МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ
INTERREGIONAL ACADEMY OF PERSONNEL MANAGEMENT

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СУСПІЛЬСТВО

INFORMATION TECHNOLOGY AND SOCIETY

ВИПУСК 1
ISSUE 1

2021

Видавничий дім
«Гельветика»
2021

Рекомендовано до друку Вченою радою
Міжрегіональної Академії управління персоналом
(протокол № 2 від 26 травня 2021 року)

Інформаційні технології та суспільство / [головний редактор О. Попов]. – Київ: Міжрегіональна Академія управління персоналом, 2021. – Випуск 1. – 92 с.

Журнал «Інформаційні технології та суспільство» є науковим рецензованим виданням, в якому здійснюється публікація матеріалів науковців різних рівнів у вигляді наукових статей з метою їх поширення як серед вітчизняних дослідників, так і за кордоном.

Редакційна колегія не обов'язково поділяє позицію, висловлену авторами у статтях, та не несе відповідальності за достовірність наведених даних і посилань.

Свідоцтво про державну реєстрацію друкованого засобу масової інформації
«Інформаційні технології та суспільство» Серія КВ № 24815-14755Р від 27.04.2021 р.

Усі електронні версії статей журналу оприлюднюються на офіційній сторінці видання
http://journals.maup.com.ua/index.php/it

Статті у виданні перевірені на наявність плагіату за допомогою програмного забезпечення
StrikePlagiarism.com від польської компанії Plagiat.pl.

Recommended for publication
by Interregional Academy of Personnel Management
(Minutes No. 2 dated 26.05.2021)

Information Technology and Society / [chief editor Oleksandr Popov]. – Kyiv: Interregional Academy of Personnel Management, 2021. – Issue 1. – 92 p.

Journal «Information Technology and Society» is a peer-reviewed scientific edition, which publishes materials of scientists of various levels in the form of scientific articles for the purpose of their dissemination both among domestic researchers and abroad.

Editorial board do not necessarily reflect the position expressed by the authors of articles, and are not responsible for the accuracy of the data and references.

Print media registration certifi cate «Information Technology and Society»
series KV No. 24815-14755P dated 27.04.2021

All electronic versions of articles in the collection are available on the official website edition
http://journals.maup.com.ua/index.php/it

The articles were checked for plagiarism using the software
StrikePlagiarism.com developed by the Polish company Plagiat.pl.

ЗМІСТ

CONTENTS

УДК 378.018.43:37.016:
DOI https://doi.org/10.32689/maup.it.2021.1.1

Володимир БРОДКЕВИЧ
кандидат економічних наук, доцент кафедри комп'ютерних інформаційних систем та технологій, Інститут комп'ютерно-інформаційних технологій та дизайну, ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», вул. Фрометівська 2, Київ, Україна, індекс 03039 (v.brodkevych@gmail.com)

ORCID: https//orcid.org/0000-0003-4282-8888

Volodymyr BRODKEVYCH
Candidate of Economic Sciences, Associate Professor of the Department of Computer Information Systems and Technologies, Institute of Computer Information Technologies and Design, Interregional Academy of personnel management, 2 Frometivska Street, Kyiv, Ukraine, postal code 03039 (v.brodkevych@gmail.com)

Бібліографічний опис статті: Бродкевич В. Онлайн-навчання: еволюція МООС і LMS в епоху постковіда. Новітні задачі освітньої сфери. *Інформаційні технології та суспільство*. 2021. Вип. 1. С. 6–18. DOI: https://doi.org/10.32689/maup.it.2021.1.1

Bibliographic description of the article: Brodkevych, V. (2021). Onlain-navchannia: evoliutsiia MOOS i LMS v epokhu postkovida. Novitni zadachi osvitnoi sfery [Online-learning: the evolution of MOOS and LMS in the post-covid. The latest tasks of the educational sphere]. *Informatsiini tekhnolohii ta suspilstvo – Information technology and society*, 1, 6–18. DOI: https://doi.org/10.32689/maup.it.2021.1.1

ОНЛАЙН НАВЧАННЯ: ЕВОЛЮЦІЯ МООС І LMS В ЕПОХУ ПОСТКОВІДА. НОВІТНІ ЗАДАЧІ ОСВІТНЬОЇ СФЕРИ

Анотація. *В багатьох країнах світу можливостями отримання освіти через Інтернет користуються вже не перший рік і успішно. В Україні масові онлайн курси набувають певної розповсюдженості лише зараз. Досвід використання онлайн курсів свідчить, що якість освіти в Інтернеті не поступається університетському рівню. Інтернет ресурси у вигляді масових відкритих онлайн курсів МВОК (в англійському означенні Massive Open Online Courses – MOOCs) та систем керування навчанням – СКН (Learning Management System – LMS англ.) дозволяють покращити рівень знань, пропонують і надають можливість вдосконалити навички, які ми отримали від вищої освіти та слугують прекрасним помічником для саморозвитку.* ***Метою статті*** *є дослідження специфіки та можливостей навчального процесу та навчання з використанням систем курсів електронного навчання через інтернет мережі. Узагальнення результатів аналізу функціоналу МООС, LMC і висновки до їх практичного застосування в навчальних програмах. Висвітлення проблем пов'язаних з використанням електронних систем онлайн навчання.* ***Наукова новизна.*** *У статті піднімається проблема переходу освітніх закладів на нові технології навчальних процесів з використанням електронного онлайн навчання та способи їх застосування в процесі виконання існуючих навчальних програм. Автор на основі аналізу світових онлайн ресурсів МООС LMS в сфері освіти, актуалізує ці проблемні питання та підкреслює, що ця проблема потребує нагального її конструктивного вирішення. Даються рекомендаціє по вирішенні основних аспектів даної проблемної сфери. Як* ***висновок****, у статті наголошується, що створення розвинутої системи онлайн освіти в країні диктується умовами постковідного світу і тенденціями розвитку світової освіти. Це вимагає додаткових зусиль в сфері освіти, підготовки стандартизованих рішень ц вій царині є одним із важливих завдань нашої держави в соціальному і загальнолюдскому вимірах.*

Ключові слова: *електронне навчання, навчальні онлайн ресурси, масові відкриті онлайн курси – МВОК, системи керування навчанням – СКН, постковідна епоха.*

ONLINE LEARNING: THE EVOLUTION OF MOOS AND LMS IN THE POST-COVID. THE LATEST TASKS OF THE EDUCATIONAL SPHERE

Abstract. *In many countries of the world, the possibilities of obtaining education via the Internet have been used for more than a year and successfully. In Ukraine, mass online courses are gaining some distribution only now. The experience of using online courses shows that the quality of education on the Internet is not inferior to the university level. Online resources in the form of Massive Open Online Courses (MOOCs) and Learning Management System (LMS) allow us to improve the level of knowledge, offer and provide an opportunity to improve the skills we have received from higher education and serve as an excellent assistant for self-development. The purpose of the article is to study the specifics and possibilities of the educational process and training using e-learning course systems via the Internet. Generalization of the results of the analysis of MOOC, LMC, functionality and conclusions to their practical application in educational programs. Highlighting the problems associated with the use of electronic online learning systems.* ***Scientific novelty****. The article raises the problem of the transition of educational institutions to new technologies of educational processes using e-online learning and how to use them in the process of implementing existing curricula. The author, based on the analysis of MOOC LMS world online resources in the field of education, actualizes these problematic issues and emphasizes that this problem requires an urgent*

constructive solution. Recommendations are given to solve the main aspects of this problem area. As a ***conclusion****, the article emphasizes that the creation of a developed system of online education in the country is dictated by the conditions of the post-covid world and trends in the development of world education. This requires additional efforts in the field of education, preparation of standardized decisions in the field of war is one of the important tasks of our state in the social and human dimensions.*

Key words: *educational online resources, Mass open online courses – MOOC, Learning Management Systems – LMS, post-covid times.*

Актуальність проблеми. Переваги, що надають географічні та політичні кордони завжди були важливою домінуючою характеристикою вищих навчальних закладів. Ця їхня залежність була з початку моменту їх створення. Тим не менш, нові технології та зростаюча влада суспільства споживацтва кидають виклик статус-кво.

Прикладні Інтернет базовані додатки що використовують інформаційні і комунікаційні технологію для навчальних процесів е-навчання, роблять можливим навчання в трансцендному просторі, часі і незалежно від політичних кордонів. В електронному навчанні зміст і режим доставки навчальних послуг все частіше визначаються зовнішніми групами: студентами, а також роботодавцями. Поява електронного навчання послаблює домінування традиційних постачальників вищої та безперервної освіти – некомерційних коледжів та університетів. Вони отримують виклик від все більш розповсюджених альтернативних установ та постачальників з послуг, що забезпечують набуття відповідних навичок і рівнів, необхідних для досягнення успіху на новому освітньому ринку.

Партнерство дозволяє традиційним постачальникам та посередникам зробити свій внесок у відповідні порівняльні переваги. У загальній моделі, що розвивається, традиційні університети надають інтелектуальний капітал, контент та підтримку контенту.

Університети можуть і залишають за собою право оцінити ефективність навчання студентів; і присудити відповідний диплом кредиту або сертифікації. Посередники сприяють у таких сферах, як апаратне та програмне забезпечення, навчальний дизайн для Інтернету, веб-сайти та комунікація для обслуговування, обліку, навчання вчителів та технічної підтримки для розробки та маркетингу навчальних програм.

Хоча ця тенденція ще не дуже розвинена в нашій країні, вже є кілька успішних кейсів використання порівняльної переваги на освітньому ринку. Інтерес до цього зростає серед основних груп зацікавлених сторін – адміністративні і керівні установи держави, включаючи Міністерство освіти іта науки, Національне агенство з якості вищої освіти, традиційні академічні установи, традиційні студенти, нові посередники, професіонали з необхідністю безперервної освіти, і корпорації приватного сектору, у яких є необхідність надання можливостей освітніх послуг для своєї робочої сили. Проблема розвитку е-навчання з усіма її аспектами потребує нагального, ефективного вирішення з участю всіх зацікавлених сторін. Шляхи розвитку, базові ресурси е-навчання і перспективи використання онлайн навчальних платформ і є те, чому і присвячене це дослідження. Крім того в статті актуалізується проблема пошуку шляхів оптимізації процесів онлайн навчання до умов навчальних програм вишів і шкіл.

Аналіз останніх досліджень і публікацій. Аналіз наукової літератури свідчить про те, що існує чимало досліджень, спрямованих на вирішення проблеми активізації і підвищення можливостей вишів при використанні електронних онлайн навчальних курсів та систем управління навчальними процесами. Так, в статті «Quality enhancement for e-learning courses: The role of student feedback» проводиться аналіз якості використання електронних онлайн курсів в навчальному процесі через опитування студентів.

Автори вказують, що зібрані матеріали і документація із забезпечення якості та опитування зацікавлених сторін – студентів (репрезентантів) та персоналу (адміністраторів, освітніх технологів, лекторів) і порівняльний аналіз наборів даних показав, що основні стратегії збору зворотного зв'язку студентів на курсах електронного навчання, не змогли належним чином підтримати факти підвищення якості. Причинами зниження рейтингових модульних оцінок вважається віддалене розміщення студентів. На функцію вдосконалення оцінки модуля негативно вплинула відсутність відповідного управління курсами, що виникла внаслідок дезагрегації курсових процесів та неоднозначності у розподілі обов'язків. (Jara, Mellar, pp. 709–714).

Деякі автори зазначають, що в межах регіону або держави ефективним інструментом в розвитку електронного навчання може бути створення регіонального технологічного центра, що є прикладом нової організації-посередника. Робота центру (Азіатсько-Тихоокеанський регіональний технологічний центр – APRTC) спирається майже виключно на електронне навчання для надання освіти і виконує свою функції через багатосекторальні партнерства. Початковий досвід свідчить про те, що цей підхід працює в регіоні і є економічно ефективним, і що всі партнери та клієнти можуть і отримують вигоду від співпраці (Raab, Ellis & Abdon, 2001, pp. 217–229).

Метою статті є дослідження специфіки навчальної роботи та організація занять з застосуванням систем керування курсів електронного навчання через інтернет мережі. Отримання аналітичних результати вивчення функціоналу і можливостей сучасних МООС, LMC і забезпечення корисних результатів для їх можливого практичного застосування в навчальних програмах при викладанні в вишах і школі. Висвітлення основних аспектів проблем пов'язаних з використанням електронних систем онлайн навчання в вищій школі.

Виклад основного матеріалу.

Масові відкриті онлайн курси – переваги використання в освіті. Надзвичайної популярності серед студентів та професіоналів набирають онлайн-курси на базі систем керування навчанням (LMS англ.) та масових відкритих онлайн-курсів (MOOCs англ.). Обсяг пропозицій МООС у 2018 році перетнув позначку в 100 мільйонів учнів, досягнувши в цілому 101 мільйона. Платформи МООС на даний момент отримують значне збільшення надходжень в оплаті від студентів. 19 і пов'язані з ним карантини і локдауни радикально збільшили заінтересованість в е-навчанні, породили великі запити на віддалені послуги конференц- і відеозв'язку, як основних ресурсів дистанційної роботи. В освітній сфері це призвело до активного використання Інтернет ресурсів у вигляді комунікаційних технологій (Zoom, MsTime, Google Meet, Skype та ін.) та систем підтримки онлайн курсів LMS (Moodle та ін.), Наразі спостерігається збільшення як числа учасників МООС – провідних університетів та і пропозицій навчання за онлайн-ступенями та спеціалізації через платформи МООС.

Масові відкриті онлайн-курси (MOOCs) – це безкоштовні онлайн-курси, доступні для всіх, хто в них зареєструвався. MOOCs забезпечують доступний і гнучкий спосіб засвоїти нові навички, просунути свою кар'єру і забезпечити якісний освітній досвід в масштабі (www.mooc.org).

Переваги МООС це:

- забезпечення доступного і гнучкого способу освоєння нових навичок, забезпечення якісної освітньої підготовки,
- можливість безперервного процесу зростання свого професійного і освітнього рівня,
- забезпечення кар'єрного росту.

Як засвідчено у Вікіпедії – мільйони людей по всьому світу використовують МООС для навчання з різних причин, включаючи: розвиток кар'єри, зміну кар'єри, підготовку до коледжу, додаткове навчання, навчання протягом усього життя, корпоративне навчання тощо (https://en.wikipedia.org/wiki/Massive_open_online_course).

МООС кардинально змінили спосіб навчання у світі. Аналіз наукових досліджень і практики свідчить про те, що майбутнє навчання і його результати в значній мірі будуть залежати від створення і використання стратегії електронного навчання в масштабах країни або регіону.

МООС теоретично можуть вмістити необмежену кількість учнів. Однак, на практиці більшість корпоративних тренінгів МООС не є відкриті для загальної публіки. Але разом з тим, вони все є значно більшими від традиційних курсів. Багато сотень або навіть тисяч учнів можуть навчатись, будучи розподіленими по різних локаціях. Це також призводить до появи проблеми вибору серед учнів – яку платформу МООС обрати (Peter, Berking, 2016).

МООС і LMS. МООС може бути запущений на LMS, але це не є обов'язково. У той же час, LMS може бути використаний для проведення курсу, який не є МООС. Непорозуміння часто виникає, тому що основні платформи МООС – Coursera, edX і так далі – ідентифікують себе як LMS і МООС.

Традиційні курси, що проводяться на LMS, як правило, є дискретні сутності, а це означає, що вони починаються в певний день, закінчуються в певний день, мають конкретні терміни тощо. Як і навчання під керівництвом інструкторів (ILT). Це включає вартості роботи інструктора та розкладу занять. МООС можуть також бути організовані аналогічно, але вони також можуть пропонуватись на постійній основі для розміщення за шаховими графіками. Наприклад, така ж орієнтація МООС може бути використана (в той час, якщо це необхідно) для нових наймачів, які починають з середини тижня, місяця чи року.

Електронне навчання і що дає LMS? На сьогодні це поняття достатньо добре розкрито в багатьох наукових джерелах. За визначенням дослідників Лабораторії архітектури навчальних систем в Карнегі-Меллоні зазначається: «Система управління навчанням (LMS) – це програмний пакет, який використовується для адміністрування одного або одного або більше курсів для одного або більшої кількості учнів. LMS – це, як правило, веб-система, яка дозволяє учням автентифікуватися, реєструватися на курси, завершувати курси та отримати оцінки» (LSAL, 2004 in Gallagher, 2007).

Система управління навчанням (Learning Management System – LMS) – це програмне забезпечення для адміністрування, документації, відстеження, звітності, автоматизації та доставки освітніх курсів,

навчальних програм та програм розвитку. Концепція системи управління навчанням виникла безпосередньо з електронного навчання. Хоча перші LMS з'явилися у сфері вищої освіти, більшість LMS сьогодні орієнтуються на корпоративний ринок. Системи управління навчанням – LMS складають найбільший сегмент ринку навчальних систем. Перше LMS було запроваджено наприкінці 1990-х років (https://www.irrodl.org/index.php/irrodl/article/view/17/354).

Навчання через Інтернет: поява перших LMS. До перших зародкових систем е-навчання можна віднести FirstClass, – клієнт-серверна групова програму, куди включена електронна пошта, онлайн-конференції, голосові та факсимільні служби, а також система дошки оголошень для Windows, macOS та Linux. Первинними ринками FirstClass є сектори вищої освіти та освіти К-12, включаючи чотири з десяти найбільших шкільних округів Сполучених Штатів.

Проєкт фірми SoftArc, який використовувався Відкритим університетом Великобританії (Open University) в 1990-х і 2000-х роках для онлайн-навчання по всій Європі, був одним з найбільш ранніх інтернет-LMS.

Перша повнофункціональна система управління навчанням (LMS) отримала назву ЕККО, розроблена і випущена Норвезькою мережею дистанційної освіти NKI в 1991 році (Long, Phillip D.,2004). Через три роки Нью-Брансвік в NB Learning Network представив аналогічну систему, орієнтовану для викладання на основі DOS, і призначену виключно для бізнес-навчання.

Аспекти організації LMS. LMS може бути розміщено локально або через послуги постачальника. Хмарна система, розміщена постачальником, має тенденцію слідувати моделі Послуг SaaS (Software as a service) (програмне забезпечення як послуга).

Застосунки SaaS також відомі як програмне забезпечення за запитом та веб-програмне забезпечення, розміщене на веб-сайті.

Всі дані в системі, розміщеній постачальником, розміщуються постачальником і отримують доступ до них через Інтернет, на комп'ютері або мобільному пристрої. Системи, розміщені постачальниками, зазвичай прості у використанні та вимагають меншої технічної експертизи. Якщо LMS локально розміщена, вона бачить всі дані, що стосуються LMS, що розміщені всередині на внутрішніх серверах користувачів. Локальна архітектура програмного забезпечення LMS часто використовує відкритий вихідний код, тобто користувачі отримуватимуть (або через оплату, або безкоштовно) програмне забезпечення LMS та його код. При цьому користувач може змінювати і підтримувати програмне забезпечення через внутрішню команду. Приватні особи та менші організації, як правило, дотримуються використання хмарних систем через витрати на внутрішній хостинг та обслуговування.

Переваги LMS. Деякі автори виділяють шість основних переваг LMS:

- сумісність,
- доступність,
- багаторазове використання,
- довговічність,
- придатність до технічного обслуговування,
- адаптивність.

Цей перелік сам по собі складає концепцію LMS.

Недоліки LMS. Впровадження LMS вимагає добре побудованої технологічної інфраструктури. Викладачі повинні бути готові адаптувати свої навчальні плани від лекцій віч-на-віч до онлайн-лекцій Schoonenboom, Judith (February 2014).

Провідні постачальники електронного навчання та MOOC. Нинішня світова онлайнова навчальна галузь включає Інтернет ресурси, які у вигляді MOOC та LMS, можуть бути розміщені у формі Веб-сторінок як на серверних платформах та і в хмарних локаціях. Їх число вже може вимірюватись в сотнях чи може і в тризначних числах. Однак, існують найбільш використовувані платформи, до яких можна віднести перераховані в наступному розділі нижче. Розглянемо ці ресурси з точки зору їх придатності до використання в навчальних процесах чи бути включеними в навчальні програми в школах і вишах.

EDX. Коли користувач заходить на сайт MOOC, його зустрічає привітання з поясненням «Mooc.org є продовженням edX.org, лідера онлайн-курсів. Незалежно від того, чи зацікавлені ви в навчанні для себе, використовувати онлайн-курси для навчання вашої робочої сили або створення MOOC, edX може допомогти».

Курси EdX складаються з щотижневих послідовностей навчання, і кожна послідовність навчання складається з коротких відео з інтерактивними навчальними вправами, де студенти можуть негайно практикувати концепції з відео. Він також має об'єкт онлайн-дискусійного форуму, де студенти можуть розміщувати та переглядати питання та відповідати один з одним. Кращі MOOC та онлайн-платформи для навчання індійських користувачів.

Онлайн програми edX.

Програма мікробакалаврів.

На рівні бакалаврату, для кар'єрного просування або дипломного шляху.

Програма мікромагістрів.

Вища освіта, для кар'єрного просування або продовження дипломного шляху.

Професійний сертифікат.

Від роботодавців або університетів, щоб побудувати сьогодні затребувані навички.

XSeries.

Серія курсів для глибокого вивчення і розуміння теми.

Онлайн ступінь магістра.

Найпопулярніші доступні програми, та повністю онлайн. Шлях для подальшого кар'єрного зростання і просування. Програми від провідних професорів відомих університетів – безкоштовно, лише платний сертифікат університету X (https://www.edx.org/search?tab=course&utm_campaign=mooc-cta&utm_medium= referral&utm_source=mooc.org).

Відкритий університет. Відкритий університет Open University (OU) є найбільшим академічним закладом Великобританії і світовим лідером у гнучкому дистанційному навчанні.

З моменту його початку в 1969 році, OU навчив більше 1,8 мільйона студентів і має майже 250000 нинішніх студентів, у тому числі більш ніж 15000 за кордоном. OU оцінюється в п'ятірці кращих університетів Великобританії за задоволеністю студентів в Національному опитуванні студентів. Оскільки опитування почалося в 2005 році то у 2012/13 роках він мав рейтинг задоволеності 92%. Понад 70% студентів працюють на денній або заочній роботі, а чотири з п'яти компаній що входять в список FTSE100 спонсорували співробітників, щоб вони проходили курси OU.

В останніх британських дослідженнях Research Assessment Exercise з оцінки досліджень (RAE 2008) Відкритий університет зайняв перше місце в верхній третині вищих навчальних закладів Великобританії. Більше 50% досліджень OU оцінювалися в RAE як чудові на міжнародному рівні, а 14% – як провідні у світі.

OU вважається головним закладом електронного навчання в Британії, є світовим лідером у розробці технологій для збільшення доступу до освіти в глобальному масштабі. Його величезне «відкрите портфоліо контенту» включає безкоштовні навчальні розділи на OpenLearn. OpenLearn мав понад 26,7 мільйонів відвідувань. Великий успіх мав контент та матеріали на iTunesU. Там зафіксовано понад 60 мільйонів завантажень. OU має 41-річне партнерство з BBC, яка перейшла від лекцій пізньої ночі в 1970-х роках до прайм-тайм програм, таких як Frozen Planet, Bang Goes Theory, Великі ідеї Джеймса Мей та Програма грошей (http://www.open.ac.uk).

Особливості навчальних курсів Coursera. Заснована в 2012 році професорами Стенфорда Ендрю Нго і Дахпне Koller, в даний час Coursera є найпопулярнішим постачальником MOOC у всьому світі. Амбітна компанія, яка співпрацює з топ-університетами по всьому світу, пропонує безкоштовні та платні онлайн-курси, спеціалізації та повноцінні онлайн-ступені. Курси викладають провідні професори з усього світу. За даними CNBC «більше 150 університетів запропонували понад 4000 курсів через Coursera, який включає в себе більше двох десятків програм ступеня за цінами, які нижче, ніж багато особистих шкільних пропозицій».

Курси Coursera призначені для отримання нових навичок протягом 4-6 тижнів. При успішному закінчення курсу студент отримує сертифікат цього курсу. Вартість курсів коливається в межах $ 29 – $ 99. При цьому можна також пройти ці курси безкоштовно, з деякими обмеженнями на матеріал курсу та / або без сертифіката по закінченні.

В навчальній системі Coursera включені опційні можливості. Серед яких можна виділити:

- спеціалізації Coursera,
- онлайн ступені Coursera,
- навчальні програми Coursera для університетів.

Спеціалізація Coursera. Ця опція – це можливість отримати повну освіту в галузі де учень можете вибрати довший і комбінований набір курсів Coursera, які в сукупності називаються спеціалізацією. Оплата в розмірі $ 39 – $ 79 на місяць протягом від 3 до 6 місяців.

По закінченні курсів спеціалізації можна отримати сертифікат спеціалізації, що видається відповідним університетом чи партнером Coursera.

Онлайн наукові ступені Coursera. Студенти, які мають більш серйозні прагнення, можуть вибрати більш тривалий термін навчання, – від одного до трьох років, для отримання визнаного наукового ступеня онлайн з акредитованим університетом. Навчання закінчується акредитованим ступенем магістра з вимогою онлайн-прийому. Це коштує дорожче порівняно із звичайними по ціні в діапазоні від $ 15000 до $ 25000, в залежності від теми. Ці курси є зручним і більш розумним варіантом продовження

освіти, особливо для працюючих фахівців. Пропоновані предмети включають MBA, інформатику, науку про дані, аналітику, маркетинг, бухгалтерський облік тощо.

Для навчальних закладів не менш важливим є можливість створити за підтримки Coursera спільну програму курсів, орієнтованих на конкретні дисципліни, з урахуванням галузевих навчальних програм університету.

Згідно з Навчальною програмою (див. рис. 1) за базовим навчальним планом, узгодженою між закладом вищої освіти (університетом, інститутом) та Coursera Campus Basic Plan, студенти і працівники вишу отримують доступ до контенту курсів. По успішному закінченні можуть отримати сертифікат.

Серед останніх пропозицій в навчальній програмі Coursera, крім того кожен зареєстрований користувач може отримати один навчальний курс безкоштовно протягом одного року. Для прикладу, цей курс викладач може добавити до конкретної програми, розширивши навчальний контент для студентів і збагативши можливості навчального процесу.

Необхідно відмітити, що на час першого карантину (Lockdown) з квітня і до жовтня 2020 року для учасників Навчальних програм Coursera для усіх університетів було надано відкритий доступ до безкоштовного проходження курсів без обмежень.

Крім цього гуманного поступку (акції благодійності), зауважимо, що, Coursera також пропонує можливість фінансової допомоги для завершення спеціалізацій та онлайн-ступенів. Люди, що приєднуються до курсу Coursera, також будуть частиною глобальної спільноти, яка налічує тисячі студентів.

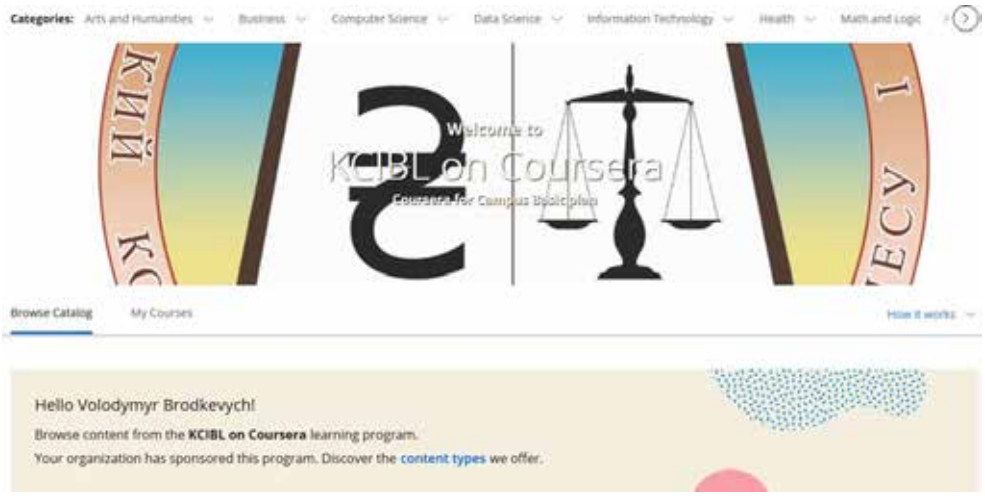


Рис. 1. Приклад початкової сторінки навчальної програми вишу на вебсайті Coursera

Як працюють навчальні програми Coursera? Навчальна програма – це місце, де група запрошених учнів має доступ до каталогу курсів, які допомагають їм розвивати відповідні навички, які допоможуть їм виконувати поточну роботу та виконувати свої майбутні кар'єрні цілі.

Учнів потрібно запросити приєднатися до навчальної програми, а учитель сам може приєднатися до кількох навчальних програм.

Кожна навчальна програма має спеціальний каталог курсів, до яких можуть отримати доступ лише учні, запрошені приєднатися до цієї програми.

Адміністратори програм можуть редагувати каталог рекомендацій курсу та додавати нові елементи колекцій курсів. Вони також можуть запрошувати, видаляти та переглядати звіти для учнів цієї навчальної програми.

Постановка проблеми. Для багатьох університетів онлайн-навчання та змішані, гібридні аудиторії продовжать відігравати центральну роль в освіті в найближчому майбутньому, що є результатом існуючих тенденцій та розвитку, пов'язаного з пандемією. Це представляє собою проблемний блок завдань, які треба вирішувати освітній галузі, що накладає нові вимоги і до навчальних процесів у вищій освіті. Розглянемо деякі з них, що можна вважати провідними, існуючі онлайн навчальні системи. Їх можна вважати орієнтиром в для отримання відповіді на питання:

1. Офіційна оцінка та затвердження ефективних існуючих практик використання електронних онлайн навчальних ресурсів в якості базових для забезпечення (в тому числі в правовому аспекті) ефективного, якісного навчального процесу.

2. Розробка методик і стандартів використання LMS в навчальному процесі.

3. Вибір перспектив напрямку розвитку і основні кроки в процесі розвитку онлайн навчання та вирішення задач і технології побудови нових LMS або центру організації функціонування і використання електронних навчальних онлайн ресурсів в масштабі країни.

Khan Academy. Ідея академії Khan сформульована на першій сторінці їх сайту «Ми некомерційна організація з місією забезпечити безкоштовну освіту світового рівня для будь-кого, де завгодно» (https://www.khanacademy.org/) (рис. 2).

Заснована була ця онлайн академія педагогом Салманом Ханом, який вирішив створити ресурс, який дозволятиме людям з усього світу займатися самоосвітою, не виходячи з власного будинку. Таким чином, у 2006 році в Інтернеті народився проект Khan Academy, що розпочав новий етап розвитку освіти в сучасному світі.

Всі матеріали, курси та лекції знаходяться у вільному безкоштовному доступі для будь-якої людини на планеті, яка має можливість користуватися Інтернетом.

Фінансування проекту відбувається на волонтерських засадах, проте основні кошти на розвиток сайту виділяють благодійний фонд Google і фонд Мелінди та Білла Гейтс.

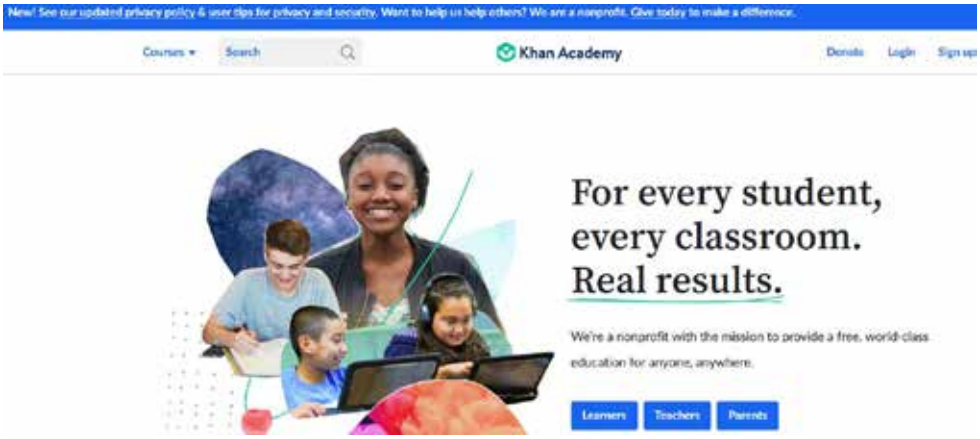


Рис. 2. Перша сторінка сайту Khan Academy

Онлайн-курси Udemy. Компанія Udemy була заснована в 2010 році (в Кремнієвій долині) для поліпшення життя за допомогою електронного навчання. Це всесвітньо відомий форум онлайн-навчання, де 10 мільйонів+ студентів проходять курси у всьому, від програмування, йоги, фотографії та багато іншого. Кожен з цих курсів викладають інструктори-експерти. Платформа дозволяє інструкторам будувати онлайн-курси на теми на свій вибір. Вони також можуть завантажувати відео, презентації PowerPoint, PDF-файли, аудіо- та zip-файли та живі заняття для створення курсів. Інструктори також можуть взаємодіяти між собою та взаємодіяти з користувачами через онлайн-обговорення (https://www.udemy.com/).

Інтерактивна навчальна платформа Edureka. Edureka – одна з найбільш інтерактивних платформ електронного навчання. Платформа виділяється інтерактивним і привабливим методом навчання. Edureka надає розширені програми по актуальних напрямках з Штучного інтелекту і машинного навчання, Післядипломні Програми і сертифікації випускників (Post Graduate Certification Program) (https://www.edureka.co/). Курси включають Науку про данні (Data Science), Пректний менеджмент (Project Management), Комп'ютерні науки (Computer Science) – Python, SQL, Big Data, Cloud computing, DevOps, Бізнес аналітика і візуалізація (BI and Visualization) Статистика. Крім того студенти можуть освоїти магістерські програми, щоб отримати ступінь магістра в галузі науки про дані, професійний сертифікат а також та мікро-магістри та багато іншого. Платформа також надає актуальні сценарії проектів для бізнесу на веб-платформах компанії Амазон- (Amazon Web Service AWS). Сертифікація Edureka розроблена і курується та оцінена професіоналами та експертами галузі.

Інші інтернет-навчальні ресурси. В таблиці 1 вказані особливості сервісу популярних інтернет платформ онлайн навчання з доменними іменами.

До вищезазначених сайтів, можна добавити деякі інші популярні платформи MOOC. До них належать:

- FutureLearn
- Udacity
- Cognitive Class

- Iversity
- Kadenze
- Canvas
- Lynda

Таблиця 1

Назва платформи	Інтернет ресурс	Особливості освітніх послуг
SIMPLILEARN	https://www.simplilearn.com/	Пропонують університетську сертифікацію професійного рівня та координують навчання з компаніями та приватними особами
SKILLWISE	https://www.bbc.co.uk/teach/skillswise	Колекція безкоштовних відео та завантажуваних сторінок, які допоможуть дорослим удосконалити навички читання, письма та нумерації. Проєкт підтримується BBC.
UPGRAD	https://www.upgrad.com/ua/	Це передова платформа онлайн-навчання в США розрахована на самовдосконалення. На курсах викладаються складні теми простим способом, і в основному зосереджується на резюме з зворотним зв'язком та імітації інтерв'ю з експертами галузі.
SPRINGBOARD	https://www.springboard.com/	Девіз курсів «Навчіться онлайн з гарантією роботи».
WIZIQ	https://www.wiziq.com/	Платформа оцінюється як одна серед найбільших хмарних навчальних рішень у світі. Система забезпечує віртуальне навчання в класі з управління курсами, створення контенту, потокового відео, інсайтів та аналітики, мобільного навчання тощо.
ALISON	https://alison.com/	Це безкоштовна онлайн-платформа для людей, які хочуть навчатися на сертифікованому і класичному рівні. Alison відома своїми далекосяжними можливостями в апгрейдингу навчання
SKILLSHARE	https://www.skillshare.com/	Skillshare – це спільнота онлайн-навчання для людей, які хочуть вчитися на освітніх відео. Курси, які не акредитовані, доступні через підписку. Більшість курсів зосереджені на взаємодії, а не на лекціях, з основною метою навчання досягненою через завершення проекту.

Українські навчальні інтернет-платформи.

Prometeus. Prometheus, вітчизняний преовайдер онлайн курсів. Платформа започаткована з жовтня 2014 року Іваном Примаченком разом зі своєї командою волонтерів Мал. 3. Перші курси були запропоновані викладачами КНУ ім. Шевченко, КПІ та Києво-Могилянською Академією. Згодом до партнерства приєдналися УКУ та Львівська ІТ-школа (https://prometheus.org.ua/courses-catalog/data-analysis/).

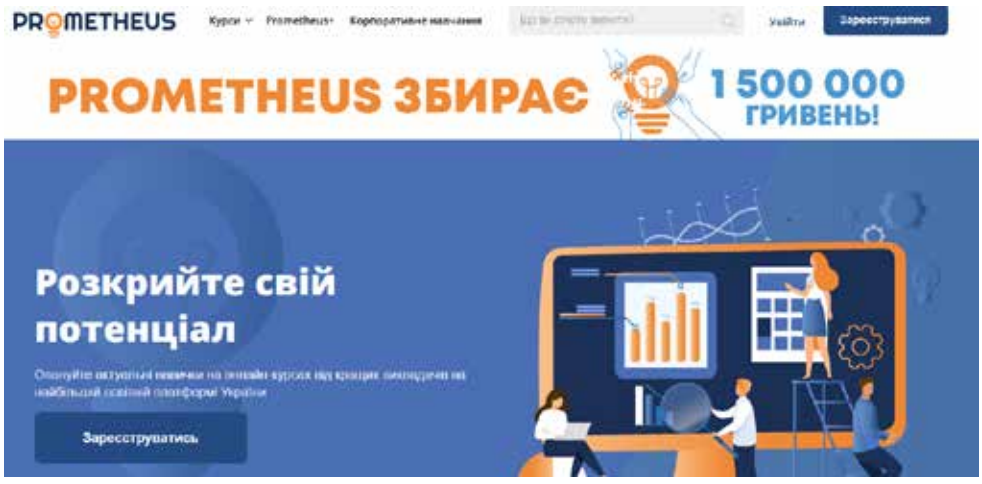


Рис. 3. Заголовок сайту порталу Prometeus

(https://prometheus.org.ua/courses-catalog/data-analysis/)

На перших порах доступно для користувачів було до 20-ти безкоштовних онлайн курсів провідних українських викладачів. 70 тисяч користувачів зареєструвалося на порталі за перші півроку.

Кількість користувачі курсів щоденно зростає. Prometheus отримав великий приплив користувачів після підключення безкоштовного онлайн курсу Гарвардського університету CS50 «Основи програмування». В короткий термін менш, ніж за 2 місяці, на сайті зареєструвалося близько 40 000 користувачів.

Серед основних завдань, автори проекту вбачають надання онлайн доступу до кращих навчальних матеріалів України всім охочим людям; підтягування стандартів своєї роботи до світового рівня та запуск експерименту, пов'язаного з наданням змішаного освітнього процесу в одному з університетів України.

Навчання на порталі є повністю безкоштовними. «Викладач може рекомендувати навчальну літературу, щоб Ви могли глибше вивчити ту чи іншу тему, але доступних в рамках курсу матеріалів буде достатньо для успішного його завершення. «Все що Вам знадобиться, – доступ до мережі Інтернет на швидкості, достатній для перегляду відеолекцій», вказується в роз'ясненнях на сайті.

Після успішного завершення всіх завдання курсу, якщо ж ви готові здійснити благодійний внесок, Prometheus пропонує вам отримати верифікований сертифікат.

Одним з недоліків порталу можна назвати те, що деякі курси не передбачають отримання безкоштовних сертифікатів.

Міністерство освіти і науки спільно з платформою масових відкритих онлайн-курсів Prometheus представляють повний цикл безкоштовних онлайн-курсів з підготовки до зовнішнього незалежного оцінювання з математики, української мови і літератури та історії України. ГО «ПРОМЕТЕУС» є суб'єктом надання освітніх послуг з підвищення кваліфікації педагогічних працівників. Враховуючи запити працівників освіти Prometheus упорядкував свої безкоштовні онлайн-курси підвищення кваліфікації освітян відповідно до нових вимог зазначених в «Порядку підвищення кваліфікації педагогічних і науково-педагогічних працівників» (Постанова КМУ від 21 серпня 2019 р. № 800 зі змінами та доповненнями від 27 грудня 2019 р. № 1133). А це означає, що сертифікати онлайн-курсів Prometheus для вчителів відтепер можуть бути офіційно зараховані як підвищення кваліфікації.

Відеолекції, завдання та форум будуть доступні в будь-який час протягом курсу.

Важливі переваги української платформи онлайн курсів Prometheus:

- Можливість проходження унікальних лекцій, що пов'язані конкретно з Україною, та її історією;
- Наявність повного циклу безкоштовних онлайн-курсів з підготовки до зовнішнього незалежного оцінювання з математики, української мови і літератури та історії України також можливість пройти підготовчі курси до зовнішнього незалежного оцінювання;
- Можливість для освітян отримати сертифікати онлайн-курсів Prometheus які відтепер можуть бути офіційно зараховані як підвищення кваліфікації.

Edera. Портал Educational Era позиціонується як Студія онлайн-освіти. Включає освітні курси для вчителів, курси по створені онлайн ресурсів, курси юридичної і політичної просвіти (https://www.ed-era.com/)

Онлайн платформа з цифрової грамотності «Цифрова освіта». Інноваційний навчальний ресурс з амбітними планами. В результаті позитивного закінчення видається сертифікат про рівень цифрової грамотності (https://osvita.diia.gov.ua/) Перша сторінка сайту – магічне заклинання на рис. 4.

