three meters above it. At the same time, it was assumed that multiple sensors would be used to ensure accurate triangulation of the sound source to determine the location of the UAV. Typically, the distance between sensors to cover a large radius is fifty meters or 100-150 meters.

b) Capture and pre-processing of audio data: Audio signals are continuously recorded and the information is stored for further processing on a sensor device.

c) Extraction of acoustic features: after filtering the frequency domains of audio signals, the main elements of the UAV sound begin to be identified at the feature extraction stage. That is, at the first stage, the spectral power density of the audio signal, frequency peaks and time dependencies are processed. For this, signal processing methods are used: fast Fourier transform (FFT) and further processing of frequency-time characteristics. These methods allow identifying distinctive spectral features from the UAV sounds.

d) Classification based on Machine and Deep Learning: the accuracy of recognizing the acoustic signatures of UAVs is improved by using machine learning or deep learning

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

methods. The training process uses a database of the sound characteristics of different drone models that have been captured. And Machine Learning and Deep Learning algorithms are trained to identify different types of drones based on their acoustic properties. Real-time classification is performed for each sound event that the system senses.

e) Performance evaluation and testing in real-world conditions: The final stage of development will involve testing the intelligent acoustic sensor system. To confirm the reliability of the neural network-based model, experimental data is used to evaluate the system performance metrics, such as overall recognition accuracy and classification accuracy report. The percentage of correctly classified events indicates the UAV detection accuracy, which is the main performance statistic.

Thus, intelligent acoustic sensors can provide better recognition capabilities through Deep Learning and Machine Learning methods in recognizing UAV sounds, their payloads, and their various states. However, its main limitation is the recognition range (Wang et al., 2021; Jeon et al., 2017; Katta et al., 2022; Utebayeva et al., 2021).

Software-Defined Radio (SDR)

Unmanned aerial vehicles (UAVs) emit radio frequency (RF) signals that can be detected and analyzed by software-defined radios (SDRs), which are incredibly versatile devices. Most drone operations rely on these RF signals (Flak et al., 2023), as they are commonly used for several mission-critical tasks such as data transmission, remote control, and GPS navigation. With SDR technology, receivers can be easily tuned to different frequencies and configured to support different communication protocols such as Wi-Fi, Bluetooth, or proprietary RF protocols unique to specific UAV models (Wen-Tzu Chen et al., 2017; Chiper et al., 2023).

SDR devices can use this adaptability to identify radio emissions from UAVs operating in different frequency bands, whether they are using GPS signals for autonomous navigation or are in direct communication with a ground station. SDR systems can obtain important information about UAVs in addition to detecting their existence due to their ability to track and interpret these radio frequency emissions. Thus, SDR technology is another effective tool for UAV detection and identification due to its adaptability and flexibility. It provides real-time intelligence in various operational scenarios (Chiper et al., 2023; Seidaliyeva et al., 2024; Utebayeva et al., 2023).

Table 1 - Comparative Analysis for “Intelligent Acoustic Sensor” and “SDR Sensor” for UAV Detection Systems

Methods	Advantages	Limitations
Smart Acoustic Sensor	- Since they do not emit any signals, acoustic sensors are harder to detect. - They are not too expensive to use. - Not requiring line of sight, passive detection is advantageous in densely populated areas.	- The detection range of acoustic sensors is often llimited. - Ambient noises can impede the precision of detection. - Similar noises coming from other sources may cause false alarms.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

SDR technology	- Depending on the RF signal strength and surrounding conditions, SDRs can detect UAVs for longer distances. - SDRs are capable of being adjusted to many frequency bands and protocols, such as Wi-Fi, GPS, and proprietary protocols. - More specific information about the UAV	- SDR systems need more advanced hardware to process and acquire data. - The RF spectrum is very crowded in urban settings, which can cause signal masking and interference. - Certain UAVs employ frequency-hopping or encrypted communications, which makes it more difficult for SDRs to identify them.

Considering the advantages and disadvantages of these two methods, the following section analyzes the aspects discussed in Table 1.

Results and discussion

We tried to consider the general capabilities of Smart Acoustic Sensor and Software-Defined Radio approaches in terms of recognition area, accuracy, sensitivity to the environment, response time and cost. The reason for this is that these characteristics are crucial for the real-time functionality of the system.

Detection Range

In terms of detection range, the SDR system performed significantly better than the acoustic sensor. This is consistent with the inherent limitations of sound waves propagating through the atmosphere, as opposed to radio frequency transmissions.

Detection Accuracy

Both systems demonstrated high detection accuracy in quiet, controlled conditions, but SDR performed better. However, the accuracy of acoustic sensors drops sharply in noisy urban environments. The main reason for this discrepancy is that background noise obscures the UAV's audio characteristics due to acoustic interference.

Environmental Robustness

SDRs proved to be very robust in a variety of environments. Although densely populated RF spectrums presented challenges in urban environments, sophisticated filtering strategies allowed SDRs to successfully separate UAV transmissions. In contrast, background noise significantly impacted the performance of acoustic sensors, especially when it came from sources with identical frequency characteristics. These sensors also struggled to operate in noisy environments. But these systems are very suitable for border areas.

Response Time

Both systems demonstrated real-time detection capabilities. Acoustic sensors typically exhibit faster response times due to their immediate audio transmission and simple signal processing. Due to the complexity of RF signal processing and decoding, SDRs have slightly higher latency, although they can operate in real time.

Cost-effectiveness

Acoustic sensors, especially for close-range detection in controlled situations, are significantly cheaper and easier to install than SDRs. SDR systems can cover larger areas and provide more detailed information, so despite their higher cost, they are more suitable for high-security facilities.

Conclusion

Comparative analysis shows that although their performance varies depending on the specific application and environment, both acoustic sensors and SDR systems offer signifi-

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

cant capabilities for UAV detection and identification. SDRs perform better in large, complex environments and provide more specific data on UAV properties, while acoustic sensors are less expensive and more suitable for confined, monitored locations with little noise interference. The use of intelligent acoustic sensors for drones with payloads is becoming more reliable. Thus, integrating these two approaches to create a complex framework is the best solution for reliable real-time systems.

Future research *could explore fusion systems that combine both acoustic and RF detection methods, thereby capitalizing on the advantages of each technology to develop a more comprehensive and adaptive UAV detection system.*

REFERENCES

Bisio I., Garibotto C., Haleem H., Lavagetto F., Sciarrone A. (2024). RF/WiFi-based UAV surveillance systems: A systematic literature review, Internet of Things. — Volume 26. —101201. — ISSN 2542–6605. https://doi.org/10.1016/j.iot.2024.101201.

Chiper F.-L., Martian A., Vladeanu C., Marghescu I., Craciunescu R., Fratu O. (2022). Drone Detection and Defense Systems: Survey and a Software-Defined Radio-Based Solution. Sensors. — 22. — 1453. https://doi.org/10.3390/s22041453

Dumitrescu C., Minea M., Costea I.M., Cosmin Chiva I., Semenescu A. (2020). Development of an Acoustic System for UAV Detection. Sensor. — 20. — 4870. https://doi.org/10.3390/s20174870

Flak P. and Czyba R., (2023). "RF Drone Detection System Based on a Distributed Sensor Grid With Remote Hardware-Accelerated Signal Processing," in IEEE Access. — Vol. 11. — Pp. 138759–138772. DOI: 10.1109/ACCESS.2023.3340133.

Kashyap A., Tyagi K.D. and Singh P. (2023). "CRNN-based UAV Detection using Acoustic Signature," 2023 IEEE International Symposium on Smart Electronic Systems (iSES). — Ahmedabad, India. — Pp. 186–190. DOI: 10.1109/iSES58672.2023.00046.

Katta S.S., Nandyala S., Viegas S. and AlMahmoud A. (2022). "Benchmarking Audio-based Deep Learning Models for Detection and Identification of Unmanned Aerial Vehicles," 2022 Workshop on Benchmarking Cyber-Physical Systems and Internet of Things (CPS-IoTBench). — Milan, Italy. — Pp. 7–11. DOI: 10.1109/CPS-IoTBench56135.2022.00008.

Gelman I.S., Loftus J.P., Hassan A.A. (2019). Adversary UAV Localization with Software Defined Radio; Worcester Polytechnic Institute: Worcester. — MA, USA. — 2019. — Tech. Rep. — E-project-041719-144214.

Jeon S., Shin J.-W., Lee Y.-J., Kim W.-H., Kwon Y. and Yang Y. (2017). "Empirical study of drone sound detection in real-life environment with deep neural networks," 2017 25th European Signal Processing Conference (EUSIPCO). — Kos, Greece. — Pp. 1858–1862. DOI: 10.23919/EUSIPCO.2017.8081531.

Taha B. and Shoufan A. (2019). "Machine Learning-Based Drone Detection and Classification: State-of-the-Art in Research," in IEEE Access. — Vol. 7. — Pp. 138669–138682. DOI: 10.1109/ACCESS.2019.2942944.

Tian Y., Wen H., Zhou J., Duan Z., Li T. (2024). Optimized Radio Frequency Footprint Identification Based on UAV Telemetry Radios. Sensors. — 24. — 5099. https://doi.org/10.3390/s24165099

Seidaliyeva U., Akhmetov D., Ilipbayeva L., Matson E.T. (2020). Real-Time and Accurate Drone Detection in a Video with a Static Background. Sensors. — 20. — 3856. https://doi.org/10.3390/s20143856

Seidaliyeva U., Ilipbayeva L., Taissariyeva K., Smailov N., Matson E.T. (2024). Advances and Challenges in Drone Detection and Classification Techniques: A State-of-the-Art Review. — Sensors. — 24. —125. https://doi.org/10.3390/s24010125

Samaras S., Diamantidou E., Ataloglou D., Sakellariou N., Vafeiadis A., Magoulianitis V., Lalas A., Dimou A., Zarpalas D., Votis K. et al. (2019). Deep Learning on Multi-Sensor Data for Counter UAV Applications — A Systematic Review. Sensors. —19. — 4837.

Shi L., Ahmad I., He Y., Chang K. (2018). Hidden Markov model-based drone sound recognition using MFCC technique in practical noisy environments. — J. Commun. Netw. — 20. — Pp. 509–518.

Sonain J., Fawad; Rahman M., Ullah A., Badnava S., Forsat M., Mirjavadi S.S. (2020). Malicious UAV Detection Using Integrated Audio and Visual Features for Public Safety Applications. Sensors. — 20. — 3923.

Utebayeva D., Ilipbayeva L., Matson E.T. (2023). Practical Study of Recurrent Neural Networks for Efficient Real-Time Drone Sound Detection: A Review. Drones. — 7. — 26. https://doi.org/10.3390/drones7010026

Wen-Tzu Chen and Chen-Hsun Ho (2017). Spectrum monitoring with unmanned aerial vehicle carrying a

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

receiver based on the core technology of cognitive radio – A software-defined radio design. — *Journal of Unmanned Vehicle Systems*. — 5(1): — 1–12. https://doi.org/10.1139/juvs-2016-0011

Wang Y., Fagian Y., Ho K.E. and Matson E.T. (2021). "A Feature Engineering Focused System for Acoustic UAV Detection," 2021 Fifth IEEE International Conference on Robotic Computing (IRC). — Taichung, Taiwan. — Pp. 125–130. DOI: 10.1109/IRC52146.2021.00031.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

АҚПАРАТТЫҚ ҚАУІПСІЗДІК ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАРҒА АРНАЛҒАН

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

INFORMATION SECURITY AND COMMUNICATION TECHNOLOGIES

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Vol. 5. Is. 3. Number 19 (2024). Pp. 99–114
Journal homepage: https://journal.iitu.edu.kz
https://doi.org/10.54309/IJICT.2024.19.3.009

DEVELOPMENT OF METHODS FOR ENSURING THE SECURITY OF INDUSTRIAL AUTOMATION AND CONTROL NETWORKS AT ENTERPRISES

N.T. Duzbayev, A. Makeyev*, Y.Y. Ospanov
International Information Technology University , Almaty, Kazakhstan.
E-mail: 36169@iitu.edu.kz

Duzbayev Nurzhan Tokkuzhaevich — PhD, International Information Technology University, Almaty, Kazakhstan
E-mail: n.duzbayev@iitu.edu.kz, https://orcid.org/0000-0002-7989-9463;
Alibek Makeyev — Master's student,Computer Systems and Software Engineering, International In-formation Technology University, Almaty, Kazakhstan
E-mail: 36169@iitu.edu.kz, https://orcid.org/0009-0001-5174-825X;
Ospanov Yerlan Yerzhanovich, **—** PhD, First Deputy Head of the NSC ACADEMY
E-mail: acade-my@knb.kz, https://orcid.org/0009-0002-9256-9909.