Платформа включає освітні серіали згруповані (на сьогоднішній день) в 23 категорії (рис. 5).

Доступ до освітніх серіалів є абсолютно безкоштовним для всіх громадян. Кожен, хто успішно здасть фінальне тестування, отримає електронний сертифікат. Ви зможете поділитися ним у соціальних мережах в якості свого досягнення або використати під час працевлаштування.

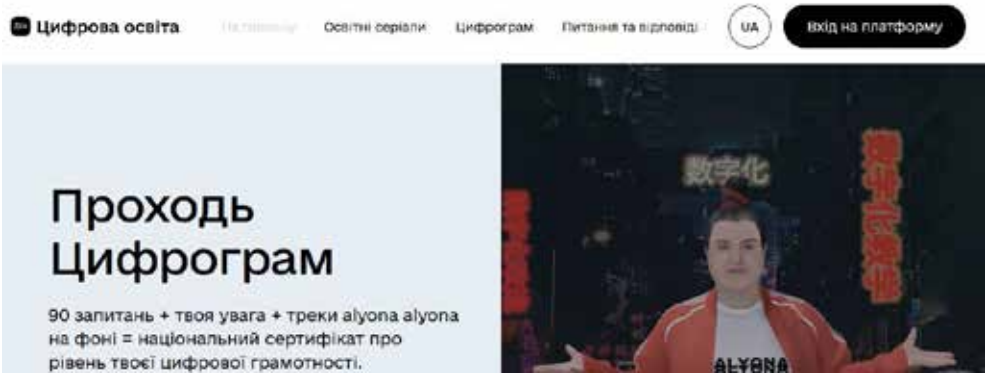


Рис. 4. Головна сторінка порталу «Цифрова освіта»

Рис. 5. Навчальні категорії порталу Цифрова освіта

Проєкт курує Міністерство цифрової трансформації України. А безпосередньою розробкою освітніх серіалів займалась студія онлайн-освіти EdEra. Також підтримку в розробці надавали компанії Google, Microsoft, Академія ДТЕК, CISCO та багато інших провідних компаній. Проєкт втілено за підтримки швейцарсько-української Програми EGAP, що фінансується Швейцарською агенцією з розвитку та співробітництва та реалізується Фондом Східна Європа та Фондом Innovabrige. На сайті також зазначається, – «Жодна політична сила не брала участі в створенні освітніх серіалів».

Мета проєкту – навчити цифровій грамотності 6 млн українців за 3 роки. Вільний доступ до освітніх серіалів на національній онлайн-платформі з цифрової грамотності – один із шляхів досягнення цієї мети. Цифрова грамотність українців буде однією з національних конкурентних переваг і дозволить комфортно проживати в країні.

Курси використовують органічне поєднання розваг із навчанням. Новий підхід до освітніх процесів під назвою «едьютейнмент». Така форма навчання довела свою ефективність і дозволяє отримувати високу мотивацію до набуття нових знань і навичок.

Сертифікати після проходження курсів з кредитами ЄКТС зараховуються як підвищення кваліфікації для державних службовців, відповідно до постанови КМУ № 106.

Портал BYMonline – громадянська освіта в Україні. Портал включає 76 курсів, 113690 (на 07.21) слухачів 167 викладачів.

Відкритий університет майдану ВУМ (https://vumonline.ua) – це освітня ініціатива, яка поширює ідеї і сприяє розвитку громадянського суспільства в Україні. Навчальні курси, сформовані з відео-лекцій, практичних завдань та контрольних запитань (для перевірки набутих знань). Це курси від провідних викладачів бізнес-шкіл, громадського сектору, практиків з бізнесу та соціальної сфери. Теми навчальних курсів пов`язані з: персональним розвитком та реалізацією вашого потенціалу, підприємництвом, як механізмом якісного розвитку громади і суспільства, розумінням побудови та діяльності відкритого суспільства і його формування в Україні.

Wisecow вільний відеолекторій. Портал, що позиціонується як вільний відеолекторій WiseCow створений для того, «щоб люди по всій Україні могли навчатися безкоштовно» (https://wisecow.com.ua/).

На сайті 9 розділів: література, кіно, мистецтво, музика, журналістика, театр, історія, мода та соціум, а також розділ «Міста» – карта соціальних ініціатив України та афіша подій. У кожному з розділів планується по 10 курсів. Кожен курс у свою чергу вміщує 10 відео та 10 додаткових матеріалів.

Цей формат актуальний для жителів великих міст у яких є можливість відвідувати найрізноманітніші лекції, але немає часу. Та особливо відеолекторій знадобиться жителям маленьких міст і сіл, куди не так часто привозять крутих спікерів з масштабними лекціями. WiseCow прагне, щоб доступ до структурованих знань у всіх був однаковий.

Головна мета проекту: надати українцям можливість вчитися вдома безкоштовно.

Розглянуті вище системи онлайн навчання далеко не становлять завершеного списку LMS. Умови постковідної реальності і зміни, що відбуваються в ході 4-ої Індустріальної революції рухають вперед

технологічні процеси в усіх галузях, в тому числі і освітній. Це призводить до появи нових підходів в ідеології онлайн навчання і створення LMS на інших принципах, як наприклад технологія «едью-тейнмент» на Онлайн платформі з цифрової грамотності. В Таблиці 2 вказані показники доступних інформаційних даних та деяких освітніх послуги, що надаються з урахуванням наявності матеріалів для викладачів, сертифікатів, е-дипломів.

Таблиця 2

Підсумкова таблиця основних освітніх послуг онлайн курсів

Назва	Кількість курсів/ напрямків наук-галузь знань	Доступ (безк./ плат)	Кількість унів-тів/ органз. співпр. по ств. курсів	Наявність матеріалів для викладачів	Серти-фікати	Електронний диплом
edX	3457/6	-/+	>33млн./2	+	+	-
Coursera	5100	+/+	200		+	-
Open courses MIT	100	+/+		+		Блоксерт
Canvas Network	-	+/+	6 млн./4000	+		-
Khan Academy	>100			+	+	-
Open University	/19	+	2 млн.			+
Udemy	155000	+/+	40млн./70000	+	+	-
WizIQ	70000	/+	4,5 млн	+		-
Udacity		/+	11,5 млн	+		-
Prometeus	>200	+/	1,5 млн.	+	+	-
ВУМonlinен	76 курсів,		113690/176	+	+	-

Основні переваги онлайн-навчання.

***Легкодоступна інформація*.** Завдяки онлайн-навчанню інформація легко доступна і за нижчою ціною. При цьому скорочуються накладні витрати, такі як фізичний простір для класів, обладнання і т.д. Будь-який учитель з будь-якого куточка світу може мати доступ до глобального вмісту з будь-якого місця і в будь-який час. Це надзвичайно корисно для осіб, які готуються до конкурсних іспитів, і для студентів оскільки вони можуть мати доступ до численних навчальних матеріалів, не виходячи з власних будинків і безкоштовно.

***Взаємодія та краще збереження вивченого в пам'яті*.** В традиційній системі освіти, яка в основному сконцентрована на ролі вчителя, активність обмежується лише письмовими дошками. З онлайн технологією це сильно змінилося. Тепер викладання вже не обмежується лише письмовими дошками. Онлайн уроки включають різні анімації та інші візуальні ефекти для підвищення залученості учнів. Завдяки кращій залученості студенти не тільки краще розуміють поглиблені концепції, але й зберігають у пам'яті вивчений матеріал і теми занять довше.

Персоналізоване навчання. Адаптивна технологія зробила можливим персоналізоване навчання. В даний час більшість платформ онлайн-навчання використовують великі дані та хмарні обчислення, щоб зрозуміти унікальний стиль навчання конкретного студента і дозволити їм вчитися у своєму власному темпі та стилі.

Гнучкість навчання. Використовуючи інструменти онлайн-навчання, учні можуть вчитися залишаючись в своєму комфортному середовищі, не виходячи з власного приміщення, залишаючи свій стиль та часові обмеження. Будь-яка людина з будь-якого куточка світу тепер може вчитися як їй зручно. Це надзвичайно корисно для студентів, оскільки тепер вони можуть завантажити будь-який ресурс, задати запитання тощо. Використовувати і звертатися до навчальних ресурсів студенти можуть, коли вони хочуть.

Порівняльні витрати на навчальний процес. Електронне навчання полегшить необхідність розміщення студентів та викладачів у централізованому просторі для навчання. Це економить гроші, які можуть бути витрачені на інші потреби: подорожі, проживання спорт, та інші види самовдосконалення, чого ті учні, які навчаються в школі, не можуть собі дозволити. Найважливіший життєвий ресурс – час, який витрачається на поїздки до школи, може бути використаний і для інших справ.

Недоліки. Звичайно, що будь-які новації в процесах і запровадження технологічних змін можуть нести і негативні наслідки. Так, більшість наших колег-викладачів переконані, що онлайн навчання суттєво обмежує практичні, лабораторні заняття за програмою. Це в свою чергу лімітує повноцінне засвоєння матеріалу студентами, особливо в галузі природничих дисциплін. Учні недоотримають можливість контактувати з лабораторними матеріалами, приладами, навчальними стендами і установками. Таким чином видається неможливим отримання тих фахових навичок і засвоєння технологій на основі практичних занять на навчальному устаткуванні, які, наприклад, вказуються в документах, затверджених стандартами вищої освіти.

Висновки та перспективи розвитку і подальших досліджень. Розглянуті вище системи онлайн навчання не становлять завершеного списку LMS. Умови постковідної реальності і зміни, що відбуваються в ході 4-ої Індустріальної революції рухають вперед технологічні процеси в усіх галузях, в тому числі і освітній. Це призведе і вже призводить до появи нових підходів в ідеології онлайн навчання і створення архітектури LMS на інших принципах, як наприклад використана технологія «едьютейнмент» на Онлайн платформі з цифрової грамотності. В свою чергу наші вітчизняні LMS мають потенціал развиватися для забезпечення можливості електронного онлайн навчання з повноцінним процесом сертифікації на рівні факультетів вишів.

Висновки і рекомендації. Тут перераховано лише деякі переваги онлайн-навчання. Ці переваги доводять, що онлайн-навчання, безумовно, має потенціал для революції в галузі освіти і, безумовно, може зробити навчання більш ефективним, привабливим та дружнім до студентів.

Цілком прийнятним і корисним може бути використання МООС онлайн курсів та LMS для навчання викладачів та аспірантів, підготовки магістерських дипломних робіт, включення їх до основної програми для більш поглибленого вивчення предметів та вузьких спеціалізацій, а також для використання в школі разом з електронними підручниками..

Доцільним видається використання гібридних навчальних курсів. При гібридному підході, коли лекційний матеріал може бути наданий студентам протягом тижня в онлайн режимі, з використанням можливостей LMS тому числі, а кілька днів на тиждень проводяться заняття віч-на-віч в аудиторіях. Таким чином можна компенсувати недоліки і виконувати заплановані по програмі практичні і лабораторні завдання.

Проблема переходу на електронне онлайн навчання в сфері освіти є своєчасною і потребує нагального її конструктивного вирішення. Оскільки:

по-перше, це диктується умовами постковідного світу і тенденціями розвитку світової освіти;

по-друге, в Україні ще не створено і не затверджено стандарти, що регламентували б навчальні процеси і правила роботи з онлайн навчальними системами і інструментами, підготовки, оцінювання та затвердження контенту курсів хоч би для шкільних програм;

по-третє, практично неможливо ефективно вирішувати цю проблему без наявності достатніх ресурсів інфраструктурного характеру (надійний доступ до інтернету у всіх локаціях навчальних закладів, шкіл), підготовки викладачів до роботи з новими технологіями і інструментами.

Крім того відсутня система підготовки програмного забезпечення і наповнення контенту онлайн систем за усіма дисциплінами в школі – тобто створення LMS курсів для галузей і спеціальностей освітньої сфери. Наявні сьогодні українські онлайн навчальні ресурси розроблені спільно з підрозділами Міністерства освіти і науки та волонтерами громадських організацій, потребують розвитку для підтримки самих курсів, так і підготовки вчителів та викладачів з орієнтацією на онлайн-навчальні системи.

Список використаних джерел:

1. Про MOOCs. URL: www.mooc.org.
2. Танмой Рей, Парініта Гупта (2019). Кращі платформи MOOC та онлайн-навчання.
3. Пітер Беркінг (2016). Вибір LMS. URL: https://www.stoodnt.com/blog/best-mooc-online-learning-platforms.
4. Система управління навчанням. URL: https://en.wikipedia.org/wiki/Learning_management_system.
5. Інтернет-коледж NKI: огляд 15-річної доставки 10 000 онлайн-курсів». URL: https://www.irrodl.org/index.php/irrodl/article/view/17/354.
6. Лонг Філіп Д. Системи управління навчанням (LMS). *Енциклопедія розподіленого навчання. Тисяча дубів: Публікації SAGE, Inc*. 2004. С. 291–293.
7. Шоненбоум Дж. Використовуючи адаптовану модель прийняття технологій на рівні завдань, щоб пояснити, чому викладачі вищої освіти мають намір використовувати деякі інструменти системи управління навчанням більше, ніж інші. *Комп'ютери та освіта*. 2014. № 71. С. 247–256.
8. Курси edX. URL: https://www.edx.org/search?tab=course&utm_campaign=mooc-cta& utm_medium=referral&utm_source=mooc.org.
9. Відкритий університет. URL: http://www.open.ac.uk.
10. Магдалена Яра, Гарві Меллар. Підвищення якості електронних навчальних курсів: роль зворотного зв'язку з студентом. С. 709–714.
11. Роберт Т. Рааб, В. Він Елліс, Буенафе Р. Абдон. Освіта «Мультисекторальні партнерства в електронному навчанні: потенційна сила для поліпшення розвитку людського капіталу в Азіатсько-Тихоокеанському регіоні». *Інтернет і вища освіта*. С. 217–229.

References:

1. About MOOCs. Retrieved from: www.mooc.org
2. Tanmoy, Ray, Parinita, Gupta (2019). Best MOOC and Online Learning Platforms.
3. Peter, Berking (2016). Choosing an LMS. Retrieved from: https://www.stoodnt.com/blog/best-mooc-online-learning-platforms.
4. Learning management system. Retrieved from: https://en.wikipedia.org/wiki/Learning_management_system.
5. The NKI Internet College: A review of 15 years delivery of 10,000 online courses. Retrieved from: https://www.irrodl.org/index.php/irrodl/article/view/17/354.
6. Long, Phillip D. (2004). Learning Management Systems (LMS). *Encyclopedia of Distributed Learning. Thousand Oaks: SAGE Publications, Inc*. P. 291–293.
7. Schoonenboom, Judith (February 2014). Using an adapted, task-level technology acceptance model to explain why instructors in higher education intend to use some learning management system tools more than others. *Computers & Education*, 71. P. 247–256.
8. Courses edX. Retrieved from: https://www.edx.org/search?tab=course&utm_campaign=mooc-cta&utm_medium=referral&utm_source=mooc.org;
9. The Open University. Retrieved from: http://www.open.ac.uk.
10. Magdalena Jara, Harvey Mellar. Quality enhancement for e-learning courses: The role of student feedback. P. 709–714.
11. Robert T. Raab, W. Wyn Ellis, Buenafe R. Abdon. Education «Multisectoral partnerships in e-learning: A potential force for improved human capital development in the Asia Pacific» *The Internet and Higher Education*. P. 217–229.

УДК 004.9
DOI https://doi.org/10.32689/maup.it.2021.1.2

Андрій ДУДНІК
кандидат технічних наук, доцент, доцент кафедри мережевих та інтернет технологій, Київський національний університет імені Тараса Шевченка, вул. Володимирська, 60, м. Київ, Україна, індекс 01033

ORCID: https://orcid.org/0000-0001-5725-5942

Юрій БОНДАРЕНКО
аспірант кафедри комп'ютерних мультимедійних технологій, Національний авіаційний університет, просп. Гузара Любомира, 1, м. Київ, Україна, індекс 03058

ORCID: https://orcid.org/0000-0003-2681-5526

Andrey DUDNIK
Candidate of Technical Sciences, Associate Professor, Associate Professor at the Department of Network and Internet Technologies, Taras Shevchenko National University of Kyiv, 60 Volodymyrska Street, Kyiv, Ukraine, postal code 01601

Yuriy BONDARENKO
Post-Graduate Student at the department of Computer Multimedia Technologies, National Aviation University, 1 Husar Lubomyr Avenue, Kyiv, Ukraine, postal code 03058

Бібліографічний опис статті: Дуднік А., Бондаренко Ю. Оцінка рівня сигналу безпровідних комп'ютеризованих систем вимірювання механічних величин при сталій відстані у середовищі вогню. *Інформаційні технології та суспільство*. 2021. Вип. 1. С. 19–22. DOI: https://doi.org/10.32689/maup.it.2021.1.2

Bibliographic description of the article: Dudnik, A. & Bondarenko, Yu. (2021). Otsinka rivnia syhnalu bezprovidnykh komp'iuteryzovanykh system vymiriuvannia mekhanichnykh velychyn pry stalii vidstani u seredovyshchi vohniu [Evaluation of wireless signal computerized systems of measurement of mechanical quantities at constant distance in medium fire]. *Informatsiini tekhnolohii ta suspilstvo – Informati on technology and society*, 1, 19–22. DOI: https://doi.org/10.32689/maup.it.2021.1.2

ОЦІНКА РІВНЯ СИГНАЛУ БЕЗПРОВІДНИХ КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ВИМІРЮВАННЯ МЕХАНІЧНИХ ВЕЛИЧИН ПРИ СТАЛІЙ ВІДСТАНІ У СЕРЕДОВИЩІ ВОГНЮ

Анотація. *Інтерес до дослідження поширення електромагнітних хвиль в лісових масивах традиційно залишається великий, особливо в останні роки. Значну актуальність такі дослідження набули з розвитком технології передачі сигналу стандарту IEEE802.11, що працює на частоті 2,4 і 5 ГГц. Це пов'язано з тим, що лісові пожежі завдають колосальних екологічні та економічні втрати в усьому світі і, зокрема, в Україні.*

Розглядаються питання оцінки потужності і якості передачі радіохвиль стандарту IEEE 802.11 в частотному діапазоні 2,4 ГГц в нормальних умовах поширення, а також в умовах розсіювання і поглинання при безпосередньому проходженні радіохвиль через лісовий масив. Показано вплив полум'я на потужність радіосигналу. Складено графіки залежностей потужності радіосигналу з урахуванням перешкод.

Ключові слова: *вогонь, задимленість, безпровідна мережа, відстань, рівень сигналу, якість сигналу.*

EVALUATION OF WIRELESS SIGNAL COMPUTERIZED SYSTEMS OF MEASUREMENT OF MECHANICAL QUANTITIES AT CONSTANT DISTANCE IN MEDIUM FIRE

Abstract. *Interest in the study of the propagation of electromagnetic waves in forest massifs has traditionally remained great, especially in recent years. Significant relevance of such studies acquired with the development of technology for the transmission of a radio signal standard IEEE802.11, operating at a frequency of 2.4 and 5 GHz. This is due to the fact that forest fires cause colossal environmental and economic losses throughout the world and, in particular, in Ukraine.*

The questions of estimation of power and quality of transmission of radio waves of the standard IEEE 802.11 in the frequency range of 2.4 GHz under normal propagation conditions, as well as in the conditions of scattering and absorption in the direct passage of radio waves through the forest array are considered. The influence of a flame on the power of a radio signal is shown. Charts of dependencies of radio signal strength are made taking into account obstacles.

Key words: *fire, smoke, wireless network, distance, signal level, signal quality.*

Постановка задачі. В 1993 и 1998 роках в Ялтинському горно-лісному природному заповіднику виникли великі пожежі з знищенням лісу площею 459 і 107 га відповідно [1]. В 2012 році на території України на протязі пожежонебезпечного періоду з квітня по жовтень 1990 року відбулися лісові пожежі на загальну площу 3500 га, а в 2013 році – 806 лісових пожеж на площі 220 га [2]. Застосування IEEE 802.11 дає можливість швидкої передачі інформації в реальному режимі часі таких, як відео, фото, біометричні дані співробітників аварійно-відновлення підрозділів, їх розташування в зоні ліквідації надзвичайної ситуації. Суттєвий вплив на умови поширення радіохвиль і на роботу всього радіозв'язку в лісі в цілому має рослинність і грунтоволокнисті настили. Радіохвилі, проходячи через лісові масиви, мають властивість розсіюватися і поглинатися. Так, як при цьому рівень випромінювання зменшується, то даний спосіб розповсюдження ефективний на невеликих дистанціях. Дослідження ослаблення радіохвиль лісовими покровами є предметом інтенсивного вивчення спеціалістів з різних країн. Ці дослідження допоможуть проаналізувати вплив лісу на якість радіозв'язку в цілому, що впливає на визначення відстані між об'єктами в лісі.

Аналіз останніх досліджень і публікацій. Аналіз літературних джерел показує, що поширенням радіохвиль в лісовому масиві займалися велика кількість провідних вчених. Перші дослідження в області поширення радіохвиль в лісовому масиві проводилися в сорокових роках двадцятого століття, при цьому було відмічено, що рівень сигналу на відкритій місцевості більше, ніж в лісі [3]. У сучасному світі, в роботі [4] були представлені результати експериментальних досліджень впливу видових і структурних властивостей лісової рослинності на особливості поширення в ній електромагнітних хвиль в метровому діапазоні.

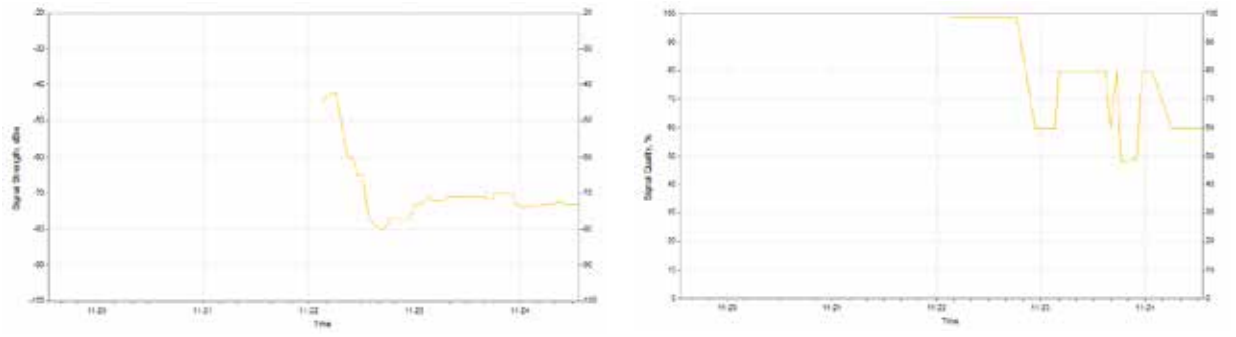
У науковій статті [5] описуються результати експериментів, які показують істотну відмінність у зміні спектрів імпульсних сигналів при поширенні в різних типах лісової рослинності.

У статті [6] показані експериментальні дані по ослабленню потужності радіохвиль кронами окремих дерев, а також залежно погонного ослаблення на вертикальній і горизонтальній поляризаціях для хвойних і листяних дерев в діапазоні частот 0,476 – 2,4 ГГц.

В роботі [7] проведено огляд електродинамічних моделей і методів аналізу поширення радіохвиль в лісових масивах при різних частотах і відстанях. В [8] наведені дані по ослабленню потужності радіохвиль при імітації лісової пожежі в лабораторних умовах, при цьому на полум'я пальника сипали солі металів, емітуючи цим горіння листя в лісі, яке містить луги.

Основний матеріал. Експеримент проводився на лісовій галявині на відстані між пристроями 5715 мм. Використовувались радіохвилі стандарту IEEE 802.11 в частотному діапазоні 2,4 ГГц.

На початку дослідження були отримані дані параметрів радіопередачі без застосування полум'я, що зображені на рис. 1 а та б.

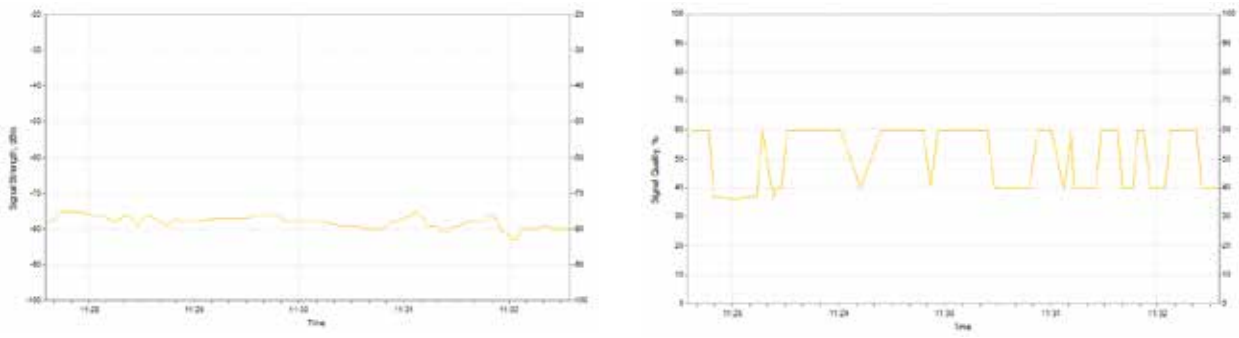


а) б)

Рис 1. Параметри передачі безпровідної мережі до використання полум'я: а) рівень сигналу, б) якість сигналу

З графіків видно, що у середньому рівень сигналу складає -73 dBm, а якість – 60%.

Далі були отримані дані на початку горіння вогнища, що було розпалене між пристроями, що зображені на рис. 2 а та б.

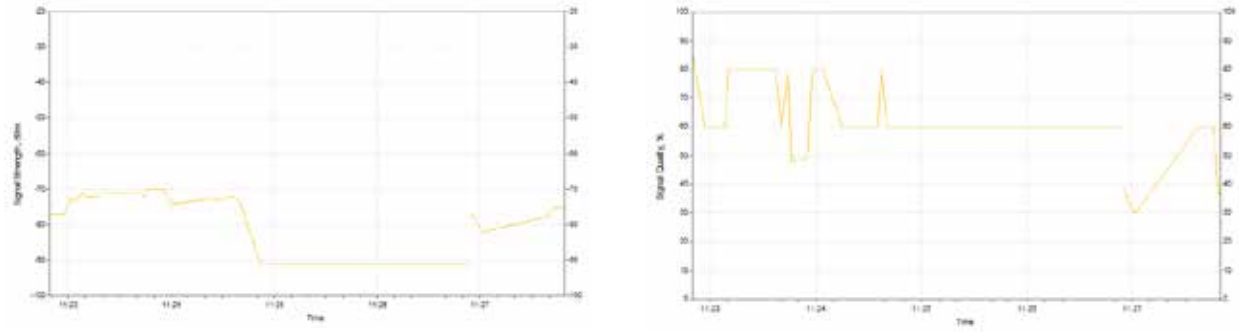


а) б)

Рис 2. Параметри передачі безпровідної мережі на початку горіння вогнища: а) рівень сигналу, б) якість сигналу

З графіків видно, що у середньому рівень сигналу складає -80 dBm, а якість – 40%.

Далі були отримані дані на стадії задимлення вогнища, що було розпалене між пристроями, що зображені на рис. 3 а та б.



а) б)

Рис 3. Параметри передачі безпровідної мережі на стадії задимлення вогнища: а) рівень сигналу, б) якість сигналу

З графіків видно, що у середньому рівень сигналу складає -75 dBm, а якість – 37%.

Висновки та рекомендації. З проведених досліджень видно, що виникнення пожежі може суттєво вплинути на параметри передачі сигналу у лісовій місцевості, адже найкращі показники сигналу були зафіксовані до розпалювання вогнища.

У подальших дослідженнях будуть детально проаналізовані дані цього дослідження. Будуть вирахувані показники похибок, які вносить полум'я у процес вимірювання відстані між об'єктами. Також будуть проаналізовані графічні характеристики не тільки рівня і якості сигналу, але і інших його параметрів.

Список використаних джерел:

1. Охрана лесов от пожаров: Официальный сайт Государственного комитета по лесному и охотничьему хозяйству АР Крым. URL: http://rescomles.nnmgr.net/rus/index.php?v=5&tek=16par=5.

2. Національна доповідь про стан техногенної та природної безпеки в Україні у 2013 році. Київ : УНДІЦЗ, 2014. 542 с.

3. Доржиев Б.Ч. Электродинамические свойства лесных сред в диапазоне ультракоротких волн : автореф. дис. ... канд. физ.-мат. наук : 01.04.03 «Радиофизика». Т., 1993. 19 с.

4. Басанов Б.В., Ветлужский А.Ю., Калашников В.П. Метод определения эффективной диэлектрической проницаемости лесного полога. *Радиоэлектроника.* 2010. № 4.

5. Ветлужский А.Ю., Калашников В.П. Широкополосное радиопросвечивание растительных покровов лесной поверхности. *Вестник СибГАУ*. 2013. № 5. С. 126–128.

6. Гранков А.Г., Дьяконова О.А., Мильшин А.А., Чухланцев А.А., Язерян Ж.Г. Экспериментальные спектральные зависимости погонного ослабления радиоволн деревьями в ДМ диапазоне. *Труды LVIX научной сессии, посвящ. Дню радио*, т. 1 (Москва,19-20 мая 2004 г.) Москва : РНТО РЭиС им. А.С. Попова, 2004. С. 149–151.

7. Пермяков В.А. Электродинамические модели распространения радиоволн в лесу. II Всероссийские Армандовские. *Радиофизические методы в дистанционном зондировании Сред. Матер. V Всерос. научной конф.* (Муром, 26-28 июня 2012 г.). Муром : МИ ВлГУ, 2012. С. 264–270. URL: http://www.mivlgu.ru/conf/armand2012/pdf/S2_17.pdf.

8. Dissanayake C.M. Dept. of Civil & Environ. Eng., Univ. of Melbourne, Parkville, VIC, Australia. The signal propagation effects on IEEE 802.15.4 radio link in fire environment. C.M. Dissanayake, M.N. Halgamuge, K. Ramamohanarao, B. Moran, P. Farrell. Information and Automation for Sustainability (ICIAFs), 2010 5th International Conference on. Date 17–19 Dec. 2010. Colombo, Sri-Lanka. P. 411–414.

References:

1. Okhrana lesov ot pozharov: Ofitsial'nyy sayt Gosudarstvennogo komiteta po lesnomu i okhotnich'emu khozyaystvu AR Krym [Protection of forests from fires: Official site of the State Committee for Forestry and Hunting of the Autonomous Republic of Crimea]. Retrieved from: http://rescomles.nnmgr.net/rus/index.php?v=5&tek= 16par=5 [in Russian].

2. Natsionalna dopovid pro stan tekhnohennoi ta pryrodnoi bezpeky v Ukraini u 2013 rotsi [National report on the state of man-made and natural security in Ukraine in 2013] (2014). Kyiv: UNDICZ, 542 p. [in Ukrainian].

3. Dorzhiev, B.Ch. (1993). Elektrodinamicheskie svoystva lesnykh sred v diapazone ul'trakorotkikh voln [Electrodynamic properties of forest media in the range of ultrashort waves]. *Extended abstract of candidate's thesis,* 19 p. [in Russian].

4. Basanov, B.V., Vetluzhskiy, A.Yu., Kalashnikov, V.P. (2010). Metod opredeleniya effektivnoy dielektricheskoy pronitsaemosti lesnogo pologa. Method for determining the effective dielectric constant of the forest canopy. *Radioelektronika – Radioelectronics.* № 4. [in Russian].

5. Vetluzhskiy, A.Yu., Kalashnikov, V.P. (2013). Shirokopolosnoe radioprosvechivanie rastitel'nykh pokrovov lesnoy poverkhnosti. [Broadband radio scanning of forest surface vegetation]. *Vestnik Sibirskogo gosudarstvennogo aerokosmicheskogo universiteta – Bulletin of the Siberian State Aerospace University.* № 5. P. 126–128 [in Russian].

6. Grankov, A.G., D'yakonova, O.A., Mil'shin, A.A., Chukhlantsev, A.A., Yazeryan, Zh.G. (2004). Eksperimental'nye spektral'nye zavisimosti pogonnogo oslableniya radiovoln derev'yami v DM diapazone [Experimental spectral dependences of the linear attenuation of radio waves by trees in the DM range]. *Proceedings of the LVIX Scientific Session, dedicated to Radio Day.* (Moscow, May 19-20, 2004). Moscow. P. 149–151 [in Russian].

7. Permyakov, V.A. (2012). Elektrodinamicheskie modeli rasprostraneniya radiovoln v lesu. II Vserossiyskie Armandovskie. Radiofizicheskie metody v distantsionnom zondirovanii sred [Electrodynamic models of radio wave propagation in the forest. II All-Russian Armandovsky. Radiophysical methods in remote sensing of media]. *Materials of the V All-Russian Scientific Conference* (Murom, June 26–28, 2012). Murom. P. 264–270. Retrieved from: http://www.mivlgu.ru/conf/armand2012/pdf/S2_17.pdf [in Russian].

8. Dissanayake C.M. Dept. of Civil & Environ. Eng., Univ. of Melbourne, Parkville, VIC, Australia. The signal propagation effects on IEEE 802.15.4 radio link in fire environment. C.M. Dissanayake, M.N. Halgamuge, K. Ramamohanarao, B. Moran, P. Farrell. Information and Automation for Sustainability (ICIAFs), 2010 5th International Conference on. Date 17–19 Dec. 2010. Colombo, Sri-Lanka. P. 411–414. [in English].

УДК 519.6:504.064
DOI https://doi.org/10.32689/maup.it.2021.1.3

Олександр ПОПОВ
доктор технічних наук, старший науковий співробітник, член-кореспондент НАН України, заступник директора з науково-організаційної роботи, Державна установа «Інститут геохімії навколишнього середовища Національної академії наук України», просп. Академіка Палладіна, 34а, м. Київ, Україна, 03142; професор кафедри комп'ютерних інформаційних систем і технологій, Міжрегіональна Академія Управління персоналом, вул. Фрометівська, 2, м. Київ, Україна, індекс 03039 (sasha.popov1982@gmail.com)

ORCID: https://orcid.org/0000-0002-5065-3822

Андрій ЯЦИШИН
доктор технічних наук, старший науковий співробітник, провідний науковий співробітник відділу цивільного захисту та інноваційної діяльності, Державна установа «Інститут геохімії навколишнього середовища Національної академії наук України», просп. Академіка Палладіна, 34а, м. Київ, Україна, індекс 03142 (iatsyshyn.andriy@gmail.com)

ORCID: https://orcid.org/0000-0001-5508-7017

Володимир АРТЕМЧУК
кандидат технічних наук, старший науковий співробітник, старший науковий співробітник відділу математичного і економетричного моделювання, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, вул. Генерала Наумова, 15, м. Київ, Україна, індекс 03164 (ak24avo@gmail.com)

ORCID: https://orcid.org/0000-0001-8819-4564

Валентина КОВАЛЕНКО
кандидат педагогічних наук, старший науковий співробітник відділу технологій захисту довкілля та радіаційної безпеки, Державна установа «Інститут геохімії навколишнього середовища Національної академії наук України», просп. Академіка Палладіна, 34а, м. Київ, Україна, індекс 03142 (vako88@ukr.net)

ORCID: https://orcid.org/0000-0002-4681-5606

Oleksandr POPOV
Corresponding Member of NAS of Ukraine, Doctor of Technical Sciences, Senior researcher, Deputy Director for Research and Organizational Work, State Institution "The Institute of Environmental Geochemistry of National Academy of Sciences of Ukraine", 34a Palladin Ave., Kyiv, Ukraine, postal code 03142; Professor at the Department of Computer Information Systems and Technologies, Interregional Academy of Personnel Management, 2 Frometivska Str., Kyiv, Ukraine, postal code 03039 (sasha.popov1982@gmail.com)

Andrii IATSYSHYN
Doctor of Technical Sciences, Senior researcher, Leading Researcher of the Department of Civil Protection and Innovation, State Institution "The Institute of Environmental Geochemistry of National Academy of Sciences of Ukraine", 34a Palladin Ave., Kyiv, Ukraine, postal code 03142 (iatsyshyn.andriy@gmail.com)

Volodymyr ARTEMCHUK
Candidate of Technical Sciences, Senior researcher, Senior researcher of the Department of Mathematical and Econometric Modeling, G.E. Pukhov Institute for Modelling in Energy Engineering of NAS of Ukraine, 15 General Naumova Str., Kyiv, Ukraine, postal code 03164 (ak24avo@gmail.com)

Valentyna KOVALENKO
Candidate of Pedagogical Sciences, Senior researcher of the Department of environmental protection technologies and radiation safety, State Institution "The Institute of Environmental Geochemistry of National Academy of Sciences of Ukraine", 34a Palladin Ave., Kyiv, Ukraine, postal code 03142 (vako88@ukr.net)

Бібліографічний опис статті: Попов О., Яцишин А., Артемчук В., Коваленко В. Нові підходи та геоінформаційні засоби вирішення екологічних задач техногенно-навантажених територій. *Інформаційні технології та суспільство*. 2021. Вип. 1. С. 23–33. DOI: https://doi.org/10.32689/maup.it.2021.1.3

Bibliographic description of the article: Popov, O., Iatsyshyn, A., Artemchuk, V. & Kovalenko, V. (2021). Novi pidkhody ta heoinformatsiini zasoby vyrishennia ekolohichnykh zadach tekhnohenno-navantazhenykh terytorii [New approaches and geoinformation means to solve ecological problems of technogenically loaded territories]. *Informatsiini tekhnolohii ta suspilstvo – Information technology and society*, 1, 23–33. DOI: https://doi.org/10.32689/maup.it.2021.1.3

НОВІ ПІДХОДИ ТА ГЕОІНФОРМАЦІЙНІ ЗАСОБИ ВИРІШЕННЯ ЕКОЛОГІЧНИХ ЗАДАЧ ТЕХНОГЕННО-НАВАНТАЖЕНИХ ТЕРИТОРІЙ

Анотація. *Для виконання зобов'язань України перед світовою спільнотою стосовно запобігання зміни клімату необхідно дотримуватися підписаних документів щодо розвитку відновлювальної енергетики, модернізації підприємств паливно-енергетичного сектору, поводження з різними відходами та ін. Тому актуальним є розробка програмного забезпечення, що дозволяє вирішувати задачі візуального аналізу динаміки екологічного стану територіальних систем та визначення меж стійкості окремих територій. Важливим є також підвищення кваліфікації фахівців, зокрема працівників міністерств, підприємств та організацій, які відповідають за прийняття рішень щодо зменшення негативного впливу на довкілля та підготовка майбутніх фахівців у цьому напрямі.* ***Метою*** *статті є дослідження особливостей застосування програмних засобів для задач стійкого розвитку та окреслення напрямів підвищення кваліфікації фахівців відповідальних за прийняття управлінських рішень в енергетичній, екологічній та суміжних галузях.* ***Наукова новизна.*** *Авторами обґрунтовано структурний підхід до оцінювання екологічного стану техногенно-навантажених територій та запропоновано нові форми представлення даних моніторингу техногенних навантажень та ризиків, що відображують динаміку екологічної ситуації в просторі інформативних ознак. Як* ***висновок****, у статті наголошується, що важливим є впровадження програмних засобів для підтримки прийняття управлінських рішень у процес підвищення кваліфікації фахівців в енергетичній, екологічній та суміжних галузях. Це відповідає сучасним світовим вимогам до підготовки фахівців нової технологічної ери та сприятиме реалізації концепції сталого розвитку суспільства. Опанувавши такі програмні засоби фахівці зможуть: визначати та ідентифікувати раніше невідомі взаємозв'язки між екологічними параметрами і факторами впливу; визначати й прогнозувати приховані тенденції і закономірності розвитку екологічних процесів (виявляти та розпізнавати приховані чинники впливу, в тому числі, фактори загрози; систематизувати та інтегрувати дані про стан навколишнього природного середовища; розробляти оптимізаційні рекомендації в енергетичній, екологічній та суміжних галузях; візуалізувати результати аналізу, здійснювати підготовку попередніх звітів і проектів допустимих рішень та ін.*

Ключові слова: *стійкий розвиток, атмосферне повітря, геоінформаційні системи, екологічні ризики, підготовка фахівців.*

NEW APPROACHES AND GEOINFORMATION MEANS TO SOLVE ECOLOGICAL PROBLEMS OF TECHNOGENICALLY LOADED TERRITORIES

Abstract. *In order to fulfill Ukraine's commitments to the world community on climate change prevention, it is necessary to adhere to the signed documents on the development of renewable energy, modernization of enterprises in the fuel and energy sector, various waste management strategies etc. Therefore, it is important to develop software that allows solving problems of visual analysis of the dynamics of the ecological condition of territorial systems and determining the limits of stability of individual territories. It is also important to improve the skills of specialists, in particular employees of ministries, enterprises and organizations responsible for making decisions to reduce the negative impact on the environment and training future professionals in this area.* ***The aim*** *of the article is to study the peculiarities of the use of software for sustainable development and to outline areas for professional development of specialists responsible for decision making process in energy, environmental and related fields.* ***Scientific novelty.*** *The authors substantiate the structural approach to assessing the ecological condition of technogenic areas and propose new forms of presentation of monitoring data on technogenic loads and risks, reflecting the dynamics of the ecological situation in the time of informative features.* ***In conclusion,*** *the article emphasizes that it is important to implement software tools to support management decisions in the process of professional development in energy, environmental and related fields. This meets modern world requirements for the training of specialists of the new technological era and will contribute to the implementation of the concept of society sustainable development. Having mastered such software, specialists will be able to: identify previously unknown relationships between environmental parameters and impact factors; identify and predict hidden trends and patterns of environmental processes (including threat factors; systematize and integrate data on the state of the environment; develop optimization recommendations in energy, environmental and related fields; visualize the results of analysis, and to prepare preliminary reports and drafts of management decisions etc.*

Key words: *sustainable development, atmospheric air, geographic information systems, ecological risks, training.*

Актуальність проблеми. У доповіді [1] передбачено визначення сталого розвитку як «розвитку, який відповідає потребам сучасності без шкоди для майбутніх поколінь для задоволення власних потреб». З екологічної точки зору стійкий розвиток має забезпечити цілісність і життєздатність природних систем, можливості самовідновлення та адаптації до змін. Зокрема, дослідження взаємозв'язків між природоохоронною та економічною складовими процесів стійкого розвитку потребує уточнення

граничних рівнів техногенних навантажень на довкілля та визначення меж стійкості урбанізованих територіальних систем до техногенного впливу.