© N.T. Duzbayev, A. Makeyev, Y.Y. Ospanov, 2024

Abstract. In the context of modern high demands on the efficiency and reliability of production processes, the security of industrial automation and control networks is becoming extremely important. This article is devoted to the research and development of methods for ensuring the security of industrial automation and control networks at enterprises, especially in the view of the growing threat of cyberattacks and other risks. The main objective of the work is to characterize industrial networks, their features and characteristics that affect approaches to ensuring security. The main threats are considered, including cyberattacks, physical interference and human errors, as well as their potential consequences for production. The authors develop and document methods for ensuring the security of industrial automation and control networks at enterprises. This includes analyzing current threats, identifying vulnerabilities and developing comprehensive solutions to protect industrial automation and control networks from various types of attacks and risks, as well as recommendations for their implementation and support. The results of the study emphasize the need for a comprehensive approach to ensuring security, and continuous monitoring and adaptation to new threats in a rapidly changing cyberspace. The project is aimed for specialists in the field of industrial

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

automation and information security, as well as business leaders who are interested in protecting their production systems.

Keywords: industrial automation, security, control networks, cyber threats, protection methods, network segmentation, access control

For citation: *N.T. Duzbayev, A. Makeyev, Y.Y. Ospanov. DEVELOPMENT OF METHODS FOR ENSURING THE SECURITY OF INDUSTRIAL AUTOMATION AND CONTROL NETWORKS AT ENTERPRISES // INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES. 2024. Vol. 5. No. 19. Pp. 99–114 (In Russ.). https://doi.org/10.54309/IJICT.2024.19.3.009.*

КӘСІПОРЫНДАРДАҒЫ ӨНДІРІСТІК АВТОМАТТАНДЫРУ ЖӘНЕ БАСҚАРУ ЖЕЛІЛЕРІНІҢ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТУ ӘДІСТЕРІН ӘЗІРЛЕУ

Н.Т. Дузбаев, А. Макеев*, Е.Е. Оспанов
Международный университет информационных технологий, Алматы, Казахстан.
E-mail: 36169@iitu.edu.kz

Дузбаев Нуржан Токкужаевич — PhD, Халықаралық ақпараттық технологиялар университеті, Алматы, Казахстан
E-mail: n.duzbayev@iitu.edu.kz, https://orcid.org/0000-0002-7989-9463;
Алибек Макеев — магистрант ОП «Вычислительная техника и программное обеспечение», Международный университет информационных технологий, Алматы, Казахстан
E-mail: 36169@iitu.edu. kz, https://orcid.org/0009-0001-5174-825X;
Оспанов Еран Ержанұлы — PhD, ҰҚК академиясының 1 орынбасары бастығы
E-mail: acade-my@knb.kz, https://orcid.org/0009-0002-9256-9909.

© Н. Дузбаев, А. Макеев, Е.Е. Оспанов, 2024

Аннотация. Өндірістік процестердің тиімділігі мен сенімділігіне бүгінгі күннің жоғары талаптарымен өнеркәсіптік автоматтандыру және басқару желілерінің қауіпсіздігі өте маңызды болды. Бұл жоба кәсіпорындардағы өнеркәсіптік автоматтандыру және басқару желілерінің қауіпсіздігін қамтамасыз ету әдістерін зерттеуге және әзірлеуге арналған, әсіресе кибершабуылдар мен басқа да тәуекелдердің өсіп келе жатқан қаупі жағдайында. Жұмыстың негізгі мақсаты - өндірістік желілерді, олардың ерекшеліктері мен қауіпсіздік тәсілдеріне әсер ететін сипаттамаларын сипаттау. Кибершабуылдар, физикалық кедергілер және адам қателері және олардың өндіріске ықтимал әсері сияқты негізгі қауіп-қатерлер қарастырылады. Бұл жұмыстың негізгі мақсаты кәсіпорындардағы өнеркәсіптік автоматтандыру және басқару желілерінің қауіпсіздігін қамтамасыз ету әдістерін әзірлеу және құжаттау болып табылады. Бұл ағымдағы қауіптерді талдауды, осалдықтарды анықтауды және өнеркәсіптік автоматтандыруды және басқару желілерін әртүрлі шабуылдар мен тәуекелдерден қорғау үшін кешенді шешімдерді әзірлеуді, сондай-ақ оларды енгізу және қолдау бойынша ұсыныстарды қамтиды. Зерттеу нәтижелері қауіпсіздікке кешенді көзқарас, сондай-ақ жылдам өзгеретін киберкеңістікте жаңа қауіптерге тұрақты мониторинг және бейімделу қажеттілігін көрсетеді. Жоба өнеркәсіптік автоматтандыру және ақпараттық қауіпсіздік саласындағы мамандарға, сондай-ақ олардың өндірістік

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

жүйелерін қорғауға мүдделі бизнес-менеджерлерге бағытталған.

Түйін сөздер: өнеркәсіптік автоматтандыру, қауіпсіздік, басқару желілері, киберқауіптер, қорғау әдістері, желіні сегменттеу, қол жеткізуді басқару

Дәйексөз үшін: *Н. Дузбаев, А. Макеев, Е.Е. Оспанов. КӘСІПОРЫНДАРДАҒЫ ӨНДІРІСТІК АВТОМАТТАНДЫРУ ЖӘНЕ БАСҚАРУ ЖЕЛІЛЕРІНІҢ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТУ ӘДІСТЕРІН ӘЗІРЛЕУ//ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ. 2024. Т. 5. No. 19. 99–114 бет. (орыс тілінде). https://doi.org/10.54309/IJICT.2024.19.3.009.*

РАЗРАБОТКА МЕТОДОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ СЕТЕЙ АВТОМАТИЗАЦИИ И УПРАВЛЕНИЯ НА ПРЕДПРИЯТИЯХ

Н.Т. Дузбаев, А. Макеев*, Е.Е. Оспанов
Международный университет информационных технологий, Алматы, Казахстан.
E-mail: 36169@iitu.edu.kz

Дузбаев Нуржан Токкужаевич — PhD, Международный университет информационных техно-логий, Алматы, Казахстан
E-mail: n.duzbayev@iitu.edu.kz, https://orcid.org/0000-0002-7989-9463;
Алибек Макеев — магистрант ОП «Вычислительная техника и программное обеспечение», Международный университет информационных технологий, Алматы, Казахстан
E-mail: 36169@iitu.edu. kz, https://orcid.org/0009-0001-5174-825X;
Оспанов Ерлан Ержанович, **—** PhD, первый заместитель начальника АКАДЕМИИ КНБ
E-mail: academy@knb.kz, https://orcid.org/0009-0002-9256-9909.

© Н.Т. Дузбаев, А. Макеев, Е.Е. Оспанов, 2024

Аннотация. В условиях современных высоких требований к эффективности и надежности производственных процессов безопасность промышленной автоматизации и сетей управления становится чрезвычайно важной. Этот проект посвящен исследованию и разработке методов обеспечения безопасности промышленной автоматизации и сетей управления на предприятиях, особенно в условиях растущей угрозы кибератак и других рисков. Основной целью работы является характеристика промышленных сетей, их особенностей и характеристик, влияющих на подходы к обеспечению безопасности. Рассматриваются основные угрозы, включая кибератаки, физическое вмешательство и человеческие ошибки, а также их потенциальные последствия для производства. Авторы разрабатывают и документируют методы обеспечения безопасности промышленной автоматизации и сетей управления на предприятиях. Это включает в себя анализ текущих угроз, выявление уязвимостей и разработку комплексных решений для защиты сетей промышленной автоматизации и управления от различных типов атак и рисков, а также рекомендаций по их внедрению и поддержке. Результаты исследования подчеркивают необходимость комплексного подхода к обеспечению безопасности, а также постоянного мониторинга и адаптации к новым угрозам в быстро меняющемся киберпространстве. Проект ориентирован на специалистов в области промышленной автоматизации и информационной безопасности, а также руководителей бизнеса, которые заинтересованы в защите своих производственных систем.

Ключевые слова: промышленная автоматизация, безопасность, сети управле-

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

ния, киберугрозы, методы защиты, сегментация сети, контроль доступа.

***Для цитирования**: Н.Т. Дузбаев, А. Макеев, Е.Е. Оспанов. РАЗРАБОТКА МЕТОДОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ СЕТЕЙ АВТОМАТИЗАЦИИ И УПРАВЛЕНИЯ НА ПРЕДПРИЯТИЯХ// МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ. 2024. Т. 5. No. 19. Стр. 99–114. (На русс.). https://doi.org/10.54309/IJICT.2024.19.3.009.*

Введение

Выбор темы «Разработка методов обеспечения безопасности промышленных сетей автоматизации и управления на предприятиях» обусловлен растущими вызовами и потребностями в области защиты критически важных производственных систем в контексте современного технологического развития. Промышленная автоматизация и управляющие сети играют ключевую роль в ведении бизнеса, управлении технологическими процессами, обеспечении контроля и мониторинга производственных операций. Однако с ростом сложности и степени интеграции с корпоративными ИТ-системами возрастает и риск возникновения угроз, которые могут нарушить функционирование этих систем.

Задачи работы:

- Изучить структуру и элементы сетей промышленной автоматизации и управления, включая используемое оборудование и программное обеспечение;- Определить ключевые особенности и требования к безопасности, которые отличают промышленные сети от корпоративных.

Выявление и оценка угроз безопасности:

- Проанализируйте основные угрозы и уязвимости, связанные с PSA, такие как кибератаки, физическое вмешательство и человеческий фактор; Оцените потенциальное воздействие этих угроз на функционирование и безопасность производственных процессов.

В статье анализируются основные методы обеспечения безопасности, такие как сегментация сети, контроль доступа, шифрование данных, мониторинг и анализ, обновление программного обеспечения и внесение исправлений, а также физическая безопасность. Подробно рассматриваются практические аспекты внедрения этих методов и их интеграции в существующие системы промышленной автоматизации и сети управления.

Проект включает в себя обзор современных решений и технологий, а также рекомендации по их внедрению для повышения безопасности промышленных сетей. Важная роль также отводится обучению персонала и разработке политик безопасности, что позволяет нам создавать комплексный подход к защите промышленных систем.