На даному етапі підходи до дослідження стійкого розвитку можна розділити на два напрями. Перший напрям домінує на глобальному та регіональному рівні (погляд «згори», тобто порівняльний аналіз ситуації в різних країнах або регіонах). Це дослідження, що спрямовані на обчислення індикаторів та індексів сталого розвитку за методиками, запропонованими Комісією ООН та міжнародними радами [2; 3]. До другого напряму слід віднести роботи, спрямовані на дослідження стійкості окремих процесів, що відбуваються в конкретних екологічних або соціальних системах [4, с. 119–132; 5, с. 2554–2560]. Адже лише на конкретних прикладах аналізу динаміки окремих систем можна виявити залежність траєкторії розвитку (або переходу до критичного стану) даної системи від значень тих або інших параметрів.

Для практичної реалізації принципів сталого розвитку в Україні особливої уваги потребує розвиток та модернізація системи моніторингу екологічного стану територіальних систем різного рівня, створення універсального інформаційно-програмного забезпечення задач моніторингу, удосконалення засобів прогнозування критичних ситуацій та прийняття управлінських рішень. Серед найбільш пріоритетних задач – розробка сучасних інформаційних та комп'ютерних технологій, орієнтованих на збереження, накопичення, систематизацію та інтеграцію інформації, одержаної з різних джерел, включаючи локальний рівень аналізу даних та можливості візуальної інтерпретації на основі ГІС-технологій. Про це свідчить прийнята концепція [6], реалізація якої має забезпечити дотримання міжнародних зобов'язань України у сфері охорони навколишнього природного середовища, зокрема раціонального використання, відтворення і охорони природних ресурсів.

Тому, важливими для дослідження вважаємо два аспекти: удосконалення системи моніторингу для задач прогнозування та управління екологічною безпекою на основі інформаційних технологій; підвищення кваліфікації фахівців в енергетичній, екологічній та суміжних галузях, які відповідають за прийняття рішень щодо зменшення негативного впливу на довкілля.

Аналіз останніх досліджень і публікацій. Найбільше публікацій присвячених проблематиці сталого розвитку мають наступні вчені: М. Згуровський, P. Priyadarshini, H. Fredrickson, L. Zhao, S. González-García, J. Baleta, M.-H. Yuan, S.-L. Lo, A. Dawodu, A. Cheshmehzangi та інші.

На основі аналізу праць зарубіжних і вітчизняних вчених було зроблено систематизацію наукових публікацій за такими напрямами, що безпосередньо стосуються даного дослідження:

– підходи до забезпечення сталого розвитку [4, с. 119–1325, с. 2554–2560; 7, с. 1083–1095; 8, с. 27–42; 9, с. 1424–1436; 10];

– розробка показників, індикаторів, індексів для вимірювання сталого розвитку [2; 11; 12];

– побудова математичних, програмних та апаратних засобів для оцінювання впливу потенційно небезпечних підприємств на довкілля з врахуванням економічних показників [13; 14; 15, с. 98–114; 16, с. 13–24];

– підвищення кваліфікації фахівців в галузі екологічної безпеки та суміжних галузях [17; 18, с. 1349–1360].

Проте, подальшого дослідження потребують питання щодо комплексних і прогнозних оцінок екологічної ситуації техногенно-навантажених територій в контексті сталого розвитку та підвищення кваліфікації фахівців, що працюють в енергетичній, екологічній та суміжних галузях.

Метою статті є дослідження особливостей застосування програмних засобів для задач стійкого розвитку та окреслення напрямів підвищення кваліфікації фахівців відповідальних за прийняття управлінських рішень в енергетичній, екологічній та суміжних галузях.

Результати дослідження.

Енергетика: від екологічної безпеки до сталого розвитку

Одним з критеріїв оцінювання екологічної безпеки певної екосистеми є якість життя і здоров'я населення, тому виникає необхідність цілеспрямованого впливу (управління) екологічною системою з ціллю забезпечення підвищення її організованості та досягнення певного корисного ефекту.

В дослідженні [7, с. 1083–1095] запропоновано моделі сталого розвитку для вимірювання ефективності системи, що складається з економічної, екологічної та соціальної підсистеми. Результат дослідження проілюстровано для 30 великих китайських міст та показано основні чинники, які впливають на їх економічну, екологічну та соціальну ефективність.

Щоб зберегти ресурси та гарантувати соціальні послуги та добробут громадян, необхідні здійснювати заходи щодо планування та політики, які сприяють досягненню сталого зростання. Крім екологічної перспективи, соціально-економічний аналіз має важливе значення для встановлення всебічної діагностики стійкості міських та сільських систем. У [8, с. 27–42] представлена методологія оцінки

стійкості, що базується на 38 показниках, які включають три основи стійкості: соціальну, економічну та екологічну. Дана методологія була апробована в багатьох муніципалітетах північно-західної Іспанії. Результати дослідження показали, що найбільш стійкі муніципалітети розташовані на півночі регіону, а розмір муніципалітетів є важливим для вимірювання стійкості. Автори публікації зазначають, що розроблена методологія є надійною і може застосовуватися до інших муніципалітетів та міст.

Для вирішення проблеми глобального потепління необхідно застосовувати спільні зусилля та міждисциплінарний підхід. Разом з ефективністю використання ресурсів, економіка замкнутого циклу стає в центрі уваги дослідників і, отже, політиків. Сталий розвиток є багатопрофільною темою, а взаємодія систем енергії, води та навколишнього природного середовища відіграє одну з центральних ролей. У парадигмі економіки замкнутого циклу зростає потреба в системній інтеграції, коли побічний продукт однієї системи може представляти ресурс для іншої. В роботі [9, с. 1424–1436] висвітлено питання щодо сталого розвитку систем енергетики, води та довкілля, та наголошено, що все більше зусиль потрібно прикладати для подальшої інтеграції цих систем. Це все призводить до підвищення складності такої проблеми, вирішення якої можливе тільки завдяки взаємодії багатьох науковців з різних галузей дослідження.

Інтеграція систем енергетики, води та навколишнього середовища є важливою в багатодисциплінарній концепції сталого розвитку, оскільки вони представляють основні життєві потреби людства. Тому проблеми, що виникають із концепції стійкого розвитку, потрібно ретельно вирішувати, щоб зберегти енергію, воду та ресурси довкілля для майбутніх поколінь. У роботі [10] розглядаються деякі останні події у цих основних сферах в рамках сталого розвитку.

Постановка задач моніторингу стійкого розвитку територій

Як відомо, екологічний моніторинг включає систему спостережень за чинниками, які впливають на навколишнє природне середовище, процес оцінювання фактичного стану природного середовища, прогнозні оцінки та певні можливості контролю й управління. Екологічні індикатори будемо розглядати як окремі показники, що мають істотний вплив на стан досліджуваних територій, а екологічні індекси – як комплексні показники, побудовані із врахуванням декількох індикаторів.

Для визначення індикаторів екологічного стану (інтегральних індексів) на основі даних моніторингу урбанізованих територій в роботі [14] обґрунтовано структурний підхід до оцінювання стану окремих територій, що розроблений для задач аналізу наслідків техногенного впливу. Для визначення індикаторів екологічного стану урбанізованих територій запропоновано три типи екологічних показників:

1) найбільш інформативні серед показників, зафіксованих в результаті вимірювання на постах спостереження за станом довкілля (концентрації найбільш небезпечних речовин);

2) багатовимірні індекси екологічного стану досліджуваних територій, побудовані за сукупністю виміряних показників;

3) оцінки екологічного ризику (імовірнісні розподіли, або поля ризику), розраховані на основі даних моніторингу.

На основі даних екологічного моніторингу досліджуваних територій визначаються узагальнені оцінки (індикатори) екологічного стану цих територій, за значеннями яких можна виявляти та передбачати критичні ситуації, досліджувати критичні чинники та найбільш чутливі до негативних факторів елементи природного середовища, тобто окремі території, водні екосистеми або групи ризику, які знаходяться в умовах підвищених техногенних навантажень.

До типових задач стійкого розвитку, які потребують застосування засобів та технологій просторового аналізу, можна віднести планування територій, будування та розміщення об'єктів виробничої інфраструктури, управління земельними й природними ресурсами, керування транспортними засобами, розвиток сільського господарства, моделювання наслідків аварій або надзвичайних ситуацій тощо.

Серед основних задач моніторингу, аналізу та оцінювання стійкого розвитку регіонів та окремих територій відзначимо виявлення просторової структури досліджуваних систем (розподіл техногенних навантажень, розподіл ризиків та захворювань, виявлення небезпечних зон); аналіз певних змін та визначення основних тенденцій за досліджуваний період (моніторинг динаміки техногенних навантажень); прогнозування можливих сценаріїв розвитку типових ситуацій (зокрема, оцінювання потенційного впливу небезпечних факторів та ефективності управлінських рішень).

Одна з пріоритетних задач оцінювання та моделювання процесів стійкого розвитку на територіальному рівні – це визначення меж стійкості досліджуваних територіальних систем, що перебувають під тиском досить високих техногенних навантажень.

В концепції стійкого розвитку природні межі стійкості визначають такий стан біосфери й суспільства, який дозволить зберегти нашу цивілізацію та основні природні ресурси для майбутніх поколінь.

Отже, необхідно визначити такі гранично допустимі рівні навантажень на окремі територіальні системи, для яких ще можна забезпечити стабільний стан.

Для уточнення поняття про стійкість динамічних систем нагадаємо визначення стійкості за Ляпуновим. Траєкторія динамічної системи може вважатись стійкою, якщо для скільки завгодно малих відхилень, що визначають межи стійкості цієї системи, можна вказати такі обмеження для можливих коливань, при яких система не вийде за визначені межі [19].

Наведемо основні етапи дослідження територіальних систем з метою визначення меж стійкості до впливу техногенних навантажень.

1. Просторовий аналіз даних моніторингу техногенного забруднення та виявлення зон підвищеного ризику. На попередніх етапах аналізу даних моніторингу необхідно визначити інформативні параметри (або екологічні індекси), які використовуються для ранжирування територій та побудови екологічних шкал.

2. Візуалізація результатів просторового аналізу у вигляді двовимірних семантичних шкал, тобто інформативних проекцій семантичного простору ризиків, які забезпечують оцінювання та ранжирування досліджених територій за індексами екологічного стану.

3. Візуальний аналіз динаміки техногенних навантажень за певний період часу в зонах підвищеного ризику (точках максимальної напруги) за допомогою шкал стійкості та візуальне визначення меж стійкості.

Засоби аналізу та результати

Для дослідження просторово-розподілених задач аналізу техногенного впливу на територіальні системи, авторами даної публікації розроблено аналітико-інформаційну систему моніторингу техногенних навантажень на довкілля, де передбачено можливості аналізу складних процесів та явищ, які відображують дані моніторингу окремих міст, регіонів або територіальних систем. Дане програмне забезпечення складається з декількох блоків, а саме: блок статистичного аналізу й попередньої оцінки техногенних навантажень на атмосферне повітря; блок математичного моделювання та прогнозування рівнів забруднення атмосфери і ризиків для населення; блок візуалізації та побудови екологічних карт [13].

Дана система може бути використана як допоміжний інструмент для інформаційної підтримки задач екологічного моніторингу, моніторингу забруднення від потенційно-небезпечних об'єктів, управління екологічною безпекою в умовах техногенного забруднення приземного шару атмосфери, що необхідні для підтримки прийняття рішень з питань забезпечення цивільного захисту населення і територій, що зазнають підсилені техногенні навантаження. Розроблені програмні засоби можуть оперативно забезпечувати місцеві органи управління та інші зацікавлені структури цінною інформацією, необхідною для прийняття найбільш ефективних рішень з урахуванням місцевих особливостей.

На рис. 1 показано структурну схему програмного забезпечення для управління екологічною безпекою урбанізованих територій, яка включає засоби моделювання та прогнозування техногенних навантажень на довкілля (зокрема, на атмосферне повітря) від стаціонарних джерел забруднення.

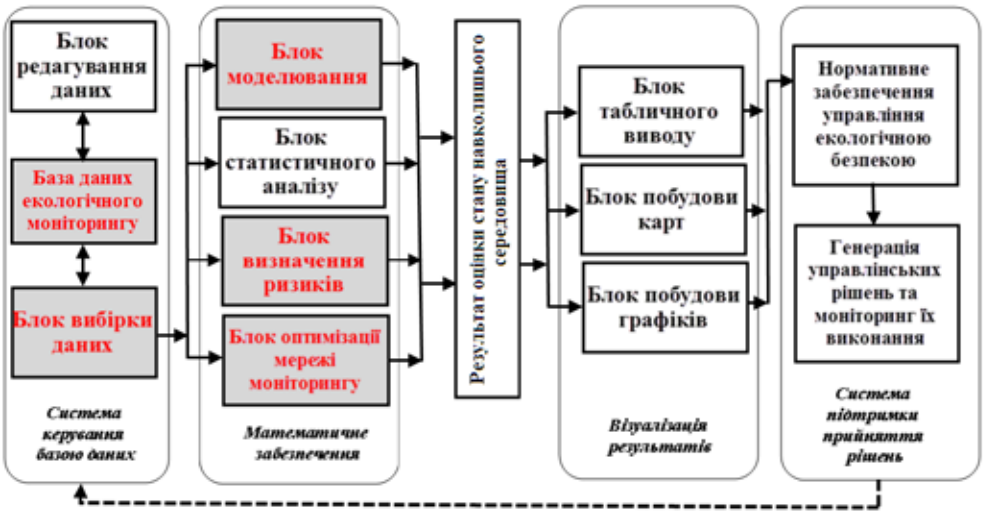


Рис. 1. Програмне забезпечення задач управління безпекою

Методичний аналіз процесів стійкого розвитку потребує визначення критеріїв стійкості досліджуваних територіальних систем, які необхідно знати для розрахунку обмежень на техногенні навантаження.

На локальному рівні задачу визначення таких критеріїв можна розглядати як обернену до задачі моніторингу техногенних навантажень, тобто задачу уточнення тих меж, порушення яких може привести до катастрофічних змін в досліджуваних системах.

Серед методичних засобів, спрямованих на визначення меж стійкості урбанізованих територій, особливої уваги потребує розвиток засобів візуального аналізу даних моніторингу та технологій побудови екологічних шкал, які забезпечують наочне відображення динаміки змін екологічного стану територіальної системи за досліджуваний період.

Далі розглянемо окремі можливості візуалізації досліджуваних процесів у графічному вигляді, реалізовані на основі комп'ютерних засобів візуального спостереження за процесом наближення до граничних умов із врахуванням даних моніторингу та нормативних даних щодо обмежень на гранично допустимі концентрації та ризики.

Запропоновані засоби аналізу динаміки змін екологічного стану та визначення меж стійкості урбанізованих територій до техногенного впливу апробовано на прикладі територіальної системи міста Києва. Дослідження проводилось з використанням даних моніторингу стану атмосферного повітря міста, одержаних від Центральної геофізичної обсерваторії імені Бориса Срезневського за період з 2005 до 2018 рр. [20].

На попередніх етапах аналізу для моніторингу динаміки техногенних навантажень на місто було визначено найбільш інформативні показники забруднення, які мають високий клас небезпеки, великий діапазон сезонних коливань та суттєво перевищують граничні норми, визначені діючим законодавством. Особливості динаміки техногенного впливу на приземний шар повітря досліджувались на прикладах таких небезпечних речовин – забруднювачів як формальдегід, діоксид азоту та оксид вуглецю.

На основі даних моніторингу було визначено значення ризиків для населення різних районів міста Києва. Значення ризиків хронічної інтоксикації (РХІ) та ризиків миттєвих токсичних ефектів (РМТЕ) розраховувались за формулами, що описані в роботі [21]. За цими даними можна відстежувати динаміку ризиків для здоров'я в окремих точках міста. Оцінки ризиків для населення за досліджуваний період наведені в табл. 1. На рис. 2 наведені приклади карт ризиків внаслідок забруднення повітря в м. Києві за січень – грудень 2017 р.

Згідно з наведеними даними, найбільші значення техногенних навантажень та ризиків за досліджуваний період спостерігались для району Бесарабської площі, який відзначено як зону підвищеного ризику (пункт спостережень № 7). Також підвищені значення ризиків протягом всього періоду спостережень було відзначено на пунктах спостереження за забрудненням атмосферного повітря (ПСЗ) інших центральних районів міста (на Майдані Незалежності, Площі Перемоги тощо).

Для моніторингу сезонної динаміки техногенних навантажень на окремі території та визначення найбільш небезпечних ситуацій розроблено спеціалізовані візуальні засоби відображення даних моніторингу щодо перевищень норм гранично допустимих концентрацій та відповідних значень ризиків.

Порівнюючи одержані авторами результати, можна сформулювати певну послідовність дослідження побудованих графічних образів та визначення найбільш небезпечних відхилень від стабільного стану.

Таблиця 1

Динаміка значень ризиків для здоров'я населення м. Києва

Рік / Місце	2005 р.		2008 р.		2011 р.		2017 р.	
	РХІ	РМТЕ	РХІ	РМТЕ	РХІ	РМТЕ	РХІ	РМТЕ
Гідропарк	0,085	0,137	0,063	0,140	0,068	0,025	0,077	0,026
Національний комплекс «Експоцентр Україна»	0,061	0,051	0,053	0,120	0,071	0,032	0,087	0,067
Деміївська площа	0,192	0,406	0,060	0,089	0,144	0,157	0,178	0,160
Площа Перемоги	0,170	0,458	0,136	0,298	0,210	0,306	0,219	0,226
Бессарабська площа	0,193	0,693	0,275	0,472	0,255	0,321	0,296	0,211
Майдан Незалежності	0,173	0,514	0,202	0,390	0,212	0,264	0,241	0,202
Дарницька площа	0,163	0,386	0,151	0,358	0,174	0,215	0,182	0,187

На першому етапі необхідно окреслити образ нормального стану, розташований ближче до початку координат, де перевищення граничних норм не досягає критичних значень. Потім можна виділити максимальні відхилення від норми, спрямовані в протилежному напрямку.

а)

б)

Рис. 2. Карта розподілу інтегральних ризиків РМТЕ (а) та РХІ (б) внаслідок забруднення повітря м. Києва за 2017 рік [13]

На рис. 3 відображено динаміку індексу забруднення атмосфери за період спостережень з 2015 по 2018 рр. на ПСЗ № 7 (район Бесарабської площі). Одержаний графік можна вважати найбільш змістовним відображенням результатів спостережень, що враховує дані по основним забруднювачам повітря за останні роки.

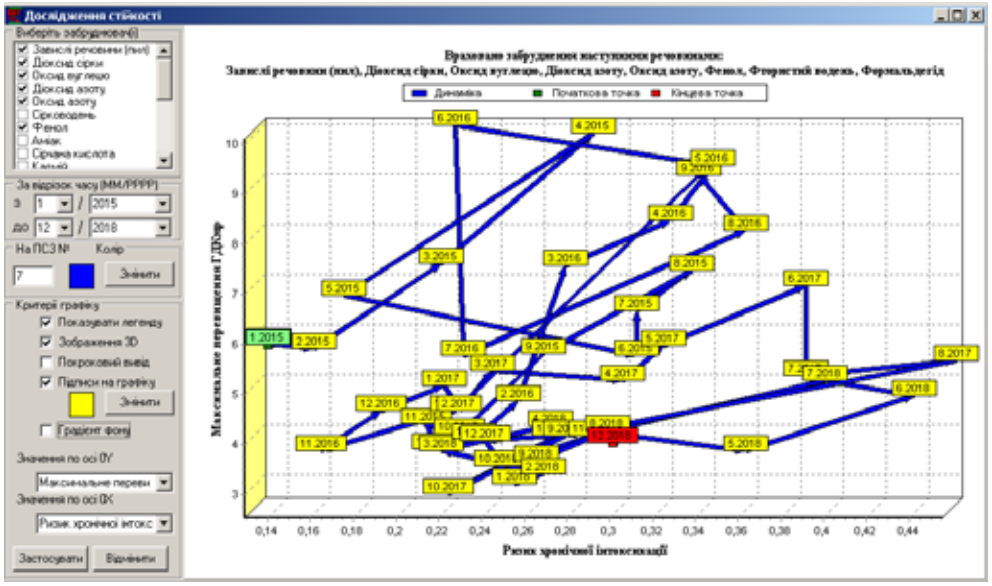


Рис. 3. Динаміка індексу забруднення атмосфери на ПСЗ № 7 (2015–2018) [14]

Значення, що відповідають нормі, сконцентрувались ближче до координатних осей, нижче п'ятикратного перевищення максимальних значень. Найбільш небезпечні ситуації утворюють зовнішній контур відносно інших значень, який починається з точки вгорі (6.2016) й обмежується максимальними ризиками, показаними в правій частині графіка.

Окремі спостереження (середньомісячні дані про забруднення) позначені прямокутниками, в яких показано місяць і рік спостереження. На графіку середньомісячні значення поєднані між собою у тій послідовності, в якій відбувалось проведення вимірювань.

За допомогою запропонованих програмних засобів моніторингу техногенних навантажень на окремі території можна візуально визначати найбільш небезпечні ситуації (або періоди максимального відхилення від норми), коли з високою імовірністю виникають локальні порушення стабільного стану, які характеризується суттєвим підвищенням захворюваності населення прилеглих територій.

Таким чином, для аналізу процесів сталого розвитку на локальному та регіональному рівнях, згідно з рекомендаціями, наданими в [3], індекси екологічного стану урбанізованих територій було розраховано на основі даних моніторингу м. Києва. Наразі модулі розробленого програмного забезпечення впроваджено в Департаменті організації заходів цивільного захисту ДСНС України, відокремленому підрозділі «Науково-технічний центр» державного підприємства «НАЕК «Енергоатом» (ДП «НАЕК «Енергоатом»), отримано рекомендації щодо застосування розроблених програмних засобів в роботі територіальних та міжрегіональних територіальних органах Державної екологічної інспекції України тощо.

Розроблені програмні засоби можуть забезпечити населення інформацією про стан навколишнього середовища, існуючі екологічні ризики/загрози для безпечної життєдіяльності, які представлені в електронному вигляді, що особливо важливо при створенні загальнодержавної автоматизованої інформаційно-аналітичної системи «Відкрите довкілля».

Отже, для визначення меж стійкості урбанізованих територій необхідно співвіднести оцінки, одержані в результаті аналізу реальних даних моніторингу та моделювання техногенних навантажень на окремі райони, з тими граничними умовами, які відповідають критеріям стійкості, затвердженим міжнародними та державними законодавчими актами.

Напрями застосування програмних засобів для підвищення кваліфікації фахівців в енергетичній, екологічній та суміжних галузях

Здійснивши аналіз пропозиції закладів вищої освіти України (Національний університет біоресурсів і природокористування України, Одеський державний екологічний університет, Державна екологічна академія післядипломної освіти та управління та ін.) станом на 2019 р., визначено, що ці заклади пропонують навчання за програмами додаткової професійної освіти коротко- та довгострокових курсів підвищення кваліфікації, в очній (з відривом від виробництва) і очно-заочній формах. Програми підвищення кваліфікації розроблені в галузі наук про Землю (спеціалізації метеорологія, агрометеорологія, гідрологія), екології та ін. Пропонуються курси підвищення кваліфікації за різними напряма-

ми і темами: оцінка стану та техногенного впливу автотранспортного комплексу на навколишнє середовище, охорона атмосферного повітря, проектування та експлуатація сучасних систем моніторингу навколишнього природного середовища, підвищення кваліфікації громадських інспекторів з охорони довкілля, основи геоінформаційних систем і технологій (практичний курс для користувачів) та інше. Запропоновані курси підвищення кваліфікації спрямовані на вдосконалення професійної діяльності фахівців для роботи на посадах керівників та провідних виконавців з менеджменту, екології та природокористування. Також для підвищення кваліфікації персоналу в енергетичній галузі України, науковим підприємством «Інфотек» було розроблено інноваційне віртуальне середовище (що складається з повнофункціонального режимного веб-тренажера та дистанційного навчального курсу) для навчання та тренажу персоналу об'єднаної енергетичної системи України під час очно-дистанційної форми навчання.

Вважаємо, що важливим є впровадження програмних засобів для підтримки прийняття управлінських рішень у процес підвищення кваліфікації фахівців в енергетичній, екологічній та суміжних галузях. Це відповідає сучасним світовим вимогам до підготовки фахівців нової технологічної ери та сприятиме реалізації концепції сталого розвитку суспільства. Опанувавши такі програмні засоби фахівці зможуть: визначати та ідентифікувати раніше невідомі взаємозв'язки між екологічними параметрами і факторами впливу; визначати й прогнозувати приховані тенденції і закономірності розвитку екологічних процесів (виявляти та розпізнавати приховані чинники впливу, в тому числі, фактори загрози; систематизувати та інтегрувати дані про стан навколишнього природного середовища; розробляти оптимізаційні рекомендації в енергетичній, екологічній та суміжних галузях; візуалізувати результати аналізу, здійснювати підготовку попередніх звітів і проектів допустимих рішень та ін.

У 2019 р. авторами статті було розроблено алгоритми та математичні та програмні засоби перевірки екологічної ефективності прийняття управлінських рішень, що є важливою складовою для оцінювання сталого розвитку екологічних систем. Також, автори даної статті надають консультативну допомогу та науковий супровід організаціям і установам щодо підвищення кваліфікації фахівців в енергетичній, екологічній та суміжних галузях, зокрема в аспекті застосування програмних засобів підтримки прийняття управлінських рішень.

Висновки. Розроблено програмне забезпечення, що дозволяє вирішувати задачі візуального аналізу динаміки екологічного стану територіальних систем та визначення меж стійкості окремих територій. Для аналізу динаміки техногенного впливу та визначення меж стійкості територіальних систем запропоновано нові форми представлення даних моніторингу техногенних навантажень та ризиків, що відображують динаміку екологічної ситуації в просторі інформативних ознак.

Також, важливим є підвищення кваліфікації фахівців, зокрема працівників міністерств, підприємств та організацій, які відповідають за прийняття рішень щодо зменшення негативного впливу на довкілля та підготовка майбутніх фахівців у цьому напрямі. У 2019 р. тільки кілька закладів вищої освіти пропонували курси підвищення кваліфікації для фахівців, що працюють на посадах керівників та провідних виконавців з менеджменту, екології та природокористування, проте, у навчальних програмах, недостатньо уваги приділено саме навчанню застосовувати програмні засоби підтримки прийняття управлінських рішень. Основними напрямами підвищення кваліфікації фахівців відповідальних за прийняття управлінських рішень є: проведення семінарів-тренінгів на базі міністерств, установ і відомств, що зацікавлені у впровадженні розроблених систем; науково-методична підтримка та консультативна допомога для процесу впровадження розроблених програмних засобів; розробка та вдосконалення навчально-методичного забезпечення для аспірантів, студентів та слухачів курсів підвищення кваліфікації фахівців відповідальних за прийняття управлінських рішень в енергетичній, екологічній та суміжних галузях.

Список використаних джерел:

1. Brundtland G.H., Khalid M., Agnelli S., Al-Athel S., Chidzero B. Our common future. New York, 1987.
2. Згуровський М.З. Аналіз сталого розвитку: глобальний і регіональний контексти : монографія. К. : НТУУ «КПІ», 2012. 312 с.
3. Report On Aggregation Indicators for Sustainable Development. New York : UN Division on Sustainable Development, 2001.
4. Yıldız-Geyhan E., Yılan G., Altun-Çiftçioğlu G.A., Kadırgan M.A.N. Environmental and social life cycle sustainability assessment of different packaging waste collection systems. *Resources, Conservation and Recycling*. 2019. Vol. 143. P. 119–132.
5. Niemmanee T., Kaveeta R., Potchanasin C. Assessing the Economic, Social, and Environmental Condition for the Sustainable Agricultural System Planning in Ban Phaeo District, Samut Sakhonn Province, Thailand. *Procedia – Social and Behavioral Sciences.* 2015. Vol. 197. P. 2554–2560.

6. Про схвалення Концепції створення загальнодержавної автоматизованої системи «Відкрите довкілля». Розпорядження Кабінету Міністрів України. Концепція від 07.11.2018 № 825-р. https://zakon.rada.gov.ua/laws/show/825-2018-%D1%80.

7. Zhao L., Zha Y., Zhuang Y., Liang L. Data envelopment analysis for sustainability evaluation in China: Tackling the economic, environmental, and social dimensions. *European Journal of Operational Research*. 2019. Vol. 275(3). P. 1083–1095.

8. González-García S., Rama M., Cortés A., et al. Embedding environmental, economic and social indicators in the evaluation of the sustainability of the municipalities of Galicia (northwest of Spain*). Journal of Cleaner Production*. 2019. Vol. 234. P. 27–42.

9. Baleta J., Mikulčić H., Klemeš J.J., Urbaniec K., Duić N. Integration of energy, water and environmental systems for a sustainable development. *Journal of Cleaner Production*. 2019. Vol. 215. P. 1424–1436.

10. Mikulčić H., Wang X., Duić N., Dewil R. Environmental problems arising from the sustainable development of energy, water and environment system. *Journal of Environmental Management*. 2020. Vol. 259. 109666.

11. Reid J., Rout M. Developing sustainability indicators – The need for radical transparency. *Ecological Indicators*. 2020. Vol. 110. 105941.

12. Chowdhury T., Chowdhury H., Chowdhury P., Sait S.M., Paul A., Ahamed J. Uddin, Saidur R. A case study to application of exergy-based indicators to address the sustainability of Bangladesh residential sector. *Sustainable Energy Technologies and Assessments*. 2020. Vol. 37. 100615.

13. Popov O.O., Iatsyshyn A.V., Kovach V.O. et al. Risk Assessment for the Population of Kyiv, Ukraine as a Result of Atmospheric Air Pollution. *Journal of Health and Pollution*. 2020. Vol. 10(25). 200303.

14. Iatsyshyn A.V., Iatsyshyn Anna V., Artemchuk V.O. et al. Software tools for tasks of sustainable development of environmental problems: peculiarities of programming and implementation in the specialists' preparation. *E3S Web of Conferences*. 2020. Vol. 166. 01001.

15. Suo C., Li Y.P., Sun J., Yin S. An air quality index-based multistage type-2-fuzzy interval-stochastic programming model for energy and environmental systems management under multiple uncertainties. *Environ. Res.* 2018. Vol. 167. P. 98–114.

16. Rönkkö M., Heikkinen J., Kotovirta V., Chandrasekar V. Automated preprocessing of environmental data. *Future Generation Computer Systems*. 2015. Vol. 45. P. 13–24.

17. Vergara A., Rubio M.P., Lorenzo M. On the Design of Virtual Reality Learning Environments in Engineering. *Multimodal Technologies and Interactions*. 2017. Vol. 1. 11 p.

18. Grodotzki J., Ortelt T.R., Tekkaya A.E. Remote and Virtual Labs for Engineering Education 4.0. *Procedia Manufacturing*. 2018. Vol. 26. P. 1349–1360.

19. Демидович Б.П. Лекции по математической теории устойчивости. Москва : Изд. «Наука», 1967. 472 с.

20. Щомісячний бюлетень забруднення атмосферного повітря в Києві та містах Київської області. К. : Центральна геофізична обсерваторія імені Бориса Срезневського, 2005–2018 рр.

21. Алымов В.Т., Тарасова Н.П. Техногенный риск: Анализ и оценка: Учебное пособие для вузов. М. : ИКЦ «Академкнига», 2004. 118 с.

References:

1. Brundtland, G.H., Khalid, M., Agnelli, S., Al-Athel S., Chidzero, B. (1987). Our common future. New York.

2. Zghurovs'kyj, M.Z. (2012). *Analiz staloho rozvytku: hlobal'nyj i rehional'nyj konteksty. [Analysis of Sustainable Development: Global and Regional Contexts].* Kyiv: NTUU "KPI" [in Ukrainian].

3. Report On Aggregation Indicators for Sustainable Development (2001). New York: UN Division on Sustainable Development.

4. Yıldız-Geyhan, E., Yılan, G., Altun-Çiftçioğlu, G.A., Kadırgan, M.A.N. (2019). Environmental and social life cycle sustainability assessment of different packaging waste collection systems. *Resources, Conservation and Recycling*. 143, 119–132.

5. Niemmanee, T., Kaveeta, R., Potchanasin, C. (2015). Assessing the Economic, Social, and Environmental Condition for the Sustainable Agricultural System Planning in Ban Phaeo District, Samut Sakhonn Province, Thailand. *Procedia – Social and Behavioral Sciences.* 197, 2554–2560.

6. Pro skhvalennya Kontseptsiyi stvorennya zahal'noderzhavnoyi avtomatyzovanoyi systemy "Vidkryte dovkillya". Rozporyadzhennya Kabinetu Ministriv Ukrayiny. *[About the approval of the Concept of creation of the national automated system «Open environment». Order of the Cabinet of Ministers of Ukraine. Conception on 7.11.2018 № 825-p.]* https://zakon.rada.gov.ua/laws/show/825-2018-%D1%80.

7. Zhao, L., Zha, Y., Zhuang, Y., Liang, L. (2019). Data envelopment analysis for sustainability evaluation in China: Tackling the economic, environmental, and social dimensions. *European Journal of Operational Research*. 275(3), 1083–1095.

8. González-García, S., Rama, M., Cortés, A. et al. (2019). Embedding environmental, economic and social indicators in the evaluation of the sustainability of the municipalities of Galicia (northwest of Spain). *Journal of Cleaner Production*. 234, 27–42.

9. Baleta, J., Mikulčić, H., Klemeš, J.J., Urbaniec, K., Duić, N. (2019). Integration of energy, water and environmental systems for a sustainable development. *Journal of Cleaner Production*. 215, 1424–1436.

10. Mikulčić, H., Wang, X., Duić, N., Dewil, R. (2020). Environmental problems arising from the sustainable development of energy, water and environment system. *Journal of Environmental Management.* 259, 109666.

11. Reid, J., Rout, M. (2020). Developing sustainability indicators – The need for radical transparency. *Ecological Indicators*. 110, 105941.

12. Chowdhury, T., Chowdhury, H., Chowdhury, P., Sait, S.M., Paul, A., Ahamed, J. Uddin, Saidur, R. (2020). A case study to application of exergy-based indicators to address the sustainability of Bangladesh residential sector. *Sustainable Energy Technologies and Assessments*. 37, 100615.

13. Popov, O.O., Iatsyshyn, A.V., Kovach, V.O. et al. (2020). Risk Assessment for the Population of Kyiv, Ukraine as a Result of Atmospheric Air Pollution. *Journal of Health and Pollution*. 10(25), 200303.

14. Iatsyshyn, A.V., Iatsyshyn, Anna V., Artemchuk, V.O. et al. (2020). Software tools for tasks of sustainable development of environmental problems: peculiarities of programming and implementation in the specialists' preparation. *E3S Web of Conferences*. 166, 01001.

15. Suo, C., Li, Y.P., Sun, J., Yin, S. (2018). An air quality index-based multistage type-2-fuzzy interval-stochastic programming model for energy and environmental systems management under multiple uncertainties. *Environ. Res.* 167, 98–114.

16. Rönkkö, M., Heikkinen, J., Kotovirta, V., Chandrasekar, V. (2015). Automated preprocessing of environmental data. *Future Generation Computer Systems*. 45, 13–24.

17. Vergara, A., Rubio, M.P., Lorenzo, M. (2017). On the Design of Virtual Reality Learning Environments in Engineering. *Multimodal Technologies and Interactions*. 1, 11.

18. Grodotzki, J., Ortelt, T.R., Tekkaya, A.E. (2018). Remote and Virtual Labs for Engineering Education 4.0. Procedia Manufacturing. 26. 1349–1360.

19. Demidovich, B.P. (1967). *Lektsii po matematicheskoy teorii ustoychivosti. [Lectures on the Mathematical Stability Theory]*. Moscow : Nauka [in Russian].

20. *Shchomisyachnyy byuleten' zabrudnennya atmosfernoho povitrya v Kyevi ta mistakh Kyivs'koyi oblasti. [Monthly Bulletin of air pollution in the cities of Kyiv and Kyiv region*]. Kyiv : Central Geophysical Observatory named after Boris Sreznevsky, (2005–2018) [in Ukrainian].

21. Alyimov, V.T., Tarasova, N.P. (2004). *Tekhnogennyy risk: Analiz i otsenka: Uchebnoye posobiye dlya vuzov. [Technogenic risk: Analysis and evaluation: A manual for higher education institutions]*. Moscow : IKTs "Akademkniga" [in Russian].

УДК 004.9
DOI https://doi.org/10.32689/maup.it.2021.1.4

Пилип ПРИСТАВКА
доктор технічних наук, професор, завідувач кафедри прикладної математики, Національний авіаційний університет, вул. Любомира Гузара, 1, м. Київ, Україна, індекс 03058 (chindakor37@gmail.com)

ORCID: https://orcid.org/0000-0002-0360-2459

Ольга ЧОЛИШКІНА
кандидат технічних наук, доцент, директор Ісінституту комп'ютерно-інформаційних технологій та дизайну, ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», вул. Фрометівська 2, Київ, Україна, індекс 03039 (greenhelga5@gmail.com)

ORCID: https://orcid.org/0000-0002-0681-0413

Pylyp PRYSTAVKA
Doctor of Technical Sciences, Professor, Head of the Department of Applied Mathematics, National Aviation University, 1 Liubomyra Huzara str., Kyiv, Ukraine, postal code 03058 (chindakor37@gmail.com)

Olha CHOLYSHKINA
Candidate of Technical Sciences, Associate Professor, Director of the Institute of Computer Information Technology and Design, Interregional Academy of personnel management, 2 Frometivska Street, Kyiv, Ukraine, postal code 03039 (greenhelga5@gmail.com)

Бібліографічний опис статті: Приставка П., Чолишкіна О. Піраміда зображень на основі сплайн-моделі у вигляді лінійної комбінації B-сплайнів. *Інформаційні технології та суспільство*. 2021. Вип. 1. С. 34–42. DOI: https://doi.org/10.32689/maup.it.2021.1.4

Bibliographic description of the article: Prystavka, P., Cholyshkina, O. (2021). Piramida zobrazhen na osnovi splain-modeli u vyhliadi liniinoi kombinatsii V-splainiv [Pyramid of images based on spline-model in the form of a linear combination of B-splines]. *Informatsiini tekhnolohii ta suspilstvo – Informati on technology and society*, 1, 34–42. DOI: https://doi.org/10.32689/maup.it.2021.1.4

ПІРАМІДА ЗОБРАЖЕНЬ НА ОСНОВІ СПЛАЙН-МОДЕЛІ У ВИГЛЯДІ ЛІНІЙНОЇ КОМБІНАЦІЇ B-СПЛАЙНІВ

Анотація. *У статті на основі формалізації моделі зображення, як лінійної комбінації B-сплайнів, що є близькою до інтерполяційних, у середньому подано її відповідні явні вигляди та оператори низькочастотної фільтрації та масштабування. Подано згорткові оператори низькочастотної фільтрації ЦЗ на основі сплайн-моделі. Подано оператори масштабування для побудови пірамід зображень, з метою подальшого пошуку особливих точок ЦЗ (sift-подібні методи) Результати досліджень можливо застосовувати в галузі інформаційної технології обробки цифрованих зображень, що отримано за даними аерофотозйомки з камер безпілотного повітряного судна (БПС). При обробці зображень в умовах обмежених технічних ресурсів (операційна пам'ять, тощо) на борту БПС нагальною є потреба мінімізації обчислювальних затрат алгоритму. Основним недоліком існуючих методів обробки є артефакти вихідного зображення, а саме так званий «драбинний ефект», коли пікселі зображення нагадують сходинки. Шляхом вирішення вказаних проблеми може бути побудова моделі цифрового зображення на основі базису фінітних функцій, що близькі за властивостями до властивостей аналогового зображення в спектральній області. Лінійні комбінації B-сплайнів є обчислювальним засобом обробки послідовностей відліків функцій, якому притаманні ряд цінних властивостей: обчислювальна простота, можливість враховувати локальні «особливості» сигналу, згладжувальні властивості та інші.*

Ключові слова: *піраміда зображень, моделі зображення, лінійна комбінація, B-сплайни.*

PYRAMID OF IMAGES BASED ON SPLINE-MODEL IN THE FORM OF A LINEAR COMBINATION OF B-SPLINES

Abstract. *The article is based around the formalization of the image model as a linear combination of B-splines, which is close to interpolation. The authors present, on average, its corresponding explicit aspects and low-frequency filtering and scaling operators. The possibility to obtain digital images scaled to an arbitrary, not necessarily integer, number of times is demonstrated in the article and the corresponding algorithm is provided. The research results can be applied in the field of information technology for digital image processing, obtained from aerial photography from the cameras of unmanned aerial*

vehicles (drons). When processing images in conditions of limited technical resources (RAM, etc.) on board the BPS, there is an urgent need to minimize the computational costs of the algorithm. The main disadvantage of existing processing methods is the artifacts of the original image, namely the so-called "ladder effect", when the pixels of the image resemble steps. By solving these problems can be the construction of a digital image model based on the basis of finite functions that are close in properties to the properties of the analog image in the spectral region. Linear combinations of B-splines are a computational tool for processing sequences of functions, which has a number of valuable properties: computational simplicity, the ability to take into account local "features" of the signal, smoothing properties and others.