В современном промышленном производстве автоматизация и управление играют ключевую роль в обеспечении эффективности и стабильности процессов. Сети промышленной автоматизации и управления включают в себя оборудование и программное обеспечение, которые обеспечивают контроль, мониторинговое и управляющее управление технологическими процессами. Однако с ростом взаимосвязанности и интеграции различных систем возрастает и риск возникновения угроз безопасности. Важность промышленной и управленческой безопасности возрастает в связи с потенциальными кибератаками, которые могут привести к серьезным последствиям, таким как сбои в производстве, ущерб окружающей среде или даже угроза жизни персонала. В данной статье рассматриваются основные методы

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

обеспечения безопасности промышленных сетей, их характеристики и практическое применение. Предметом исследования являются методы и технологии обеспечения безопасности промышленной автоматизации и сетей управления. Это включает в себя: разработку и внедрение мер по защите от киберугроз. Технологии и протоколы для обеспечения защиты данных и систем. Подходы к сегментации сети, контролю доступа, шифрованию данных и мониторингу безопасности. Методы защиты от естественных помех и человеческих ошибок. Предмет исследования: предметом исследования является промышленная автоматизация и сети управления на предприятиях. Сюда входят: инфраструктура и компоненты промышленной автоматизации и сетей управления, такие как контроллеры, датчики, исполнительные механизмы и системы управления. Сетевые протоколы и каналы связи, используемые в сетях промышленной автоматизации и управления.

Процессы и системы, которые взаимодействуют с промышленными сетями автоматизации и управления, включая корпоративные IT-системы и облачные платформы.

Методологии и практики обеспечения безопасности, применяемые в контексте промышленных сетей автоматизации и управления.

Таким образом, исследование сосредоточено на разработке и оценке методов безопасности, направленных на защиту сложных и критически важных промышленных сетей автоматизации и управления, с целью обеспечения их надежности, защиты от угроз и минимизации рисков для предприятия.

Материалы и методы исследования

Изучение международных и национальных стандартов, таких как ISO/IEC 27001, IEC 62443, NIST Cybersecurity Framework, которые определяют требования и лучшие практики для обеспечения безопасности промышленных сетей. Научные статьи и монографии: Анализ научных публикаций, посвященных современным методам и технологиям защиты промышленных сетей, а также тенденциям в области кибербезопасности и автоматизации.

Результаты

На сегодняшний день специалисты отмечают увеличение числа специалистов, обладающих современными навыками в области автоматизации зданий, и реализацию множества проектов в этой области. В то же время существует осознание необходимости перехода на новые стандарты.

В области информационных технологий необходимость защиты от киберугроз больше не ставится под сомнение. Эта потребность становится все более актуальной для промышленных систем управления. Успешная кибератака на такую систему может привести к значительным производственным потерям, нарушениям безопасности и ущербу окружающей среде, а также к утечке интеллектуальной собственности (Афонин и др., 2019). Промышленные сети, работающие непрерывно и в соответствии со строгими правилами, часто игнорируют многие политики безопасности, применимые к информационным сетям.

Ранее основной причиной защиты промышленных сетей считался человеческий фактор или сбои в их работе. В результате автоматизированное оборудование было разработано без учета риска нежелательного или неподходящего сетевого трафика. Угрозы кибератак, особенно международного характера, нацеленных на промышленные системы, практически игнорировались.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

Совсем недавно в системах управления, которые не имели прямого доступа к информационным сетям компании и Интернету, использовались закрытые протоколы передачи данных. Это обеспечило безопасность промышленной сети за счет ее изоляции. Однако за последние 10–20 лет произошел переход от запатентованных технологий и стандартов к коммерчески доступным решениям в промышленных сетях (Баранова и др., 2020). Необходимость получения технологических данных из Интернета требует подключения технологических сетей к информационным системам и глобальной сети. Современные технологические сети требуют постоянного удаленного доступа и обновления данных, что делает невозможным их изоляцию. Например, промышленный Ethernet стал стандартом в области технологических коммуникаций. Аппаратное обеспечение теперь использует протоколы на основе IP, включая TCP / IP и UDP, унаследовав их уязвимости. В связи с необходимостью интеграции систем управления производством (SCADA/DMS) с высокоуровневыми ERP/MES-системами изолированность промышленной сети утратила свое значение. Кроме того, необходимо учитывать возможность проникновения вредоносных программ через интерфейсы удаленного управления и USB-порты рабочей станции, что увеличивает риски для безопасности.

Конечные устройства в технологической сети (контроллеры) были разработаны с акцентом на высокую надежность. Однако средства защиты от несанкционированного доступа к ним сегодня находятся на начальном уровне и не могут противостоять современным киберугрозам, требуя совершенствования. Использование методов кибербезопасности IT-сетями не всегда возможно из-за различий в архитектуре, типах оборудования, схемах трафика, внешних условиях и установленных правилах (Бирюков, 2020). Спектр угроз также меняется. Появление специфических промышленных вредоносных программ требует использования специализированных методов и средств защиты. Поэтому важно использовать решения, разработанные специально для промышленного сектора.

Сейчас можно утверждать, что сформировалось новое научное направление — безопасность промышленных сетей. В связи с этим было проведено исследование многих уязвимостей промышленных систем управления и исходных кодов вредоносных программ.

Стандарты ANSI/ISA99, которые обеспечивают кибербезопасность систем автоматизации и управления, обеспечивают хорошую основу для разработки политики безопасности, ориентированной на промышленные системы. Эти стандарты представляют собой общую концепцию кибербезопасности, а также модели и отдельные элементы системы безопасности и являются важными документами для стандарта IEC 62443 «Безопасность систем управления».

В стандарте IEC 62443 описаны методы повышения безопасности в промышленных сетях, охватывающие всю область промышленной безопасности без отраслевых ограничений (Вихляев, 2020). Промышленные брандмауэры, разработанные в соответствии с этим стандартом, уже представлены на рынке, которые позволяют создавать безопасные зоны с помощью ПЛК и OPC-серверов.

В некоторых отраслях промышленности существуют свои собственные специфические стандарты сетевой безопасности. Например, стандарт NERC CIP разработан для энергетики Северной Америки. В отличие от стандарта IEC 62443, сертификация NERC CIP является обязательной в США, в то время как для стандарта

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

IEC 62443 — это добровольный процесс.

Современный рынок промышленной автоматизации открывает большие возможности, но его рост значительно замедляется из-за экономических и политических факторов. Очевидно, что автоматизация является главным двигателем прогресса и должна продолжать развиваться (Воронцов, 2019).

Промышленная автоматизация обеспечивает высокое качество продукции, снижает финансовые затраты, увеличивает конкурентоспособность многих товаров и улучшает безопасность на производстве для сотрудников.

Этапы производства различных продуктов имеют свои особенности, такие как:

- сложность выполнения отдельных процессов;
- высокая чувствительность к сбоям и отклонениям в определенных режимах;
- присутствие вредных летучих веществ в производственной зоне.

Эти факторы подчеркивают необходимость применения современных технологий автоматизации как важной меры безопасности.

Следует отметить, что все системы управления на промышленных предприятиях основаны на программных комплексах, которые учитывают особенности производственных процессов. Поскольку производственные предприятия относятся к объектам повышенной безопасности, для повышения надежности систем внедряются резервные копии файлов и данных автоматизации. Системы автоматического управления создаются по модульному принципу, что позволяет быстро заменять неисправные элементы и восстанавливать их функции.

Сегодня целесообразность автоматизации должна быть продемонстрирована на примере успешных проектов с использованием цифровых данных, которые показывают важность приложения для конкретного бизнеса (Иванов, 2021). Важно донести до целевой аудитории, что автоматизация промышленного предприятия обходится не так дорого, как установка турбины или строительство нового цеха.

Создание защищенной технологической сети основано на принципе глубокой защиты. Это означает, что защита сети передачи данных не ограничивается только периметром, но и включает в себя фрагментацию сети с выделением критических областей в безопасные зоны. Каждая зона должна быть защищена отдельным промышленным брандмауэром, который обеспечит высокий уровень безопасности и поддержит необходимые коммуникации. Промышленные брандмауэры оптимизированы для работы с протоколами Modbus и OPC, а их усовершенствование позволяет ограничить доступ к критически важным сегментам сети.

Помимо технических решений в области кибербезопасности, важно уделять внимание организационным аспектам, в частности обучению персонала. Сотрудники должны быть знакомы с правилами и средствами обеспечения информационной безопасности, а также с разработанными политиками и стандартами. Поскольку специалисты по автоматизированным системам часто обладают ограниченными знаниями в области кибербезопасности, важно объяснить им важность этого вопроса и ввести обязательную программу обучения бизнесу (Камаев и др., 2019). Различные категории сотрудников, такие как посетители, подрядчики, операторы, инженеры, обслуживающий персонал и менеджеры, должны быть осведомлены о своих ролях и обя-занностях, а также получать информацию о разрешенных и запрещенных действиях.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

В производственной зоне технический персонал должен уметь обращаться с охранным оборудованием, менеджеры должны знать алгоритмы действий в случае возникновения угроз безопасности автоматизированных систем управления.

В настоящее время основной проблемой кибербезопасности промышленных предприятий является непонимание специалистами автоматизированных систем управления важности применения соответствующих инструментов, даже при наличии необходимых технологий. Владельцы критически важных объектов часто недооценивают информационные угрозы по целому ряду причин. Наблюдается заметная нехватка необходимых процедур, таких как проверка информации, тестирование на проникновение, сканирование уязвимостей и обучение персонала (Кирсанов, 2021). На сегодняшний день не установлено никаких обязательных стандартов промышленной кибербезопасности.

Также не существует единой, понятной методологии, в рамках которой эксперты по информационной безопасности могли бы рекомендовать меры по достижению адекватного уровня защиты автоматизированных систем управления.

Кроме того, на ситуацию негативно влияет сложный бюрократический процесс внесения изменений в работу ответственных технологических центров. Строгие внутренние правила компании не допускают внесения изменений в уже сертифицированные системы, даже если речь идет об обновлениях операционной системы. При приемке систем методы тестирования программного обеспечения часто не предполагают проверки встроенных функций информационной безопасности (Клепиков и др., 2019). К сожалению, уровень безопасности в основном обеспечивается только за счет ограничения доступа пользователей с помощью пароля, который часто хранится в виде обычного текста в базе данных приложения или на листке бумаги, приклеенном к экрану.

Если говорить о вычислительном оборудовании, используемом в автоматизированных системах управления технологическими процессами, то оно обычно начинает свою работу с устаревшего внутреннего исполняемого кода. Несмотря на наличие на сайте производителя обновленной прошивки, которая может устранить известные проблемы с информационной безопасностью, никто не проверяет ее доступность даже на этапе разработки системы, поскольку это не является приоритетом.

Также стоит учитывать, что автоматизация технологических процессов часто осуществляется сторонними подрядчиками, которые в основном сосредоточены на операционных аспектах проекта, поскольку за это они получают оплату (Клюев и др., 2019). В этом контексте внедрение эффективных мер информационной безопасности можно рассматривать как ненужные затраты. Поэтому заказчикам необходимо осознавать важность кибербезопасности, формулировать соответствующие требования к подрядчикам и контролировать их выполнение.

Промышленная автоматизация — это совокупность методов и технологий, а также программного обеспечения, используемых для создания автоматизированных систем управления и технологических процессов производства без необходимости непосредственного участия оператора.

Автоматизация производственных процессов помогает улучшить качество продукции, снизить затраты и повысить конкурентоспособность.

Использование автоматизированных систем управления технологическими

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

процессами снижает затраты на содержание менее квалифицированного персонала, что, в свою очередь, повышает долговечность оборудования и надежность машин.

Современная промышленная автоматизация также способствует экономии материалов, сырья и ресурсов, а также повышает безопасность производственных процессов и условия труда сотрудников (Кондаков и др., 2021). Внедрение современных автоматизированных компонентов позволяет достичь следующих результатов:

1. снижение простоя оборудования на 10–15 %;
2. сокращение потребления электрической энергии и других энергоресурсов до 35 %;
3. уменьшение затрат на обслуживание производства до 30 %;
4. снижение объемов бракованной продукции.

Учитывая текущее экономическое положение, эти аспекты становятся особенно важными.