Key words: *image pyramid, image models, linear combination, B-splines.*

Формалізація моделі зображення, як лінійної комбінації *B*-сплайнів. Оскільки за способом реєстрації ЦЗ, дані, що його подають, є усередненими значеннями, при фіксації аналогового зображення має місце наступне. Нехай площина зображення визначається осями T та Q. Крок дискретизації за напрямами T, Q однаковий $h>0$ (за замовченням $h=1$), отже, задано рівномірне розбиття $\Delta_{hh}: t_i = ih$, $q_j = jh$, $i=\overline{0,H-1}$, $j=\overline{0,W-1}$, де H та W – лінійні розміри ЦЗ, що фіксується. Нехай $\phi(t,q)$ – функція імпульсного відклику системи, що реєструє $p(t,q)$ – функцію інтенсивність освітлення об'єктів просторової сцени (аналогове зображення). Тоді в силу суто технічних властивостей систем реєстрації, результатом згортки $p(t,q)$ та функції відклику буде значення, усереднене в області дискретизації, зокрема:

$$(p*\phi)(ih,jh)=\frac{1}{h^2}\int_{ih-\frac{h}{2}}^{ih+\frac{h}{2}}\int_{jh-\frac{h}{2}}^{jh+\frac{h}{2}} p(t,q)\phi(t-ih,q-jh)dtdq=\bar{p}_{i,j}. \quad (1)$$

Тому дискретизовані значення інтенсивності світлового потоку (цифрове зображення) можна подати у вигляді:

$$p_{i,j}=\bar{p}_{i,j}+\varepsilon_{i,j},\ i=\overline{0,H-1},\ j=\overline{0,W-1}, \quad (2)$$

де $\varepsilon_{i,j}$ – випадкова вада. Стосовно вади $\varepsilon_{i,j}$ можна припускати будь–який розподіл, наприклад Гаусів. Отже, при побудові моделі зображень за даними (1) виникає задача використовувати апроксимації, що враховують і випадкову природу даних, і фізичні властивості систем реєстрації – зокрема, оператори інтерполяційні в середньому або близькі до інтерполяційних у середньому [1].

Традиційно задача моделювання аналогового зображення вирішується так [2; 3]. Якщо дискретизація аналогового зображення проведена растуванням, то ідеальне інтерполяційне відновлення $p(t,q)$ виконується за допомогою двовимірного фільтру з прямокутною частотною характеристикою, отриманої за допомогою зворотного перетворення Фур'є:

$$w(t,q)=\frac{\sin(\pi t)}{\pi t}\cdot\frac{\sin(\pi q)}{\pi q}.$$

Продукт фільтрації може бути визначений за допомогою двовимірної згортки ЦЗ і даної імпульсної характеристики. Після виконання згортки має місце:

$$p(t,q)=\sum_i\sum_j p_{i,j}\frac{\sin(\pi(t-i))}{\pi(t-i)}\cdot\frac{\sin(\pi(q-j))}{\pi(q-j)}.$$

Наведене співвідношення є двовимірним варіантом теореми Котельникова–Найквіста і вказує спосіб точного інтерполяційного відтворення неперервного зображення за відомою послідовністю його двовимірних відліків. Тобто, для точного відновлення в ролі інтерполюючої функції повинні використовуватися двовимірні функції виду $\sin(x)/x$. Наведене твердження є справедливим, якщо двовимірний спектр сигналу є фінітним, а інтервали дискретизації досить малі. Справедливість зроблених висновків порушується, якщо хоча б одна з цих умов не виконується. Реальні зображення рідко мають спектри з яскраво вираженими граничними частотами. Однією з причин, що призводять до необмеженості спектра, є обмеженість розмірів зображення.

Шляхом вирішення вказаної проблеми може бути побудова моделі ЦЗ на основі базису фінітних функцій, що близькі за властивостями до властивостей аналогового зображення в спектральній області. Наприклад, лінійні комбінації *B*–сплайнів [4-8] є обчислювальним засобом обробки послідовностей відліків функцій, якому притаманні ряд цінних властивостей: обчислювальна простота, можливість враховувати локальні «особливості» сигналу, згладжувальні властивості та інші. Тому актуальним може бути розгляд питання про можливість використання згаданих сплайнів на випадок побудови моделі аналогового зображення [1].

У монографії [9] для апроксимації функції $p(t,q)$ за значеннями типу (1) у вузлах розбиття $\Delta_{h,h}$, подано лінійні комбінації *B*–сплайнів, що є близькими до інтерполяційних у середньому. Наприклад, сплайн–оператори нульового та першого ступеня уточнення на основі *B*–сплайнів другого порядку такі:

$$S_{2,0}(p,t,q)=\sum_{i\in Z}\sum_{j\in Z}p_{i,j}B_{2,h}(t-ih)B_{2,h}(q-jh), \tag{3}$$

$$S_{2,1}(p,t,q)=\sum_{i\in Z}\sum_{j\in Z}\left(p_{i,j}-\frac{1}{6}\left(\Delta_i^2p_{i,j}+\Delta_j^2p_{i,j}\right)+\frac{1}{36}\Delta_{ij}^2p_{i,j}\right)B_{2,h}(t-ih)B_{2,h}(q-jh), \tag{4}$$

де (з точністю до аргументу)

$$B_{2,h}(t)=\begin{cases}0, & t\notin[-3h/2;3h/2],\\ (3+2t/h)^2/8, & t\in[-3h/2;-h/2],\\ 3/4-(2t/h)^2/4, & t\in[-h/2;h/2],\\ (3-2t/h)^2/8, & t\in[h/2;3h/2];\end{cases} \tag{5}$$

$$\Delta_i^2p_{i,j}=p_{i-1,j}-2p_{i,j}+p_{i+1,j};\ \Delta_j^2p_{i,j}=p_{i,j-1}-2p_{i,j}+p_{i,j+1};$$

$$\Delta_{ij}^2p_{i,j}=\Delta_i^2p_{i,j-1}-2\Delta_i^2p_{i,j}+\Delta_i^2p_{i,j+1}=\Delta_j^2p_{i-1,j}-2\Delta_j^2p_{i,j}+\Delta_j^2p_{i+1,j}.$$

Обґрунтуванням обрання розглянутих сплайнів в якості моделі аналогового зображення можуть бути міркування, відповідні тим, що викладені в роботі [10] для моделювання аналогових одновимірних сигналів з кінцевою енергією на основі аналогічних одновимірних лінійних комбінацій *B*–сплайнів. Зокрема, виходячи з положення, що базис *B*–сплайнів є базисом Риса та з того факту, що фундаментальні сплайни на основі *B*–сплайнів [11] прямують до нуля експоненціально швидко при віддалені від локальної (i,j)–ої області наближення, прийнятним є використання введених в роботі [9] двовимірних локальних поліноміальних сплайнів, близьких до інтерполяційних у середньому в якості моделі ЦЗ.

Якщо обрати в якості моделі зображення $p(t,q)$ сплайни (3), (4), то така оцінка за певних умов є фактично асимптотично точною. Зокрема, якщо $p(t,q)\in C^{2,2}$, $\left|\varepsilon_{i,j}\right|<\varepsilon$, $i,j\in Z$ і $\forall\varepsilon>0$, то справедлива оцінка [9] така:

$$\left\|p(t,q)-S_{2,0}(p,t,q)\right\|\le\frac{h^2}{6}\left\|p''_{t^2}(t,q)\right\|+\frac{h^2}{6}\left\|p''_{q^2}(t,q)\right\|+$$

$$+\frac{h^4}{36}\left\|p^{(4)}_{t^2q^2}(t,q)\right\|+\varepsilon\cdot\|p(t,q)\|+o\left(h^4\right), \tag{6}$$

для $\forall p(t,q)\in C^{3,3}$ і $\forall\varepsilon>0$ справедлива нерівність

$$\left\|p(t,q)-S_{2,1}(p,t,q)\right\|\le\frac{h^3}{12\sqrt{3}}\left\|p'''_{t^3}(t,q)\right\|+\frac{h^3}{12\sqrt{3}}\left\|p'''_{q^3}(t,q)\right\|+$$

$$+\frac{h^6}{432}\left\|p^{(6)}_{t^3q^3}(t,q)\right\|+\varepsilon\cdot\frac{16}{9}\|p(t,q)\|+o\left(h^6\right) \tag{7}$$

Вираз (4) надає високоточне наближення, а сам сплайн, що уточнює (та інші аналогічні [9]) є операторами близькими до інтерполяційних у середньому в асимптотичному сенсі. Якщо ж в якості апроксимації зображення обрати вираз (3) або будь–яку іншу комбінацію *B*–сплайнів такого типу:

$$S_{r,0}(p,t,q)=\sum_{i\in Z}\sum_{j\in Z}p_{i,j}B_{r,h_t}\left(t-ih_t\right)B_{r,h_q}\left(q-jh_q\right),\ r=2,3,\dots, \tag{8}$$

то отримаємо модель з властивостями імпульсного нерекурсивного низькочастотного фільтру [12], де, наприклад (з точністю до аргументу)

$$B_{6,h}(t)=\begin{cases}0, & t\notin\left[-\frac{7h}{2},\frac{7h}{2}\right],\\ \frac{1}{720}\left(\frac{t}{h}+\frac{7}{2}\right)^6, & t\in\left[-\frac{7h}{2},-\frac{5h}{2}\right],\\ -\frac{1}{120}\left(\frac{t}{h}\right)^6-\frac{7}{60}\left(\frac{t}{h}\right)^5-\frac{21}{32}\left(\frac{t}{h}\right)^4-\frac{133}{72}\left(\frac{t}{h}\right)^3-\frac{329}{128}\left(\frac{t}{h}\right)^2-\frac{1267}{960}\left(\frac{t}{h}\right)+\frac{1379}{7680}, & t\in\left[-\frac{5h}{2},-\frac{3h}{2}\right],\\ \frac{1}{48}\left(\frac{t}{h}\right)^6+\frac{7}{48}\left(\frac{t}{h}\right)^5+\frac{21}{64}\left(\frac{t}{h}\right)^4+\frac{35}{288}\left(\frac{t}{h}\right)^3-\frac{91}{256}\left(\frac{t}{h}\right)^2+\frac{7}{768}\left(\frac{t}{h}\right)+\frac{7861}{15360}, & t\in\left[-\frac{3h}{2},-\frac{h}{2}\right],\\ -\frac{1}{36}\left(\frac{t}{h}\right)^6+\frac{7}{48}\left(\frac{t}{h}\right)^4-\frac{77}{192}\left(\frac{t}{h}\right)^2+\frac{5887}{11520}, & t\in\left[-\frac{h}{2},\frac{h}{2}\right],\\ \frac{1}{48}\left(\frac{t}{h}\right)^6-\frac{7}{48}\left(\frac{t}{h}\right)^5+\frac{21}{64}\left(\frac{t}{h}\right)^4-\frac{35}{288}\left(\frac{t}{h}\right)^3-\frac{91}{256}\left(\frac{t}{h}\right)^2-\frac{7}{768}\left(\frac{t}{h}\right)+\frac{7861}{15360}, & t\in\left[\frac{h}{2},\frac{3h}{2}\right],\\ -\frac{1}{120}\left(\frac{t}{h}\right)^6+\frac{7}{60}\left(\frac{t}{h}\right)^5-\frac{21}{32}\left(\frac{t}{h}\right)^4+\frac{133}{72}\left(\frac{t}{h}\right)^3-\frac{329}{128}\left(\frac{t}{h}\right)^2+\frac{1267}{960}\left(\frac{t}{h}\right)+\frac{1379}{7680}, & t\in\left[\frac{3h}{2},\frac{5h}{2}\right],\\ \frac{1}{720}\left(\frac{t}{h}-\frac{7}{2}\right)^6, & t\in\left[\frac{5h}{2},\frac{7h}{2}\right]\end{cases} \tag{9}$$

Зокрема, в роботі [11], приведено доведення, що як і функція Гауса, будь–який *B*–сплайн порядку вище першого може бути використаний для визначення коротковіконного перетворення Фур'є (КВПФ). Отже, якщо $B_r(t)$, $r\geq 2$ – *B*–сплайн порядку r, то [13]:

$$\hat{B}_r(\omega)=\left(\frac{e^{i\omega/2}-e^{-i\omega/2}}{i\omega}\right)^{r+1}=\left(\frac{\sin(\omega/2)}{(\omega/2)}\right)^{r+1}.$$

Зазначимо, що вже починаючи з порядку $r=5$ і *B*–сплайн, і гаусіан в частотній області фактично мало чим відрізняються, при цьому обрахунок *B*–сплайну п'ятого порядку [14] потребує менше обчислювальних затрат. Тож, якщо є потреба в отриманні цифрового низькочастотного фільтру ЦЗ, то достатньо в моделі (8) визначити значення сплайну у вузлах розбиття $\Delta_{h,h}$ [15]. Наприклад, якщо ввести заміну

$$x=\frac{2}{h}(t-ih),\ |x|\leq 1,\ y=\frac{2}{h}(q-jh),\ |y|\leq 1, \tag{10}$$

можна подати (3) в розгорнутому вигляді

$$\begin{aligned}S_{2,0}(p,t,q)=\frac{1}{64}\Big((1-x)^2(1-y)^2p_{i-1,j-1}+(1-x)^2\left(6-2y^2\right)p_{i-1,j}+\\ +(1-x)^2(1+y)^2p_{i-1,j+1}+\left(6-2x^2\right)(1-y)^2p_{i,j-1}+\left(6-2x^2\right)\left(6-2y^2\right)p_{i,j}+\\ +\left(6-2x^2\right)(1+y)^2p_{i,j+1}+(1+x)^2(1-y)^2p_{i+1,j-1}+(1+x)^2\left(6-2y^2\right)p_{i+1,j}+\\ +(1+x)^2(1+y)^2p_{i+1,j+1}\Big).\end{aligned} \tag{11}$$

Далі, поклавши в (10) $x=0$, $y=0$ отримаємо лінійний оператор $L\left(p^{i,j}\right)$ низькочастотної фільтрації:

$$\begin{aligned}L\left(p^{i,j}\right)=S_{2,0}(p,ih,jh)=\Big(p_{i-1,j-1}+6p_{i-1,j}+p_{i+1,j+1}+\\ +6p_{i,j-1}+36p_{i,j}+6p_{i,j+1}+p_{i+1,j-1}+6p_{i+1,j}+p_{i+1,j+1}\Big)\Big/64,\ i,j\in\mathbb{Z}\end{aligned}$$

Використовуючи запис у формі дискретної згортки послідовності $p_{i,j}$, $i,j\in\mathbb{Z}$ з маскою фільтра γ, оператори низькочастотної фільтрації на основі лінійних комбінацій *B*-сплайнів 2-го порядку можна записати так:

$$L\left(p^{i,j}\right)=\sum_{ii=i-1}^{i+1}\sum_{jj=j-1}^{j+1}\gamma^{(r)}_{ii-i,jj-j}p_{ii,jj},\ i,j\in\mathbb{Z},$$

де $r=\{2,3\}$,

$$\gamma^{(2)}=\frac{1}{64}\begin{pmatrix}1 & 6 & 1\\ 6 & 36 & 6\\ 1 & 6 & 1\end{pmatrix}; \tag{12}$$

Використання, наприклад, *B*-сплайну шостого порядку надасть такий оператор:

$$L\left(p^{i,j}\right)=\sum_{ii=i-3}^{i+3}\sum_{jj=j-3}^{j+3}\gamma^{(6)}_{ii-i,jj-j}p_{ii,jj},\ i,j\in\mathbb{Z},$$

$$\gamma^{(6)}=\frac{1}{21233664}\begin{pmatrix}0{,}01 & 7{,}22 & 105{,}43 & 235{,}48 & \cdots\\ 7{,}22 & 5212{,}84 & 76120{,}46 & 170016{,}56 & \cdots\\ 105{,}43 & 76120{,}46 & 1111548{,}49 & 2482665{,}64 & \cdots\\ 235{,}48 & 170016{,}56 & 2482665{,}64 & 5545083{,}04 & \cdots\\ \vdots & \vdots & \vdots & \vdots & \ddots\end{pmatrix}. \tag{13}$$

Зауважимо, що маска (13) має розміри (7x7), а значення, яких не достає в поданні визначаються з урахуванням симетрії.

Побудова піраміди зображень за використанням лінійних операторів на основі лінійних комбінацій *B*-сплайнів. Моделі зображення з властивостями імпульсного нерекурсивного низькочастотного фільтру на зразок (8) традиційно мають застосування при обробці ЦЗ для реалізації масштабного (кратномаштабного) аналізу та при побудові пірамід зображень в методах, що потребують визначення особливих точок, наприклад, SIFT-подібних методах розпізнавання [16; 17].

Серед різноманітних ядер в зготковій моделі зображення у просторі масштаб-положення найбільше поширення традиційно має гаусова функція. Тож дозволимо собі відступ від введеної моделі на основі лінійної комбінації *B*-сплайнів для викладення відомих положень про використання функцій Гауса при масштабуванні ЦЗ. Отже, простір масштаб-положення для вихідного зображення $p(t,q)$ визначається функцією

$$L(t,q,\sigma)=\int_{(\xi,\eta)}p(t-\xi,q-\eta)G(\xi,\eta,\sigma)d\xi d\eta, \tag{14}$$

яка є згорткою гаусової функції змінного масштабу

$$G(t,q,\sigma)=\frac{1}{2\pi\sigma}\exp\left(-\frac{t^2+q^2}{2\sigma}\right),$$

з функцією інтенсивності освітлення $p(t,q)$:

$$L(t,q,\sigma)=G(t,q,\sigma)*p(t,q),$$

де '*' – це операція згортки по координатам *t* та *q*.

Щоб з обчислювальної точки зору ефективно знаходити стійкі (стабільні) положення ключових точок (t,q,σ) (keypoint locations) в просторі масштаб-положення (scale-space), в роботі [17] екстремуми в просторі масштаб-положення визначаються для $D(t,q,\sigma)$ – згорток різниць гаусових функцій двох ближніх масштабів, розділених постійними множниками *k*, з вихідним зображенням $p(t,q)$:

$$D(t,q,\sigma)=\big(G(t,q,k\sigma)-G(t,q,\sigma)\big)*p(t,q)=L(t,q,k\sigma)-L(t,q,\sigma), \tag{15}$$

Обчислення згортки вихідного зображення з гаусовими функціями (згладжування гаусових зображень) $L(t,q,\sigma)$ (14) необхідно для опису особливостей в просторі масштаб-положення (scale-space feature description). Але після їх визначення згортка $D(t,q,\sigma)$ (15) може бути визначена простим відніманням гаусових зображень (14). Крім цього, різниця гаусових функцій дає замкнену апроксимацію нормованого масштабом лапласіана $\sigma^2\nabla^2G$:

$$\nabla^2_{norm}L=t\left(L_{xx}+L_{yy}\right) \tag{16}$$

(нормований множник σ^2 потрібен для інваріантності відносно масштабу). Зв'язок між $D(t,q,\sigma)$ (15) і $\sigma^2\nabla^2G$ випливає з рівняння дифузії

$$\frac{\partial G}{\partial \sigma} = \sigma \nabla^2 G. \tag{17}$$

З (17) бачимо, що $\nabla^2 G$ може бути обрахований з кінцево-різницевої апроксимації похідної $\partial G / \partial \sigma$ при використанні різниці гаусових функцій для з'єднання масштабів $k\sigma$ та σ:

$$\sigma \nabla^2 G = \frac{\partial G}{\partial \sigma} \approx \frac{G(t,q,k\sigma) - G(t,q,\sigma)}{k\sigma - \sigma}$$

і тому

$$G(x,y,k\sigma) - G(x,y,\sigma) \approx (k-1)\sigma^2 \nabla^2 G. \tag{18}$$

Формула (18) показує, якщо обчислюється різниця гаусових функцій (difference-of-Gaussian function) з масштабами, які відрізняються на постійний множник (фактор) *k*, ця різниця містить σ^2 – нормування масштабу, необхідне для масштабно інваріантного лапласіана (16). В формулі (18) множник (фактор) $(k-1)$ є константою для усіх масштабів, і відповідно, не впливає на положення екстремумів. Помилка апроксимації прямує до нуля при $k \to 1$, але на практиці виявляється, що ця апроксимація не впливає на стабільність виявлення або локалізації екстремумів, як наприклад $k = \sqrt{2}$.

Обчислюються гаусові зображення, розділені постійним множником (фактором) k в просторі масштаб-положення. Вони показані у вигляді стека у лівому стовбці (рис. 1.2). Кожна октава в просторі масштаб-положення (тобто гаусові зображення до подвоєння варіації) розділена на цілу кількість s інтервалів, тому $k = 2^{1/s}$. В стек для кожної октави поміщуються $(s+3)$ розмитих зображень, тому знаходження кінцевих екстремумів (final extrema detection) охоплює повну октаву. Зображення сусідніх масштабів віднімаються, даючи $(s+1)$ різниці гаусових зображень $D(\cdot)$ (15). Після формування кожної повної октави з $n = 1,2,...$ гаусове зображення $L(t,q,2^n\sigma)$, $n = 1,2,...$, яке має в два рази більшу варіацію ніж вихідне для цієї октави значення $2^{n-1}\sigma$, $n = 1,2,...$ на половину проріджується так, щоб залишався кожний другий піксель в кожному рядку і кожному стовпці. Це відповідає переходу на наступний рівень гаусової піраміди [18].

Якщо ж здійснювати побудову піраміди зображень, модель яких задана у вигляді (8), для зменшення розмірів зображення доцільно використовувати оператори на зразок низькочастотних фільтрів з масками (12) – (13). Нехай задано деякий растр, кожному пікселу якого поставлено у відповідність двійка індексів $\{(i,j)\}_{i,j \in Z}$, що визначають його місцеположення. Не зменшуючи загальності позначимо $\{p_{i,j,0}\}$ для запису обчислювальної схеми при роботі з послідовностями кольорових складових – червоною, зеленою та синьою. Для рекурентного двократного збільшення масштабу (двократного зменшення горизонтального та вертикального розмірів) зображення необхідно на кожному κ–му ($\kappa = 1,2,\ldots$) кроці рекурсії чотирикратно зменшувати кількість пікселів, звільнюючи у новому κ–му растрі місце з під трьох старих пікселів праворуч, зверху та зверху–навскіс від кожного (i,j)–го піксела $(\kappa-1)$–го растру. Тобто, якщо $\{p_{i,j,\kappa}\}_{i,j \in Z}$ – послідовність кольорових складових κ–го зменшеного растру, то

$$p_{i,j,\kappa} = p_{2i,2j,\kappa-1}, \tag{19}$$

при цьому пам'ять під розміщення величин $p_{2i+1,2j,\kappa-1}$, $p_{2i,2j+1,\kappa-1}$, $p_{2i+1,2j+1,\kappa-1}$, може бути вивільнена.

Окрім тривіального визначення членів послідовності $\{p_{i,j,\kappa}\}_{i,j \in Z}$ згідно виразу (19), реалізують збільшення масштабу зображення зі згладжуванням, контрастуванням, направленою фільтрацією, тощо, залежно від конкретних потреб. В такому разі величини $p_{i,j,\kappa}$ визначаються на підставі деякого лінійного функціоналу $p_{i,j,\kappa} = A\left(p^{\kappa-1,2i,2j}\right)$, $i,j \in Z$, що побудований на даних попереднього кроку рекурсії. Наприклад, зменшення зі згладжуванням за використанням низькочастотного фільтру з маскою (12), може бути реалізовано так:

$$p_{i,j,\kappa} = \frac{1}{64}\Big(p_{2i-1,2j-1,\kappa-1} + 6p_{2i-1,2j,\kappa-1} + p_{2i-1,2j+1,\kappa-1} + 6p_{2i,2j-1,\kappa-1} + 36p_{2i,2j,\kappa-1} +$$

$$+6p_{2i,2j+1,\kappa-1} + p_{2i+1,2j-1,\kappa-1} + 6p_{2i+1,2j,\kappa-1} + p_{2i+1,2j+1,\kappa-1}\Big).$$

В загальному випадку при збільшенні масштабу зображення, що описується слайн-моделлю (8) можна подати у наступному вигляді:

$$p_{i,j,\kappa} = \sum_{ii=2i-1}^{2i+1} \sum_{jj=2j-1}^{2j+1} \gamma_{L,ii-2i,jj-2j}^{(2)} p_{ii,jj,\kappa-1}, \tag{20}$$

для операторів з маскою (12) або, як приклад,

$$p_{i,j,\kappa} = \sum_{ii=2i-3}^{2i+3} \sum_{jj=2j-3}^{2j+3} \gamma_{L,ii-2i,jj-2j}^{(6)} p_{ii,jj,\kappa-1}, \tag{21}$$

для оператору з маскою (13).

На рисунку (рис. 1) показано приклад піраміди з чотирьох рівнів ЦЗ, яку отримано після $\kappa = 3$ кроків рекурсії за допомого оператора (21). При обробці ЦЗ використання пірамідальної структури даних забезпечує зменшення часу обробки зображення, низькочастотну фільтрацію для придушення високочастотних осциляцій функції інтенсивності освітлення, а отже отримання глобальних особливостей (особливих точок), що характерні для зображень на усіх рівнях – більш точних початкових наближень особливостей для обробки нижніх рівнів по результатам верхніх рівнів піраміди.

Рис. 1. Піраміда з чотирьох рівнів для тестового зображення

Оператори на зразок (20)-(21) можна застосовувати і для реалізації побудови октави згідно (15). По суті, різниця низькочастотних складових зображення, які отримані за допомогою фільтрації зображення операторими з масками (12)-(13) дає у результаті високочастотну складову зображення. Наприклад, маска оператору на основі різниці низькочастотних фільтрів на основі *B*–сплайнів 3–го та 2–го порядку є такою:

$$\delta L_{3,2} = \gamma_L^{(3)} - \gamma_L^{(2)} = \frac{1}{576}\begin{pmatrix} 7 & 10 & 7 \\ 10 & -68 & 10 \\ 7 & 10 & 7 \end{pmatrix}. \tag{22}$$

Аналогічно, використовуючи фільтри на основі *B*-сплайнів 3, 4, 5 та 6 порядків можна ввести наступні маски:

$$\delta L_{4,3} = \gamma_L^{(4)} - \gamma_L^{(3)} = \frac{1}{147456}\begin{pmatrix} 1 & 76 & 230 & 76 & 1 \\ 76 & 1680 & 1096 & 1680 & 76 \\ 230 & 1096 & -12636 & 1096 & 230 \\ 76 & 1680 & 1096 & 1680 & 76 \\ 1 & 76 & 230 & 76 & 1 \end{pmatrix}; \tag{23}$$

$$\delta L_{5,4} = \gamma_L^{(5)} - \gamma_L^{(4)} = \frac{1}{33177600}\begin{pmatrix} 2079 & 42804 & 100314 & \cdots \\ 42804 & 257904 & 20664 & \cdots \\ 100314 & 20664 & -1866276 & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}; \tag{24}$$

$$\delta L_{6,5} = \gamma_L^{(6)} - \gamma_L^{(5)} = \frac{1}{21233664}\begin{pmatrix} 0{,}01 & 7{,}22 & 105{,}43 & 235{,}48 & \cdots \\ 7{,}22 & 3738{,}28 & 37781{,}9 & 72695{,}6 & \cdots \\ 105{,}43 & 37781{,}9 & 114745{,}93 & -47679{,}32 & \cdots \\ 235{,}48 & 72695{,}6 & -47679{,}32 & -878100{,}32 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}. \tag{25}$$

Тобто, для побудови піраміди зображень положень ключових точок, операторами, що близькі до (15) можна використати такі вирази:

на основі маски (22)

$$p_{i,j,\kappa} = \sum_{ii=2i-1}^{2i+1} \sum_{jj=2j-1}^{2j+1} \delta L_{3,2} p_{ii,jj,\kappa-1}, \tag{25}$$

на основі масок (23)-(24)

$$p_{i,j,\kappa} = \sum_{ii=2i-2}^{2i+2} \sum_{jj=2j-2}^{2j+2} \delta L_{rr} p_{ii,jj,\kappa-1}, \ rr = \{"4,3","5,4"\} \tag{26}$$

та за використання маски (25)

$$p_{i,j,\kappa} = \sum_{ii=2i-3}^{2i+3} \sum_{jj=2j-3}^{2j+3} \delta L_{6,5} p_{ii,jj,\kappa-1}. \tag{27}$$

Висновки. За матеріалами проведених досліджень можна сформулювати наступні висновки.

1. Формалізовано модель ЦЗ на основі двовимірних поліноміальних сплайні на основі *B*-сплайнів другого-шостого порядків, що є близькими до інтерполяційних у середньому.

2. Подано згорткові оператори низькочастотної фільтрації ЦЗ на основі сплайн-моделі.

3. Подано оператори масштабування для побудови пірамід зображень, з метою подальшого пошуку особливих точок.

4. Подальші дослідження, можуть мати за мету отримання безпосередньо операторів визначення особливих точок та їх детекторів.

Список використаних джерел:

1. Приставка П.О., Рябий М.О. Модель реалістичних зображень на основі двовимірних сплайнів, близьких до інтерполяційних у середньому. *Наукоємні технології*. 2012. № 3 (15). С. 67–71.

2. Грузман И.С., Киричук В.С. и др. Цифровая обработка изображений в информационных системах : учебное пособие. Новосибирск : Изд-во НГТУ, 2000. 168 с.

3. Ярославский Л.П. Введение в цифровую обработку изображений. М. : Сов. Радио, 1979. 312 с.

4. Schoenberg I.J. Contributions to the problem of approximation of equidistant data by analytic functions. Part A. Quart. Appl. Math. 4, P. 45–99. Part B. ibid 4. 1946. P. 112–141.

5. Лигун А.А., Шумейко А.А. Асимптотические методы востановления кривых. К. : ИМ НАУ, 1997. 358 с.

6. Корнейчук Н.П. Сплайны в теории приближения. М. : Наука, 1984. 351 с.

7. Де Бор К. Практическое руководство по сплайнам, М. : Радио и связь, 1985. 303 с.

8. Приставка П.О. Лінійні комбінації В-сплайнів, близькі до інтерполяційних у середньому, в задачі моделювання аналогових сигналів. *Актуальні проблеми автоматизації та інформаційних технологій* : зб. наук. праць. 2011. Т. 15. С. 4–17.

9. Приставка П.О. Поліноміальні сплайни при обробці даних, Д. : Вид-во Дніпропетр. ут-ту, 2004. 236 с.

10. Приставка П.О. Лінійні комбінації В-сплайнів, близькі до інтерполяційних у середньому, в задачі моделювання аналогових сигналів. *Актуальні проблеми автоматизації та інформаційних технологій* : зб. наук. праць. 2011. Т. 15.

11. Чуи Ч. Введение в вэйвлетты, М. : Мир, 2001.

12. Василенко В.А., Зюзин М.В., Ковалков А.В. Сплайн-функции и цифровые фильтры / под ред. А.С. Алексеева. Новосибирск : Вычислительный центр СО АН СССР, 1984.

13. Unser M. Splines: A Perfect Fit for Signal and Image Processing, IEEE Signal Processing Magazine, 1999. P. 22–38.

14. Приставка П.О. Чолишкіна О.Г. Дослідження В-сплайну п'ятого порядку та їх лінійної комбінації. *Математичне моделювання*. 2007.

15. Приставка П.О. Обчислювальні аспекти застосування поліноміальних сплайнів при побудові фільтрів. *Актуальні проблеми автоматизації та інформаційних технологій*. 2006. Т. 10. С. 3–14.

16. Lowe D.G. Object recognition from local scale-invariant features. *Computer Vision (ICCV). The proceedings of the seventh IEEE international conference*. 1999. P. 1150–1157.

17. Lowe D. G. Distinctive image features from scale-invariant keypoints. *International Journal of Computer Vision*. 2004. V. 60. N 2. P. 91–110.

18. Кухаренко Б.Г. Алгоритмы анализа изображений для определения локальных особенностей и распознавания объектов и панорам. *Информационные технологии*. 2011. № 7. Приложение. 32 с.

References:

1. Prystavka, P.O. and Ryabiy, M.O. (2012). Model of realistic images on the basis of double splines, close to interpolation in the middle. *Science technology*. No. 3 (15), pp 67–71.

2. Gruzman, I.S. and Kirichuk, V.S. et al. (2000). Digital image processing in information systems. Textbook. Novosibirsk: Publishing house of NSTU, 168 p.

3. Yaroslavsky, L.P. (1979). Introduction to digital imaging. Moscow: Sov. Radio, 312 p.
4. Schoenberg, I.J. (1946). Contributions to the problem of approximation of equidistant data by analytic functions, Part A. Quart. Appl. Math. 4, pp. 45–99. Part B. ibid 4, pp. 112–141.
5. Ligun, A.A. and Shumeiko, A.A. (1997). Asymptotic methods for restoring curves. Kiev: IM NAU, 358 p
6. Korneichukm, N.P. (1984). Splines in approximation theory. Moscow: Nauka, 351 p.
7. De Bohrm K.A. (1985). Practical Guide to Splines. Moscow: Radio and Communication, 303 p.
8. Prystavka, P.O. (2011). Linear combinations of B-splines, close to interpolation on average, in the problem of analog signal modeling. *Actual problems of automation and information technology*: coll. Science. wash, vol. 15, pp. 4–17.
9. Prystavka, P.O. (2004). Polynomial splines in data processing. Dnipropetrovsk: Dnipropetrovsk Publishing House, 236 p.
10. Prystavka, P.O. (2011). Linear combinations of B-splines, close to interpolation on average, in the problem of modeling analog signals. *Actual problems of automation and information technology* : coll. science. proceedings, vol. 15.
11. Chui, C.K. (2001). Introduction to Wavelets. Moscow: Mir.
12. Vasilenko, V.A., Zyuzin, M.V. and Kovalkov, A.V. (1984) Spline functions and digital filters (edited by A.S. Alekseev). Novosibirsk: Computing Center of the Siberian Branch of the USSR Academy of Sciences.
13. Unser, M. (1999). Splines: A Perfect Fit for Signal and Image Processing, *IEEE Signal Processing Magazine*, pp. 22–38.
14. Prystavka, P.O., Cholyshkina, O.G. (2007). Fifth-order B-spline study and their linear combination. *Mathematical modeling*.
15. Prystavka, P.O. (2006). Numeric aspects of storing polynomial splines when prompting filters. *Actual problems of automation and information technologies*, vol. 10, pp. 3–14.
16. Lowe, D.G. (1999) Object recognition from local scale-invariant features. *Computer Vision (ICCV). The proceedings of the seventh IEEE international conference,* pp. 1150–1157.
17. Lowe, D.G. (2004). Distinctive image features from scale-invariant keypoints. *International Journal of Computer Vision*, vol. 60, issue 2, pp. 91–110.
18. Kukharenko, B.G. (2011). Image analysis algorithms for determining local features and recognizing objects and panoramas. *Information Technologies*, no. 7, Appendix, 32 p.

УДК 004.9
DOI https://doi.org/10.32689/maup.it.2021.1.5

Микола РУДНІЧЕНКО
кандидат технічних наук, доцент кафедри інформаційних технологій, Державний університет «Одеська Політехніка», просп. Шевченко, 1, м. Одеса, Україна, індекс 65001 (nickolay.rud@gmail.com)

ORCID: https://orcid.org/0000-0002-7343-8076

Володимир ВИЧУЖАНІН
доктор технічних наук, професор, завідувач кафедри інформаційних технологій, Державний університет «Одеська Політехніка», просп. Шевченко, 1, м. Одеса, Україна, індекс 65001 (vint532@yandex.ua)

ORCID: https://orcid.org/0000-0002-5244-5808

Наталя ШИБАЄВА
кандидат технічних наук, доцент кафедри інформаційних технологій, Державний університет «Одеська Політехніка», просп. Шевченко, 1, м. Одеса, Україна, індекс 65001 (nati.shibaeva@gmail.com)

ORCID: https://orcid.org/0000-0002-7869-9953

Ігор ПЕТРОВ
доктор технічних наук, професор кафедри морських перевезень національного університету «Одеська морська академія», вул. Дідріхсона, 8, м. Одеса, Україна, індекс 65029 (firmness@list.ru)

ORCID: https://orcid.org/0000-0002-8740-6198

Олександр МАЗУРЕНКО
Студент Міжрегіональної Академії управління персоналом, вул. Фрометівська, 2, м. Київ, Україна, індекс 03039 (alexmazur@gmail.com)

ORCID: https://orcid.org/0000-0002-3320-1348

Mykola RUDNICHENKO
PhD in Technical Sciences, Associate Professor of Information Technology, Odessa Polytechnic State University, ave. Shevchenko, 1, Odessa, Ukraine, postal code 65001 (nickolay.rud@gmail.com)

Vladimir VYCHUZHANIN
Doctor of Technical Sciences, Professor, Head of the Department of Information Technologies, Odessa Polytechnic State University, ave. Shevchenko, 1, Odessa, Ukraine, postal code 65001 (vint532@yandex.ua)

Natalia SHIBAYEVA
Candidate of Technical Sciences, Associate Professor of Information Technology, Odessa Polytechnic State University, ave. Shevchenko, 1, Odessa, Ukraine, postal code 65001 (nati.shibaeva@gmail.com)

Igor PETROV
Doctor of Technical Sciences, Professor of the Department of Maritime Transport of the National University «Odessa Maritime Academy», str. Didrichson, 8, Odessa, Ukraine, postal code 65029 (firmness@list.ru)

Alexander MAZURENKO
Student of the Interregional Academy of Personnel Management, str. Frometivska, 2, Kyiv, Ukraine, postal code 03039 (alexmazur@gmail.com)

Бібліографічний опис статті: Рудніченко М., Вичужанін В., Шибаєва Н., Петров І., Мазуренко О. Розробка проекту кроссплатформеної розподіленої інформаційної системи прототипування зовнішнього вигляду програмних застосувань. *Інформаційні технології та суспільство*. 2021. Вип. 1. С. 43–50. DOI: https://doi.org/10.32689/maup.it.2021.1.5

Bibliographic description of the article: Rudnichenko, M., Vychuzhanin, V., Shybaieva, N., Petrov, I., Mazurenko, O. (2021). Rozrobka proektu krossplatformenoi rozpodilenoi informatsiinoi systemy prototypuvannia zovnishnoho vyhliadu prohramnykh zastosuvan [Crossplatform distributed information system of prototyping software applications interface project]. *Informatsiini tekhnolohii ta suspilstvo – Information technology and society*, 1, 43–50. DOI: https://doi.org/10.32689/maup.it.2021.1.5

РОЗРОБКА ПРОЕКТУ КРОССПЛАТФОРМЕНОЇ РОЗПОДІЛЕНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПРОТОТИПУВАННЯ ЗОВНІШНЬОГО ВИГЛЯДУ ПРОГРАМНИХ ЗАСТОСУВАНЬ

Анотація. *Останні роки все більшої важливості набуває завдання превентивного узгодження та обговорення специфіки реалізації проектів програмних застосувань та систем з замовниками, що стає можливим на базі створення структурованих та гнучких прототипів інтерфейсів користувачів.* ***Метою*** *статті є опис особливостей проектування інформаційної системи прототипування інтерфейсу програмних застосувань. Реалізація поставленої мети передбачає вирішення низки* ***завдань****: 1) аналізу ключових концепцій та підходів до створення прототипів інтерфейсів програмних систем; 2) розробки схеми головного вікна інформаційної системи; 3) створенні об'єктної моделі системи на базі використання діаграм в нотації мови UML.* ***Наукова новизна.*** *У статті методика розробки прототипів інтерфейсів користувачів є розділеною на окремі архітектурні шаблони програмних застосувань, зокрема на десктопні, мобільні та веб-орієнтовані системи, що забезпечує цільових підхід до використання компонентів та елементів інтерфейсу. Як* ***висновок****, у статті наголошується, що розробка прототипів інтерфейсів користувачів для програмних застосувань та систем різної направленості та прикладної сфери є актуальним та затребуваним на практиці завданням, вирішення якого дозволяє забезпечити більш чітке та послідовне розуміння загального бачення проекту замовником та командою розробників. Створені об'єктні моделі роботи системи дозволяють виявити її архітектурні переваги та особливості, що полягають у гнучкості розподілу функціоналу та сутностей об'єктів. Наведені результати проектування інформаційної системи є основою для її програмної імплементації засобами сучасних мов програмування високого рівня, зокрема, мовою Javascript. Подальшим шляхом розвитку системи може стати більш цільових вектор впровадження у її архітектуру технологій розподілених систем та паралельних обчислень, що дозволить забезпечити комфортне її використання у асинхронному режимі на базі мікросервісного підходу.*

Ключові слова: *проектування інформаційних систем, об'єктно-орієнтоване проектування, прототипування інтерфейсу користувача*

CROSSPLATFORM DISTRIBUTED INFORMATION SYSTEM OF PROTOTYPING SOFTWARE APPLICATIONS INTERFACE PROJECT

Abstract. *In recent years, the task of preventive coordination and discussion of the specifics of the implementation of software applications and systems projects with customers has become increasingly important, which is possible through the creation of structured and flexible prototypes of user interfaces.* ***The aim*** *The purpose of the article is to describe the design features of the information system for prototyping the interface of software applications. Realization of the set purpose provides the decision of a number of* ***tasks****: 1) the analysis of key concepts and approaches to creation of prototypes of interfaces of software systems; 2) development of the scheme of the main window of the information system; 3) creating an object model of the system based on the use of diagrams in UML notation.* ***Scientific novelty.*** *In the article, the method of developing prototypes of user interfaces is divided into separate architectural templates of software applications, in particular desktop, mobile and web-oriented systems, which provides a targeted approach to the use of components and elements of the interface. In* ***conclusion****, the article emphasizes that the development of prototypes of user interfaces for software applications and systems of various directions and applications is a relevant and popular task, the solution of which allows to provide a clearer and more consistent understanding of the overall vision of the project by the customer and development team. The created object models of the system allow to reveal its architectural advantages and features, which consist in the flexibility of the distribution of the functionality and essences of the objects. These results of information system design are the basis for its software implementation by means of modern high-level programming languages, in particular, Javascript. A further target of the system development may be a more targeted vector of introduction into its architecture of distributed systems technologies and parallel computing, which will ensure its comfortable use in asynchronous mode based on the microservice approach.*

Key words: *information systems design, object-oriented design, user interface prototyping*

Актуальність проблеми. У розробці сучасного програмного забезпечення (ПЗ) ключових фактором виробничого процесу є проектування. Даний процес створення проекту системи часто підрозділяється на 2 окремі частини: проектування функціоналу і інтерфейсу [1].

Для проектування функціоналу використовуються існуючі нотації UML і IDEF0, є фактично промисловими стандартами при розробці ПЗ. У проектуванні графічного інтерфейсу користувача (GUI) в даний час відсутні усталені стандарти, проте існують окремі рекомендації, закони дизайну, прийоми, традиції, різні умови експлуатації ПЗ [2]. При цьому важливою частиною цього процесу є прототипування або макетування, тобто операція, яка полягає в створенні макета або прототипу майбутньої системи.

Макети в практиці бувають: паперовими, презентаційними, імітаційними та ін. Велика частина сучасних інтегрованих середовищ програмування (IDE) дозволяє розробляти деякі типи макетів, однак це сильно залежить від знань і навичок у використанні конкретної середовища і мови програмування. При цьому в разі створення великого проекту GUI реалізується окремим фахівцем, який не завжди повинен бути фахівцем в області розробки програмного коду. У зв'язку з цим на практиці розробнику зручно мати гнучкий інструмент для прототипування GUI, що підтримує можливості швидкого створення складних макетів, насичених елементами та об'єктами [3].

Більшість існуючих програмних продуктів, які застосовуються для вирішення завдань створення GUI, не є спеціалізованими і функціональними інструментами прототипування, однак дозволяють створювати прийнятні макети різного ступеня складності.

Останнім часом у зв'язку з підвищенням вимог до розробки інтерфейсів проявляються тенденції використання спеціалізованого ПЗ, націленого на створення прототипів GUI. Подібні системи підтримують створення прототипів для різних видів ПО: десктопних, веб і мобільних додатків [4].

Перевагами створення прототипу GUI є [5]:

– можливість побачити і протестувати інтерфейс програми, оцінивши зручність взаємодії його частин без необхідності програмування всього функціоналу, що знижує витрати по зміні GUI (чим швидше інтерфейс буде приведений до підсумкового виду, тим дешевше вийде підсумковий програмний продукт);
– наочна демонстрація можливостей замовнику;
– перевірка зручності використання GUI;
– тестування нестандартних підходів до зовнішнього вигляду інтерфейсу.

Саме прототипування GUI користувача дозволило сформуватися тенденції по відділенню розробки зовнішнього вигляду програми від безпосереднього програмування всього функціоналу. Фактично, це означає, що здійснюється не розробка дизайну інтерфейсу, на базі чого далі йде його реалізація, а паралельна розробка функціональної та графічної складової проекту [6].

Все це обумовлює актуальність проведення досліджень в даній області.

Аналіз останніх досліджень і публікацій. Прототип являє собою узагальнену модель, прообраз кінцевого ПО [7]. Прототипи найчастіше розрізняються за ступенем точності і близькості до підсумкового ПО, створюваному командою розробників або одним програмістом. Різні види прототипів GUI використовуються для різних цілей і призначені для вирішення різних завдань [8]. За стадії готовності прототипи поділяються на 3 етапи: концептуальні, інтерактивні і анімовані.

Прототипи надають зручну можливість для розробників не тільки для залучення в процес дизайну потенційних користувачів, а також і для оперативного створення потрібного ПО, відповідного очікуванням клієнта [9].

Прототипи ПО дозволяють спростити процес обговорення з замовником деталей реалізації, є наочною картиною для програмістів і здатні уявити ідею компанії [10].

Концептуальний прототип (КП) є структурованим схематичне відображення майбутніх екранів (форм) і розробляється на ранніх етапах проектування ПО [11].

КП слід робити завжди в разі розробки GUI нової програми. Це обумовлено тим, що подібний спосіб дозволить на ранніх стадіях вирішити більшу частину проблем з використанням функціоналу програм.

КП підходить для оперативного тестування ідей в рамках команди, що пов'язано з підтримкою швидкого розміщення основних елементів форм екранів. При цьому для розробки подібного прототипу не потрібно володіти навичками роботи зі спеціалізованими інструментами, досить скористатися підручними засобами. КП є незамінним в тих випадках, коли потрібно перенести призначені для користувача сценарії на екрани програми [12].

Перевагою КП є можливість підтримки режиму командної роботи. На практиці часто трапляється, що в разі візуалізації функціоналу потрібна підтримка окремих фахівців у вузьких областях. КП може виглядати як результат в області мислення групи людей і є досить ефективним методом вирішення проблем щодо використання проекту та пошуку рівноваги між цілями користувачів і цілями бізнесу [13].

Інтерактивний прототип (ІП) найчастіше збирається з екранів, які пройшли стадію КП. ІП стає наочним і реалістичним для подальшого його тестування на кінцевих користувачів [14].

Анімований прототип (АП) є самим високорівневим прототипом з усіх існуючих. Деякі з АП здатні досить точно моделювати роботу ПО. Ключовою перевагою розробки анімованого прототипу відрізняється рівнем інтерактивності. На даному етапі дизайнер активно працює, розробляючи аспект UX – взаємодія програми з користувачем, специфіка візуалізація [15].

Анімація є методом комунікації ПО з користувачем. Вона дозволяє користувачеві активно слідкувати за відображенням подій, що в рази збільшує юзабіліті інтерфейсу. Коли руху об'єктів в програмі

моделюють природні фізичні процеси, вони зчитуються мозком на початковому (підсвідомому) рівні, а користувач не замислюючись розуміє, що відбувається. Таким чином, рух процесу є орієнтованим на користувача [16].

Метою статті є розробка проекту кроссплатформеної розподіленої інформаційної системи прототипування зовнішнього вигляду програмних застосувань.

Виклад основного матеріалу. Розробку системи доцільно почати з макетування інтерфейсу, який є основним орієнтиром при побудові функціонального складу ПЗ [14–16].

Концептуальний прототип інтерфейсу системи, що розробляється в рамках даної статті наведено на рис. 1.

У лівому верхньому куті розташований компонент головного меню системи, праворуч від нього знаходиться палітра (панель) робочих компонентів, за допомогою яких буде здійснюватися обробка і зміна властивостей окремих елементів в робочому просторі.

Зліва розташовані 3 окремі вкладки, які можуть бути розгорнуті в панельному режимі і будуть необхідні для вибору з бібліотеки і використання відповідних елементів інтерфейсу на робочому полотні (розташоване посередині вікна макета).

У правій частині розташована вкладка властивостей обраного елемента, за допомогою якої користувачеві буде надана можливість змінювати і наносити окремі параметри текстових полів, міток і інших елементів інтерфейсу.

У нижній частині розташована панель управління і подій, на якій можна буде виконувати дії зі створення нових робочих полотен і їх конфігурації.

З метою формування більш чіткого уявлення про порядок використання системи розроблений загальний алгоритм взаємодії користувача з системою.

Спочатку виконується розгортання системи і установка всіх необхідних залежностей проекту.

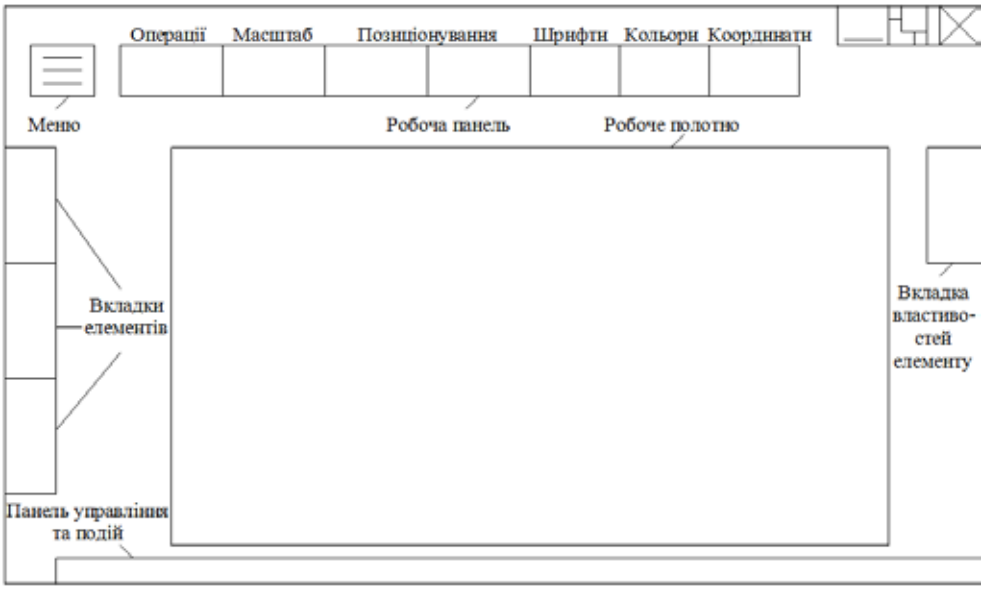


Рис. 1. Схема інтерфейсу системи

Після цього, коли система запущена на локальній станції і завантажений її інтерфейс, відбувається створення нового проекту прототипу інтерфейсу за вибором користувача.

Після цього створюється нове робоче полотно і за допомогою передбачених вище вкладок користувачем системи здійснюється пошук, вибір і компонування елементів інтерфейсу прототипу відповідно до його завданнями в робочому просторі.

В результаті, коли всі компоненти вибрані і додані до робочого полотна здійснюється настройка їх позиціонування і вибір параметрів відображення в робочому просторі.

Якщо всі елементи відображені належним чином і якщо користувач не має більше намірів по створенню нових прототипів в проекті, то система дозволяє здійснити операції по збереженню або експорту отриманих результатів в файли відповідних розширень і закінчити роботу з програмою (закрити проект). У разі, якщо елементи відображені некоректно, користувачем здійснюється попередня коригувальна операція. У разі, якщо користувач, наприклад, проектує прототипи інтерфейсу кількох веб-сто-

рінок, він може створити відповідну кількість робочих полотен в системі і редагувати їх окремим чином. З метою детального опису функціональних можливостей створюваної системи використовуємо нотацію Use case діаграм, що дозволить розділити специфікації для розробки системи і представити їх в ієрархічному вигляді. Розроблена діаграма варіантів використання системи приведена на рис. 2.

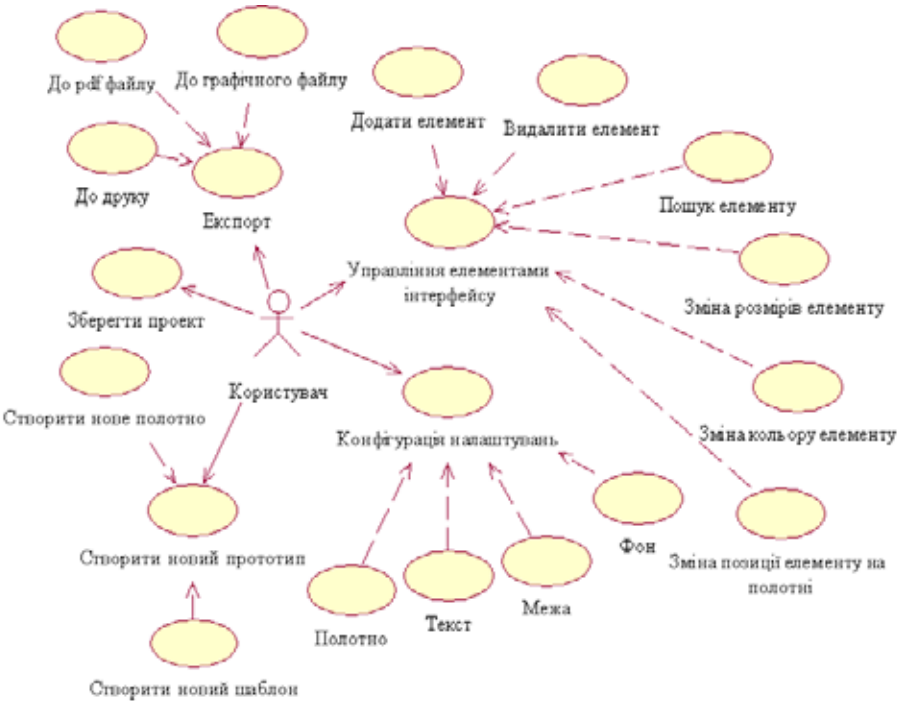


Рис. 2. Діаграма варіантів використання системи

Користувач має наступні основні можливості:

– створювати новий прототип інтерфейсу (в рамках нього він може створити нове полотно і новий шаблон);

– зберегти проект в файли відповідного типу (сериализация даних);

– завантажити проект з файлу;

– експортувати результати на активному робочому полотні в друк (на принтер, в графічний файл *.png і в *.pdf формат);

– виконувати управління елементами інтерфейсу створюваного прототипу (додавати, видаляти, змінювати розміри, кольори, позиції елемента на полотні, здійснювати пошук елемента в бібліотеці);

– конфігурувати налаштування системи по окремих елементах (робочого полотна, тексту або кордону).

Фрагмент діаграми класів наведено на рис. 3. Клас Canvas відповідає за відображення елементів інтерфейсу системи, головними його нащадками є класи Exporter, Browser та Configuration, що потрібні для реалізації функціоналу з створення окремих моделей прототипів згідно до дій користувача на головній формі системи.

Оскільки склад системи планується у вигляді великої кількості компонентів (модулів Node.js, програмних файлів і бібліотек) необхідно винести на таку діаграму тільки найбільш загальні з них. Розроблена діаграма основних компонентів системи приведена на рис. 4.

Дана діаграма складається з наступних загальних компонентів:

– MainProgram – пакет головних програмних файлів реалізації системи.

– LocalHost – локальний сервер, на якому має відбуватися розгортання проекту (базується на платформі NodeJS і Electron).

– Файли CSS і HTML – для забезпечення можливостей настройки і візуалізації інтерфейсу в веб-браузері.

– UserInterface – пакет, що містить всі view-елементи системи для їх коректної взаємодії.

– Recources – пакет, що містить графічні елементи для побудови прототипів інтерфейсу.

– Bootstrap – набір інструментів і стилів для верстки та розробки веб-додатків.

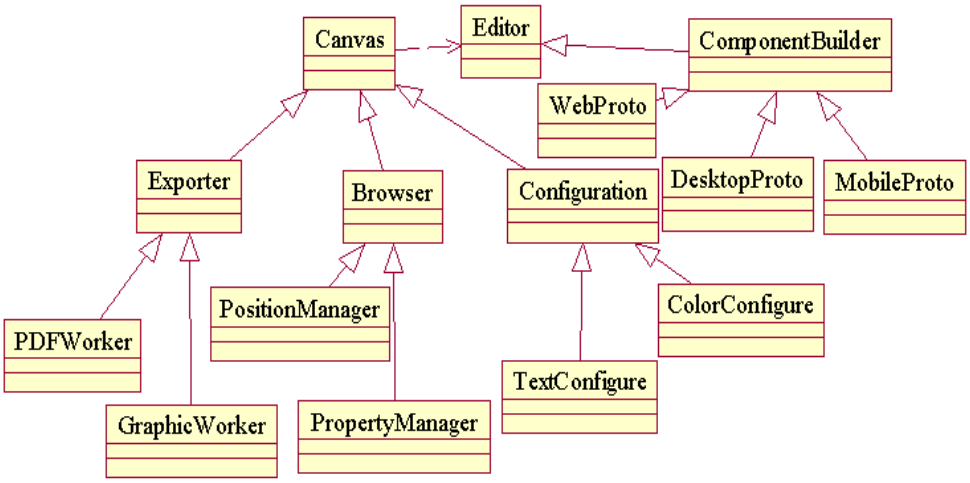


Рис. 3. Фрагмент діаграми класів системи

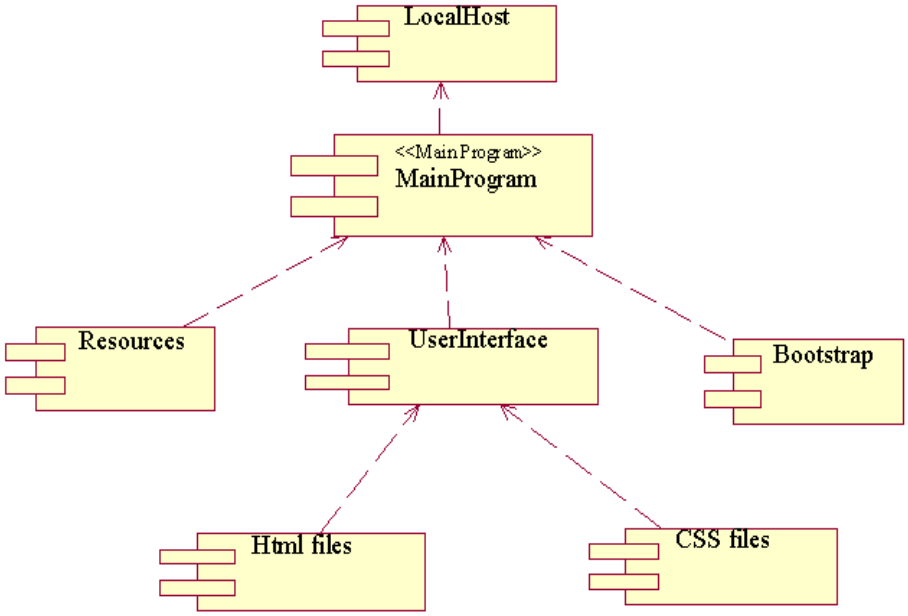


Рис. 4. Діаграма головних компонентів системи

Створені програмні файли розділені на 2 типу: контролери та подання. Основними методами розроблених контролерів є наступні:

– commonBehaviors, відповідає за загальну поведінку системи при її завантаженні;
– commonFunctions, реалізує функції відображення головного вікна системи;
– SVGTextLayout, імплементує функції підтримки і обробки векторної графіки;
– canvasHelper, відповідає за побудову базового контейнера для створення робочого полотна;
– canvasCareTaker, реалізує функції оновлення елементів в робочому просторі, де створюється прототип інтерфейсу.

Основними уявленнями є наступні:

– ApplicationPane, призначене для розмітки і розташування елементів головної робочої панелі;
– EditPageNoteDialog, виконує функції відображення вікна діалогу по модифікації налаштувань;
– ExportDialog, містить розмітку вікна обрання типу експорту створеного прототипу до файлу;
– PageDetailDialog, відповідає за зберігання елементів інтерфейсу вікна вибору типу контейнера;
– MainMenu, призначене для відображення елементів і складу головного меню системи.

Висновки та перспективи подальших досліджень. Розроблений проект кроссплатформеної розподіленої інформаційної системи прототипування зовнішнього вигляду програмних застосувань може бути використано різними групами користувачів для завдань швидкого створення концептуальних

інтерфейсів користувачів для різних цільових платформ, як то веб, десктоп чи мобільні програмні застосування. Завдяки ієрархічній структурі класів та використанню можливостей об'єктно-орієнтованого проектування стає можливим подальше наповнення проекту функціоналом шляхом гнучкого додавання нових чи розширення існуючих модулів системи. Можливими напрямками подальшого розвитку проекту є імплементація інших типів прототипів, підтримка додаткових засобів створення макетів та розширення компонентної бази окремих об'єктів інфографіки.

Список використаних джерел:

1. Слива М.В. Прототипування графічного інтерфейсу користувача як невід'ємна частина процесу розробки програмного забезпечення. *Вісник Нижневартовского державного університету*. 2013. № 1. С. 74–76.
2. Прототипування програми: від ідеї до робочого екрану. URL: https://habr.com/company/mobile_dimension/blog/327452/.
3. Мардан А. Швидке Прототипування з JS. Гнучка Розробка на JavaScript. М. : ІТУС, 2014. 236 с.
4. Немтінов В.А. Віртуальне моделювання, прототипування і промисловий дизайн. Тамбов : ТДТУ, 2019. 339 с.
5. Поляков О.М. Основи швидкого прототипування. Оренбург : ОДУ, 2014. 128 с.
6. Глухова Л.А. Технології розробки програмного забезпечення. Мінськ : БДУІР, 2014. 97 с.
7. Варфел Т. Прототипування. М. : Манн, Іванов і Фербер, 2013. 389 с.
8. Вершиніна Е.В. Огляд моделей життєвого циклу розробки програмного забезпечення. Нижній Новгород : НДУ ім. Н.І. Лобачевського, 2010. 38 с.
9. 20 інструментів для прототипування: від швидкого і брудного wireframe до функціонального прототипу. URL: https://medium.com/@denysergushki/.
10. Николенко О.И., Олейник П.П. Прототипирование и реализация графической формы заказа для информационной системы ресторанов быстрого питания. *Объектные системы*. 2015. № 10. С. 68–73.
11. Шибанов С.В., Пашкин А.А. Автоматизированное проектирование пользовательских интерфейсов. *Вестник Пензенского государственного университета*. 2016. № 16. С. 67–73.
12. Искра Н.А., Макоед В.Н., Куница Е.Ю. Изучение и оценка походов к разработке графического интерфейса пользователя. *Объектные системы*. 2015. № 10. С. 63–68.
13. Рудниченко Н.Д., Вычужанин В.В., Козлов А.Е. Модель front-end прототипа системы поддержки принятий решений мониторинга и управления рисками сложных технических систем. *Інформаційні управляючі системи та технології: Матеріали Міжнародної науково-практичної конференції (Іуст-Одеса-2015)*. 2015. С. 198–201.
14. Рудниченко Н.Д., Манькевич В.Н. Прототип программного обеспечения проектирования экспертных систем. *Інформатика, інформаційні системи та технології: тези доповідей п'ятнадцятої всеукраїнської конференції студентів і молодих науковців, м. Одеса, 27 квітня 2018 р.* Одеса, 2018. С. 71.
15. Rudnichenko N.D., Shibaeva N.O., Boyko V.D. Model prototype development of interactive interface of information system for monitoring ship technical system. *Інформаційні технології та комп'ютерна інженерія: матеріали статей п'ятої міжнародної науково-практичної конференції, м. Івано-Франківськ, 27-29 травня 2015 року.* Івано-Франківськ, 2015. С. 217–218.
16. Vychuzhanin V.V., Rudnichenko N.D., Shibaeva N.O., Boyko V.D. The development of user interface prototype of decision support system for risk management of complex technical systems. *Sustainability and Competitiveness in Business.* 2016. PP. 162–172.

References:

1. Sliva, M.V. (2013). Prototipuvannja grafichnogo interfejsu koristuvacha jak nevid'emna chastina procesu rozrobki programnogo zabezpechennja [Prototyping of the graphical user interface as an integral part of the software development process]. *Visnik Nizhnevartovskogo derzhavnogo universitetu – Herald of Nizhnevartovsk State University,* 1, 74–76 [in Ukrainian].
2. *Prototipuvannja programi: vid ideї do robochogo ekranu [Elektronij resurs]. [Prototyping of the program: from the idea to the working screen].* Rezhim dostupu: https://habr.com/company/mobile_dimension/ blog/327452/.
3. Mardan, A. (2014). *Shvidke Prototipuvannja z JS. Gnuchka Rozrobka na JavaScript* [Rapid Prototyping with JS. Flexible Development on JavaScript]. M.: ITUS [in Ukrainian].
4. Nemtinov, V.A. (2019). *Virtual'ne modeljuvannja, prototipuvannja i promislovij dizajn [Virtual modeling, prototyping and industrial design]*. Tambov: TDTU [in Ukrainian].
5. Poljakov, O.M. (2014). *Osnovi shvidkogo prototipuvannja [Basics of rapid prototyping].* Orenburg: ODU [in Ukrainian].
6. Gluhova L.A. (2014). *Tehnologiї rozrobki programnogo zabezpechennja [Software development technologies].* Mins'k: BDUIR [in Ukrainian].
7. Varfel T. (2013). *Prototipuvannja [Prototyping].* M: Mann, Ivanov i Ferber [in Ukrainian].
8. Vershinina, E.V. (2010). *Ogljad modelej zhittєvogo ciklu rozrobki programnogo zabezpechennja [Overview of software development lifecycle models].* Nizhnij Novgorod: NDU im. N.I. Lobachevs'kogo [in Ukrainian].
9. *20 instrumentiv dlja prototipuvannja: vid shvidkogo i brudnogo wireframe do funkcional'nogo prototipu [20 tools for prototyping: from fast and dirty wireframe to a functional prototype]*. Rezhim dostupu: https://medium.com/@denysergushki/.
10. Nikolenko, O.I., Olejnik P.P. (2015). Prototipirovanie i realizacija graficheskoj formy zakaza dlja informacionnoj sistemy restoranov bystrogo pitanija [Prototyping and implementation of a graphic order form for the information system of fast food restaurants]. *Objektnye sistemy – Object systems,* 10, 68–73 [in Russian].

11. Shibanov, S.V., Pashkin, A.A. (2016). Avtomatizirovannoe proektirovanie pol'zovatel'skih interfejsov [Automated design of user interfaces]. *Vestnik Penzenskogo gosudarstvennogo universiteta – Herald of Penza State University*, 16, 67–73 [in Russian].

12. Iskra, N.A., Makoed, V.N., Kunica, E.Ju. (2015). Izuchenie i ocenka pohodov k razrabotke graficheskogo interfejsa pol'zovatelja [Study and evaluation of campaigns to develop a graphical user interface]. *Objektnye sistemy*, 10, 63–68 [in Russian].

13. Rudnichenko, N.D., Vychuzhanin, V.V., Kozlov, A.E. (2015). Model' front-end prototipa sistemy podderzhki prinjatij reshenij monitoringa i upravlenija riskami slozhnyh tehnicheskih system [The front-end model of the prototype of the decision support system for monitoring and risk management of complex technical systems]. *Materiali Mizhnarodnoï naukovo-praktichnoï konferenciï «Informacijni upravljajuchi sistemi ta tehnologii» – Proceedings of the International Scientific and Practical Conference "Information Control Systems and Technologies",* 198–201 [in Russian].

14. Rudnichenko, N.D., Man'kevich, V.N. (2018). Prototip programmnogo obespechenija proektirovanija jekspertnyh system [Prototype software for designing expert systems]. Informatika, informacijni sistemi ta tehnologiï: tezi dopovidej p'jatnadcjatoï vseukraïns'koï konferenciï studentiv i molodih naukovciv. Odesa, 27 kvitnja 2018 – Informatics, information systems and technologies: abstracts of the reports of the fifteenth All-Ukrainian Conference of Students and Young Scientists. Odessa, April 27, 2018 [in Russian].

15. Rudnichenko, N.D., Shibaeva, N.O., Boyko, V.D. (2015). Model prototype development of interactive interface of information system for monitoring ship technical system. *Informacijni tehnologiï ta komp'juterna inzhenerija: materiali statej p'jatoï mizhnarodnoï naukovo-praktichnoï konferenciï, m. Ivano-Frankivs'k, 27-29 travnja 2015 roku – Information Technologies and Computer Engineering: Proceedings of the Fifth International Scientific and Practical Conference, Ivano-Frankivsk, May 27-29,* 217–218 [in English].

16. Vychuzhanin, V.V., Rudnichenko, N.D., Shibaeva, N.O., Boyko, V.D. (2016). The development of user interface prototype of decision support system for risk management of complex technical systems. *Sustainability and Competitiveness in Business*, 162–172 [in English].

УДК 004.932
DOI https://doi.org/10.32689/maup.it.2021.1.6

Микола РУДНІЧЕНКО
кандидат технічних наук, доцент кафедри інформаційних технологій, Державний університет «Одеська Політехніка», просп. Шевченко, 1, м. Одеса, Україна, індекс 65001 (nickolay.rud@gmail.com)

ORCID: https://orcid.org/0000-0002-7343-8076

Володимир ВИЧУЖАНІН
доктор технічних наук, професор, завідувач кафедри інформаційних технологій, Державний університет «Одеська Політехніка», просп. Шевченко, 1, м. Одеса, Україна, індекс 65001 (vint532@yandex.ua)

ORCID: https://orcid.org/0000-0002-5244-5808

Наталя ШИБАЄВА
кандидат технічних наук, доцент кафедри інформаційних технологій, Державний університет «Одеська Політехніка», просп. Шевченко, 1, м. Одеса, Україна, індекс 65001 (nati.shibaeva@gmail.com)

ORCID: https://orcid.org/0000-0002-7869-9953

Ігор ПЕТРОВ
доктор технічних наук, професор кафедри морських перевезень національного університету «Одеська морська академія», вул. Дідріхсона, 8, м. Одеса, Україна, індекс 65029 (firmness@list.ru)

ORCID: https://orcid.org/0000-0002-8740-6198

Роман ОГРОДЮК
студент, ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», вул. Фрометівська, 2, м. Київ, Україна, індекс 03039 (romaorgodukkk@gmail.com)

ORCID: https://orcid.org/0000-0041-1799-7678

Mykola RUDNICHENKO
PhD in Technical Sciences, Associate Professor of Information Technology, Odessa Polytechnic State University, ave. Shevchenko, 1, Odessa, Ukraine, postal code 65001 (nickolay.rud@gmail.com)

Vladimir VYCHUZHANIN
Doctor of Technical Sciences, Professor, Head of the Department of Information Technologies, Odessa Polytechnic State University, ave. Shevchenko, 1, Odessa, Ukraine, postal code 65001 (vint532@yandex.ua)

Natalia SHIBAYEVA
Candidate of Technical Sciences, Associate Professor of Information Technology, Odessa Polytechnic State University, ave. Shevchenko, 1, Odessa, Ukraine, postal code 65001 (nati.shibaeva@gmail.com)

Igor PETROV
Doctor of Technical Sciences, Professor of the Department of Maritime Transport of the National University «Odessa Maritime Academy», str. Didrichson, 8, Odessa, Ukraine, postal code 65029 (firmness@list.ru)

Roman OGRODUK
Student, Interregional Academy of Personnel Management, str. Frometivska, 2, Kyiv, Ukraine, postal code 03039 (romaorgodukkk@gmail.com)

Бібліографічний опис статті: Рудніченко М., Вичужанін В., Шибаєва Н., Петров І., Огродюк Р. Програмна розробка системи обробки та фільтрації растрових графічних зображень. *Інформаційні технології та суспільство*. 2021. Вип. 1. С. 51–58. DOI: https://doi.org/10.32689/maup.it.2021.1.6

Bibliographic description of the article: Rudnichenko, M., Vychuzhanin, V., Shybaieva, N., Petrov, I., Ohrodiuk, R. (2021). Prohramna rozrobka systemy obrobky ta filtratsii rastrovykh hrafichnykh zobrazhen [Rast graphic images processing and filtration system software]. *Informatsiini tekhnolohii ta suspilstvo – Information technology and society*, 1, 51–58. DOI: https://doi.org/10.32689/maup.it.2021.1.6

ПРОГРАМНА РОЗРОБКА СИСТЕМИ ОБРОБКИ ТА ФІЛЬТРАЦІЇ РАСТРОВИХ ГРАФІЧНИХ ЗОБРАЖЕНЬ

Анотація. *Враховуючи тенденцію активного зростання обсягів графічного контенту у глобальній мережі Інтернет та у прикладних сферах практичної діяльності різних галузей бізнесу, все більшої актуальності набувають інформаційні системи та сервіси обробки цифрових зображень, зокрема, що підтримують відповідні операції накладення різних типів фільтрів на растрову графіку.* ***Метою*** *статті є програмна розробка системи обробки та фільтрації растрових графічних зображень для швидкого редагування файлів контент менеджерами. Реалізація поставленої мети передбачає вирішення низки* ***завдань****: 1) аналізу особливостей складу та побудови графічних векторних зображень та сучасних графічних редакторів; 2) розробка та реалізація класової структури системи; 3) опис створеного інтерфейсу системи та головних функцій з накладення фільтрів на зображення.* ***Наукова новизна.*** *У статті описано можливості інтеграції ряду візуальних перетворень та фільтрації з підтримкою створення ефектів по згортці за допомоги обраної матриці ядра для растрових зображень рівного рівня деталізації та розподільної здатності. Як* ***висновок****, у статті наголошується, що процеси обробки графічних растрових зображень та додавання до них відповідних фільтрів мають пріоритетне значення для вирішення прикладних завдань контент-менеджерів веб-сайтів чи груп соціальних мереж. Перевагою використання розробленої системи обробки та фільтрації растрових графічних зображень є її висока швидкодія, продуктивність обробки паралельної обробки великої кількості зображень та портативність, завдяки чому систему можуть використовувати різні користувачі без необхідності встановлення додаткових засобів. Розроблена модульна структура система дозволяє гнучким чином доповнювати чи розширювати її функціонал, зокрема, доступна швидка інтеграція інших алгоритмів фільтрації даних до основної програмної логіки системи.*

Ключові слова: *обробка графічних зображень, фільтрація растрових зображень*

RAST GRAPHIC IMAGES PROCESSING AND FILTRATION SYSTEM SOFTWARE

Abstract. *Given the trend of active growth of graphic content on the World Wide Web and in the applied areas of practice of various industries, information systems and digital image processing services are becoming increasingly important, in particular, supporting appropriate operations for applying different types of filters to raster graphics.* ***The aim*** *of the article is to software development of a system for processing and filtering raster graphics for quick editing of files by content managers. Realization of the set purpose provides the decision of a number of* ***problems****: 1) the analysis of features of structure and construction of graphic vector images and modern graphic editors; 2) development and implementation of the class structure of the system; 3) description of the created system interface and the main functions for applying filters to the image.* ***Scientific novelty.*** *The article describes the possibilities of integrating a number of visual transformations and filtering with the support of creating convolution effects using the selected kernel matrix for raster images of equal level of detail and resolution. In* ***conclusion****, the article emphasizes that the processes of processing graphic bitmaps and adding appropriate filters to them are a priority for solving the application tasks of content managers of websites or groups of social networks. The advantages of using the developed system of processing and filtering of raster graphic images are its high speed, productivity of processing of parallel processing of a large number of images and portability, thanks to which the system can be used by different users without the need to install additional tools. The developed modular structure of the system allows to flexibly supplement or expand its functionality, in particular, quick integration of other data filtering algorithms into the basic software logic of the system is available.*

Key words: *graphic image processing, raster image filtering*

Актуальність проблеми. Після появи сучасних кольорових моніторів у світі зросли вимоги до відображення та використання графічної інформації. Сучасний користувач вже не здатний використовувати персональний комп'ютер, що не містить засобів графічного інтерфейсу.

Така інформація активно проникла до нашого буття, наприклад у сфері рекламування товарів чи послуг, публікації фотографії чи відео.

Найбільш затребувані області застосування – це наукова та прикладна сфери бізнесу, а також культурна та мистецька галузі, бо вони значним чином базуються на аналізі комп'ютерних зображень. Активно розвинутий потенціал ПК забезпечує велику базу для капіталовкладень, просування даного напрямку та його досконалості [1].

Слід зазначити, що сьогодні особливо доцільними та цікавими для інвесторів є проекти та компанії, які мають у своєму складі ідеї з розробки систем, які базуються на графічних вподобаннях користувачів, віртуальної реальності та стислого відображення великих даних [2].

Науковий термін комп'ютерна графіка (КГ) полягає у поєднанні процесів створення, зберігання і обробки цифрових моделей графічних об'єктів засобами ЕОМ. Під інтерактивною КГ часто розуміють розділ даної дисципліни, який ґрунтується на вивченні шляхів динамічного управління з боку корис-

тувача змістом та структурою графічного зображення, його властивостями, окремою формою, параметрами розміру засобами інтерактивних механізмів взаємодії [3].

Таким чином дослідження науково-практичного напрямку обробки графічних даних є у сучасних реаліях актуальною задачею.

Аналіз останніх досліджень і публікацій. Для комплексного аналізу даної галузі необхідно відзначити особливу рису КГ. Зокрема, графічні зображення можна періодично та поступово деталізувати, що підтримає можливості пошуку нових кольорових схем та їх відтінків. Графічні зображення, що розташовані у пам'яті комп'ютера, завжди являються не повною моделлю фрагменту реального світу, незалежно від типу їх отримання та візуалізації. Їх деталізація можлива тільки з закладеним при створенні ступенем, через що колірна гамма моделі буде не обумовленою заздалегідь [4].

Але, графічні зображення можуть бути відображені пам'яті ЕОМ 2 окремими способами для генерації 2 різних типів зображення: растрові чи векторні. Під растровими методами розуміють перелік способів уявлення зображення у вигляді деякої зведеної сукупності окремих пікселів різних кольорів або їх відповідних відтінків. Завдяки цьому стає можливим представлення графічного зображення, адже це імплементує наші зорові можливості, через тільки таку модель відображення даних користувачам [5]. Перевагою подібного методу є функціональна можливість отримання фотореалістичннх графічних зображень, що містять у собі значні можливості деталізації потрібних графічних зображень в різному кольоровому діапазоні. Недоліком цього підходу є те, що досить значний час необхідно отримати зазеленіть передбачений діапазон кольорів з метою зберігання зображення і задіяної оперативної пам'яті для його подальшої обробки х6ї.

Прості растрові картинки займають невеликий обсяг пам'яті (кілька десятків або сотень кілобайт). Зображення фотографічної якості часто вимагають кілька мегабайт. Растрове зображення після масштабування або обертання може втратити свою привабливість [7].

Для векторної графіки (ВГ) типовим є розбиття графічного зображення на частку графічних примітивів, це можуть бути окремі точки, прямі, дуги чи полігони. Завдяки цьому з'являється можливість обробляти не всі точки графічного зображення, а тільки координати та властивості вузлів примітивів (наприклад колір, зв'язок між узлами та характер їх відносин). Тобто ілюстрація ВГ являє собою деякий набір геометричних примітивів. Однак, слід зазначити, що важливою рисою є те, що об'єкти можуть бути задані незалежно один від одного, що може призводити до перекривання між собою [8].

В процесі зберігання растрових зображень (РЗ), користувачам необхідно обробляти файлами великого розміру. Це зумовлює доцільний аналітичний вибір потрібного формату файлу, яких є доволі багато. При цьому слід враховувати, що файли ВГ підтримують процедури зберігання в собі елементи РЗ. Але, у тому випадку, якщо не виникає викривлення в перенесенні кольорів, зображення може взагалі не містити об'єктів ВГ, тому доцільним є використання пріоритетних растрових формати [9].

Растровий графічний редактор (РГР) є прикладною програмою, що дозволяє виконувати процедури створення та обробки РЗ. Такі системи знайшли застосування в виробничих процесах художників-ілюстраторів або під час підготовки зображень до проведення друку відповідним способом чи на основі на фотопаперу, завантаження до мережі Інтернет, тощо.

РГР реалізують функціонал малювання, створення та редагування РЗ засобами екрану комп'ютера та миші. РГР підтримують засоби зберігання даних в різних растрових форматах, зокрема дуже популярними на практиці є JPEG та TIFF, перевагою яких є підтримка збереження РГ з невеликим зниженням якості шляхом використання алгоритмів стиснення даних з втратами. Формати PNG і GIF реалізують алгоритми стиснення без втрат, доволі якісним є формат BMP, який підтримує алгоритм стиснення але за замовчуванням є нестисненим форматом зображення [10]. РГР, на відміну від растрових, базуються на матриці крапок для відображення графічних файлів. Але суттєва більшість РГР містять додаткові векторні інструменти модифікації зображень як допоміжні.

РГР формалізує зображення на основі застосування кольорових крапок, що мають назву пікселів, які розташовані на сітці. Зокрема, зображення деревного листа може бути зазначено завдяки розташуванню та кольору точок сітки, що дозволяє створити графічне зображення стилю мозаїки [11].

Метою статті є програмна розробка системи обробки та фільтрації растрових графічних зображень для швидкого редагування файлів контент менеджерами.

Виклад основного матеріалу. В даний час існує велика кількість підходів до проектування та розробки програмних додатків, для чого використовуються різні програмні засоби, середовища розробки, мови програмування фреймворки і бібліотеки.

В результаті проведення аналізу особливостей сучасних засобів розробки в рамках даної роботи здійснено вибір мови програмування C#, середовища розробки MS Visual Studio та бібліотеки AForge. NET. яка призначена для розробників і дослідників в області комп'ютерного зору і штучного інтелекту –

обробки зображень, нейронних мереж, генетичних алгоритмів, нечіткої логіки, машинного навчання, робототехніки.