Автоматизированная система включает в себя ряд компонентов, обеспечивающих управление объектами и сбор информации о текущих процессах на предприятии (Пищик, 2020). Основные компоненты промышленной автоматизации и их классификация включают:

1. устройства для защиты от импульсного перенапряжения в силовых и информационных линиях;
2. блоки питания, размещаемые в шкафах управления;
3. промышленные сетевые коммутаторы, выполненные в прочных защитных корпусах, что делает их подходящими для промышленного применения;
4. устройства, включающие интерфейсные реле для измерений и контроля;
5. модули ввода и вывода, которые объединяют системы сбора данных и полностью соответствуют требованиям решаемых задач, совместимы с любыми PLS и IPC системами.

Благодаря использованию новых компонентов автоматизация промышленных установок становится более понятной и прозрачной, так как осуществляется контроль и управление через единую информационную базу, к которой подключены все отделы (Попова и др., 2019).

Таким образом, промышленно-технологическая автоматизация предлагает множество преимуществ, таких как:

1. ведение оперативного учета производства;
2. управление затратами и своевременное принятие управленческих решений;
3. планирование работы и распределение трудовых ресурсов и мощностей;
4. оперативное управление производственным циклом;
5. формирование производственной отчетности;
6. комплексный анализ и мониторинг деятельности предприятия;
7. расчет себестоимости производимых товаров.

Важно отметить, что большинство систем промышленной автоматизации организованы по трехуровневой модели:

1. На первом уровне находятся системы контроля и автоматического регулирования технологических подсистем и объектов, основанные на микропроцессорных контроллерах, а также оборудовании КИПиА, измерителях и счетчиках.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

2. Второй уровень включает компоненты для концентрации, обработки и передачи информации между нижним и верхним уровнями.

3. Верхний уровень состоит из устройств для передачи, хранения, накопления и предоставления информационных файлов, включая средства локальной вычислительной сети, которая связывает рабочие подсистемы.

Автоматизация промышленных объектов позволяет получить полностью механизированные ключевые производственные и управленческие бизнес-процессы.

Что в свою очередь значительно уменьшает рутину и повышает производительность труда рабочих на производстве, а само предприятие становится конкурентоспособным, увеличивая тем самым на рынке свою себестоимость.

Сети промышленной автоматизации и управления — это сложные системы, состоящие из аппаратных и программных компонентов, которые обеспечивают управление технологическими процессами на предприятиях (Селевцов, 2019). Эти сети обладают уникальными особенностями, отличающими их от обычных корпоративных сетей, которые требуют особых подходов к обеспечению безопасности. Давайте рассмотрим основные возможности промышленной автоматизации и сетей управления более подробно:

Программируемые логические контроллеры (PLC), используются для автоматизации задач управления и мониторинга технологических процессов. PLC выполняют функции сбора данных, обработки сигналов и управления исполнительными механизмами. Распределённые управляющие системы (DCS), применяются для управления сложными процессами на крупных предприятиях, таких как нефтехимические заводы. DCS обычно включают в себя несколько уровней контроля и взаимодействуют с различными процессами (Снытников, 2020). Системы управления на основе SCADA, предоставляют мониторинг и управление в реальном времени, собирая данные от различных датчиков и контроллеров и представляя их в удобной форме для операторов. Исполнительные механизмы, включают в себя насосы, клапаны, двигатели и другие устройства, которые выполняют физическое воздействие на технологический процесс. Датчики и измерительные приборы, служат для сбора данных о состоянии технологического процесса, таких как температура, давление, уровень и другие параметры. Коммуникационные устройства и протоколы: коммутаторы и маршрутизаторы: обеспечивают связь между различными компонентами сети и передачу данных между контроллерами, датчиками и исполнительными механизмами. Протоколы связи, включают в себя специализированные промышленные протоколы, такие как Modbus, Profibus, Ethernet/IP, OPC, которые предназначены для обмена данными между компонентами ПСАУ и имеют особенности в области надежности и реального времени (Стрельцов, 2019).

Промышленные сети автоматизации и управления должны обеспечивать работу в реальном времени, что означает необходимость немедленного отклика на изменения в процессе и поддержания бесперебойного контроля. Это требует высокой надежности и низкой задержки передачи данных.

Промышленные сети автоматизации и управления должны быть высоко отказоустойчивыми, обеспечивать непрерывную работу даже в случае сбоя отдельных компонентов. Это достигается за счет резервирования критических компонентов и реализации механизмов аварийного восстановления.

Промышленные сети автоматизации и управления часто интегрируются с

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

другими системами, такими как корпоративные ИТ-системы, облачные платформы и системы бизнес-аналитики. Это требует возможности масштабирования и интеграции с различными технологическими решениями (Хорев, 2019).

Промышленные сети автоматизации и управления требуют строгого контроля доступа, чтобы предотвратить несанкционированное вмешательство. Это включает в себя аутентификацию и авторизацию пользователей, а также управление доступом к критическим компонентам системы.

Для обеспечения безопасности данных и предотвращения утечек используется шифрование данных и защитные механизмы для коммуникационных каналов (Чернобровцев, 2019). Это важно для защиты от перехвата данных и их модификации.

Промышленные сети автоматизации управления должны иметь системы мониторинга и управления событиями для своевременного обнаружения и реагирования на инциденты безопасности. Это включает в себя использование систем обнаружения вторжений (IDS), систем управления событиями безопасности (SIEM) и других инструментов.

Промышленные сети играют ключевую роль в автоматизации и управлении производственными процессами. Эти сети обеспечивают связь между различными устройствами, такими как контроллеры, датчики и системы управления, позволяя эффективно обмениваться данными и координировать действия в реальном времени. Важно понимать их характеристики, компоненты и протоколы, используемые в промышленной среде. Ниже представлена таблица, которая обобщает основные аспекты промышленных сетей, включая их типы, устройства, протоколы связи и меры безопасности. Информация, представленная в таблице 1 поможет глубже понять структуру и функциональность промышленных сетей.

Таблица 1. Промышленные сети и характеристика их компонентов

Компонент или характеристика	Описание	Примеры
Тип сети	Сети, используемые для управления промышленными процессами.	Ethernet, Profibus, Modbus.
Устройства	Основные устройства, подключенные к сети.	PLC, SCADA-системы, датчики.
Протоколы связи	Протоколы, используемые для передачи данных.	TCP/IP, MQTT, OPC UA.
Типология сети	Структура, в которой организованы соединения.	Звезда, шина, кольцо.
Безопасность сети	Меры, принимаемые для защиты сети от угроз.	Системы IDS/IPS, шифрование данных.
Управление доступом	Механизмы контроля доступа к сети.	Аутентификация по ролям, VPN.
Мониторинг сети	Инструменты для контроля состояния сети.	SNMP, NetFlow.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

Резервирование	Методы обеспечения непрерывности работы сети.	Дублирование оборудования, горячие резервуары.
Интеграция с IT-системами	Связь между промышленными и информационными системами.	Использование API, шлюзов.
Поддержка стандартов	Соответствие отраслевым стандартам и нормативам.	ISA/IEC 62443, ISO 27001.

Безопасность промышленных сетей является важным аспектом, учитывающим угрозы и уязвимости, которые могут повлиять на стабильность и безопасность производственных процессов. Механизмы управления доступом и мониторинга состояния сети помогают защитить системы от несанкционированного доступа и атак.

Кроме того, поддержка отраслевых стандартов, таких как ISA/IEC 62443 и ISO 27001, способствует созданию надежных и безопасных инфраструктур, что является необходимым условием для успешной работы в условиях современного производства.

Важным аспектом является защита физического доступа к критическим компонентам промышленных сетей автоматизации и управления. Это может включать в себя контроль доступа в серверные помещения, использование видеонаблюдения и системы сигнализации.

Развитие технологий IoT и Industry 4.0:

Внедрение технологий Интернета вещей (IoT) и концепций Industry 4.0 изменяет структуру промышленных систем автоматизации и управления добавляя новые устройства и узлы. Это требует дополнительных мер безопасности и новых подходов к защите.

Увеличение числа кибератак и уязвимостей в системах управления требует постоянного обновления и адаптации методов защиты (Шишов, 2021). Новые виды угроз, такие как атаки на промышленные интернет-протоколы, требуют особого внимания.

Для систематизации подходов к обеспечению безопасности промышленных сетей автоматизации и управления, в таблице 2 представлены ключевые методы и технологии, применяемые для защиты промышленных сетей. Таблица 2 охватывает различные аспекты безопасности, включая управление доступом, сетевые и коммуникационные меры, программные и аппаратные средства, а также организационные меры. Каждая категория включает в себя конкретные методы, их цели и примеры применения.

Таблица 2. Методы обеспечения безопасности промышленных сетей автоматизации и управления

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

Категория	Метод/Технология	Описание	Цели	Примеры
1. Управление доступом	Аутентификация и авторизация	Процедуры для проверки идентичности пользователей и их прав доступа.	Процедуры для проверки идентичности пользователей и их прав доступа.	Использование двухфакторной аутентификации ролевого контроля доступа.
	Управление правами доступа	Определение и управление правами доступа пользователей и групп.	Гарантия, что только авторизованные пользователи имеют доступ к критическим системам.	Системы контроля доступа (IAM), управление правами.
2.Сетевые и коммуникационные меры	Сегментация сети	Разделение сети на логические сегменты для ограничения распространения угроз.	Локализация и минимизация воздействия атак.	Виртуальные локальные сети (VLAN), межсетевые экраны (firewalls).
	Шифрование данных	Использование криптографических методов для защиты данных при передаче и хранении.	Защита данных от перехвата и несанкционированного доступа.	Протоколы SSL/ TLS, шифрование в облаке.
	Мониторинг и управление трафиком	Слежение за сетевым трафиком и выявление аномалий, потенциальных угроз.	Обнаружение и предотвращение атак в реальном времени.	Системы управления событиями безопасности (SIEM), IDS/IPS.
3.Программные и аппаратные меры	Антивирусные и антивредоносные программы	антивредоносные программы ПО для обнаружения, удаления и предотвращения вредоносного ПО.	Защита от вирусов, червей и других вредоносных программ.	Антивирусные решения, системы обнаружения вредоносных программ.
	Патчи и обновления	Регулярное обновление программного обеспечения для устранения известных уязвимостей.	Устранение уязвимостей и улучшение безопасности.	Автоматическое обновление ПО, управление патчами.
	Физическая безопасность	Меры по защите оборудования и инфраструктуры от физического доступа.	Защита от физического вмешательства и кражи.	Контроль доступа в серверные комнаты, видеонаблюдение.
4.Организационные методы	Политики и процедуры безопасности	Разработка и внедрение внутренних политик и процедур для обеспечения безопасности.	Стандартизация и упрощение процессов обеспечения безопасности.	Политики безопасности, процедуры инцидент-менеджмента.
	Обучение и повышение осведомленности	Обучение сотрудников принципам кибербезопасности и методам предотвращения угроз.	Снижение риска ошибок человеческого фактора.	Программы обучения по безопасности, тренинги по реагированию на инциденты.
5.Инструменты и технологии	Системы обнаружения и предотвращения вторжений (IDS/IPS)	Системы для обнаружения и предотвращения попыток несанкционированного доступа и атак.	Реагирование на угрозы и предотвращение атак.	Внедрение IDS/IPS в сети предприятия.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

	Системы управления событиями безопасности (SIEM)	Инструменты для сбора, анализа и корреляции данных безопасности из различных источников.	Обеспечение централизованного управления и анализа безопасности.	Решения SIEM, такие как Splunk, ArcSight.