На головній формі системи використані наступні компоненти забезпечення користувальницького інтерфейсу:

1. ContextMenuStrip – доповнює елемент управління і розширює функціональні можливості ContextMenu; забезпечуючи зручний вибір опцій і зворотну сумісність для використання. Контекстне меню у системи відкривається в положенні покажчика та використовується для забезпечення управління у клієнтській області або елементами керування.

2. MenuStrip – служить для розміщення згрупованих команд. Елемент управління підтримує інтерфейс MDI, злиття меню, спливаючі підказки і переповнення. В рамках системи використовується для створення стандартного меню навігації між формами, що підтримує широкий набір можливостей компонування і призначеного для користувача інтерфейсу, таких як впорядкування і вирівнювання тексту і зображень, операції перетягування, інтерфейс MDI, переповнення і альтернативні режими доступу до пунктів меню, підтримки типового вигляду і поведінки операційної системи, а також для узгодженої обробки подій для всіх контейнерів аналогічно обробці подій для інших елементів управління.

3. ToolStrip – утворює загальну структуру, що об'єднує елементи призначеного для користувача інтерфейсу в панелі інструментів, рядка стану і меню.

4. StatusStrip – використовується у якості області, що відображається в нижній частині вікна, у яку виводяться інформаційні повідомлення та відомості про стан використання системи.

5. Panel – призначений для об'єднання в окремі групи інших елементів управління, зокрема контейнерів та їх складових.

Загалом створено 7 функціональних форм:

1. AboutForm – необхідна для виводу інформації довідки.
2. FourierDoc – забезпечує обробку даних по фільтру.
3. HistogramWindow – надає функцію побудови гістограми зображення.
4. ImageDoc – забезпечує обробку графічного зображення за наданими параметрами.
5. ImageStatisticsWindow – виконує перегляд статистичних даних та параметрів графічного зображення.
6. MainForm – надає доступ до основних функцій системи з редагування та обробки графічних зображень.
7. SelectImageForm – вікно обирання графічного зображення для подальшого виконання обробки.

Перелік фрагменту основних класів проекту у загальному вигляді наведено на рис. 1.

Рис. 1. Основні класи обробки даних системи

Кожен з класів реалізує підключення відповідних функцій бібліотеки AForge для розробляє мого програмного забезпечення, зокрема це можливості зміни яскравості, фільтрація кольорів, фільтрація частот, морфінг, насиченість, поріг та інші.

Схема викликів основних функціональних класів системи наведена на рис. 2. Головна форма здійснює виклики форм перегляду довідок, формування документів, накладання фільтрів, перегляду статистичних даних по зображенням (за червоним, зеленим на синім кольорами), вибору даних до імпорту у систему та побудови гістограми активного зображення.

Для забезпечення функцій експорту даних використано інтерфейс IDocumentalHost.

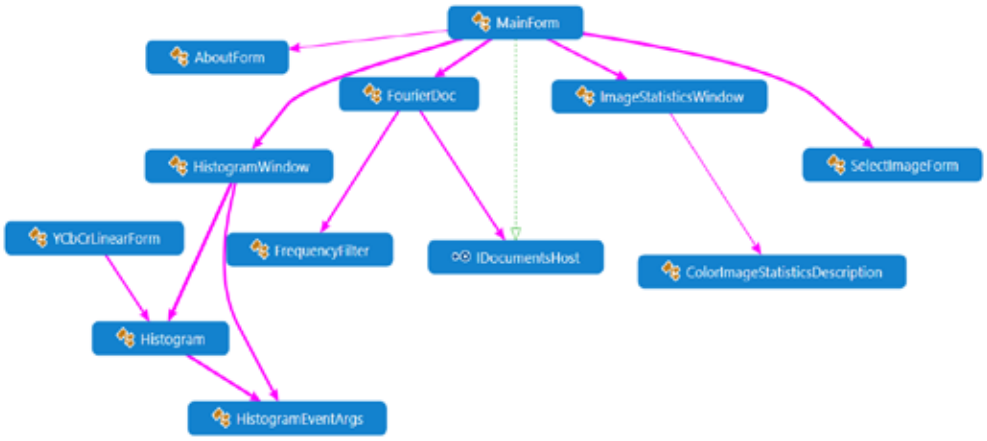


Рис. 2. Схема викликів основних функціональних класів системи

Перелік реалізованих у програмному забезпеченні опцій з кольорової фільтрації графічного зображення у головному меню користувача наведено на рис. 3.

Підтримуються можливості з перетворення кольорового зображення до відтінків сірого, сепії (оригінал стає більш тонованим, в коричневих тонах), інверсії кольорів, витягнення червоного, зеленого чи синього каналів, обертання, та кольорової фільтрації.

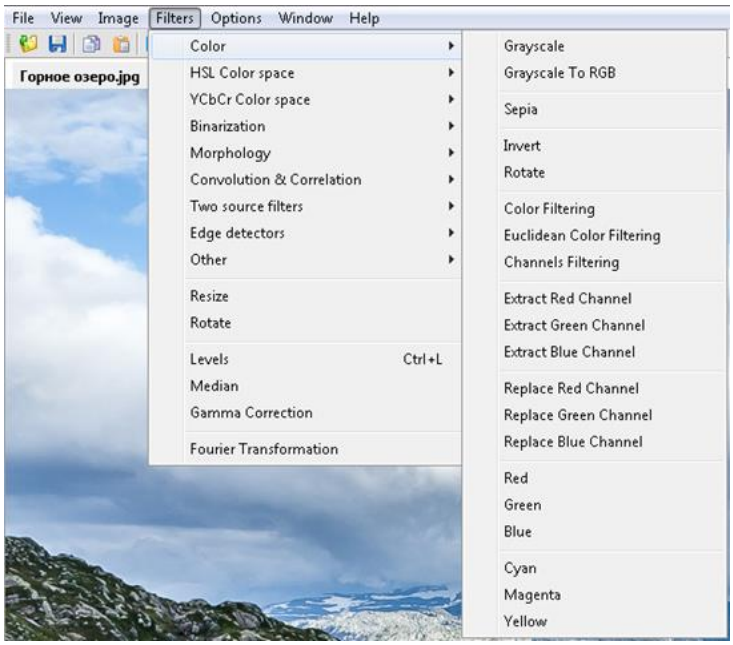


Рис. 3. Перелік реалізованих опцій з кольорової фільтрації графічного зображення

Додатково підтримуються опції з редагування графічного зображення згідно до фільтрів кольорів пурпурного, блакитного та жовтого, що додає відповідні ефекти до зразка.

Приклад інтерфейсу форми з виконання ефектів по згортці за допомоги обраної матриці ядра наведено на рис. 4. Користувач має можливість завдання розмірів ядра, зокрема передбачені опції 3 на 3, 5 на 5, 7 на 7, 9 на 9, 11 на 11, 13 на 13 та 15 на 15.

Збільшуючи розмір матриці досягається більша точність виконуваної операції, яку користувач може обрати у відповідному елементі інтерфейсу – ComboBox.

Для перегляду попереднього результату використовується компонент перегляду зображень PictureBox у групі Preview.

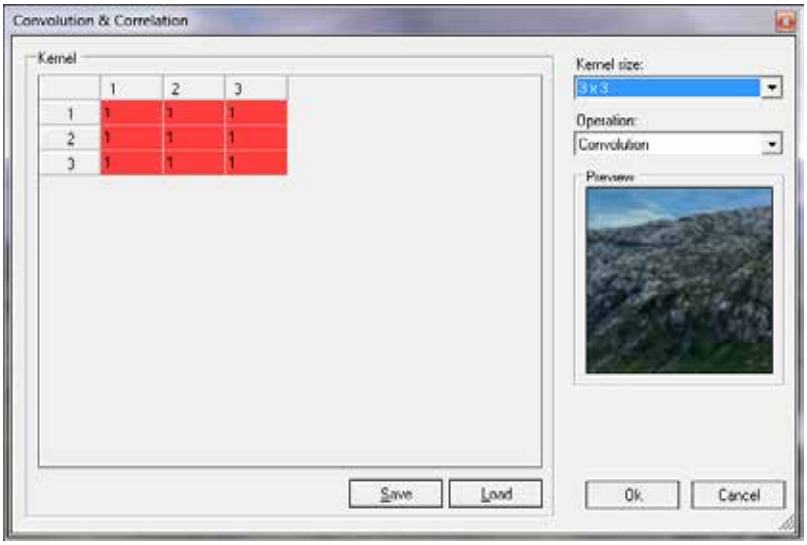


Рис. 4. Приклад інтерфейсу форми системи з виконання ефектів по згортці за допомоги обраної матриці ядра

Також передбачені кнопки завантаження до програми налаштувань (Load) та збереження відповідних користувальницьких дії.

Для підтвердження накладення відповідного ефекту чи його відміни використано кнопки «Ок» та «Cancel».

Приклад зміни рівнів червоного, зеленого та синього кольорів по відповідних каналах наведено на рис. 5.

Користувач системи може обрати відповідний колір, та вести значення вхідного та вихідного рівнів кольору від 0 до 255. Також, для більшої зручності реалізовано можливість прокручення компоненту у вигляді смуги, на базі елемента TrackBar. Попередній перегляд результатів можливий на базі використання компоненту PictureBox, а підтвердження операції зміни рівня чи її скасування відбувається завдяки використанню відповідних кнопок (компонентів типу Button з надписами «Ок» та «Cancel»).

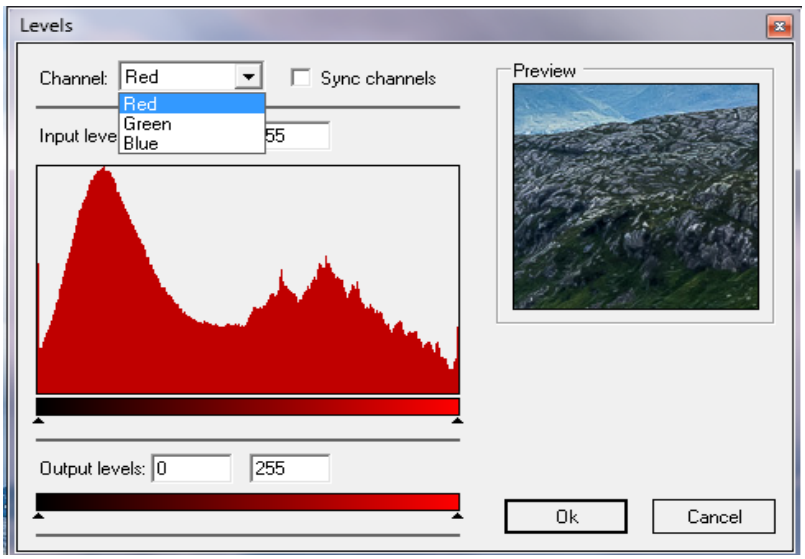


Рис. 5. Приклад зміни рівнів червоного, зеленого та синього кольорів по відповідних каналах

Форма перегляду статистики надає структурований опис ряду показників зображення. Дана форма дозволяє побачити загальні параметри зображення, налаштування червоного, зеленого та синього ко-

льорів з чорним та окремо до нього, насиченість і яскравість з чорним та без нього та інші статистичні дані по зображенню.

Окрім графіку гістограми також виводяться дані по обраному, за допомоги вказівника миші, пікселю.

Виводиться інформація щодо середнього значення, медіани, мінімального та максимального рівнів, процентилю. Користувач може переглянути рівень масштабу зображення, його роздільність у пікселях, поточні координати вказівника миші по x та y, параметри адитивної колірної моделі (RGB), що описує спосіб синтезу кольору, за якою червоне, зелене та синє світло накладаються разом, змішуючись у різноманітні кольори, параметри колірна моделі (HSL).

Колір визначається трьома характеристиками: кольоровим тоном, насиченістю (частиною чистого кольору, без домішки чорної та білої фарб), яскравістю (близькістю зображення до білого кольору) та параметри сімейства колірних просторів (YCbCr), які використовуються для передачі кольорових зображень. Y – компонента яскравості, Cb і Cr є синьою і червоною компонентами.

Передбачено можливості накладання ефекту розмиття, загострення, завдання користувальницького набору налаштувань згортки, обробки краєвих елементів та виконання обробки перетворення Гауса.

Підтримуються можливості з перетворення кольорового зображення до відтінків сірого, сепії (оригінал стає більш тонованим, в коричневих тонах), інвертації кольорів, витягнення червоного, зеленого чи синього каналів, обертання, та кольорової фільтрації.

Додатково підтримуються опції з редагування графічного зображення згідно до фільтрів кольорів пурпурного, блакитного та жовтого, що додає відповідні ефекти до зразка.

Реалізовано опції з бінарізації графічного зображення, зокрема, у системі підтримується звичайне розмивання та розмивання Байера, алгоритм розмивання Флойда-Стейнберга. Опція зміни порогу (Threshold) перетворює активний шар графічного кольорового чи сірого зображення в чорно-біле зображення, де білий колір представляє всі точки, чиї значення потрапили в діапазон порога, а чорний – всі інші точки. Морфологічні операції також можуть бути застосовані до напівтонових зображень таким чином, що їх функції перенесення світла невідомі і тому їх абсолютні значення пікселів не мають значної важливості. Зокрема підтримується можливість дилатації, яка використовує обраний структурний елемент для розширення форм зображення.

Висновки та перспективи подальших досліджень. Розроблена система обробки та фільтрації растрових графічних зображень має відкритий вихідний код, орієнтована на використання під управлінням операційної системи Windows, є швидкою у використанні, займає малу кількість апаратних ресурсів (до 200 мегабайт оперативної пам'яті у режимі обробки великих зображень роздільністю більше 4 000 пікселів), не потребує встановлення додаткових компонентів окрім стандартного.NET Framework та може ефективним чином використовуватися для швидкого редагування файлів контент менеджерами. Подальшим шляхом розвитку системи може бути її наповнення більшим функціоналом з точки зору редагування зображень та їх конвертації.

Список використаних джерел:

1. Симонович С.В. Графічні засоби обробки даних. М. : Наука, 2009. 479 с.
2. Горячев А. Практикум з інформаційних технологій. М. : Лабораторія Базових Знань, 2009. 272 с.
3. Шафрін Ю.А. Технології комп'ютерної графіки. М. : Лабораторія Базових Знань, 2008. 704 с.
4. Мураховський В.І. Комп'ютерна графіка: Популярна енциклопедія. М. : АСТ, 2002. 640 с.
5. Гукасов А. С. All of Photoshop. М. : Ракурс, 2005. 81 с.
6. Мосту В. Комп'ютерна графіка. Енциклопедія. СПб : Пітер, 2013. 768 с.
7. Роджерс Д. Математичні основи машинної графіки. М. : Світ, 2011. – 604 с.
8. Тихомиров Ю. Програмування тривимірної графіки. СПб : ВН – Санкт-Петербург, 2008. 256 с.
9. Стругайло В.В. Обзор методов фильтрации и сегментации цифровых изображений. *Машиностроение и компьютерные технологии*. 2012. № 5. С. 17.
10. Тамьяров А.В., Шестов Р. В. Анализ методов предварительной обработки изображения на основе усредняющих фильтров. *Вестник Волжского университета им. В. Н. Татищева*. 2011. № 18. С. 109–115.
11. Коваль Ю.А., Филиппов М.В. Метод предварительной фильтрации изображений для повышения точности распознавания образов. *Инженерный журнал: наука и инновации*. 2014. № 36. С. 12.

References:

1. Simonovich, S.V. (2009). *Grafichni zasobi obrobki danih* [Graphic data processing tools]. M.: Nauka [in Ukrainian].
2. Gorjachev, A. (2009). *Praktikum z informacijnih tehnologij* [Workshop on information technology]. M.: Laboratorija Bazovih Znan '[in Ukrainian].
3. Shafrin, Ju.A. (2008). *Tehnologii komp'juternoї grafiki* [Computer graphics technology]. M.: Laboratorija Bazovih Znan' [in Ukrainian].

4. Murahovs'kij, V.I. (2002). *Komp'juterna grafika: Populjarna enciklopedija* [Computer Graphics: A popular encyclopedia]. M.: AST [in Ukrainian].

5. Gukasov, A.S. (2005). *All of Photoshop*. M.: Rakurs [in Ukrainian].

6. Mostu, V. (2013). *Komp'juterna grafika. Enciklopedija* [Computer graphics. Encyclopedia]. SPb: Piter [in Ukrainian].

7. Rodzhers, D. (2011). *Matematichni osnovi mashinnoï grafiki* [Mathematical foundations of machine graphics]. M.: Svit [in Ukrainian].

8. Tihomirov, Ju. (2008). *Programuvannja trivimirnoï grafiki* [Programming of three-dimensional graphics]. SPb: BH – Sankt-Peterburg [in Ukrainian].

9. Strugajlo, V.V. (2012). Obzor metodov fil'tracii i segmentacii cifrovyh izobrazhenij [An overview of digital image filtering and segmentation techniques]. *Mashinostroenie i komp'juternye tehnologii – An overview of digital image filtering and segmentation techniques,* 5, 17 [in Russian].

10. Tam'jarov, A.V., Shestov, R.V. (2011). Analiz metodov predvaritel'noj obrabotki izobrazhenija na osnove usrednjajushhih fil'trov [Analysis of image pretreatment methods based on averaging filters]. *Vestnik Volzhskogo universiteta im. V. N. Tatishheva – Herald of the Volga University,* 18, 109–115 [in Russian].

11. Koval, Ju.A., Filippov, M.V. (2014). Metod predvaritel'noj fil'tracii izobrazhenij dlja povyshenija tochnosti raspoznavanija obrazov [Filippov MV An image pre-filtering method to increase image recognition accuracy]. *Inzhenernyj zhurnal: nauka i innovacii – Engineering Journal: Science and Innovation,* 36, 12 [in Russian].

УДК 619.12
DOI https://doi.org/10.32689/maup.it.2021.1.7

Руслан СКУРАТОВСЬКИЙ
викладач кафедри обчислювальної математики і компютерного моделювання, ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», вул. Фрометівська, 2, м. Київ, Україна, індекс 03039

ORCID: https://orcid.org/0000-0002-5692-6123

Ruslan SKURATOVSKYI
Lecturer at the Department of Computational Mathematics and Computer Modeling, Interregional Academy of personnel management, 2 Frometivska Street, Kyiv, Ukraine, postal code 03039

Бібліографічний опис статті: Скуратовський Р. Підхід до перевірки суперсингулярності еліптичних кривих і обчислення їх порядку. *Інформаційні технології та суспільство*. 2021. Вип. 1. С. 59–69. DOI: https://doi.org/10.32689/maup.it.2021.1.7

Bibliographic description of the article: Skuratovskyi, R. (2021). Pidkhid do perevirky supersynhuliarnosti eliptychnykh kryvykh i obchyslennia yikh poriadku [Approach to checking the supersingularity of elliptic curves and calculating their order]. *Informatsiini tekhnolohii ta suspilstvo – Informati on technology and society*, 1, 59–69. DOI: https://doi.org/10.32689/maup.it.2021.1.7

ПІДХІД ДО ПЕРЕВІРКИ СУПЕРСИНГУЛЯРНОСТІ ЕЛІПТИЧНИХ КРИВИХ І ОБЧИСЛЕННЯ ЇХ ПОРЯДКУ

Анотація. *Більшість криптосистем сучасної криптографії природним чином можна «перекласти» на еліптичні криві. Ми розглядаємо алгебраїчні криві Едвардса над скінчнним полем, які на даний час є одним з найбільш перспективних носіїв множин точок, що використовують для швидких групових операцій [1; 2; 14], які наявні в асиметричних криптосистемах, зокрема для побудови випадкових криптостійких послідовностей.*

Показано, що проективна крива $E_{a,d}$ не є еліптичною. Метою роботи є пошук критерію і достатніх умов суперсингулярності кривої Едвардса і еліптичної кривої у формі Монтгомері над простим полем $\mathbb{F}_p$, а потім узагальнення цього критерія для скінченного алгебраїчного розширення цього поля до F_{p^n}. Отриманий результат дозволяє побудувати всі суперсингулярні криві Едварса і Монтгомері не розкладаючи на множники многочлен від x який наявний у записі кривої.

В роботі [10] було представлене доведення суперсингулярності кривої E_d лише для коефіцієнтів $d=2,\ d=2^{-1}$ над $\mathbb{F}_p$, нашою ж метою є дослідження всіх коефіцієнтів при яких ця крива є суперсингулярною. В нашій роботі знайдено критерії і достатні умови суперсингулярності кривої Едвардса і еліптичної кривої у формі Монтгомері над полем F_{p^n}, тобто досліджено при яких коефіцієнтах отримується пара кривих зі слідом Фробеніуса рівним 0. При цьому криві Монтгомері над полем характристики 2 мають нульовий j-інваріант. Знайдено не тільки конкретну множину коефіцієнтів з відповідними характеристиками полів при яких ці криві є суперсингулярними а й загальну формулу за якою можна визначити чи є крива суперсингуярною над даним полем чи ні. В роботі узагальнено результат про суперсингулярність кривої над $\mathbb{F}_p$ отриманий в [10] для коефіцієнтів $d=2,\ d=2^{-1}$ на випадок довільного розширення простого поля $\mathbb{F}_{p^n}$ та уточнено формулювання теореми 3 з [10]. Зроблено аналогічне дослідження і для еліптичних кривих у формі Монтгомері.

Ключові слова: *скінченне поле, еліптична крива, крива Едвардса, порядок кривої, квадратичний лишок, символ Лежандра, алгебраїчна крива, група точок еліптичної кривої, порядок точки, криві кручення.*

APPROACH TO CHECKING THE SUPERSINGULARITY OF ELLIPTIC CURVES AND CALCULATING THEIR ORDER

Abstract. *Most cryptosystems in modern cryptography can naturally be "translated" into elliptical curves. We consider algebraic Edwards curves over a finite field, which are currently one of the most promising carriers of sets of points used for fast group operations [1; 2; 14], which are available in asymmetric cryptosystems, in particular for the construction of random cryptocurrency sequences.*

It is shown that the projective curve $E_{a,d}$ is not elliptical. The aim of this work is to find a criterion and sufficient conditions for the supersingularity of the Edwards curve $\mathbb{F}_p$ and an elliptic curve in the form of Montgomery over a simple field and then generalize this criterion for a finite algebraic extension of this field to F_{p^n}. The obtained result allows us to construct all supersingular curves of Edwards and Montgomery without factorizing the polynomial from which the curve is present in the record.

In [10], the proof of the supersingularity of a curve E_d was presented only for the coefficients $d=2,\ d=2^{-1}$ over $\mathbb{F}_p$, and our goal is to study all the coefficients at which this curve is supersingular. In our work we found the criteria and sufficient conditions for the supersingularity of the Edwards curve and the elliptic curve in the form of Montgomery over the field F_{p^n},

ie we investigated at what coefficients a pair of curves with a Frobenius trace equal to 0. The Montgomery curves over the field of characteristic 2 have zero j-invariant. Not only a specific set of coefficients with the corresponding characteristics of the fields at which these curves are supersingular is found, but also a general formula by which it is possible to determine whether the curve is supersingular over a given field or not. The paper summarizes the result on the supersingularity of the curve over $\mathbb{F}_p$ *obtained in [10] for the coefficients* $d=2,\ d=2^{-1}$ *in the case of arbitrary expansion of a simple field* $\mathbb{F}_{p^n}$ *and clarifies the formulation of Theorem 3 from [10]. A similar study was performed for elliptic curves in the form of Montgomery.*

Key words: *finite field, elliptic curve, Edwards curve, curve order, quadratic excess, Legendre symbol, algebraic curve, group of elliptic curve points, point order, torsion curves.*

Вступ. Вперше криві Едвардса E_d представлено Едвардсом в роботі [1] і розвинуті в роботі Бернштейна і Ланге [2]. Відомо, що суперсингулярні криві, на відміну від несуперсингулярних, над алгебраїчно замкненим полем, зокрема, над $\mathbb{C}$, мають не комутативне кільце ендоморфізмів *End* ($\mathbb{C}$). Внаслідок чого суперсингулярні криві окрім n -мультиплікативного множення, наділені ще і комплексним множенням.

Ще більш складні властивості суперсингулярні криві мають над скінченними полями. Ці властивості ще далеко не повністю вивчено, а класи суперсинулярних кривих над $\mathbb{F}_{p^n}$ ще не знайдено. Ці властивості викликають інтерес як з точки зору теорії кілець ендоморфізмів, так і з точки зору алгебраїчної геометрії. Їх дослідження є одною з цілей даної роботи.

Одною з головних задач даного дослідження є узагальнення результата про суперсингулярність кривої отриманого в [10] для коефіцієнтів $d=2,\ d=2^{-1}$ над $\mathbb{F}_p$ на випадок довільного не простого поля $\mathbb{F}_{p^n}$ та виправлення неточності у кількості точок афінної кривої Едвардса над полем характеристики $p\equiv 7(\mathrm{mod}8)$, яка була в теоремі 3 з [10]. Окрім цього метою нашого дослідження є пошук всієї множини параметрів при яких крива E_d стає суперсингулярною. Не менш важливою метою цієї роботи є проведення аналогічного дослідження для еліптичних кривих у формах Монтгомері і Веєрштрасса. Суперсингулярність кривих Едвардса досліджувалася в [10] лише для простих полів $\mathbb{F}_p$, тому *наша мета дослідити її* над скінченим алгебраїчним розширенням тобто над полем – $\mathbb{F}_{p^n}$.

Актуаліність даного питання полягає в тому, що в еліптичній криптографії дуже важливо знати ті криві, які є суперсингулярними (ті, що мають нульовий *j*-інварівант при $p=2$), бо вони є крипографічно слабкими. Корисною є відсутність ділення точки на 2 при виконанні подвоєння точки на суперсингулярних кривих. Водночас одними з найбільш придатних для швидких обчислень є криві Едвардса [14], що потребують найменших обчислювальних затрат для проведення групової операції додавання точок а також подвоєння точок.

Суперсингулярність кривих Едвардса раніше досліджувалася лише в [10] і лише для простих полів $\mathbb{F}_p$ і автори обмежилися доведенням суперсингулярності лише для кривої з коефіцієнтами $d=2,\ d=2^{-1}$, *тому* ***задача дослідження*** *її над скінченим алгебраїчним розширенням тобто над полем –* $\mathbb{F}_{p^n}$ ***є новою***.

Авторами статті [10] було знайдено суперсингулярність кривої E_d лише для коефіцієнтів $d=2,\ d=2^{-1}$ і $d=(\sqrt{3}\pm 2)/(\sqrt{3}-(\pm 2))$ над $\mathbb{F}_p$ при відповідних p, **метою** нашої статті є пошук множини всіх коефіцієнтів при яких ця крива є суперсингулярною.

Метою роботи є пошук критерію і достатніх умов суперсингулярності кривої Едвардса і еліптичної кривої у формі Монтгомері над полем F_{p^n}, тобто досліджено при яких коефіцієнтах над полями відповідної характристики ці криві мають нульовий *j*-інварівант.

Властивості скрученої кривої Едвардса.

З точки зору алгебраїчної геометрії, крива Едвардса не є еліптичною, бо є сингулярною.

Криві Едвардса також як і скручені криві Едвардса мають афінне представленя ізоморфне деякій афінній частині еліптичної кривої, що містить в порядку групи кривої множник 4, що доведено автором в [8] у твердженні про необхідні і достатні умови існування точок 8-го порядку.

Згідно теореми Хассе порядок групи алгебраїчної кривої $N_E=p+1\pm t$. Якщо слід Фробеніуса $t=0$, то маємо вироджену пару кривих (крива *E* і крива зі скрутом), тому порядки обох кривих співпадають і рівні $N_E=p+1$. Такі криві є суперсингулярними кривими. Таким чином, порядок групи точок для суперсингулярних кривих над простим полем рівний $N_E=p+1$, тому період генератора криптостійкої послідовності [7] є мінімальним серед еліптичних кривих над заданим полем.

Дані криві задовольняють самим сильним вимогам по стійкості до MOV-атаки, про що неодноразово зазначалось у працях вітчизняних [7; 9; 11; 12; 20] та закордонних вчених [3; 4; 21]: неможливість застосувати цей метод забезпечується через відсутність можливості вкласти групу точок кривої в мультипликативну групу поля достатньо малого порядку. Для цього достатньо, щоб мінімальне натуральне t, $p^t\equiv 1 mod|N_E|$ було достатньо великим. Для скручених кривих Едвардса $t=|N_E|-1$, що є максимально можливим. Великою перевагою є можливість побудови скрученої кривої Едвардса порядку $4p$, $p\in\mathbf{P}$, тому не може бути використана атака підміни точки, що належить рекомендованій кривій на точку

зі скрученої кривої тобто так званої кривої кручення. Також це не дає противнику використовувати китайську теорему про лишки для визначення секретного ключа [4], бо маємо великий множник p в $|N_E|$. З точки зору алгебраїчної геометрії, крива не є еліптичною, бо є сингулярною.

Також важливість визначення не суперсингулярності еліптичної кривої для побудови генераторів випадкових чисел є показано в роботі [5] для побудови "elliptic curve power generator" генератора "Naor–Reingold" використовують не суперсингулярну еліптичну криву і її точку P великого простого порядку, якщо ж порядок l точки P не простий, то вибирають початкове заповнення e таке, що $(e,l)=1$. У випадку побудови такого генератора ще важливо і те, що для суперсингулярних кривих відсутня операція ділення при подвоєнні точки.

Особливі точки скрученої кривої Едвардса.

Розглянемо скручену криву Едвадрса $E_{a,\mathrm{d}}$

$$ax^2+y^2=1+dx^2y^2,\ a,d\in F_p^*,\ ad(a-d)\neq 0,\ d\neq 1,\ p\neq 2,\ a\neq d, \tag{1}$$

При $a=d$ крива перетворюється до вигляду $ax^2+y^2=1+ax^2y^2$ звідки $ax^2-ax^2y^2-1+y^2=0$ або $ax^2(1-y^2)-(1-y^2)=0$. Отже, крива розкладається у добуток двох пар прямих $(ax^2-1)(y^2-1)=0$. Якщо $a=1$, то $E_{a,\mathrm{d}}$ перетворюється у криву E_{d}. З умови гладкості знаходимо особливі точки афінної кривої.

Для цього зробимо проективізацію кривої. Нехай $x=\frac{X}{Z}, y=\frac{X}{Z}$, тоді $a\frac{x^2}{z^2}+\frac{y^2}{z^2}=1+d\frac{x^2y^2}{z^4}$, звідси $F(x,y,z)=ax^2z^2+y^2z^2=z^4+dx^2y^2$ перевіримо умови гладкості (для алгебраїчних кривих поняття гладкості і нормальності співпадають.

Пошукаємо інші корені в припущенні $z=0$ коренем є також точка $(0,y_0,0)=(0,1,0)$. Тобто маємо 2 особливі точки $p_1=(1,0,0)$ і $p_2=(0,1,0)$. Це прості особливості.

Особливими точками є (нескінченно віддаленні точки) $(1,0,0)$ і $(0,1,0)$, тому маємо особливості на нескінченності у відповідних афінних компонентах

$$A^1: az^2+y^2z^2=z^4+dy^2 \text{ і } A^2:\ ax^2z^2+z^2=z^4+dx^2.$$

Опишемо будову локального кільця в точці p_1, його елементами є дроби з функцій виду $F(x,y,z)=\frac{f(x,y,z)}{g(x,y,z)}$, знаменники яких не обертаються в 0 у точці p_1. Локальне кільце, що має особливості в 2-ух точках має функції у яких знаменники не діляться на $(x-1)(y-1)$.

Знайдемо $\delta_{\mathrm{p}}=\dim\overline{\mathcal{O}_{\mathrm{p}}}/\mathcal{O}_p$, де $\mathcal{O}_{\mathrm{p}}$ – локальне кільця в особливій точці p, це кільце породжується відношеннями регулярних функцій $\mathcal{O}_{\mathrm{p}}=\left\{\frac{f}{g}:(g,(x-1)(y-1))=1\right\}$, $\overline{\mathcal{O}}_{\mathrm{p}}$ – ціле замикання локального кільця в особливій точці p. Позначимо $\delta_p=\dim\overline{\mathcal{O}_p}/\mathcal{O}_p=1$ розмірність фактора як векторного простору. Оскільки, базис розширення $\overline{\mathcal{O}}_p$ над $\mathcal{O}_p$ складається з одного елемента в кожній з двох особливих точок, то $\delta_p=1$.

Отже, підрахуємо род кривої за Рідом [13] $\rho^*(C)=\rho_\alpha(\mathrm{C})-\sum_{p\in E}\delta_p=\ =\frac{(n-1)(n-2)}{2}-\sum_{p\in E}\delta_p=3-2=1$ бо $n=4$. де $\rho_\alpha(C)$ – арифметичний рід кривої C, параметр $n=degC=4$.

Оскільки вона роду 1, то вона ізоморфна плоскій кубічній кривій але не є еліптичною, бо має особливості в проективній частині. Крива Едварса як і скручена крива Едвардса ізоморфна деякій афінній частині еліптичної кривої. Нормалізація кривої Едвардса – крива в формі Веєрштраса, що запропонована Монтгомері E_M [2].

Суперсингулярні криві Едвардса і еліптичні криві в формі Монтгомері.

Для виявлення суперсингулярних кривих, згідно дослідженням Кобліца [16], можна скористатися пошуком таких параметрів при яких крива і відповідна їй крива зі скрутом мають однакові кількості розв'язків.

Як показано в [2] крива $E_{1,d}$ є кривою кручення для $E_{1,d^{-1}}$. Також в більш загальному випадку для кривої $E_{a,d}$ перехід до кривої кручення задається відображенням $(\overline{x},\overline{y})\mapsto(x,y)=\left(\overline{x},\frac{1}{\overline{y}}\right)$ [2]. Тому скористаємося цим відображенням для пошуку суперсингулярних кривих. Ми виявили суттєву неточність в роботі [10], в умові суперсингулярності для кривої Едвардса $E_{1,d}$. Більш точно, якщо $p\equiv -3(mod 8)$, то не маємо виродженої (суперсингулярної) пари кривих, не дивлячись на те, що це стверджують-

ся в теоремі 3 з [10]. Крім того якщо $p \equiv 7(mod 8)$, то порядки пари скручених кривих є наступними $N_{E_2} = N_{E_2^{-1}} = p-3$, що не співпадає з p + 1, як це стверджується в теоремі 3 з [10]. Це підтверджують приклади, так якщо $p=31$, то $N_{E_2} = N_{E_2^{-1}} = p-3=28$ над $\mathbb{F}_p$, що не дорівнює $p+1$. Також ми узагальнили теорему 3 з [10], отримавши умови суперсингулярності цих кривих не тільки для простого поля а й для його алгебраїчного розширення $\mathbb{F}_{p^n}$ довільної скінченної степені n.

Зауваження 1. Має місце симетрія квадратів лишків:

$$(\frac{p-1}{2}-k)^2 \equiv (\frac{p-1}{2}+1+k)^2 (\mathrm{mod}\, p), 0 \le k \le \frac{p-1}{2}.$$

Доведення. Справді, виконується конгруенція

$$(\frac{p-1}{2})-k = p-((\frac{p-1}{2})+1+k) \equiv -((\frac{p-1}{2})+1+k)(\mathrm{mod}\, p).$$

Отже,

$$(\frac{p-1}{2}-1)^2 \equiv (\frac{p-1}{2}+2)^2, (\frac{p-1}{2}-2)^2 \equiv (\frac{p-1}{2}+3)^2, \ \ldots, (\frac{p-1}{2}-k)^2 \equiv (\frac{p-1}{2}+k+1)^2 (\mathrm{mod}\, p).$$

Без квадратів маємо антисиметричну конгруенцію

$$(\frac{p-1}{2}-k) \equiv -(\frac{p-1}{2}+1+k)(mod p).$$

Нагадаємо лему про суму степенів [6].

Лема 1. Нехай $k \in \mathbb{N}$, $p \in \mathbb{P}$. Тоді

$$\sum_{k=1}^{p-1} k^n \equiv \begin{cases} 0\,(mod p), & n \nmid (p-1), \\ -1\,(mod p), & n \vdots (p-1), \end{cases}$$

Теорема. Якщо $p \equiv 3(mod\, 4)$ і p – просте число, то для $d=2$ і $d=2^{-1}$ кількості точок кривої $x^2+y^2=1+dx^2y^2$ та кривої $x^2+y^2=1+d^{-1}x^2y^2$ над F_p співпадають і дорівнюють $N_E = p+1$ якщо, $p \equiv 3(\mathrm{mod}\, 8)$ та $N_E = p-3$, якщо $p \equiv 7(\mathrm{mod}\, 8)$. Над полем F_{p^n}, де $n \equiv 1(mod 2)$, порядки вище вказаних кривих $N_E = p^n+1$, якщо $p \equiv 3(\mathrm{mod}\, 8)$ і $N_E = p^n-3$, якщо $p \equiv 7(\mathrm{mod}\, 8)$.

Доведення. Розглянемо криву

$$x^2+y^2 = 1+2x^2y^2 \tag{2}$$

Перетворимо рівняння (1) на $y^2 = \frac{x^2-1}{2x^2-1}$. У випадку $p \equiv 3 \pmod 8$ вираз $2x^2-1$ зі знаменника не може бути нулем, бо $(\frac{2}{p}) \equiv -1$. Тому за умови $p \equiv 3(mod 8)$ крива $y^2 = (x^2-1)(2x^2-1)$ має стільки ж точок, що і (1), бо для кожного x з F_p символ Лежандра від елементів $(x^2-1)/(2x^2-1)$ та $(x^2-1)(2x^2-1)$ буде однаковим. У випадку $p \equiv 7(\mathrm{mod}\, 8)$ крива $y^2 = (x^2-1)(2x^2-1)$ буде мати на 2 точки більше, ніж (1), оскільки з'являться точки $(\frac{1}{\sqrt{2}}, 0)$ і $(-\frac{1}{\sqrt{2}}, 0)$, бо $(\frac{2}{p}) \equiv 1$.

Отже, потрібно показати, що число N_2, що рівне кількості точок на кривій

$$y^2 = (x^2-1)(2x^2-1), \tag{3}$$

задовільняє умову $N_2 \equiv 1(\mathrm{mod}\, p)$ для $p \equiv 3(\mathrm{mod}\, 8)$ і $N_2 \equiv -1(\mathrm{mod}\, p)$ для $p \equiv 7(\mathrm{mod}\, 8)$. Тоді матимемо $N_2 = p+1$ для $p \equiv 3(mod 8)$ та $N_2 = p-1$ для $p \equiv 7 \pmod 8$. (Випадки $N_2 = 1$ або $N_2 = 2p-1$ неможливі, бо $N_2 \ge 2$ і $N_2 \le 2p-2$, бо випадки $(x^2-1)=0$ і $(2x^2-1)=0$ дають лише один розв'язок рівняння (2), де $y=0$ на відміну від 2-ох розв'язків коли ліва частина (2) є лишком.) Звідси слідуватиме твердження про кількість точок на вихідній кривій (1).

Покажемо, що кількість розв'язків рівняння $y^2 = (x^2-1)(2x^2-1)$ тобто N_2, порівнянна з $(-a_{2p-2} - a_{p-1}) \mathrm{mod}\, p$, де a_{2p-2}, a_{p-1} – коефіцієнти многочлена, бо коефіцієнти при інших степенях згідно з Лемою 1 конгруентні 0 за modp. Тому, порівняння $N_2 \equiv -a_{2p-2} - a_{p-1} (\mathrm{mod}\, p)$ слідує з леми 1. Обчислимо значення символу Лежандра [17,18,19] від лівої частини рівняння $y^2 = (x^2-1)(2x^2-1)$ за допомогою формули Ейлера $(x^2-1)^{\frac{p-1}{2}} (2x^2-1)^{\frac{p-1}{2}} = a_0 + a_1 x + \ldots + a_{2p-2} x^{2p-2}$.

Для фіксованого значення x кількість розв'язків рівняння (2) дорівнює $1+(\frac{(x^2-1)(2x^2-1)}{p})$, де $\left(\frac{a}{p}\right)$ – символ Лежандра. Як відомо, $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} (\mathrm{mod}\, p)$, тому для фіксованого x кількість розв'язків

рівняння (2) порівняння за модулем p з $1+((x^2-1)(2x^2-1))^{\frac{p-1}{2}}$. Отже, підсумовуючи за всіма x, маємо $N_2 \equiv \sum_{x=0}^{p-1} 1+((x^2-1)(2x^2-1))^{\frac{p-1}{2}} \equiv p+\sum_{x=0}^{p-1}(x^2-1)^{\frac{p-1}{2}}(2x^2-1)^{\frac{p-1}{2}} \bmod p$. Перетворимо вираз $(x^2-1)^{\frac{p-1}{2}}(2x^2-1)^{\frac{p-1}{2}}$, за допомогою бінома Ньютона маємо $(x^2-1)^{\frac{p-1}{2}}(2x^2-1)^{\frac{p-1}{2}} = N_2 \equiv (\sum_{x=0}^{p-1} C_{\frac{p-1}{2}}^{k} x^{2k}(-1)^{\frac{p-1}{2}-k})(\sum_{x=0}^{p-1} C_{\frac{p-1}{2}}^{j} 2^j x^{2j}(-1)^{\frac{p-1}{2}-j})$. З цих дужок виберемо степені, що рівні $p-1$ і додавши їх отримаємо коефіцієнт при x^{p-1}.

Звідси отримуємо, що $a_{2p-2} = 1^{\frac{p-1}{2}} \cdot 2^{\frac{p-1}{2}} \equiv (\frac{2}{p}) (\bmod p)$.