Итак, в таблице показан контроль доступа, который включает в себя меры аутентификации и авторизации, управление правами доступа, которые необходимы для обеспечения того, чтобы только авторизованные пользователи могли получить доступ к критически важным системам и данным. Сетевые и коммуникационные меры, охватывающие такие технологии и приемчики, как сегментация сети, шифрование данных и мониторинг трафика, направленные на защиту данных во время передачи и предотвращение несанкционированного доступа. Программные и аппаратные меры включают использование антивирусных решений, регулярные обновления программного обеспечения, а также меры по обеспечению безопасности физического оборудования, которые помогают защититься от вредоносных программ и физического вмешательства (Язов, 2019). Организационные меры указывают на важность разработки и внедрения политики в области безопасности, а также обучения сотрудников, что способствует установлению стандартов безопасности и повышению осведомленности сотрудников. Инструменты и технологии, использование специализированных систем обнаружения и предотвращения вторжений, а также управление инцидентами безопасности, что обеспечивает эффективное реагирование на угрозы и инциденты.

Эта таблица предназначена для того, чтобы дать исчерпывающий обзор методов обеспечения безопасности для промышленной автоматизации и сетей управления, которые могут быть адаптированы и внедрены в соответствии со спецификой и потребностями конкретного предприятия. Включение различных категорий методов и технологий в таблицу позволяет в полной мере понять подходы к защите промышленных сетей и способствует созданию эффективной системы безопасности.

Обеспечение безопасности промышленных сетей автоматизации и управления на предприятиях представляет собой комплексную задачу, требующую интеграции различных аспектов — технических, организационных и человеческих. Важно применять современные технологии, такие как шифрование и системы обнаружения вторжений, а также уделять внимание обучению персонала.

Выводы

Адаптация к постоянно меняющемуся ландшафту угроз является ключевым элементом защиты, что подразумевает регулярную оценку рисков и обновление мер безопасности в соответствии с новыми вызовами. Учет существующих стандартов и рекомендаций, таких как ISA/IEC 62443, помогает выработать эффективные политики безопасности и минимизировать риски.

С учетом растущего взаимодействия информационных и операционных технологий необходимо разрабатывать методы, которые обеспечат совместную безопасность этих систем, учитывая их уникальные характеристики. Эффективные системы мониторинга и быстрого реагирования на инциденты играют критически важную роль в минимизации последствий потенциальных атак, что требует наличия четких протоколов действий.

Безопасность должна стать приоритетом на всех уровнях организации — от руководства до операционного персонала. Создание культуры безопасности, где все

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

сотрудники вовлечены в процессы защиты, способствует снижению рисков. Важно также активно исследовать и внедрять новые технологии, такие как искусственный интеллект и машинное обучение, чтобы повысить уровень автоматизации и эффективности защиты промышленных сетей. Таким образом, безопасность промышленных сетей требует постоянного совершенствования методов и стратегий, а также взаимодействия всех заинтересованных сторон для обеспечения надежной защиты.

ЛИТЕРАТУРА

Афонин А.М., Царегородцев Ю.Н., Петрова А.М. (209). Теоретические основы разработки и моделирования систем автоматизации: Учебное пособие. — М.: Форум. — 336 с.

Баранова Е.К., Бабаш А.В. (2020). Информационная безопасность и защита информации: учебное пособие. 3-е изд. перераб. и доп. — М.: РИОР; ИНФРА-М. — 322 с.

Бирюков А.А. (2020). Информационная безопасность: защита и нападение. 2-е изд. перераб. и доп. — М.: ДМК Пресс. — 434 с.

Вихляев А.А. (2020). К вопросу совершенствования методов обработки, хранения, анализа и систематизации больших данных на современном этапе. — В: Государственное управление и развитие: глобальные угрозы и структурные изменения: Сб. ст. междунар. конф. сессий. — С. 137–141.

Воронцов А.А. (2019). Автоматизированные системы управления технологическими процессами. Вопросы безопасности. Jetlnfo. — № 5. — С. 89–96.

Иванов А.А. (2021). Автоматизация технологических процессов и производств: Учебное пособие. — М.: Форум. — 224 с.

Камаев В.А., Лежебоков В.В. (2019). Разработка и применение модели автоматизированной системы управления информационными процессами к задаче мониторинга состояния оборудования. Вестник компьютерных и информационных технологий. — № 9. — 18–22.

Кирсанов С.В. (2021). Метод оценки угроз информационной безопасности АСУ ТП газовой отрасли. — Доклады ТУСУР. — № 2(28). — 112–115.

Клепиков В.В., Схиртладзе А.Г., Султан-заде Н.М. (2019). Автоматизация производственных процессов: Учебное пособие. — М.: Инфра-М. — 351 с.

Клюев А.С., Ротач В.Я., Кузищин В.Ф. (2019). Автоматизация настройки систем управления. — М.: Альянс. — 272 с.

Кондаков В.В., Краснобородько А.А. (2021). Информационная безопасность систем физической защиты: Учебное пособие. — М.: МИФИ. — 48 с.

Пищик Б.Н. (2020). Безопасность АСУ ТП. Вычислительные технологии. — Спецвыпуск. — Т. 18. — 170–175.

Попова А.Д., Богданов П.А., Быков Д.В. (2019). Разработка автоматизированной системы моделирования угроз безопасности. Студенческий: электрон. научн. Журн. — № 7(27). URL: https://sibac.info/journal/student/27/103048

Селевцов Л.И. (2019). Автоматизация технологических процессов: Учебник. — М.: Academia. — 160 с. Снытников А.А. (2020). Лицензирование и сертификация в области защиты информации. —М.: Гелиос АРВ. — 192 с.

Стрельцов А.А. (2019). Правовое обеспечение информационной безопасности: теоретические и методологические основы. — Минск. — 304 с.

Хорев А.А. (2019). Защита информации от утечки по техническим каналам: Учебное пособие. — М.: МО РФ. — 350 с.

Чернобровцев А. (2019). Защита АСУ ТП. Computerworld Россия. — № 10. — 25–32.

Шишов О.В. (2021). Современные технологии промышленной автоматизации: учебное пособие. — Саранск: Изд-во Мордов. ун-та. — 276 с.

Язов Ю.К. (2019). Основы методологии количественной оценки эффективности защиты информации в компьютерных сетях. — Ростов-на-Дону: Издательство СКНЦ ВШ. — 220 с.

REFERENCES

Afonin, A.M., Caregorodcev, Ju.N., Petrova, A.M. (2019). Teoreticheskie osnovy razrabotki i modelirovanija sistem avtomatizacii: Uchebnoe posobie [Theoretical foundations of the development and modeling of automation

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

systems: A textbook]. —Moscow: Forum. — 336 p. [In Russ.].

Baranova E.K., Babash A.V. (2020). Informacionnaja bezopasnost' i zashhita informacii: ucheb. posobie [Information security and data protection: A textbook]. 3rd ed. — Moscow: RIOR; INFRA-M. — 322 p. [In Russ.].

Birjukov A.A. (2020). Informacionnaja bezopasnost': zashhita i napadenie [Information security: Defense and attack]. 2nd ed. — Moscow: DMK Press. — 434 p. [In Russ.].

Vihljaev A.A. (2020). K voprosu sovershenstvovanija metodov obrabotki, hranenija, analiza i sistematizacii bol'shih dannyh na sovremennom jetape [On the improvement of methods for processing, storage, analysis, and systematization of big data at the current stage]. In: Gosudarstvennoe upravlenie i razvitie: global'nye ugrozy i strukturnye izmenenija: Sbornik statej mezhdunarodnoj konferencii [State Governance and Development: Global Threats and Structural Changes: Proceedings of the International Conference]. — Pp. 137–141. [In Russ.].

Voroncov A.A. (2019). Avtomatizirovannye sistemy upravlenija tehnologicheskimi processami. Voprosy bezopasnosti [Automated control systems for technological processes. Security issues]. — Jetlnfo. — 5. — 89–96. [In Russ.].

Ivanov A.A. (2021). Avtomatizacija tehnologicheskih processov i proizvodstv: — Uchebnoe posobie [Automation of technological processes and productions: A textbook]. — Moscow: Forum. — 224 p. [In Russ.].

Kamaev V.A., Lezhebokov V.V. (2019). Razrabotka i primenenie modeli avtomatizirovannoj sistemy upravlenija informacionnymi processami k zadache monitoringa sostojanija oborudovanija [Development and application of an automated system management model for monitoring equipment condition]. Vestnik komp'juternyh i informacionnyh tehnologij [Bulletin of Computer and Information Technologies]. — 9. — 18–22. [In Russ.].

Kirsanov S.V. (2021). Metod ocenki ugroz informacionnoj bezopasnosti ASU TP gazovoj otrasli [Method for assessing information security threats of the industrial control system in the gas industry]. — Doklady TUSUR. — 2(28). — 112–115. [In Russ.].

Klepikov V.V., Shirtladze A.G., Sultan-zade N.M. (2019). Avtomatizacija proizvodstvennyh processov: Uchebnoe posobie [Automation of production processes: A textbook]. — Moscow: Infra-M. — 351 p. [In Russ.].

Kljuev A.S., Rotach V.Ja., Kuzishhin V.F. (2019). Avtomatizacija nastrojki sistem upravlenija [Automation of control system settings]. — Moscow: Al'jans. — 272 p. [In Russ.].

Kondakov V.V., Krasnoborod'ko A.A. (2021). Informacionnaja bezopasnost' sistem fizicheskoj zashhity: uchebnoe posobie [Information security of physical protection systems: A textbook]. — Moscow: MIFI. — 48 p. [In Russ.].

Pishhik B.N. (2020). Bezopasnost' ASU TP [Safety of industrial control systems]. Vychislitel'nye tehnologii [Computational Technologies]. — Special Issue. — 18. — 170–175. [In Russ.].

Popova A.D., Bogdanov P.A., Bykov D.V. (2019). Razrabotka avtomatizirovannoj sistemy modelirovanija ugroz bezopasnosti [Development of an automated system for modeling security threats]. Studencheskij: jelektronnyj nauchnyj zhurnal [Student: Electronic Scientific Journal]. — 7(27). Available at: https://sibac.info/journal/student/27/103048 [In Russ.].

Selevcov L.I. (2019). Avtomatizacija tehnologicheskih processov: Uchebnik [Automation of technological processes: A textbook]. — Moscow: Academia. — 160 p. [In Russ.].

Snytnikov A.A. (2020). Licenzirovanie i sertifikacija v oblasti zashhity informacii [Licensing and certification in the field of information protection]. — Moscow: Gelios ARV. — 192 p. [In Russ.].

Strel'cov A.A. (2019). Pravovoe obespechenie informacionnoj bezopasnosti: teoreticheskie i metodologicheskie osnovy [Legal provision of information security: Theoretical and methodological foundations]. — Minsk. — 304 p. [In Russ.].

Horev A.A. (2019). Zashhita informacii ot utechki po tehnicheskim kanalam: Uchebnoe posobie [Information leakage protection through technical channels: A textbook]. — Moscow: MO RF. — 350 p. [In Russ.].

Chernobrovcev A. (2019). Zashhita ASU TP [Protection of industrial control systems]. Computerworld Rossija [Computerworld Russia]. — 10. — 25–32. [In Russ.].

Shishov O.V. (2021). Sovremennye tehnologii promyshlennoj avtomatizacii: uchebnoe posobie [Modern technologies of industrial automation: A textbook]. — Saransk: Mordov. un-ta. — 276 p. [In Russ.].

Jazov Ju.K. (2019). Osnovy metodologii kolichestvennoj ocenki jeffektivnosti zashhity informacii v komp'juternyh setjah [Fundamentals of methodology for quantitative assessment of information security efficiency in computer networks]. — Rostov-na-Donu: Izdatel'stvo SKNC VSh. — 220 p. [In Russ.].

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Vol. 5. Is. 3. Number 19 (2024). Pp. 115–127
Journal homepage: https://journal.iitu.edu.kz
https://doi.org/10.54309/IJICT.2024.19.3.010

AUTOMATED SECURITY SYSTEM FOR INDUSTRIAL ENTERPRISES

A. Makeyev
LLC "Terralink Technologies", Almaty, Kazakhstan.
E-mail: alibekmakeyev@gmail.com

Alibek Makeyev — analyst, LLC "Terralink Technologies", Almaty, Kazakhstan
E-mail: alibek-makeyev@gmail.com, https://orcid.org/0009-0001-5174-825X.

© A. Makeyev, 2024

Abstract. Security systems have become an integral part of the existence of modern industrial enterprises. For such a system to function smoothly, it is necessary to create better conditions and automate this process. Trends in the development of modern security systems are directly related to extensive automation and integration, which affect not only security systems, but also other processes at the enterprise, for example, the automated enterprise management system. Design process and comprehensive study play an important role in the creation of an automated security system, since at this stage all the qualitative characteristics of the future security system are laid down. The author analyzed modern trends and challenges in the market related to the implementation of automated security systems, as well as their impact on the level of security at an industrial enterprise. The main focus of the article is on the concept of integrating monitoring, control, and threat prediction technologies, which can significantly improve the effectiveness of risk management. The results of the study demonstrate that the implementation of automated systems helps to reduce the number of incidents, and increases the overall discipline and level of responsibility of employees.

Keywords: automation; integration; security system; enterprise; industrial enterprise processes

For citation: *A. Makeyev. AUTOMATED SECURITY SYSTEM FOR INDUSTRIAL ENTERPRISES// INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES. 2024. Vol. 5. No. 19. Pp. 115–127 (In Russ.). https://doi.org/10.54309/IJICT.2024.19.3.010.*

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

ӨНЕРКӘСІПТІК КӘСІПОРЫНДАРДЫ ҚОРҒАУДЫҢ АВТОМАТТАНДЫРЫЛҒАН ЖҮЙЕСІ

А. Макеев
ЖШС «Терралинк Технолоджис», Алматы, Қазақстан.
E-mail: alibekmakeyev@gmail.com

Алибек Макеев — ЖШС «Терралинк Технолоджис», талдаушысы, Алматы, Қазақстан
E-mail: alibekmakeyev@gmail.com, https://orcid.org/0009-0001-5174-825X.

© А. Макеев, 2024

Аннотация. Қауіпсіздік жүйелері қазіргі заманғы өнеркәсіптік кәсіпорындардың өмір сүруінің ажырамас бөлігіне айналды. Мұндай жүйе бірқалыпты жұмыс істеуі үшін жақсы жағдай жасап, бұл процесті автоматтандыру қажет. Заманауи қауіпсіздік жүйелерінің даму тенденциялары тек қауіпсіздік жүйелеріне ғана емес, сонымен қатар кәсіпорында бар басқа да процестерге, мысалы, кәсіпорынды басқарудың автоматтандырылған жүйесіне әсер ететін кең таралған автоматтандыру мен интеграцияға тікелей байланысты. Автоматтандырылған қауіпсіздік жүйелерін құруда маңызды рөлді жобалау және бар нюанстарды жан-жақты зерттеу процесі атқарады, өйткені дәл осы кезеңде болашақ қауіпсіздік жүйесінің барлық сапалық сипаттамалары белгіленеді. Автор автоматтандырылған қауіпсіздік жүйелерін енгізуге байланысты нарықтағы ағымдағы үрдістер мен қиындықтарды, сондай-ақ олардың өнеркәсіптік кәсіпорындағы қауіпсіздік деңгейіне әсерін талдаған. Мақаланың негізгі бағыты тәуекелдерді басқару тиімділігін айтарлықтай арттыра алатын мониторинг, бақылау және қауіптерді болжау технологияларын біріктіру тұжырымдамасына арналған. Зерттеу нәтижелері автоматтандырылған жүйелерді енгізу оқыс оқиғалардың санын азайтуға көмектесетінін, сонымен қатар қызметкерлердің жалпы тәртібі мен жауапкершілігін арттыратынын көрсетті.

Түйін сөздер: автоматтандыру; интеграция; қауіпсіздік жүйесі; кәсіпорын; өнеркәсіптік кәсіпорынның процестері

Дәйексөз үшін: *А. Макеев. ӨНЕРКӘСІПТІК КӘСІПОРЫНДАРДЫ ҚОРҒАУДЫҢ АВТОМАТТАНДЫРЫЛҒАН ЖҮЙЕСІ // ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ. 2024. Т. 5. No. 19. 115–127 бет. (орыс тілінде). https://doi.org/10.54309/IJICT.2024.19.3.010.*

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ

А. Макеев
ТОО «Терралинк Технолоджис», Алматы, Казахстан.
E-mail: alibekmakeyev@gmail.com

Алибек Макеев — аналитик, ТОО «Терралинк Технолоджис»
E-mail: alibekmakeyev@ gmail.com, https://orcid.org/0009-0001-5174-825X.

© А. Макеев, 2024

Аннотация. Системы обеспечения безопасности стали неотъемлемой частью существования современных промышленных предприятий. Для того, чтобы такая система функционировала бесперебойно, необходимо создать лучшие условия и автоматизировать данный процесс. Тенденции развития современных систем безопасности напрямую имеют связь с широкой автоматизацией и интеграцией, которые затрагивают не только системы безопасности, но и остальные существующие на предприятии процессы, например, автоматизированные системы управления предприятия. Важную роль при создании автоматизированной системы обеспечения безопасности играет процесс проектирования и всестороннего изучения существующих нюансов, поскольку именно на этом этапе заложены все качественные характеристики будущей системы безопасности. Автор проанализировал современные тенденции и вызовы на рынке, связанные с внедрением автоматизированных систем обеспечения безопасности, а также их влияние на уровень безопасности на промышленном предприятии. Основное внимание в статье направлено на концепцию интеграции технологий мониторинга, контроля и предвидение угроз, что позволяет существенно повысить эффективность управления рисками. Результаты исследования демонстрируют, что внедрение автоматизированных систем способствует снижению числа инцидентов, а также повышает общую дисциплину и уровень ответственности сотрудников.

Ключевые слова: автоматизация; интеграция; система обеспечения безопасности; предприятие; процессы промышленного предприятия

***Для цитирования**: А. Макеев. АВТОМАТИЗИРОВАННАЯ СИСТЕМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ // МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ. 2024. Т. 5. No. 19. Стр. 115–127 (На русс.). https://doi.org/10.54309/IJICT.2024.19.3.010.*

Введение

Актуальность данной темы обусловлена тем, что в последние годы постоянно возрастает число инцидентов, связанных с нарушениями безопасности на крупных промышленных предприятиях. Это включает в себя как физические угрозы безопасности, так и систематические кибератаки, а также иные различные риски. Поэтому создание эффективной автоматизированной системы для обеспечения безопасности становится особенно важным. Увеличение числа киберугроз и физической преступности ставит промышленные предприятия перед необходимостью внедрения современных систем

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

безопасности, а в свою очередь, атаки на промышленные объекты могут привести к значительным экономическим потерям и поставить под угрозу жизни людей. Внедрение таких технологий в систему безопасности промышленного предприятия, как искусственный интеллект и машинное обучение, открывает новые возможности для повышения уровня безопасности на предприятиях.

Целью статьи на тему «Автоматизированная система обеспечения безопасности промышленных предприятий» выступает проведение анализа наиболее актуальных технологий и методик, которые используются прежде всего для обеспечения безопасности на промышленных объектах, с целью выявления оптимальных и актуальных решений для автоматизации систем безопасности.

Исходя из цели статьи, вытекают следующие основные задачи:

1. Исследование существующих систем обеспечения безопасности на промышленных предприятиях;
2. Определение ключевых требований к автоматизации систем обеспечения безопасности;
3. Разработка рекомендаций по внедрению автоматизированной системы обеспечения безопасности.

Гипотеза исследования заключается во внедрении автоматизированной системы обеспечения безопасности на промышленных предприятиях, что в свою очередь позволяет значительно снизить риски инцидентов, связанных с производственными авариями, киберугрозами и другими негативными факторами, которые могут возникнуть в функционировании предприятия, благодаря автоматизации и интеграции современных технологий мониторинга, анализа данных и оперативного реагирования.

Разработка гипотезы в данном случае основана на предположении о том, что автоматизированная система безопасности не только способствует улучшению контроля над производственными процессами на промышленном предприятии, но также способствует более эффективному использованию ресурсов предприятии, а вместе с тем и оптимизации затрат и повышению уровня защиты других его систем.

Методы и материалы

В статье использован такой метод, как анализ существующих систем безопасности на промышленных предприятий посредством изучения литературы по теме, а также проведен сравнительный анализ в виде оценки разных подходов к обеспечению безопасности промышленных предприятий. Среди материалов использованы: научные статьи и журналы по теме; учебные пособия.

Основная часть. На данный момент современные крупные промышленные предприятия сталкиваются с огромным количеством угроз, как внутренних, так и внешних. Эти угрозы могут иметь разный характер, начиная от несчастных случаев и утечек информации до террористических актов и атак на компьютерные системы. Поэтому на сегодняшний день возрастает реальная необходимость создание наиболее эффективной системы обеспечения безопасности, которая будет грамотно автоматизирована и интегрирована на предприятии (Абалмазов, 2023). В этом контексте автоматизированные системы обеспечения безопасности представляют собой важный инструмент, который позволяет интегрировать различные аспекты безопасности и управлять данными аспектами в единой информационной среде.

Автоматизированные системы обеспечения безопасности промышленных предприятий представляют собой целостный комплекс технических и программных

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

средств, предназначенных для защиты объектов от различных угроз, включая несанкционированный доступ, пожары, аварии, террористические акты и другие риски. Такие системы предназначены для повышения уровня безопасности, защиты персонала и имущества, а также для обеспечения выполнения нормативных требований.

Полноценная система безопасности промышленного предприятия включает в себя в том числе и мероприятия, которые обеспечивают защиту не только конфиденциальной информации, но и бизнес-процессов. Поэтому сюда же входят сохранность важных документов, обеспечение контроля доступа на предприятие, противодействие незаконной деятельности, например краже и т. д. (Буч и др., 2018).

В связи с этим, автоматизированная система обеспечения безопасности заключается не только в информационной безопасности и противодействии угрозам хакеров, но и в поддержке всех мероприятий, которые не связаны с информацией.

Промышленные сети автоматизации и управления играют ключевую роль в современных производственных процессах. Они обеспечивают связь между различными элементами системы управления, такими как датчики, контроллеры и исполнительные механизмы. Однако с увеличением сложности этих сетей возрастает и риск возникновения различных угроз, как внешних, так и внутренних.

К методам обеспечения промышленных сетей автоматизации и управления на предприятии можно отнести:

1. Использование в работе промышленного предприятия современных протоколов безопасности для защиты сетей, например: TLS/SSL; VPN; механизмы аутентификации и авторизации;
2. Полноценная разработанная система мониторинга, качественно внедренная в работу предприятия с целью своевременного обнаружения источников угроз и рисков, выявляя аномалии в реальном времени;
3. Внедрение в работу предприятия искусственного интеллекта, который в работе может сыграть ключевую роль, поскольку таким способом анализ большого количества данных будет проходить быстрее, отсюда следует и то, что потенциальные угрозы для промышленного предприятия будут найдены гораздо быстрее. Также с помощью использования искусственного интеллекта может произойти заблаговременное предотвращение возможных инцидентов;
4. Обучение персонала, поскольку именно человеческий фактор выступает как основная причина инцидентов безопасности, и поэтому обучение сотрудников на регулярной основе поможет значительно снизить риски (Галатенко, 2019).