Отже,

$$N_2 \equiv -(\frac{2}{p}) - a_{p-1} (\bmod p) \tag{4}$$

Для випадку $8k+3$ маємо

Нам потрібно було довести, що $N_2 \equiv 1(\bmod p)$ при $p \equiv 3(\bmod 8)$, $N_2 \equiv -1(\bmod p)$, $p \equiv 7(\bmod 8)$. Тобто треба буде показати, що $N_2 \equiv -(\frac{2}{p}) - a_{p-1}(\bmod p)$ для $p \equiv 3(\bmod 4)$. Це буде слідувати з (3), якщо ми покажемо, що $a_{p-1} \equiv 0(\bmod p)$. Тоді розв'язків буде або $p-1$ або $p+1$. Знайдемо a_{p-1}. Згідно з формулою бінома Ньютона a_{p-1} рівний коефіцієнту при x^{p-1} в добутку двох дужок і при підстановці у нього 2 замість x є таким $(-1)^{\frac{p-1}{2}} \sum_{j=0}^{\frac{p-1}{2}} 2^j (C_{\frac{p-1}{2}}^{j})^2$, тобто має форму зворотнього полінома. Справді

$$\sum_{j=0}^{\frac{p-1}{2}} 2^j (C_{\frac{p-1}{2}}^{\frac{p-1}{2}-j})(-1)^{\frac{p-1}{2}-(\frac{p-1}{2}-j)} \cdot 2^j (C_{\frac{p-1}{2}}^{j})^2 (-1)^{\frac{p-1}{2}-j} = (-1)^{\frac{p-1}{2}} \sum_{j=0}^{\frac{p-1}{2}} 2^j C_{\frac{p-1}{2}}^{\frac{p-1}{2}-j} \cdot C_{\frac{p-1}{2}}^{j} = (-1)^{\frac{p-1}{2}} \sum_{j=0}^{\frac{p-1}{2}} 2^j (C_{\frac{p-1}{2}}^{j})^2.$$

Покажемо що за умови $p \equiv 3(\bmod 4)$ виконуватиметься $\sum_{j=0}^{\frac{p-1}{2}} 2^j (C_{\frac{p-1}{2}}^{j})^2 \equiv 0(\bmod p)$.

Домножимо кожен біноміальний коефіцієнт у попередній сумі на $\frac{p-1}{2}!$:

$$(\frac{p-1}{2})! C_{\frac{p-1}{2}}^{j} = \frac{(\frac{p-1}{2})(\frac{p-1}{2}-1)\ldots(\frac{p-1}{2}-j+1)(\frac{p-1}{2})!}{1 \cdot 2 \cdot \ldots \cdot j} =$$

$$= (\frac{p-1}{2})(\frac{p-1}{2}-1)\ldots(\frac{p-1}{2}-j+1)[(\frac{p-1}{2})(\frac{p-1}{2}-1)\ldots(j+1)]$$

Помітимо, що має місце симетрія квадратів лишків:

$$(\frac{p-1}{2}-j)^2 \equiv (\frac{p-1}{2}+j+1)^2, \ 0 \le j \le \frac{p-1}{2},$$

Справді квадрати мають місце наступні конгруенції $(\frac{p-1}{2}-1)^2 \equiv (\frac{p-1}{2}+2)^2$, $(\frac{p-1}{2}-2)^2 \equiv (\frac{p-1}{2}+3)^2$, …, $(\frac{p-1}{2}-k)^2 \equiv (\frac{p-1}{2}+k+1)^2 (\bmod p)$. Без квадратів маємо антисиметричну конгруенцію $(\frac{p-1}{2}-k) \equiv -(\frac{p-1}{2}+1+k)(\bmod p)$.

Використаємо конгруенції описані у зауваженні 1, тобто $(\frac{p-1}{2}-k) \equiv -(\frac{p-1}{2}+1+k)(modp)$ запишемо добутки які конгруентні

$$(\frac{p-1}{2})(\frac{p-1}{2}-1)\ldots(\frac{p-1}{2}-j+1) \equiv [(\frac{p-1}{2}+1)\ldots(\frac{p-1}{2}+\frac{p-1}{2}-j)](-1)^{\frac{p-1}{2}-j} (\bmod p).$$

Переставивши множники бачимо, що з властивості 1 слідує:

$$(\frac{p-1}{2})! C_{\frac{p-1}{2}}^{j} = (\frac{p-1}{2}-j+1)(\frac{p-1}{2}-j+2)\ldots(\frac{p-1}{2})(\frac{p-1}{2}+1)\ldots(p-j-1)(-1)^{\frac{p-1}{2}-j}.$$

Піднісши дві частини до квадрату, отримаємо:

$$((\frac{p-1}{2})! C_{\frac{p-1}{2}}^{j})^2 \equiv (\frac{p-1}{2}-j+1)^2 (\frac{p-1}{2}-j+2)^2 \ldots (p-j-1)^2 (\bmod p) \tag{5}$$

Покажемо, як обчислити $N_2 (\mathrm{mod}\, p)$.

Помітимо, що для заданого x кількість розв'язків рівняння $y^2 = (x^2-1)(2x^2-1) mod$ p конгруентно значенню суми виразів $1+((x^2-1)(2x^2-1))^{\frac{p-1}{2}} \bmod p$ по x від 0 до $p-1$ всіх значень виразу.

Отже,

$$N_2 \equiv \sum_{x=0}^{p-1} 1+(x^2-1)^{\frac{p-1}{2}}(2x^2-1)^{\frac{p-1}{2}} \equiv p+\sum_{x=0}^{p-1}(x^2-1)^{\frac{p-1}{2}}(2x^2-1)^{\frac{p-1}{2}} \equiv$$

$$\equiv \sum_{x=0}^{p-1}(x^2-1)^{\frac{p-1}{2}}(2x^2-1)^{\frac{p-1}{2}} (\mathrm{mod}\, p).$$

Вираз $(x^2-1)^{\frac{p-1}{2}}(2x^2-1)^{\frac{p-1}{2}}$ – це деякий многочлен $a_{2p-2}x^{p-1}+a_{2p-3}x^{p-2}+...+a_1x+a_0$.

Для всіх $i = 0,1...,2p-2$, окрім $i = 2p-2$ і $i = p-1$, сума $\sum_{x=0}^{p-1} x^i$ рівна 0 за модулем *p.*

Для $i = 2p-2$ і $i = p-1$ ця сума порівняна з -1, що слідує з Леми 1.

Тому $\sum_{x=0}^{p-1}(x^2-1)^{\frac{p-1}{2}}(2x^2-1)^{\frac{p-1}{2}} \equiv -a_{2p-2}-a_{p-1} (\mathrm{mod}\, p)$.

Дослідимо величину $-a_{2p-2}-a_{p-1} (\mathrm{mod}\, p)$ окремо а саме, покажемо, що

$$-a_{2p-2}-a_{p-1} (\mathrm{mod}\, p) \equiv \begin{cases} 1, & p \equiv 3 (\mathrm{mod}\, 8) \\ -1, & p \equiv 7 (\mathrm{mod}\, 8) \end{cases}$$

Для цього потрібно обчислити a_{2p-2} і a_{p-1}.

a_{2p-2}, очевидно, рівне $2^{\frac{p-1}{2}} \equiv (\frac{2}{p}) (\mathrm{mod}\, p)$.

$a_{p-1} = \sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^j)^2 2^j (-1)^{\frac{p-1}{2}}$, тому, що це коофіцієнт в многочлені $(\sum_{j=0}^{\frac{p-1}{2}} C_{\frac{p-1}{2}}^j (x^2)^j (-1)^{\frac{p-1}{2}-j})(\sum_{j=0}^{\frac{p-1}{2}} C_{\frac{p-1}{2}}^j 2^j (x^2)^j (-1)^{\frac{p-1}{2}-j})$ при x^{p-1}. Оскільки $p \equiv 3 (\mathrm{mod}\, 4)$, то $(-1)^{\frac{p-1}{2}} = -1$ і $a_{p-1} = -\sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^j)^2 2^j$. Тому $N_2 \equiv -a_{p-1}-a_{2p-2} \equiv -(\frac{2}{p}) + \sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^j)^2 2^j (\mathrm{mod}\, p)$.

Нагадаємо, що $(\frac{2}{p}) = \begin{cases} -1, p \equiv 3 (\mathrm{mod}\, 8) \\ 1, p \equiv 7 (\mathrm{mod}\, 8) \end{cases}$.

Отже, в обох випадках потрібно довести співвідношення $\sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^j)^2 2^j \equiv 0 (\mathrm{mod}\, p)$, з якого слідувало б $N_2 \equiv -1 (\mathrm{mod}\, p)$ при $p \equiv 7 (\mathrm{mod}\, 8)$ і $N_2 \equiv 1 (\mathrm{mod}\, p)$ при $p \equiv 3 (\mathrm{mod}\, 8)$.

Залишилося довести, що

$$\sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^j)^2 2^j \equiv 0 (\mathrm{mod}\, p)$$

при $p \equiv 3 (\mathrm{mod}\, 4)$.

Взагалі, для випадку довільного $d \in F_p^*$ міркуючи аналогічно отримали б, що при $p \equiv 3 (\mathrm{mod}\, 4)$ крива E_d є суперсингулярною якщо і тільки якщо виконано співвідношення

$$\sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^j)^2 d^j \equiv 0 (\mathrm{mod}\, p) \quad (6)$$

Розглянемо многочлен $P(x) = \sum_{j=0}^{\frac{p-1}{2}} (j+1)^2 ... (j+\frac{p-1}{2})^2 x^j$. Тому достатньо показати, що: $P(2) \equiv 0 (\mathrm{mod}\, p)$ або в більш загальному випадку $P(d) \equiv 0 (\mathrm{mod}\, p)$.

Використовуючи конгруенцію (4) отримуємо, що $\sum_{j=0}^{\frac{p-1}{2}}(C_{\frac{p-1}{2}}^{j})^2 x^j = P(x)\frac{1}{(\frac{p-1}{2}!)^2}$ або $P(x)=\left(\frac{p-1}{2}!\right)^2\sum_{j=0}^{\frac{p-1}{2}}(C_{\frac{p-1}{2}}^{j})^2 x^j=\sum_{j=0}^{\frac{p-1}{2}}(k+1)^2(k+2)^2...\left(\left(\frac{p-1}{2}\right)+k\right)^2 x^j$. Тобто в суму (5) замість d підставлено x.

Помітимо, що $P(x)=\partial^{\frac{p-1}{2}}(\partial^{\frac{p-1}{2}}(Q(x)x^{\frac{p-1}{2}})x^{\frac{p-1}{2}})$, де $Q(x)=x^{p-1}+...+x+1$, де $\partial^{\frac{p-1}{2}}$ позначають $\frac{p-1}{2}$ похідну а не степінь. Але тоді $Q(x)=\frac{x^p-1}{x-1}=\frac{(x-1)^p}{x-1}=(x-1)^{p-1}$, тому $P(x)=(((x-1)^{p-1}x^{(\frac{p-1}{2})})x^{\frac{p-1}{2}})^{(\frac{p-1}{2})}$. Нехай $y=x-1$. Позначимо $R(y)=P(x)$ це буде для випадку $y+1=2$ це зведе випадок $x+1=2$ до $y=1$. Ця заміна зводить многочлен $P(x)$, при $x=2$ до многочлена $R(x-1)$ від $x-1=1$, тобто $P(x)=R(x-1)$, що зручно зокрема і для диференціювання, можна вважати, що $R(y)$ це многочлен $P(y)$ від нової змінної $y=x-1$. Зауважимо, що в силу лінійності заміни, диференціювання за y і за x співпадають. Застосуємо диференціювання для перетворення многочлена P(x) до такого вигляду, де явно видно потрібний коефіцієнт a_{p-1}.

Тоді $R(y)=P(y+1)=((y^{p-1}(y+1)^{(\frac{p-1}{2})})^{(\frac{p-1}{2})}(y+1)^{(\frac{p-1}{2})})^{(\frac{p-1}{2})}$. Шукаємо коефіцієнт a_{p-1} від P(y+1) в точці $y=1$. Помітимо, що $(y^{p-1}(y+1)^{(\frac{p-1}{2})})^{(\frac{p-1}{2})}=(y^{p-2})^{\frac{p-1}{2}}=|=(p-1)(p-2)...(\frac{p-1}{2}+1)y^{\frac{p-1}{2}}$. Всі доданки, окрім першого, стануть рівними 0. Тому $R(y)=\frac{(p-1)!}{(\frac{p-1}{2})!}(y^{\frac{p-1}{2}}(y+1)^{\frac{p-1}{2}})^{\frac{p-1}{2}}=\frac{(p-1)!}{(\frac{p-1}{2})!}\sum_{j=0}^{\frac{p-1}{2}}(j+1)...(j+\frac{p-1}{2})y^j C_{\frac{p-1}{2}}^{j}$.

Нам потрібно показати, що $a_{p-1}=P(1+1)=R(1)\equiv 0(\mathrm{mod}\,p)$. Маємо

$$R(1)=\frac{(p-1)!}{(\frac{p-1}{2})!}\sum_{j=0}^{\frac{p-1}{2}}C_{\frac{p-1}{2}}^{j}(j+1)...(j+\frac{p-1}{2}). \qquad (7)$$

Помітимо, що

$$(\frac{p-1}{2}-j+2)...(\frac{p-1}{2}-j+\frac{p-1}{2})=-1^{\frac{p-1}{2}}(j+1)...(j+\frac{p-1}{2})=-1(j+1)...(j+\frac{p-1}{2}),$$

Саме тому, симетричні доданки в (7) скорочуються.

Тут ми використано те, що $(-1)^{\frac{p-1}{2}}=-1$, так, як $p=Mk+3$ і $\frac{p-1}{2}=2k+1$.

Значить, $P(2)=R(1)=0$, що і потрібно було.

Отже, $\sum_{j=0}^{\frac{p-1}{2}}(C_{\frac{p-1}{2}}^{j})^2\equiv 0(\mathrm{mod}\,p)$, що завершує доведення основної частини теореми.

Аналогічний результат матиме місце для кривої $x^2+y^2=1+2^{-1}x^2y^2$.

Дійсно для доведення аналогічного твердження щодо кривої $x^2+y^2=1+2^{-1}x^2y^2$ потрібно показати, що $\sum_{j=0}^{\frac{p-1}{2}}(C_{\frac{p-1}{2}}^{j})^2 2^{-j}\equiv 0(\mathrm{mod}\,p)$. Для отримання останньої формули враховуємо, що має місце $(\frac{2}{p})=(\frac{2^{-1}}{p})$ тоді рівність $\sum_{j=0}^{\frac{p-1}{2}}(C_{\frac{p-1}{2}}^{j})^2 2^{-j}\equiv 0(\mathrm{mod}\,p)$ слідує з вже доведеної формули $\sum_{j=0}^{\frac{p-1}{2}}(C_{\frac{p-1}{2}}^{j})^2 2^{j}\equiv 0(\mathrm{mod}\,p)$, якщо її домножити на $2^{-\frac{p-1}{2}}$. Тобто

$$\sum_{j=0}^{\frac{p-1}{2}}(C_{\frac{p-1}{2}}^{j})^2 2^{-j}\equiv 0,\ \text{так, як}\ 2^{\frac{p-1}{2}}\sum_{j=0}^{\frac{p-1}{2}}(C_{\frac{p-1}{2}}^{j})^2 2^{-j}=\sum_{j=0}^{\frac{p-1}{2}}(C_{\frac{p-1}{2}}^{j})^2 2^{\frac{p-1}{2}-j}=\sum_{j=0}^{\frac{p-1}{2}}(C_{\frac{p-1}{2}}^{j})^2 2^{j}.$$

Як наслідок маємо, що криві $x^2+y^2=1+2x^2y^2$ і $x^2+y^2=1+2^{-1}x^2y^2$ мають однакове число точок для $p=4k+3$ (тобто для $p=8k+3$ і $p=8k+7$). На цьому твердження про доведення.

Доведемо твердження про порядок групи над розширенним полем.

Використовуючи теорему Степанова [15] результат можна узагальнити для довільного p^n, де $n \equiv 1(\mathrm{mod}\,2)$. Відомо, що якщо $y^2 = P(x)$, де $P(x)$ многочлен степені d, над полем F_{p^n} має кількість розв'язків рівну $p^n + w_1^n + ... + w_{d-1}^n$, де $w_1, ..., w_{d-1}$ – деякі комплексні числа.

Позначимо кількість точок на кривій Монтгомері над $\mathbb{F}_{p^k}$ як $N_{M,k}$ а на кривій Едвардса як $N_{E,k}$.

Порядок $N_{M,k}$ групи кривої Монтгомері $v^2 = u^3 + 6u^2 + u$ над F_{p^k}, яка є біраціонально еквівалентною до кривої $x^2 + y^2 = 1 + 2x^2y^2$, обчислюється за допомогою теорем Степанова і Деліня [15; 16]: $N_M = p^k + \omega_1^k + \omega_2^k$, де $\omega_i^k \in \mathbb{C}$ і $\omega_1^k = -\omega_2^k, |\omega_i| = \sqrt{p}, i \in 1,2$. Тобто знайдуться такі $\omega_1, \omega_2 \in \mathbb{C}$, що для всіх $k \in \mathbb{N}$ вірна рівність $N_M = p^k + \omega_1^k + \omega_2^k$. Оскільки $N_M = p$ для $k = 1$, то звідси маємо $\omega_1 + \omega_2 = 0$ або $\omega_1 = -\omega_2$. Згідно з теоремою Деліня: $|\omega_i| = \sqrt{p}$. А для еліптичної кривої виконується $\omega_1 = \overline{\omega}_2$ [15], тому враховуючи, що виведене вище $\omega_1 + \omega_2 = 0$, яке слідувало з $N_{M,1} = p$, маємо $\omega_1 = i\sqrt{p}$, $\omega_2 = -i\sqrt{p}$. Звідси для парних k маємо, що $N_{M,k} = p^k + 2(-p)^{\frac{k}{2}}$. Для непарних k маємо $\omega_1^k + \omega_2^k = 0$, тому $N_{M,k} = p^k$.

В силу того, що при $k \equiv 1(mod 2)$ порядок відповідної кривої Монтгомері $N_{M,k} = p^k$, то кількість точок у образі при переході від E_M до (2) є $N_{E,k} = p^k - 1 - 2(\frac{d}{p})$ для випадку $p \equiv 3(\mathrm{mod}\,4)$ і $k \equiv 1(mod 2)$, бо заміна $y = (u-1)/(u+1)$ відображає 2 точки 4-го порядку, кривої Монтгомері, з координатою $u = -1$ на нескінченність, тобто не у точку з афінної площини.

Цілком зрозуміло, що значеннями $d = -1, 2, 2^{-1}$ не вичерпується множина параметрів при яких крива Едвардса суперсингулярна.

Наслідок 1. Якщо коефіцієнт d кривої E_d задовольняє рівняння суперсингулярності $\sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^j)^2 d^j \equiv 0(\mathrm{mod}\,p)$ досліджене в теоремі 1, то E_d має $p - 1 - 2(\frac{d}{p})$ точок над F_p а біраціонально еквівалентна [2, 12, 13, 14] їй крива E_M має р +1 точок над F_p.

Доведення. З доведення теореми 1 слідує, що конгруенція (6) тобто $\sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^j)^2 d^j \equiv 0(\mathrm{mod}\,p)$ є визначальною для виконання умови суперсингулярності. З вище сказаного слідує, що суперсингулярність кривої Едвардса рівносильна тому, що рівняння (1) або рівносильне йому $y^2\left(dx^2 - 1\right) = x^2 - 1$, має в F_p рівно $p - 1 - 2\left(\frac{d}{p}\right)$ розв'язків. Це випливає з формули кількості точок (4) виведеній у теоремі 1 і умови $a_{p-1} \equiv 0(modp)$, що забезпечує виконання умови суперсингулярності (6), при цьому враховано наявність 2 особливих точок проективної кривої F(x;y;z), що знайдені у розділі 1. А це рівносильно тому, що узагальнене рівняння (3), яке має вигляд

$$y^2 = (dx^2 - 1)(x^2 - 1) \tag{8}$$

має рівно $p - 1 - 2\left(\frac{d}{p}\right) + \left(1 + (\frac{d}{p})\right) = p - \left(\frac{d}{p}\right)$ розв'язків. Справді кожний розвязок рівняння (1) відповідає розв'язку рівняння (8), але (8) має ще розвязки, при яких $dx^2 - 1 \equiv 0$ їх стільки скільки є квадратних коренів з d в F_p, тобто $1 + \left(\frac{d}{p}\right)$. Тому твердження, що $x^2 + y^2 = 1 + dx^2y^2$ має $p - 1 - 2\left(\frac{d}{p}\right)$ розвязків рівносильна тому, що рівняння $y^2 = (dx^2 - 1)(x^2 - 1)$ має $p - 1 - 2\left(\frac{d}{p}\right) + \left(1 + (\frac{d}{p})\right) = p - \left(\frac{d}{p}\right)$.

Отже, суперсингулярність кривої Едвардса рівносильно тому, що рівняння (8) має $p - 1 - 2\left(\frac{d}{p}\right) + 1 + \left(\frac{d}{p}\right) = p - \left(\frac{d}{p}\right)$. Як показано вище кількість розв'язків (2) конгруентна $-(a_{2p-2} - a_{p-1}) mod p$, де коефіцієнти многочлена $\left(dx^2 - 1\right)^{\frac{p-1}{2}} \left(x^2 - 1\right)^{\frac{p-1}{2}} = a_{2p-2}x^{2p-2} + ... + a_0$. Тому якщо $-a_{2p} - a_{p-1} \equiv p - \left(\frac{d}{p}\right) \mathrm{mod}\,p$ тобто $a_{p-1} \equiv 0(modp)$, то крива Едвардса є суперсингулярною. Випадки $N_{E_d} = -\left(\frac{d}{p}\right)$ і $N_{E_d} = 2p - \left(\frac{d}{p}\right)$ є неможливими в силу нерівності $2 \le N_{E_d} \le 2p - 2$. Дійс-

но вона має хоч 2 розв'язки $y=0$, $x=\pm 1$ а більше ніж $2p-2$ розв'язків вона мати не може, бо для $x=\pm 1$ є існує один можливий $y=0$ а для інших значень x не більше ніж 2 можливих y.

Отже, результат теореми 1 можна розширити на всі $d\in F_p^*$, що його задовольняють умову (6). Суперсингулярній кривій E_d відповідає суперсингулярна крива E_M, що має $p+1$ точок серед яких 1 нескінченно віддалена.

Наслідок 2. Якщо виконується умова $\sum_{j=0}^{\frac{p-1}{2}}(C_{\frac{p-1}{2}}^{j})^2 d^j \equiv 0(\bmod p)$, то крива Монтгомері $u^2=(d-1)v^3+2(d+1)v^2+(d-1)v$ для непарних k має рівно p^k афінних точок над $\mathbb{F}_{p^k}$.

Доведення. Як доведено в теоремі 3.4 [2] кожна крива Монтгомері над скінченним полем k, $char(k)\equiv 3(\bmod 4)$ є біраціонально еквівалентною кривій Едвардса. З формули біраціонального відображення над $k, char(k)\neq 2$ кривої $E_{a,d}$ в E_M були отримані коефіцієнти кривої E_M: $A=2\dfrac{(a+d)}{(a-d)}$ і $B=\dfrac{4}{a-d}$ [2].

Отже, образом знайденої нами суперсингулярної кривої E_d, де коефіцієнт d задовольняє вказану в умові конгруенцію є крива E_M: $\dfrac{4}{a-d}u^2=v^3+2\dfrac{a+d}{a-d}v^2+v$ враховуючи, що $a=1$ отримуємо еліптичну криву у формі Монтгомері $\dfrac{4}{1-d}u^2=v^3+2\dfrac{1+d}{1-d}v^2+v$, з відповідними коефіцієнтами $B=\dfrac{4}{1-d}$, $A=2\dfrac{1+d}{1-d}$. Оскільки $d\neq 1$, маємо рівняння еквівалентної еліптичної кривої $4u^2=(1-d)v^3+2(1+d)v^2+(1-d)v$.

Кінець доведення Наслідку 2. З умови наслідку 2 і з її біраціональної еквівалентності кривій E_d легко отримується, що властивістю суперсингулярності володіють і криві E_d з коефіцієнтами $d=17+12\sqrt{2}$ і $d=17-12\sqrt{2}$ при $p\equiv 7(\bmod 8)$ випадок $p\equiv 3(\bmod 8)$ не можливий в силу не існування $\sqrt{2}$.

Наслідок 3. Якщо коефіцієнт кривої Едвардса $d=2$ і $p^k\equiv 3(\bmod 4)$, то в полі F_{p^k} кількість розвязків $y^2=u^3+6u^2+u$ рівна p^k. Кількість розв'язків $y^2=(\mathrm{x}^2-1)(2\mathrm{x}^2-1)$ рівна p^k+1 і p^k-1 при $p^k\equiv 7(\bmod 8)$. Відповідно крива (1) має p^k+1 при $p^k\equiv 3(\bmod 4)$ і p^k-3 при $p^k\equiv 7(\bmod 8)$.

Доведення цього наслідку слідує безпосередньо з Наслідків 1 і 2.

Сформулюємо спосіб знаходження суперсингулярної еліптичної кривої у формі Веєрштрасса.

Зауваження 2. Суперсингулярній еліптичній кривій у канонічній формі Веєрштрасса $y^2=x^3+ax+b$ ізоморфна суперсингулярна еліптична крива Монгомері E_M.

Для зведення кривої E_M до канонічної форми Веєрштрасса поділимо рівняння кривої $4u^2=(1-d)v^3+2(1+d)v^2+(1-d)v$ на 4 і до отриманної кривої $u^2=4^{-1}((1-d)v^3+2(1+d)v^2+(1-d)v)=av^3+bv^2+ax$ застосуємо заміну $t=v-\dfrac{b}{3a}$, де $a=(d-1)4^{-1}$, $b=2^{-1}(1+d)$. Ця крива буде суперсингулярною еліптичною кривою у формі Веєрштрасса.

Висновки. Було знайдено умову, у вигляді конгруенції з наслідку 1, на коефіцієнти кривої Едвардса, яка є необхідною і достатньою для суперсингулярності цієї кривої це дозволило описати всю множину параметрів при яких є суперсингулярною. Узагальнено результата про суперсингулярність кривої отриманого в [10] для коефіцієнтів над на випадок довільного не простого поля та виправлено неточності у кількості точок афінної кривої Едвардса над полем характеристики, яка була в теоремі 3 з [10]. Дослідження дозволило знайти критерій суперсингулярності еліптичних кривих у формі Монтгомері, що дає можливість перевіряти криві на придатність до використання в якості носія групи точок для побудови крипто систем та електронно-цифрового підпису на еліптичній кривій.

Список використаних джерел:

1. Edwards H. A normal form for elliptic curves. *American Mathematical Society*. 2007. Vol. 44. No. 3. P. 393–422.

2. Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, Christiane Peters. Twisted Edwards Curves. *IST Programme ECRYPT, and in part by grant ITR-071649.* 2008. P. 1–17.

3. Menezes A., Okamoto T., Vanstone S. Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field. *IEEE Transactions On Information Theory*. 1993. Vol. 39. No. 5. P. 1603–1646.

4. *Алексеев Е., Ошкин И., Попов В., Смышляев С., Сонина Л.* О перспективах использования скрученных эллиптических кривых Эдвардса со стандартом ГОСТ Р 34.10-2012 и алгоритмом ключевого обмена на его основе. Материалы XVI международной конференции «РусКрипто 2014». 2014. С. 24–26.

5. Hallgren S. Linear congruential generators over elliptic curves. *Preprint CS-94-143, Dept. Of Comp. Sci., CornegieMellon Univ.* 1994. P. 1–10.

6. Виноградов И. Основы теории чисел: Учебное пособие. 12-е изд. СПб. : Издательство «Лань», 2009. 271 с.

7. Белецкий А.Я., Белецкий А.А. Симметричный блочный криптоалгоритм. *Захист інформації*. 2006. № 2 (29). С. 42–51.

8. Скуратовський Р., Мовчан П. В., Нормалізація скрученої кривої Едвардса та дослідження її властивостей над Fp. *Збірник праць 14 Всеукраїнської науково-практичної конференції. ФТІ НТУУ «КПІ»*. 2016. Том 2. С. 102–104.

9. Скуратовський Р. Дослідження властивостей скрученої кривої Едвардса. *Конференція державної служби спеціального зв'язку та захисту інформації*. URL: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?showHidden=1artid=252312catid=240232 ctime=1464080781894

10. Бессалов А., Цыганкова О. Взаимосвязь семейства точек больших порядков кривой Эдвардса над простым поле. *Захист інформації*. 2015. Т. 17. № 1. С. 73–80.

11. Skuratovskii R. V. Twisted Edwards curve and its group of points over finite field Fp. *Літня школа «Алгебра, Топологія, Аналіз»*. Одеса, 2016. С. 122–124.

12. Skuratovskii R., Skruncovich U. Twisted Edwards curve and its group of points over finite field Fp. *Akademgorodok, Novosibirsk, Russia. Conference. Graphs and Groups, Spectra and Symmetries*. URL: http://math.nsc.ru/conference/g2/g2s2/exptext/SkruncovichSkuratovskii-abstract-G2S2.pdf

13. Рид М. Алгебраическая геометрия для всех. Москва : Мир, 1991. 143 с.

14. Hisil Huseyin, Koon-Ho Wong Kenneth, Carter Gary. Twisted Edwards Curves Revisited. *ASIACRYPT LNCS 5350*. 2008. P. 326–343.

15. Степанов С. Арифметика алгебраических кривых. М. : Наука, 1991. 368 с.

16. Koblitz N. Eliptic Curve Cryptosystems. *Mathematics of Computation*. 1987. Vol. 48. No. 177. P. 203–209.

17. Сергієнко І., Задірака В., Литвин О. Елементи загальної теорії оптимальних алгоритмів та суміжні питання. К. : Наук. думка, 2012. 400 с.

18. Рибак О. Розкладність рядків та звідність многочленів. *У світі математики*. 2006. № 12(4). С. 18–29.

19. Скуратовский Р. Метод быстрого таймерного кодирования текстов. *Кибернетика и системный анализ*. 2013. Т. 49. № 1. С. 154–160.

20. Долгов В. Эллиптические кривые в криптографии. *Системи обробки інформації*. 2008. Вип. 6 (73). С. 3–10.

21. Болотов С. Б., Гашков А. Б., Фролов А. А. Часовских Элементарное введение в эллиптическую криптографию М. : КомКника, 2006. Том 2. 328 с.

References:

1. Edwards, H. (2007). A normal form for elliptic curves. *American Mathematical Society*, vol. 44, no. 3, pp. 393–422. [in English].

2. Daniel, J. Bernstein, Peter, Birkner, Marc, Joye, Tanja, Lange, Christiane, Peters. (2008). Twisted Edwards Curves. *IST Programme ECRYPT, and in part by grant ITR-071649*, pp. 1–17. [in English].

3. Menezes, A., Okamoto, T., Vanstone, S. (1993). Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field. *IEEE Transactions On Information Theory*, vol. 39, no. 5, pp. 1603–1646. [in English].

4. Alekseev, E., Oshkin, I., Popov, V., Smyshlyaev, S., Sonina, L. (2014). O perspektivah ispolzovaniya skruchennyh ellipticheskih krivyh Edvardsa so standartom GOST R 34.10-2012 i algoritmom klyuchevogo obmena na ego osnove. *Materialy XVI mezhdunarodnoj konferencii «RusKripto 2014»*, pp. 24–26. [in Russian].

5. Hallgren, S. (1994). Linear congruential generators over elliptic curves. *Preprint CS-94-143, Dept. Of Comp. Sci., CornegieMellon Univ*, pp. 1–10. [in English].

6. Vinogradov, I. (2009). Osnovy teorii chisel: Uchebnoe posobie. 12-e izd. SPb.: Izdatelstvo «Lan», 271 p. [in Russian].

7. Beleckij, A.Ya., Beleckij, A.A. (2006). Simmetrichnyj blochnyj kriptoalgoritm. *Zahist informaciyi*, no. 2 (29), pp. 42–51. [in Russian].

8. Skuratovskyi, R., Movchan, P. V. (2016). Normalizatsiia skruchenoi kryvoi Edvardsa ta doslidzhennia yii vlastyvostei nad Fp. *Zbirnyk prats 14 Vseukrainskoi naukovo-praktychnoi konferentsii. FTI NTUU «KPI»*, vol. 2, pp. 102–104. [in Ukrainian].

9. Skuratovskyi, R. Doslidzhennia vlastyvostei skruchenoi kryvoi Edvardsa. *Konferentsiia derzhavnoi sluzhby spetsialnoho zviazku ta zakhystu informatsii*. URL: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?showHidden=1artid=252312catid=240232 ctime=1464080781894 [in Ukrainian].

10. Bessalov, A., Cygankova, O. (2015). Vzaimosvyaz semejstva tochek bolshih poryadkov krivoj Edvardsa nad prostym pole. *Zahist informaciyi*, vol. 17, no. 1, pp. 73–80. [in Russian].

11. Skuratovskii, R. V. (2016). Twisted Edwards curve and its group of points over finite field Fp. *Litnia shkola «Alhebra, Topolohiia, Analiz»*, Odesa, pp. 122–124. [in English].

12. Skuratovskii, R., Skruncovich, U. Twisted Edwards curve and its group of points over finite field Fp. Akademgorodok, Novosibirsk, Russia. *Conference. Graphs and Groups, Spectra and Symmetries*. URL: http://math.nsc.ru/conference/g2/g2s2/exptext/SkruncovichSkuratovskii-abstract-G2S2.pdf [in English].

13. Rid, M. (1991). Algebraicheskaya geometriya dlya vseh. Moskva: Mir, 143 p. [in Russian].

14. Hisil Huseyin, Koon-Ho Wong Kenneth, Carter Gary. (2008). Twisted Edwards Curves Revisited. *ASIACRYPT LNCS 5350*, pp. 326–343. [in English].

15. Stepanov, S. (1991). Arifmetika algebraicheskih krivyh. M.: Nauka, 368 p. [in Russian].

16. Koblitz, N. (1987). Eliptic Curve Cryptosystems. *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209. [in English].

17. Serhiienko, I., Zadiraka, V., Lytvyn, O. (2012). Elementy zahalnoi teorii optymalnykh alhorytmiv ta sumizhni pytannia. K.: Nauk. dumka, 400 p. [in Ukrainian].

18. Rybak, O. (2006). Rozkladnist riadkiv ta zvidnist mnohochleniv. *U sviti matematyky*, no. 12(4), pp. 18–29. [in Ukrainian].
19. Skuratovskij, R. (2013) Metod bystrogo tajmernogo kodirovaniya tekstov. *Kibernetika i sistemnyj analiz*, vol. 49, no. 1, pp. 154–160. [in Russian].
20. Dolgov, V. (2008). Ellipticheskie krivye v kriptografii. *Sistemi obrobki informaciyi*, vol. 6 (73), pp. 3–10. [in Russian].
21. Bolotov, S. B., Gashkov, A. B., Frolov, A. A. (2006). Chasovskih Elementarnoe vvedenie v ellipticheskuyu kriptografiyu M.: KomKnika, vol. 2, 328 p. [in Russian].

УДК 681.3
DOI https://doi.org/10.32689/maup.it.2021.1.8

Руслан СКУРАТОВСЬКИЙ
викладач кафедри обчислювальної математики і компютерного моделювання, ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», вул. Фрометівська, 2, м. Київ, Україна, індекс 03039

ORCID: https://orcid.org/0000-0002-5692-6123

Ruslan SKURATOVSKYI
Lecturer at the Department of Computational Mathematics and Computer Modeling, Interregional Academy of personnel management, 2 Frometivska Street, Kyiv, Ukraine, postal code 03039

Бібліографічний опис статті: Скуратовський Р. Операції на скрученій кривій едварса, і її застосовність в криптографії. *Інформаційні технології та суспільство*. 2021. Вип. 1. С. 70–76. DOI: https://doi.org/10.32689/maup.it.2021.1.8

Bibliographic description of the article: Skuratovskyi, R. (2021). Operatsii na skruchenii kryvii edvarsa, i yii zastosovnist v kryptohrafii [Operations on the twisted edwars curve, and its applicability in cryptography]. *Informatsiini tekhnolohii ta suspilstvo – Information technology and society*, 1, 70–76. DOI: https://doi.org/10.32689/maup.it.2021.1.8

ОПЕРАЦІЇ НА СКРУЧЕНІЙ КРИВІЙ ЕДВАРСА, І ЇЇ ЗАСТОСОВНІСТЬ В КРИПТОГРАФІЇ

Анотація. *Більшість криптосистем сучасної криптографії природним чином можна «перекласти» на еліптичні криві. Ми розглядаємо алгебраїчні криві Едвардса над скінчнним полем F_{p^n}, які на даний час є одним з найбільш перспективних носіїв множин точок, що використовують для швидких групових операцій, які наявні в асиметричних криптосистемах, зокрема для побудови випадкових криптостійких послідовностей. Показано, що проективна крива $E_{a,d}$ не є еліптичною. Досліджено умови існування подільності навпіл елемента з групи точок скрученої кривої Едвардса $E_{a,d}$, що є важливим в алгоритмах. Знайдено род скрученої кривої Едвардса. Метою роботи є пошук критерію подільності точки кривої навпіл над полем F_{p^n} і аналіз властивостей скрученої кривої Едвардса необхідних для побудови генератора псевдовипадкових криптостійких послідовностей і побудова односторонньої функції для нього.*

Ключові слова**:** *скінчене поле, алгебраїчна крива, група точок еліптичної кривої, подільність точки кривої навпіл, генератор криптостійкої послідовності.*

OPERATIONS ON THE TWISTED EDWARS CURVE, AND ITS APPLICABILITY IN CRYPTOGRAPHY

Abstract. *Most cryptosystems in modern cryptography can naturally be «translated» into elliptical curves. We consider Edwards algebraic curves over a finite field, which are currently one of the most promising carriers of point sets used for fast group operations available in asymmetric cryptosystems, in particular, for constructing random cryptostable sequences. It is shown that the projective curve is not elliptical. The conditions for the existence of divisibility in half of an element from the group of points of a twisted Edwards curve, which is important in algorithms, are investigated. The genus of the twisted Edwards curve is found. The aim of this work is to find the criterion for dividing the point of the curve in half over the field and to analyze the properties of the twisted Edwards curve necessary to construct a generator of pseudo-random cryptostable sequences and construct a one-way function for it.*

Key words: *finite field, algebraic curve, group of points of an elliptic curve, divisibility of a point of a curve in half, generator of cryptostable sequence.*

Вступ. Електронний цифровий підпис з обраних засобів найбільш широко забезпечує захист від всіх можливих атак. Причиною цього є наявність в ньому вже хешфункції та закритого ключа шифрування. Найпрогресивнішою схемою є схема цифрового підпису еліптичної кривої (ECDSS – Elliptic Curve Digital Signature). Завдяки вищезгаданим можливостям вирішуються проблема управління та розподілу ключів шифрування. Ми досліджуємо ще одне сімейство кривих придатних для створення ECDSS.

Вперше криві Едвардса E_d представлено Едвардсом в роботі [1]. В еліптичній криптографії дуже важливо знати ті криві які є суперсингулярними (ті, що мають нульовий j-інварівант), бо вони є крипографічно слабкими і період побудованого на їх основі генератора псевдовипадкових чисел є меншим.

Відомо, що суперсингулярні криві, на відміну від несуперсингулярних, над алгебраїчно замкненим полем, мають не комутативне кільце ендоморфізмів. Криві у формі Едвардса над простим полем сьогодні є одним з найбільш перспективних носіїв множин точок, що використовують для швидких групових операцій, що використовуються в асимметричних криптосистемах. Найважливіші переваги: рекордна

продуктивність, універсальність закона додавання, симетричність точок і представлення нейтрального елемента групи точкою в афінних координатах. Ці властивості були помічені і обгрунтовані в роботах відомих фахівців по криптографії [2; 3; 4; 5].

Дані криві задовольняють самим сильним вимогам по стійкості до MOV-атаки, про що неодноразово зазначалось у працях вітчизняних та закордонних вчених [6; 7]: неможливість застосувати цей метод забезпечується через відсутність можливості вкласти групу точок кривої в мультиплікативну групу поля достатньо малого порядку. Для цього достатньо, щоб мінімальне натуральне t, $p^t \equiv 1 mod |N_E|$ було достатньо великим. Для скручених кривих Едвардса $t = |N_E| - 1$, що є максимально можливим. Великою перевагою є можливість побудови скрученої кривої Едвардса порядку $4p$, $p \in \mathbf{P}$, тому не може бути використана атака підміни точки, що належить рекомендованій кривій на точку зі скрученої кривої тобто так званої кривої кручення. Також це не дає противнику використовувати китайську теорему про лишки для визначення секретного ключа, бо маємо великий множник p в $|N_E|$. З точки зору алгебраїчної геометрії, крива не є еліптичною, бо є сингулярною.

Криві Едвардса також як і скручені криві Едвардса мають афінне представленя ізоморфне деякій афінній частині еліптичної кривої, що має в порядку групи кривої множник Цікавою є можливість побудови скрученої кривої Едвардса порядку $N_E = 4p$, $p \in \mathbb{P}$, тобто такої, яка має мінімальний кофактор. Тому природньо досліджувати такі криві і клас кривих, який узагальнює ці криві – скручені криві Едвардса. Частково, викладені результати представлено в тезах [8] та попередні дослідження є у статті [3].

З точки зору алгебраїчної геометрії, крива Едвардса не є еліптичною, бо є сингулярною. Криві Едвардса також як і скручені криві Едвардса мають афінне представленя ізоморфне деякій афінній частині еліптичної кривої, що має в порядку групи кривої множник Як зазначено в роботі [11] для побудови “elliptic curve power generator” генератора і генератора ”Naor–Reingold” використовують не суперсингулярну еліптичну криву і її точку P великого простого порядку, якщо ж порядок l точки P не простий, то вибирають початкове заповнення e таке, що $(e,l) = 1$.