Для того, чтобы обеспечить на промышленном предприятии полноценную безопасность, большинство руководителей используют целый комплекс ресурсов, которые включают в себя: материальные ресурсы; кадры; информационные ресурсы; технические ресурсы; правовые и нормативные ресурсы. На рисунке 1 рассмотрим основные моменты обеспечения системы безопасности на промышленном предприятии:

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

Рис.1 – Система безопасности объекта

К компонентам автоматизированной системы безопасности промышленных предприятий можно отнести три основных компонента. Первый компонент – это физическая безопасность. В неё входят такие компоненты, как контроль доступа, а также сигнализация и видеонаблюдение. Контроль доступа — это использование сложных или простых биометрических систем, пропусков и видеонаблюдения для управления входом на территорию промышленного предприятия. Сигнализация и видеонаблюдение — это совокупные системы, которые позволяют отслеживать попытки доступа посторонними людьми, а также осуществлять мониторинг территории предприятия в режиме реального времени.

Второй компонент – это информационная безопасность, в которую входит защита сети и управление данными. Защита сети — это использование антивирусных программ и систем обнаружения вторжений для обеспечения кибербезопасности информационных систем предприятия и предотвращение взлома с целью захвата информации. Управление данными — это защита конфиденциальной информации предприятия, а также шифрование важных данных и внедрение протоколов безопасности.

Третий компонент – это производственная безопасность, в который входит мониторинг технологических процессов предприятия и налаженные системы оповещения. Мониторинг технологических процессов — это использование специальных датчиков и автоматизированных систем для контроля за производственными процессами с целью предотвращения аварий и различных несанкционированных инцидентов. Системы оповещения — это автоматические системы оповещения о чрезвычайных ситуациях, с помощью которых представляется возможным быстро информировать сотрудников о возникших угрозах безопасности на предприятии (Домарев, 2020). На рисунке 2 рассмотрим подсистему обнаружения

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

атак автоматизированной системы безопасности:

Рис. 2 – Подсистема обнаружения атак автоматизированной системы безопасности

Исходя из рисунка 2, выделим ключевые преимущества автоматизированной системы безопасности на промышленном предприятии: интеграция информации, что позволяет значительно повысить эффективность рабочих процессов и избежать дублирования усилий; снижение рисков на предприятии, поскольку автоматизация позволяет гораздо быстрее реагировать на инциденты в реальном времени, минимизируя при этом риски для оборудования и персонала; улучшение мониторинга угроз и рисков, поскольку автоматизированные системы безопасности предприятия и их современные элементы позволяют соответствующим отделам предприятия проводить анализ возникших ранее инцидентов, а вместе с тем выявлять наиболее уязвимые места, способствуя постоянному улучшению системы безопасности; снижение затрат благодаря автоматизации процессов системы безопасности, что в разы сокращают расходы на безопасность (Зильбербург и др., 2020).

Также следует обратить внимание на большое количество видов систем обеспечения безопасности предприятия. Система контроля доступа, в которую можно отнести биометрические системы, карты доступа. Такие системы помогают предотвращать несанкционированный вход на предприятие и проводить учет посещаемости. Также они контролируют доступ сотрудников предприятия и гостей в определенные зоны (Иващенко и др., 2019).

Системы видеонаблюдения, которые включают в себя камеры видеонаблюдения, системы звуковой записи и передачи данных, что в свою очередь позволяет более точечно контролировать происходящее на территории предприятия. Такая система помогает выявлять совершенные правонарушениях, инцидентов и служат доказательством в случае чрезвычайных ситуаций.

Системы сигнализации, которые в свою очередь помогают обнаружить несанкционированные проникновения на территорию промышленного предприятия и могут включать в себя и датчики движения, разбития стекол, так и новейший интеллектуальные технологии. Благодаря подобным системам происходит мгновенное уведомление охраны о возможной угрозе предприятию и его имуществу.

Системы мониторинга и управления, которые помогают контролировать внутреннее состояние оборудования и всех производственных процессов, также такие

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

системы могут выполнять интегрированные функции безопасности процессов. Их полезность обусловлена оперативным реагированием на технические сбои и аварии.

Системы пожарной безопасности, которые составляют основу безопасности любого крупного промышленного предприятия. Включают в себя такие важные системы, как: обнаружение дыма, автоматическое тушение огня, оповещение об экстренной эвакуации. Такие системы защищают предприятие от серьезных угроз, при этом минимизируя риски для жизней людей, а также материальных ценностей.

Системы кибербезопасности внедряются с целью обеспечения защиты от атак со стороны хакеров, а также проводят мониторинг сетевой активности и тем самым предотвращают возможную утечку важных данных. Польза от подобных систем заключается в том, что они являются важным элементом защиты важных данных, систем и информации предприятия (Ивашкин, 2020).

Согласно отчету по безопасности на рабочих местах от МОТ, 30 % всех несчастных случаев на производстве можно предотвратить с помощью современных технологий безопасности. Исследование компании «Gartner» показало, что компании, внедряющие автоматизированные системы безопасности, могут сократить расходы на безопасность до 25 % в течение трех лет.

Во время автоматизации системы безопасности промышленного предприятия, представляется возможность контроля всей работы отделов компании. Также автоматизация позволяет значительно сократить количество работников, поскольку более опасные и емкие операции по предотвращению рисков и угроз безопасности можно возложить на машины и механизмы с элементами автоматики, повышая при этом безопасность и производительность труда у работников. В целом, сущность использования автоматизированных систем обеспечения безопасности на промышленном предприятии можно продемонстрировать на рисунке 3:

Рис. 3 - Сущность использования автоматизированных систем обеспечения безопасности на промышленном предприятии

Если рассмотреть примеры по реализации автоматизированных систем безопасности, то здесь можно рассмотреть компанию ООО «Северсталь» - гигант, который выходит далеко за пределы Российской Федерации. Используя автоматизированную систему обнаружения пожара, компания сумела значительно снизить количество ложных срабатываний, а именно на 40 %, что позволило в разы сократить время реакции на более реальные угрозы.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

Другая компания, Ford, которая находится в Кракове, внедрила системы видеонаблюдения с полным анализом данных. Это позволило руководству уменьшить в разы количество краж и порчи имущества компании на 30 % всего за первый год эксплуатации.

На некоторых зарубежных предприятиях, например, Bosch, давно внедрены роботизированные системы безопасности компании с целью мониторинга окружающей среды в потенциально опасных зонах, что позволило снизить казусы на 20 % (Информационная безопасность автоматизированных систем: понятие, методы обеспечения)

Автоматизированные системы обеспечения безопасности становятся необходимым элементом в деятельности промышленных предприятий. Их внедрение позволяет не только защищать ресурсы, но и оптимизировать процессы управления и повысить общую эффективность работы. С учетом растущих угроз, автоматизированные системы безопасности являются важнейшим аспектом стратегического планирования и развития бизнеса современного промышленного предприятия.

Система безопасности предприятия должна развиваться вместе с предприятием и адекватно реагировать на разнообразные угрозы извне. На основе глубокого анализа изменений бизнес-процессов промышленного предприятия, а также внешней среды, должна меняться и модернизироваться и система его безопасности. Проанализировав современные угрозы и риски, которым подвергаются производство на промышленном предприятии, показал, что традиционные подходы к обеспечению системы безопасности не всегда являются эффективными (Кузнецов, 2019) В условиях быстрого развития технологий и нарастания сложности потенциальных угроз возрастает необходимость внедрения автоматизированных систем, способных оперативно реагировать на изменения в окружающей среде и обеспечивать безопасность на всех уровнях.

Результаты и обсуждение

Результаты данного исследования демонстрируют положительное влияние на промышленное предприятие внедрения автоматизированных систем обеспечения безопасности. Это повышает производительность и способствует повышению качества мониторинга и контроля безопасности.

На сегодняшний день многие промышленные предприятия сталкиваются с недостаточной эффективностью традиционных методов обеспечения безопасности как внутренней, так и внешней, что подчеркивает необходимость внедрения автоматизированных систем, способных обеспечить более высокий уровень защиты данных предприятия. В ходе исследования были рассмотрены ключевые компоненты, принципы и технологии, применяемые в автоматизированных системах, включая адаптивные системы мониторинга, аналитические инструменты, а также системы раннего реагирования.

В ходе обсуждения основных результатов исследования важно отметить, что автоматизация процессов обеспечения безопасности на промышленных предприятиях имеет ряд значительных преимуществ. Прежде всего, это повышает уровень безопасности за счет быстрого реагирования на инциденты и снижения человеческого фактора. Разработанные алгоритмы показали свою эффективность в обнаружении аномалий, что позволяет заранее принимать меры системы безопасности предприятия против угроз (Gartner, 2021).

Однако, помимо преимуществ, существуют и угрозы при реализации автоматизированной системы обеспечения безопасности. Во-первых, это возрастание

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

киберугроз, которая обусловлена тем, что система, которая работает на основе цифровых, то есть передовых, технологий, может стать главной мишенью атак хакеров, а это опасно в случае с промышленным предприятием, поскольку может подорвать весь производственный процесс. Именно поэтому необходимо учесть постоянное обновление системы и поддержки актуальности её защиты от угроз.

Во-вторых, это затраты на обучение персонала. Поскольку новая внедренная система требует от сотрудников соответствия по части знаний, это весьма затратно не только в материальном плане, но и в плане времени. Поэтому важно находить эффективные тренинги и программы по повышению квалификации с целью качественной и безопасной эксплуатации введенной системы.

В-третьих, происходит постоянная интеграция уже с существующими системами. Это связано с тем, что на многих промышленных предприятиях уже давно существуют определенные системы безопасности, и поэтому возникает необходимость в обеспечении объединения, или интеграции, новой автоматизированной системы безопасности с существующими ранее моделями.

В-третьих, существуют и морально-этические аспекты. К ним относятся такие спорные моменты, когда, например, использование новых автоматизированных технологий мониторинга могут вызвать вопросы о свободе труда сотрудников и поэтому возникает тонкая грань между нарушением прав сотрудников и использованием новейших автоматизированных систем безопасности.

Представленные результаты исследования подчеркивают значимость автоматизации процессов обеспечения безопасности на промышленных предприятиях и открывают новые горизонты для дальнейших научных исследований и практических разработок в этой области. Внедрение эффективных и современных автоматизированных систем станет залогом повышения уровня безопасности, устойчивости и конкурентоспособности промышленных предприятий в условиях динамично развивающегося рынка.

Данное комплексное исследование показало, что автоматизированные системы обеспечения безопасности, такие, например, как системы видеонаблюдения, контроля доступа, а также системы обнаружения возгораний и утечек, способны значительно повысить уровень безопасности на промышленных объектах, при этом повысив его производительность. Кроме того, интеграция данных систем в единую платформу позволяет оптимизировать процессы мониторинга и управления, что в свою очередь снижает риск ошибок, связанных с человеческим фактором.

На основе проведенного анализа можно сделать ряд рекомендаций по дальнейшему совершенствованию автоматизированных систем безопасности. Важными направлениями являются: развитие адаптивных систем, способных к самонастройке в зависимости от меняющихся условий; использование искусственного интеллекта для повышения скорости анализа и принятия решений; а также обеспечение высокого уровня киберзащиты для защиты систем от внешних угроз.

Заключение

В заключении хочется отметить то, что автоматизированные системы обеспечения безопасности в настоящий момент становятся необходимостью для современных промышленных предприятий. Промышленные предприятия выступают как ключевые объекты в экономике, однако зачастую они подвержены различным видам рисков. Традиционные методы обеспечения безопасности не всегда выступают

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

как эффективные способы обеспечения уровня безопасности, именно поэтому автоматизированные системы могут значительно повысить уровень защиты, улучшить реакцию на инциденты и оптимизировать процессы управления безопасностью. Они позволяют не только защищать активы предприятия в целостности, но также и снизить риски, создавая при этом наиболее безопасную производственную среду для сотрудников различных отделов. В условиях современных вызовов и угроз, внедрение автоматизированных систем безопасности на промышленное предприятие является стратегическим шагом, позволяющим современным предприятиям уверенно смотреть в будущее.

Основные выводы работы можно сформулировать следующим образом:

1. Автоматизированные системы обеспечения безопасности на промышленном предприятии способны обеспечить более высокий уровень контроля и управления по сравнению с традиционными системами безопасности, что позволяет значительно снизить риски инцидентов и аварий на производстве, тем самым повышая производительность труда;

2. Внедрение таких систем обеспечения безопасности способствует повышению эффективности управления безопасностью на предприятии за счет интеграции различных видов систем безопасности и аналитических инструментов, позволяющих в реальном времени отслеживать ситуацию и принимать оперативные решения;

3. Важно учитывать человеческий фактор и обеспечивать необходимую подготовку персонала для работы с новыми технологиями, что является критическим условием успешного внедрения автоматизированных систем;

4. Перспективы дальнейших исследований включают разработку более сложных алгоритмов машинного обучения для прогноза возможных угроз, а также интеграцию с системами управления производственными процессами для создания единой среды управления безопасностью на промышленном предприятии.

Также нужно отметить то, что в современных условиях рыночной экономики, промышленные предприятия сталкиваются с многочисленными угрозами, включая угрозы физической безопасности, киберугрозы и экологические риски. В данной статье представлена разработка автоматизированной системы обеспечения безопасности на промышленном предприятии, которая способна интегрировать и довести до автоматизации современные технологии для предотвращения инцидентов и минимизации любых возникающих угроз, рисков и последствий. Описываются ключевые компоненты системы, методы анализа рисков, а также примеры внедрения с использованием реальных данных.

Также следует отметить тот факт, что автоматизированные системы обеспечения безопасности имеют потенциал значительно улучшить ситуации на промышленных предприятиях. Однако успешная реализация требует комплексного подхода, включая технические, организационные и морально-этические аспекты. Предстоит дальнейшее исследование и адаптация систем к меняющимся условиям и требованиям.

Обеспечение безопасности и надежности промышленных сетей автоматизации и управления является сложной задачей, требующей комплексного подхода. Использование современных технологий, внедрение систем мониторинга, а также обучение персонала могут существенно повысить уровень защиты предприятий от потенциальных угроз. Промышленные сети автоматизации и управления играют

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

ключевую роль в современных производственных процессах. Они обеспечивают связь между различными элементами системы управления, такими как датчики, контроллеры и исполнительные механизмы. Однако с увеличением сложности этих сетей возрастает и риск возникновения различных угроз, как внешних, так и внутренних.

ЛИТЕРАТУРА

Абалымазов Э.И. (2023). «Концепция безопасности: тактика высокоэффективной защиты. Стоимость стратегии, стратегические ресурсы, тактика защиты, сопоставимость тактических решений». — Системы безопасности. — 4. — 111–115.

АСПБ (Система управления промбезопасностью). [Электронный ресурс]. Режим доступа: https://smis-expert.com/aspb-sistema-upravleniya-prombezopasnostyu/, свободный (дата обращения: 18.09.2024).

Буч Г., Рамбо Дж., Джекобсон А. (2018). UML. Проектирование программных комплексов, информационных систем. — М.: ДМК Пресс, СПб.: Питер. — 432 с.

Галатенко В.А. (2019). Стандарты информационной безопасности / Под ред. В.Б. Бетелина. — М.: ИНТУИТ.РУ «Интернет-университет информационных технологий». — 328 с.

Домарев В.В. (2020). Безопасность информационных технологий. Методология создания систем защиты. — К.: ДиаСофт. — 614 с.

Зильбербург Л.И., Молочник В.И., Яблочников Е.И. (2020). Реинжиниринг и автоматизация технологической подготовки производства в машиностроении. — СПб.: Компьютербург. — 152 с.

Иващенко А.В., Кременецкая М.Е. (2019). Автореинжиниринг единого информационного пространства предприятия. — Самара: СНЦ РАН. — 116 с.

Ивашкин С.В. (2020). Методы защиты промышленных сетей. — М.: Научный мир.

Информационная безопасность автоматизированных систем: понятие, методы обеспечения. [Электронный ресурс]. Режим доступа: https://gb.ru/blog/informatsionnaya-bezopasnost-avtomatizirovannykh-sistem/, свободный (дата обращения: 18.09.2024).

Кузнецов Е.В. (2019). Автоматизация и управление на предприятии. — Екатеринбург: УралГТУ.

Медведовский И. (2018). «Современные методы и средства анализа и контроля рисков информационных систем компаний». iXBT.com. — 7. — 138–140.

Омельянчук А.М. (2018). «Формирование систем комплексной безопасности». Системы безопасности. — 1(85). — 100–102.

Об автоматизации процессов охраны труда в промышленности. [Электронный ресурс]. Режим доступа: https://www.cti.ru/media/publications/ob-avtomatizatsii-protsessov-okhrany-truda-v-promyshlennosti/, свободный (дата обращения: 18.09.2024).

Петров А.А. (2021). Информационная безопасность промышленности. — СПб.: Наука.

Резников Г.Я., Бабин С.А., Костогрызов А.И., Родионов В.Н. (2021). «Количественная оценка защищенности автоматизированных систем от несанкционированного доступа». Информационные технологии в проектировании и производстве. — 1. — 11–22.

Резников Г.Я. (2020). Рациональный мониторинг процессов менеджмента качества на предприятиях. — М.: Мир. — 284 с.

Садердинов А.А., Трайнев В.А., Федулов А.А. (2023). Информационная безопасность предприятия: Учебное пособие. — М.: Дашков и Ко. — 336 с.

Ярочкин В.И. (2021). Служба безопасности коммерческого предприятия. — М.: Ось-89. — 144 с.

International Labour Organization (ILO). (2021). Safety and Health at Work: — A Vision for Sustainable Prevention.

Gartner (2021). Market Guide for Security Information and Event Management.

REFERENCES

Abalmazov E.I. (2023). Kontseptsiya bezopasnosti: taktika vysokoeffektivnoy zashchity. Stoimost strategii, strategicheskie resursy, taktika zashchity, sopostavimost takticheskikh resheniy [Security concept: tactics of highly effective protection. Cost of strategy, strategic resources, defense tactics, comparability of tactical decisions]. — Sistemy bezopasnosti [Security Systems]. — 4. — 111–115. [In Russ.].

ASPB (Sistema upravleniya prombezopasnostyu). (2024). [Electronic resource]. Available at: https://smis-expert.com/aspb-sistema-upravleniya-prombezopasnostyu. — Accessed: 18 September 2024.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

Buch G., Rambo Dzh., Dzhakobson A. (2018). UML. Proyektirovaniye programmnykh kompleksov, informatsionnykh sistem [UML. Design of software packages, information systems]. — Moscow: DMK Press, St. Petersburg: Piter. — 432 p. [In Russ.].

Galatenko V.A. (2019). Standarty informatsionnoy bezopasnosti [Information security standards]. Ed. V.B. Betelin. —Moscow: INTUIT.RU "Internet University of Information Technologies". — 328 p. [In Russ.].

Domarev V.V. (2020). Bezopasnost informatsionnykh tekhnologiy. Metodologiya sozdaniya sistem zashchity [Information technology security. Methodology for creating protection systems]. — Kyiv: DiaSoft. — 614 p. [In Russ.].

Zilberburg L.I., Molochnik V.I., Yablochnikov E.I. (2020). Reinzhiniring i avtomatizatsiya tekhnologicheskoy podgotovki proizvodstva v mashinostroyenii [Reengineering and automation of technological preparation of production in mechanical engineering]. — St. Petersburg: Kompyuterburg. — 152 p. [In Russ.].

Ivaschenko A.V., Kremenetskaya M.E. (2019). Avtoereinzhiniring yedinogo informatsionnogo prostranstva predpriyatiya [Autoreengineering of the unified information space of an enterprise]. — Samara: SRC RAS. — 116 p. [In Russ.].

Ivashkin S.V. (2020). Metody zashchity promyshlennykh setey [Methods of industrial network protection]. — Moscow: Nauchny Mir. [In Russ.].

Information security of automated systems: concept, methods of provision. (2024). [Electronic resource]. Available at: https://gb.ru/blog/informatsionnaya-bezopasnost-avtomatizirovannykh-sistem. —Accessed: 18 September 2024.

Kuznetsov E.V. (2019). Avtomatizatsiya i upravleniye na predpriyatii [Automation and management at the enterprise]. — Ekaterinburg: UralSTU. [In Russ.].

Medvedovsky I. (2018). "Sovremennyye metody i sredstva analiza i kontrolya riskov informatsionnykh sistem kompaniy" [Modern methods and means of analysis and control of risks in company information systems]. iXBT.com. — 7. — 138–140. [In Russ.].

Omelyanchuk A.M. (2018). "Formirovaniye sistem kompleksnoy bezopasnosti" [Formation of integrated security systems]. Sistemy bezopasnosti [Security Systems]. — 1(85). — 100–102. [In Russ.].

On the automation of labor protection processes in industry (2024). [Electronic resource]. Available at: https://www.cti.ru/media/publications/ob-avtomatizatsii-protsessov-okhrany-truda-v-promyshlennosti. — Accessed: 18 September 2024.

Petrov A.A. (2021). Informatsionnaya bezopasnost promyshlennosti [Information security of industry]. — St. Petersburg: Nauka. [In Russ.].

Reznikov G.Ya., Babin S.A., Kostogryzov A.I., Rodionov V.N. (2021). "Kolitsevnaya otsenka zashchishchennosti avtomatizirovannykh sistem ot nesanktsionirovannogo dostupa" [Quantitative assessment of the security of automated systems from unauthorized access]. Informatsionnyye tekhnologii v proyektirovanii i proizvodstve [Information Technologies in Design and Production]. — 1. — 11–22. [In Russ.].

Reznikov G.Ya. (2020). Ratsionalnyy monitoring protsessov menedzhmenta kachestva na predpriyatiyakh [Rational monitoring of quality management processes at enterprises]. — Moscow: Mir. — 284 p. [In Russ.].

Saderdinov A.A., Trainev V.A., Fedulov A.A. (2023). Informatsionnaya bezopasnost predpriyatiya: Uchebnoye posobiye [Information security of the enterprise: A tutorial]. — Moscow: Dashkov i Ko. — 336 p. [In Russ.].

Yarochkin V.I. (2021). Sluzhba bezopasnosti kommercheskogo predpriyatiya [Security service of a commercial enterprise]. — Moscow: Os-89. — 144 p. [In Russ.].

International Labour Organization (ILO). (2021). Safety and Health at Work: A Vision for Sustainable Prevention.

Gartner (2021). Market Guide for Security Information and Event Management.

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License

ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

Правила оформления статьи для публикации в журнале на сайте:
https://journal.iitu.edu.kz
ISSN 2708–2032 (print)
ISSN 2708–2040 (online)
Собственник: АО «Международный университет информационных технологий» (Казахстан, Алматы)

ОТВЕТСТВЕННЫЙ РЕДАКТОР
Мрзабаева Раушан Жалиқызы

КОМПЬЮТЕРНАЯ ВЕРСТКА
Асанова Жадыра

Подписано в печать 14.09.2024.
Формат 60x881/8. Бумага офсетная. Печать - ризограф. 9,0 п.л. Тираж 100
050040 г. Алматы, ул. Манаса 34/1, каб. 709, тел: +7 (727) 244-51-09).

Издание Международного университета информационных технологий
Издательский центр КБТУ, Алматы, ул. Толе би, 59