Нашою метою є дослідження властивостей цих кривих що необхідні для її застосування в асиметричній криптографії а також в криптоаналізі, зокрема дослідження цієї кривої на предмет сингулярності.

Постановку проблеми полягає у виявленні ресурсів математичного апарату, що дозволить максимально швидко здійснювати групову операцію пов’язану з додавання точки до себе. Тобто операцію «експонеціювання» точки кривої, яка лежить в основі проблеми дискретного логарифма.

Аналіз особливостей скрученої кривої Едвардса.

Розглянемо скручену криву Едвадрса $E_{a,d}$

$$ax^2 + y^2 = 1 + dx^2y^2,\ a,d \in F_p^*,\ ad(a-d) \neq 0,\ d \neq 1,\ p \neq 2,\ a \neq d, \qquad (1)$$

При $a = d$ перетворимо криву $ax^2 + y^2 = 1 + ax^2y^2$ до вигляду $ax^2 - ax^2y^2 - 1 + y^2 = 0$ або $ax^2(1-y^2) - (1-y^2) = 0$. Отже, крива розкладається у добуток двох пар прямих $(ax^2 - 1)(y^2 - 1) = 0$. Якщо $a = 1$, то $E_{a,\mathrm{d}}$ перетворюється у криву E_{d}. З умови гладкості знаходимо особливі точки афінної кривої.

Знайдемо особливі точки. Позначимо $F(x,y) = ax^2 + y^2 = 1 + dx^2y^2$, $a,d \in F\mathrm{p}^*$, d ≠ 1, $p \neq 2$, $a \neq d$. $\begin{cases} \dfrac{\mathrm{F}(x,y)}{\partial x} = 0 \\ \dfrac{\mathrm{F}(x,y)}{\partial y} = 0 \end{cases}$,

$$\begin{cases} 2ax = 2dxy^2 \\ 2y = 2dx^2y \end{cases}, \quad \begin{cases} ax - dxy^2 = 0 \\ y - dx^2y = 0 \end{cases} \quad \begin{cases} x(a - dy^2) = 0 \\ y(1 - dx^2) = 0 \end{cases} \quad \left[\begin{array}{l} \begin{cases} x = 0 \\ y = 0 \end{cases} \\ \begin{cases} (a - dy^2) = 0 \\ (1 - dx^2) = 0 \end{cases} \end{array} \right. \quad \left[\begin{array}{l} (0,0) \\ \left(\pm\sqrt{\dfrac{1}{d}}, \pm\sqrt{\dfrac{a}{d}} \right) \end{array} \right.$$

Але точка $(0,0)$ кривій $E_{a,\mathrm{d}}$ не належить не залежно від поля.

Отже отримали аж 4 точки, за умови, що при цьому для F_p коефіцієнти a і d в F_p повинен бути таким, що $\left(\frac{d}{p}\right) = 1$ і $\left(\frac{ad}{p}\right) = 1$, тобто $\left(\frac{d}{p}\right) = 1$ і $\left(\frac{a}{p}\right) = 1$. Отже наявні 4 особливі точки з урахування того, що точка $(0,0)$ кривій не належить.

Як відомо [2] проективна крива дала можливість отримати більш швидкі швидкі операції над точками кривої. Тому проаналізуємо особливі точки в проективному замиканні кривої.

Для цього зробимо проективізацію кривої. Нехай $x = \frac{X}{Z}, y = \frac{X}{Z}$, тоді $a\frac{x^2}{z^2} + \frac{y^2}{z^2} = 1 + d\frac{x^2y^2}{z^4}$, звідси $F(x,y,z) = ax^2z^2 + y^2z^2 = z^4 + dx^2y^2$ перевіримо умови гладкості (для алгебраїчних кривих поняття гладкості і нормальності в проективних координатах співпадають:

$$\begin{cases} \frac{\mathrm{F}(x,y)}{\partial x} = 2axz^2 - 2dxy^2 = 0, \\ \frac{\mathrm{F}(x,y)}{\partial y} = 2yz^2 - 2dyx^2 = 0, \\ \frac{\mathrm{F}(x,y)}{\partial y} = 2azx^2 + 2zy^2 - 4z^3 = 0. \end{cases}$$

$ax^2 + y^2 - 2z^2 = 0$ з другого рівняння слідує, що $y = 0$ або $z = \pm\sqrt{d}$ тут розв'язком очевидно є $(0,0,0)$ і точка $(x_0,0,0)$.

Пошукаємо інші корені в припущенні $z = 0$ коренем є також точка $(0,y_0,0) = (0,1,0)$. Тобто маємо 2 особливі проективні точки $p_1 = (1,0,0)$ і $p_2 = (0,1,0)$. Це прості особливості.

Отже, розв'язками є лише особливі точки (нескінченно віддаленні точки) $(1,0,0)$ і $(0,1,0)$, тому маємо особливості на нескінченності у відповідних афінних компонентах

$$A^1 : az^2 + y^2z^2 = z^4 + dy^2 \text{ і } A^2 : \ ax^2z^2 + z^2 = z^4 + dx^2$$

Опишемо будову локального кільця в точці p_1, його елементами є дроби з функцій виду $F(x,y,z) = \frac{f(x,y,z)}{g(x,y,z)}$, знаменники яких не обертаються в 0 у точці p_1. Локальне кільце, що має особливості в 2-ух точках має функції у яких знаменники не діляться на $(x-1)(y-1)$.

Знайдемо $\delta_{\mathrm{p}} = \dim \bar{\mathcal{O}}_{\mathrm{p}} / \mathcal{O}_p$, де $\mathcal{O}_{\mathrm{p}}$ – локальне кільця в особливій точці p, це кільце породжується відношеннями регу лярних функцій: $\mathcal{O}_{\mathrm{p}} = \left\{ \frac{f}{g} : (g,(x-1)(y-1)) = 1 \right\}$, $\bar{\mathcal{O}}_{\mathrm{p}}$ – ціле замикання локального кільця в особливій точці p. Позначимо $\delta_p = \dim \bar{\mathcal{O}}_p / \mathcal{O}_p = 1$ розмірність фактора як векторного простору. Оскільки, базис розширення $\bar{\mathcal{O}}_p$ над $\mathcal{O}_p$ складається з одного елемента в кожній з двох особливих точок, то $\delta_p = 1$.

Отже, підрахуємо род кривої за Рідом: $\rho^*(C) = \rho_\alpha(\mathrm{C}) - \sum_{p \in E} \delta_p = = \frac{(n-1)(n-2)}{2} - \sum_{p \in E} \delta_p = 3 - 2 = 1$ бо $n = 4$. де $\rho_\alpha(C)$ – арифметичний рід кривої C, параметр $n = degC = 4$.

Оскільки вона роду 1, то вона ізоморфна плоскій кубічній кривій але не є еліптичною, бо має особливості в проективній частині. Крива Едварса як і скручена крива Едаварса ізоморфна деякій афінній частині еліптичної кривої. Нормалізація кривої Едвардса – крива в формі Веєрштраса, що запропонована Монгомері E_M отримана шляхом біраціонального відображення $u = (1+y)/(1-y)$, $v = u/x$ [12], яка вже є еліптичною. При аналізі цієї теореми де було розглянуто цю біраціональну еквівалентність авторами Бессаловим А.В., Циганковою О. В. у статті [13] даремно критикуюь теорему 3.2 з авторитетного джерела [12], де аналізується ця біраціональна еквівалентність, допускають плутанину, підмінюючи термін біраціональна еквівалентність на ізоморфізм кривих у теоремі 1 зі своєї статті [13]. Також ними [13] допущено неточності в кінці розділу 1 в теоремі 1, де стверджують існування ізомормізму між скрученою кривою Едварса і кривою Монтгомері що неможливо, бо крива завжди розглядається над полем а не над його частиною як автори стверджують у теоремі 1 дарма називаючи теорему 3.2 з [12] не коректною. Один з можливих підходів до розв'язання сингулярності у цих двух точках є застосування нормалізазаційних замін, що є біраціональними відображеннями, які дозволяють виразити старі змінні x,y,z через нові регулярно: $x:z = u:w = t:v$, $y:z = t:u = v:w$.

Це перетворить нашу криву у просторову криву (у тривимірному проективному просторі), що задана двома рівняннями:

$$\begin{cases} au^2 + v^2 = w^2 + dt^2 \\ uv = wt \end{cases}$$

Оскільки вона роду 1, вона ізоморфна плоскій кубічній кривій. Остання кри ва не має особливостей і тому елемент яким ми розширили поле часток локального кільця є цілим алгебраїчним.

Властивості скрученої кривої Едвардса.

Лема 1. Якщо (x,y) точка кривої $E_{a,d}$, тоді має місце рівність

$$\left(\frac{1-dx_1^2}{p} \right) = \left(\frac{1-ax_1^2}{p} \right).$$

Доведення. З рівняння скрученої кривої Едвардса $ax^2+y^2=(1+dx^2y^2)$ отримуємо $y^2-dx^2y^2=1-ax^2$ $y^2-dx^2y^2=1-ax^2$ звідки $y^2(1-dx^2)=(1-ax^2)$. А оскільки квадратичність лівої частини визначається лише множником $(1-dx^2)$, то має місце конгруентність $\left(\frac{1-dx_1^2}{p}\right)=\left(\frac{1-ax_1^2}{p}\right)$.

Лема 2. Якщо (x,y) точка кривої $E_{a,d}$, тоді має місце рівність

$$\left(\frac{a-dy_1^2}{p}\right)=\left(\frac{1-y_1^2}{p}\right).$$

Доведення. З рівняння скрученої кривої Едвардса $ax^2+y^2=(1+dx^2y^2)$ отримуємо $ax^2-dx^2y^2=1-y^2$ звідки $x^2(a-dy^2)=1-y^2$. А оскільки квадратичність лівої частини визначається лише множником $a-dy^2$, то має місце конгруентність $\left(\frac{a-dy_1^2}{p}\right)=\left(\frac{1-y_1^2}{p}\right)$.

Твердження 1. Для довільної точки (x_1,y_1), яка не є точкою порядку 2 чи 4, кривої (1) при $e=1$ виконується рівність

$$\left(\frac{1-ax_1^2}{p}\right)\left(\frac{1-y_1^2}{p}\right)=\left(\frac{a-d}{p}\right).$$

Доведення. Для точки $P=(x_1,y_1)$ з що задовольняє рівняння кривої (1) розглянемо добуток

$$(a-dy_1^2)(1-ax_1^2)=a+adx_1^2y_1^2-a^2x_1^2-dy_1^2=ay_1^2-dy_1^2=(a-d)y_1^2.$$

Згідно з лемою 2 маємо $\left(\frac{a-dy_1^2}{p}\right)=\left(\frac{1-y_1^2}{p}\right)$ підставивши це в останню рівність замість $(a-dy_1^2)$ отримуємо нову рівність лишків $\left(\frac{1-ax_1^2}{p}\right)\left(\frac{1-y_1^2}{p}\right)=\left(\frac{a-d}{p}\right)$ що і потрібно було довести.

Можливість виконання оберненої операції до операції подвоєння точки ще й досі не досліджена для скрученої кривої Едвардса, наступна теорема дає відповідь на це питання.

Зауважимо, що під подільністю точки (X; Y) навпіл розумітимемо знаходження її праобразу тобто точки (x; y), яка додавалася до себе при застосуванні формули подвоєння точки [1].

Теорема. Для довільної точки $G=(X,Y)$ скрученої кривої Едвардса (1), що не є точкою 2-го чи 4-го порядка, існують точки поділу на 2 тоді і тільки тоді, коли $\left(\frac{1-aX^2}{p}\right)\neq -1$.

Доведення. Для скрученої кривої Едвардса закон подвоєння має форму [11]

$$2(x_1,y_1)=\left(\frac{2x_1y_1}{y^2+ax_1{}^2},\frac{y_1^2-ax_1{}^2}{1-dx_1{}^2y_1^2}\right)=(X,\mathrm{Y})$$

звідси, скориставшись рівнянням кривої ми виводимо модифіковану формулу додавання точки до самої себе:

$$2(x_1,y_1)=\left(\frac{2x_1y_1}{1+dx_1{}^2y_1^2},\frac{y_1^2-ax_1{}^2}{1-dx_1{}^2y_1^2}\right)=(X,Y)=G. \qquad (3)$$

Розглянемо рівняння

$\frac{2x_1y_1}{1+dx_1{}^2y_1{}^2}=X$, що рівносильне $dXx^2y^2-2xy+X=0$ і зробимо заміну $t=x_1y_1$ після чого отримаємо рівняння

$$dXt^2-2t+X=0,$$

розв'язок, якого існує якщо і тільки якщо $\left(\frac{1-dX^2}{p}\right)=1$ (або $1-dX^2\equiv 0(\mathrm{mod}\,p)$).

Розв'язки мають вигляд $t_{1,2}=\frac{1\pm\sqrt{1-dX^2}}{dX}$, вони існують як тільки $\left(\frac{1-dx_1^2}{p}\right)=1$. Згідно з Лемою 1 $\left(\frac{1-dx_1^2}{p}\right)=\left(\frac{1-ax_1^2}{p}\right)$. Для точки $P=(x_1,y_1)$ з що задовольняє рівняння кривої (1) розглянемо добуток

З рівності (2) маємо для першої ще одне рівняння

$$\frac{2x_1y_1}{y_1^2+ax_1^{\,2}}=X$$

Зробимо заміну $u=\frac{y}{x}$ отримаємо $\frac{2u}{u^2+a}=X$ або $2u=X(u^2+a)$ перепишемо як квадратне рівняння відносно u $Xu^2-2u+Xa=0$ з визначником $D_2=4(1-aX^2)$. Отже, згідно з Лемою 1 рівняння $dXt^2-2t+X=0$ і $Xu^2-2u+Xa=0$ розв'язні одночасно, що дає вираз для координат точки $P_j=(x_j,y_j)$: $x_j=\sqrt{t_ju_j^{-1}}, y_j=\sqrt{t_ju_j}$ $j\in\{0,1\}$

Прирівнюючи ліві частини рівностей $\frac{2x_1y_1}{1+dx_1^{\,2}y_1^{\,2}}=X$ і $\frac{2x_1y_1}{y^2+ax_1^{\,2}}=X$ отримуємо $ax_1^2+y_1^2=1+dx_1^2y_1^2$, тобто отримані пари (x_i,y_j) задовольняє рівнянню кривої, що також слідує з замкнутості групової операції. Помітимо, що разом з (x_1,y_1) вище вказані рівняння задовольняють $(-x_1,-y_1),(-y_1,-x_1),(y_1,x_1)$

$$Y^2=\frac{1-aX^2}{1-dX^2}=\frac{1-a\frac{4t^2}{(y^2+ax^2)^2}}{1-d\frac{4t^2}{y^2+ax^2}}=\frac{(y^2+ax^2)^2-4at^2}{(y^2+ax^2)^2-4dt^2}=\frac{(y^2+ax^2)^2-4at^2}{(1+dt^2)^2-4dt^2}=\frac{(y^2-ax^2)^2}{(1-dt^2)^2}=\frac{(y^2-ax^2)^2}{(1-dx^2y^2)^2}$$

Отже, отримали рівняння, що задає другу координату після подвоєння точки (x_1,y_1), піднесене до квадрату. Це рівняння ми використаємо для вибору правильного з додаткових коренів $(-x_1,-y_1),(-y_1,-x_1),(y_1,x_1)$ до істинного кореня (x_1,y_1). Таким чином друге рівняння задовольняють точки (x_1,y_1) і $(-x_1,-y_1)$. Помітимо, що $(-x_1,-y_1)=(x_1,y_1)+D$

Врахувавши, що $y_1^2-dx_1^2y_1^2=1-ax_1^2$ звідки $y_1^2(1-dx_1^2)=1-ax_1^2$, маємо

$$\left(\frac{1-ax_1^2}{p}\right)=\left(\frac{1-dx_1^2}{p}\right).$$

З рівності (2) для другої координати маємо визначальне рівняння

$$x_{1,2}^2=\frac{Y(\mathrm{d}(\frac{1\pm\sqrt{1-dX^2}}{dX})^2-1)\pm\sqrt{Y^2(1-\mathrm{d}\frac{1\pm\sqrt{1-dX^2}}{dX})^2+4d(\frac{1\pm\sqrt{1-dX^2}}{dX})^2}}{2d} \tag{5}$$

Крім того $y^2=\frac{t^2}{x^2}=\frac{(1+\sqrt{1-dx^2})^2}{dx^3}$ тобто елемент dx, де x визначається умовою (5), повинен бути квадратичним лишком в $\mathbb{F}_p$. Помітимо, що обидва корені рівнянь (4) і (5) є спряженими ірраціональностями, тому якщо один з них задовольняє рівняння над Z чи над $\mathbb{F}_p$, що отримане операціями додавання, множення і піднесення в натуральну степінь, то всі вони його задовольняють. Тому всі знайдені координати задовольняють рівнянню кривої (1) і рівнянням операції подвоєння точки.

Зауваження.

Разом з точкою $P=(x_1,y_1)$ рівняння (2) та (3) а також рівняння самої кривої задовольняє і точка $Q=P+D=(x_2,y_2)$.

Доведення. Випливає з комутативності групи точок тому $Q+Q=P+D+P+D=2P+O$, бо точка D має порядок 2.

Твердження. Крива Едвардса містить точку порядка 8 тоді і только тільки, коли

$$\left(\frac{1-d}{p}\right)=1.$$

Правильність твердження слідує з того, що точки 8-го порядка задовольняють рівняння $2Q=F$, де $F=(\pm1,0)$ – точки 4-го порядка. Те, що точка Q має вигляд (x,x) слідує з формул додавання точок [2, 12] і з рівняння кривої (1). Звідси з рівняння кривої маємо $2(x,x)=(\pm1,0)$, де $(\pm1,0)=F$ це координати точки 4-го порядка. Значить, точка Q лежить на диагоналі, тобто $|x|=|y|$. Звідси і з рівняння кривої маємо біквадратне рівняння $2x^2=1+dx^4$, $dx^4-2x^2+1=0$. Дискримінант якого є наступним $D=4-4d=4(1-d)$. Тому, щоб розв'язок існував необхідно і достатньо, щоб $\left(\frac{1-d}{p}\right)=1$.

Нехай $\left(e,\left|E_{1,d}\right|\right)=1$, де $e\in\mathbb{N}$, тоді в якості формули генерації псевдовипадкових послідовностей над полем $\mathbb{F}_{p^n}$ можна використати $P_j=e^jP_0$, P_0 – твірний групи кривої Едварса, її важкооборотність грунтується па проблемі дискретного логарифма. А біт складності односторонньої функції визначимо через композицію $Tr(x)=x+x^p+...+x^{p^{n-1}}$, де x – це перша координата з e^jP_0 з предикатом половинності заданим як

$$f_i=\begin{cases}0,\ Tr(x_i)<\dfrac{p-1}{2},\\ 1,\ Tr(x_i)\geq\dfrac{p-1}{2}.\end{cases}$$

Висновки. Дослідження дозволило знайти критерію суперсингулярності кривих, що дає можливість перевіряти криві на придатність до використання в якості носія групи точок для генератора псевдовипадкових послідовностей великого періоду.

Список використаних джерел:

1. Edwards H. A normal form for elliptic curves. *American Mathematical Society*. 2007. Vol. 44. No. 3. P. 393–422.
2. Hisil Huseyin, Koon-Ho Wong Kenneth, Carter Gary. Twisted Edwards Curves Revisited. *ASIACRYPT LNCS 5350*. 2008. P. 326–343.
3. Скуратовський Р., Мовчан П. В., Нормалізація скрученої кривої Едвардса та дослідження її властивостей над Fp. *Збірник праць 14 Всеукраїнської науково-практичної конференції. ФТІ НТУУ «КПІ»*. 2016. Том 2. С. 102–104.
4. Скуратовський Р. Дослідження властивостей скрученої кривої Едвардса. *Конференція державної служби спеціального зв'язку та захисту інформації.* URL: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?showHidden=1artid=252312catid=240232 ctime=1464080781894
5. Сергієнко І., Задірака В., Литвин О. Елементи загальної теорії оптимальних алгоритмів та суміжні питання. К. : Наук. думка, 2012. 400 с.
6. *Алексеев Е., Ошкин И., Попов В., Смышляев С., Сонина Л.* О перспективах использования скрученных эллиптических кривых Эдвардса со стандартом ГОСТ Р 34.10-2012 и алгоритмом ключевого обмена на его основе. *Материалы XVI международной конференции «РусКрипто 2014»*. 2014. С. 24–26.
7. Menezes A., Okamoto T., Vanstone S. Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field. *IEEE Transactions On Information Theory*. 1993. Vol. 39. No. 5. P. 1603–1646.
8. Skuratovskii R. V. Twisted Edwards curve and its group of points over finite field Fp. *Літня школа «Алгебра, Топологія, Аналіз»*. Одеса, 2016. С. 122–124.
9. Skuratovskii R., Skruncovich U. Twisted Edwards curve and its group of points over finite field Fp. *Akademgorodok, Novosibirsk, Russia. Conference. Graphs and Groups, Spectra and Symmetries*. URL: http://math.nsc.ru/conference/g2/g2s2/exptext/SkruncovichSkuratovskii-abstract-G2S2.pdf
10. Fulton W. Algebraic curves. An Introduction to Algebraic Geometry. *Third Preface – January*, 2008. 121 p.
11. Deepthi P.P., Sathidevi P.S. New stream ciphers based on elliptic curve point multiplication. *Computer Communications*. 2009. Vol. 32. P. 25–33.
12. Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, Christiane Peters. Twisted Edwards Curves. *IST Programme ECRYPT, and in part by grant ITR-071649.* 2008. P. 1–17.
13. Бессалов А.В., Цыганкова О.В. Производительность групповых операций на скрученной кривой Эдвардса над простым. *Радиотехника*. 2015. Вып. 181. С. 58–63.
14. Skuratovskii R.V. Constructing of finite field normal basis in deterministic polynomial time (in Ukraine). *Bulletin of Kiev national university of Tarasa Shevchenka*. 2011. P. 49–54.

References:

1. Edwards, H. (2007). A normal form for elliptic curves. *American Mathematical Society*, vol. 44, no. 3, pp. 393–422. [in English].
2. Hisil Huseyin, Koon-Ho Wong Kenneth, Carter Gary. (2008). Twisted Edwards Curves Revisited. *ASIACRYPT LNCS 5350*, pp. 326–343. [in English].
3. Skuratovskyi, R., Movchan, P. V. (2016). Normalizatsiia skruchenoi kryvoi Edvardsa ta doslidzhennia yii vlastyvostei nad Fp. *Zbirnyk prats 14 Vseukrainskoi naukovo-praktychnoi konferentsii. FTI NTUU «KPI»*, vol. 2, pp. 102–104. [in Ukrainian].
4. 9. Skuratovskyi, R. Doslidzhennia vlastyvostei skruchenoi kryvoi Edvardsa. *Konferentsiia derzhavnoi sluzhby spetsialnoho zviazku ta zakhystu informatsii*. URL: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?showHidden=1artid=252312catid=240232 ctime=1464080781894 [in Ukrainian].
5. Serhiienko, I., Zadiraka, V., Lytvyn, O. (2012). Elementy zahalnoi teorii optymalnykh alhorytmiv ta sumizhni pytannia. K.: Nauk. dumka, 400 p. [in Ukrainian].
6. Alekseev, E., Oshkin, I., Popov, V., Smyshlyaev, S., Sonina, L. (2014). O perspektivah ispolzovaniya skruchennyh ellipticheskih krivyh Edvardsa so standartom GOST R 34.10-2012 i algoritmom klyuchevogo obmena na ego osnove. *Materialy XVI mezhdunarodnoj konferencii «RusKripto 2014»*, pp. 24–26. [in Russian].
7. Menezes, A., Okamoto, T., Vanstone, S. (1993). Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field. *IEEE Transactions On Information Theory*, vol. 39, no. 5, pp. 1603–1646. [in English].

8. Skuratovskii, R. V. (2016). Twisted Edwards curve and its group of points over finite field Fp. *Litnia shkola «Alhebra, Topolohiia, Analiz»*, Odesa, pp. 122–124. [in English].

9. Skuratovskii, R., Skruncovich, U. Twisted Edwards curve and its group of points over finite field Fp. Akademgorodok, Novosibirsk, Russia. *Conference. Graphs and Groups, Spectra and Symmetries*. URL: http://math.nsc.ru/conference/g2/g2s2/exptext/SkruncovichSkuratovskii-abstract-G2S2.pdf [in English].

10. Fulton, W. (2008). Algebraic curves. An Introduction to Algebraic Geometry. *Third Preface – January*, 121 p. [in English].

11. Deepthi, P.P., Sathidevi, P.S. (2009). New stream ciphers based on elliptic curve point multiplication. *Computer Communications*, vol. 32, pp. 25–33. [in English].

12. Daniel, J. Bernstein, Peter, Birkner, Marc, Joye, Tanja, Lange, Christiane, Peters. (2008). Twisted Edwards Curves. *IST Programme ECRYPT, and in part by grant ITR-071649*, pp. 1–17. [in English].

13. Bessalov, A.V., Cygankova, O.V. (2015). Proizvoditelnost gruppovyh operacij na skruchennoj krivoj Edvardsa nad prostym. *Radiotehnika*, vol. 181, pp. 58–63. [in Russian].

14. Skuratovskii, R.V. (2011). Constructing of finite field normal basis in deterministic polynomial time (in Ukraine). *Bulletin of Kiev national university of Tarasa Shevchenka*, pp. 49–54. [in English].

УДК 004.9
DOI https://doi.org/10.32689/maup.it.2021.1.9

Денис ШИБАЄВ
аспірант кафедри технічної кібернетики та інформаційних технологій, Одеський національний морський університет, вул. Мечникова, 34, м. Одеса, Україна, індекс 65029 (denscreamer@gmail.com)

ORCID: https://orcid.org/0000-0002-3260-5843

Наталя ШИБАЄВА
кандидат технічних наук, доцент кафедри інформаційних технологій, Державний університет «Одеська політехніка», просп. Шевченко, 1, м. Одеса, Україна, індекс 65001 (nati.shibaeva@gmail.com)

ORCID: https://orcid.org/0000-0002-7869-9953

Тетяна ОТРАДСЬКА
кандидат технічних наук, доцент кафедри інформаційних систем, Державний університет «Одеська політехніка», просп. Шевченко, 1, м. Одеса, Україна, індекс 65001 (tv_61@ukr.net)

ORCID: https://orcid.org/0000-0002-5808-5647

Артем КІКОТЬ
студент, ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», вул. Фрометівська, 2, м. Київ, Україна, індекс 03039 (artkik@gmail.com)

ORCID: https://orcid.org/0000-0001-5191-4273

Denis SHIBAYEV
Graduate student of the Department of Technical Cybernetics and Information Technologies, Odessa National Maritime University, str. Mechnikova, 34, Odessa, Ukraine, postal code 65029 (denscreamer@gmail.com)

Natalia SHIBAYEVA
Candidate of Technical Sciences, Associate Professor of Information Technology, Odessa Polytechnic State University, ave. Shevchenko, 1, Odessa, Ukraine, postal code 65001 (nati.shibaeva@gmail.com)

Tatiana OTRADSKA
PhD in Technical Sciences, Associate Professor of Information Systems Department, Odessa Polytechnic State University, ave. Shevchenko, 1, Odessa, Ukraine, postal code 65001 (tv_61@ukr.net)

Artem KIKOT
Student, Interregional Academy of Personnel Management, str. Frometivska, 2, Kyiv, Ukraine, postal code 03039 (artkik@gmail.com)

Бібліографічний опис статті: Шибаєв Д., Шибаєва Н., Отрадська Т., Кікоть А. Проектування інформаційної системи з динамічного аналізу енергетичних ресурсів. *Інформаційні технології та суспільство*. 2021. Вип. 1. С. 77–84. DOI: https://doi.org/10.32689/maup.it.2021.1.9

Bibliographic description of the article: Shybaiev, D., Shybaieva, N., Otradska, T., Kikot, A. (2021). Proektuvannia informatsiinoi systemy z dynamichnoho analizu enerhetychnykh resursiv [Design of information system on dynamic analysis of energy resources]. *Informatsiini tekhnolohii ta suspilstvo – Information technology and society*, 1, 77–84. DOI: https://doi.org/10.32689/maup.it.2021.1.9

ПРОЕКТУВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ З ДИНАМІЧНОГО АНАЛІЗУ ЕНЕРГЕТИЧНИХ РЕСУРСІВ

Анотація. *Активне використання засобів прогнозування стрімко впроваджується в різні напрямки бізнесу та економіки. Це пов'язано з великою динамікою змін цін на різні види товарів, нестабільною ситуацією з валютним курсом, а також різними зовнішніми факторами, які можуть впливати на ціноутворення в країні. Одним з напрямків товарів, прогнозування динаміки якого є суттєвою задачею, є енергетичний ринок країни. Проектування та розробка сучасного програмного засобу, який використовує ефективні алгоритми аналізу та прогнозування дина-*

міки зміни цін на енергетичному ринку, дозволить мінімізувати розбіжність цін між постачальниками сировини і готової продукції. ***Метою*** *статті є опис процесу проектування інформаційної системи динамічного аналізу та методів оцінки інформації та побудови прогнозів щодо визначення актуальних коефіцієнтів вартості на енергетичних ринках країни. Реалізація поставленої мети передбачає вирішення низки завдань: 1) організація методів збору аналітичних вхідних даних; 2) проектування логіки та компонентів інформаційної системи з використанням нотацій UML; 3) визначення функціонального алгоритму прогнозування та застосування його в якості оптимального методу побудови прогнозу в інформаційній системі.* ***Наукова новизна.*** *Спроектоване та розроблене рішення використовує комплексні аналітичні засоби які дозволяють підвищити ефективність закупівлі палива на споживацькому ринку. Таке рішення дозволить мінімізувати вартість товарів та послуг які прямим чином залежать від вартості палива чи інших енергетичних ресурсів. Як* ***висновок****, у статті наголошується, що сучасний ринок палива та енергетичних ресурсів дуже погано прогнозується та не дозволяє кінцевим користувачам аналізувати динаміку зміни вартості. Все це суттєвим чином впливає на вартість послуг та товарів, які залежать від кінцевої вартості палива. Проектування, розробка та впровадження прозорої системи з аналізу інформації та побудови прогнозу з динаміки змін вартості на паливо дозволить мінімізувати витрати серед потенційних клієнтів та зробити процес регулювання вартості енергетичних ресурсів більш прозорим.*

Ключові слова: *прогнозування, аналіз даних, парсинг, енергетика, обробка даних.*

DESIGN OF INFORMATION SYSTEM ON DYNAMIC ANALYSIS OF ENERGY RESOURCES

Abstract. *Active use of forecasting tools is rapidly being introduced in various areas of business and economy. This is due to the high dynamics of changes in prices for different types of goods, the unstable situation with the exchange rate, as well as various external factors that may affect pricing in the country. One of the areas of goods, forecasting the dynamics of which is an important task, is the country's energy market. The design and development of modern software, which uses effective algorithms for analyzing and forecasting the dynamics of price changes in the energy market, will minimize price differences between suppliers of raw materials and finished products.* ***The aim.*** *The purpose of the article is to describe the process of designing an information system for dynamic analysis and methods of information evaluation and forecasting to determine the actual cost ratios in the energy markets of the country. The implementation of this goal involves solving a number of tasks: 1) the organization of methods for collecting analytical input data; 2) designing the logic and components of the information system using UML notations; 3) determination of the functional forecasting algorithm and its application as an optimal method of forecasting in the information system.* ***Scientific novelty.*** *The designed and developed solution uses complex analytical tools that allow to increase the efficiency of fuel purchase in the consumer market. This solution will minimize the cost of goods and services that directly depend on the cost of fuel or other energy resources. In* ***conclusion,*** *The article emphasizes that the modern market of fuel and energy resources is very poorly predicted and does not allow end users to analyze the dynamics of cost changes. All this significantly affects the cost of services and goods, which depend on the final cost of fuel. The design, development and implementation of a transparent system for analyzing information and forecasting the dynamics of changes in fuel prices will minimize costs among potential customers and make the process of regulating the cost of energy resources more transparent.*

Key words: *forecasting, data analysis, parsing, energy, data processing.*

Актуальність проблеми. Дешева нафта збільшила продаж автомобілів на багатьох світових ринках, однак український ринок залишився незмінним. В Україні з її складною економікою слідом за нафтовими котируваннями впали і реальні доходи громадян, які сьогодні не мають можливість оновлювати свої автомобілі. За словами експертів, український авторинок буде відновлюватися в міру зростання цін на чорне золото, а вони можуть залишатися на нинішньому рівні ще не один рік [1–2].

Коливання нафтових котирувань відбуваються регулярно, причому це може бути і стрибкоподібне зростання ціни, і продовження падіння вартості бареля вниз. Очевидно, що така тенденція збережеться в 2021 році, тобто вартість нафти буде відрізнятися високою волатильністю. Все це дозволяє сформувати чітку стратегічну лінію поведінки автобізнесменів. До того ж зміна вартості бареля нафти не миттєво відбивається на ціні палива, причому в різних країнах зв'язок між цими параметрами різний, і не завжди зниження нафтових котирувань призводить до зменшення вартості бензину. Нарешті, в світі є досить значна група споживачів, яка практично ніяк не реагує на зміну цін на паливо і продовжує їздити на автомобілях, які споживають багато пального, і компанії не можуть нехтувати ними. Нафтовий сектор відіграє найважливішу роль в економіці України і формуванні доходів бюджетів усіх рівнів. Частка податкових платежів, пов'язаних з нафтовим сектором (включаючи сектор торгівлі нафтопродуктами), в доходах консолідованого бюджету перевищує 30% [3].

Основна частина нафтових доходів, що надходять до бюджету, вилучається через податок на видобуток корисних копалин (ПВКК)і експортне мито на нафту. Їх сукупна частка становить понад 80% надходжень з нафтового сектора в консолідований бюджет. Однак вливання коштів з нафтового сектора в бюджет відбувається і через інші податки: акцизи на нафтопродукти, а також податки, якими обкладаються різні ділянки виробничого ланцюжка випуску нафтопродуктів – нафтовидобуток, нафтопереробка, оптова і роздрібна торгівля нафтопродуктами. Нафтопродукти і газова промисловість є товаром, ціни на які в Україні представляють важливий індикатор соціально-економічного благополуччя. Тому актуальні вивчення цих цін і пошук підходів до їх прогнозування є важливою задачею в якій слід застосовувати сучасні інформаційні технології [4].

Аналіз останніх досліджень і публікацій. Ціна нафти на внутрішньому ринку визначається світовою ціною на нафту. На внутрішній ринок поставляється рівно стільки нафти, скільки необхідно для задоволення внутрішнього попиту на нафтопродукти, а інший обсяг експортується. Однак для того, щоб у нафтодобувача зберігалися стимули для поставки нафти на внутрішній ринок, її продаж повинен бути як мінімум не менш рентабельним, ніж експорт. Світова ціна визначається біржовими тенденціями, а формування внутрішньої ціни відбувається шляхом вирахування експортного мита і вартості грантсортування нафти до біржових базисів поставки [5].

Прогноз індексів цін на нафтопродукти проводиться за товарними групами в наступній номенклатурі:

- бензин автомобільний;
- дизельне паливо;
- моторні мастила (вітчизняні);
- авіагас;
- інше.

Тут слід розрізняти ціни виробників (які не включають ПДВ і непрямі податки, а також транспортні витрати) і ціни придбання (які включають ПДВ, непрямі податки і транспортні витрати).

Тепер проведемо оцінку залежності вартості бензину від курсу долара. Ціна на бензин, який роблять з закупленої нафти на території України залежить від курсу гривні по відношенню до іноземної валюти.

Справа в тому, що Українські компанії займаються виробництвом і збутом бензину, як і більша частина Українського бізнесу кредитується в іноземних банках у валюті. Тобто вони беруть кредити на розвиток бізнесу в доларах або євро. Частина цих грошей витрачається на покупку імпортного устаткування, частина змінюється на гривні для забезпечення поточних витрат в Україні, таких як виплати зарплат, податки та інше. При цьому виторг вони отримують від продажу бензину на українському ринку в гривнях, а кредити треба віддавати у валюті. І якщо котирування гривні падають, то для розрахунку з кредиторами їх треба більше. Крім того бізнес періодично повинен надавати кредиторам звітність про результати своєї діяльності. І якщо ці звіти негативні, наприклад, зафіксовано падіння прибутку, то банки можуть зажадати повернення всього боргу відразу. Так як банки іноземні, то і прибуток вони вважають в доларах або євро. І щоб зберегти рівень прибутку в валюті на поточному рівні, бізнесу нічого не залишається окрім як підвищувати гривневі ціни на свої товари слідом за ослабленням останньої. Це відноситься до всього бізнесу, не тільки до виробників бензину [6].

Таким чином, можна зробити висновок про те, що зв'язок між ціною на нафту і на бензин прямо пропорційна, так як бензин – це продукт нафтопереробки. Хоча при зростанні цін на нафту – ціни на бензин повинні підвищуватися, а при зниженні – падати. Але зростання цін на бензин спровоковані підвищенням податку на видобуток корисних копалин. В антимонопольній службі пов'язують зростання цін на паливо з низькою конкуренцією на цьому ринку і змовою торговців паливом.

При формуванні ціни повинні враховуватися чинники якості продуктів, що відпускаються з українських нафтопереробних заводів, віддаленість цих заводів від ринків споживання їх продукції, технологічна оснащеність українських НПЗ, економічна ефективність виробництва, розмір партії на локальних ринках у порівнянні зі світовими, сезонні коливання попиту і цін, інерційність внутрішнього ринку щодо світового. Слід також враховувати фактор високої волатильності, різких змін світових цін.

Методика заснована на прямому застосуванні світових оптових цін, зменшених на величину експортного мита а також з використанням методики єдиного граничного рівня цін для всіх НПЗ. Такий підхід до того ж дозволяє плавно інтегрувати біржові котирування в формулу ціноутворення.

Попит на рідкі види палива (нафтопродукти, біопалива та палива, вироблені за технологіями Gas-to-liquids і Coal-to-liquids) зростає найбільш повільними темпами в порівнянні з іншими видами палива, з уповільненням до кінця розглянутого періоду. До 2040 року в Базовому сценарії світовий попит на рідкі палива виросте приблизно на чверть у порівнянні з 2020 роком [7-10].

Метою статті є опис проектної частини інформаційної системи та методу прогнозування динаміки коливань на нафтових ринках для визначення кінцевої вартості нафтопродуктів та перероблених ресурсів на внутрішньому ринку країни.

Виклад основного матеріалу. При прогнозуванні попиту на рідкі палива використовується поєднання двох методик: методики прогнозування попиту на нафту через нафтоємність окремих економік, а також визначення попиту на нафту як суму попиту на окремі нафтопродукти (ЗВГ, бензини, нафта, дизельне паливо, мазут, гас і інші нафтопродукти), при цьому попит на окремі нафтопродукти визначався через тренди ємності економік окремих країн до кожного відповідного продукту. Попит на біопалива та інші рідкі види палива був визначений як сценарна передумова з додатковим дорахуванням через фактор міжпаливної конкуренції. Ціна на нафту (біржова та позабіржова) визначається двома ключовими факторами: поточним та очікуваним співвідношенням попиту та пропозиції, та ди-

намікою витрат. Оскільки відсутні точні дані про поточний світовий баланс між попитом та пропозицією на нафту, нафтотрейдери зосереджуються головним чином на інформації про зміни запасів нафти, стратегічних та промислових.

Процес проектування інформаційної системи складається з визначення функціональних складових системи прогнозування та етапів взаємодії системних компонентів із зовнішніми незалежними ресурсами. Діаграма варіантів використання, рис. 1, має можливість визначити архітектурну логіку та взаємодію елементів програмної системи, можливість зміни їх станів, та їх функціональне призначення. До головних структурних елементів слід віднести:

– Поточні показники. Зберігають в собі показники поточних цін на нафтопродукті, які утверджені міністерством фінансів та регулюються антимонопольним комітетом.

– Архів даних. Набір показників вартості нафтопродуктів та цін їх закупівлі, які архівуються на різних порталах. Дозволяє переглядати статистику та динаміку ціноутворення.

– Виклик прогнозованої моделі. Варіант використання який відповідає за виклик вже прогнозованої моделі та використання її для додаткового аналізу. Також цей варіант використання дозволяє зберігати різні прогнозовані моделі та зберігати статистику роботи інформаційної системи.

– Прогнозування динаміки. Набір математичних алгоритмів, які використовуються для визначення тенденції зміни цін на нафтопродукти. Є необхідним функціональним рішенням при прогнозуванні та оцінці поведінки нафтового ринку країни.

– Прогнозування зростання цін. Набір математичних алгоритмів які дозволяють побудувати ймовірнісний коефіцієнт зміни вартості палива: з використанням різних факторів та умов, які використовуються в такому типі прогнозування.

– Прогнозування зміни цін. Алгоритм винаходження коливання ціни від фактичного значення до прогнозованого з метою пошуку коефіцієнта різниці та покращенні роботи інформаційної системи та функціонального модуля прогнозування.

– Фактори залежності. Формування переліку головних факторів які можуть впливати на ціноутворення або використовуватися в змінах вартості на нафтопродукти.

– Збереження прогнозованої моделі. Відповідає за збереження спроектованої моделі в базі даних для можливості додаткового її використання.

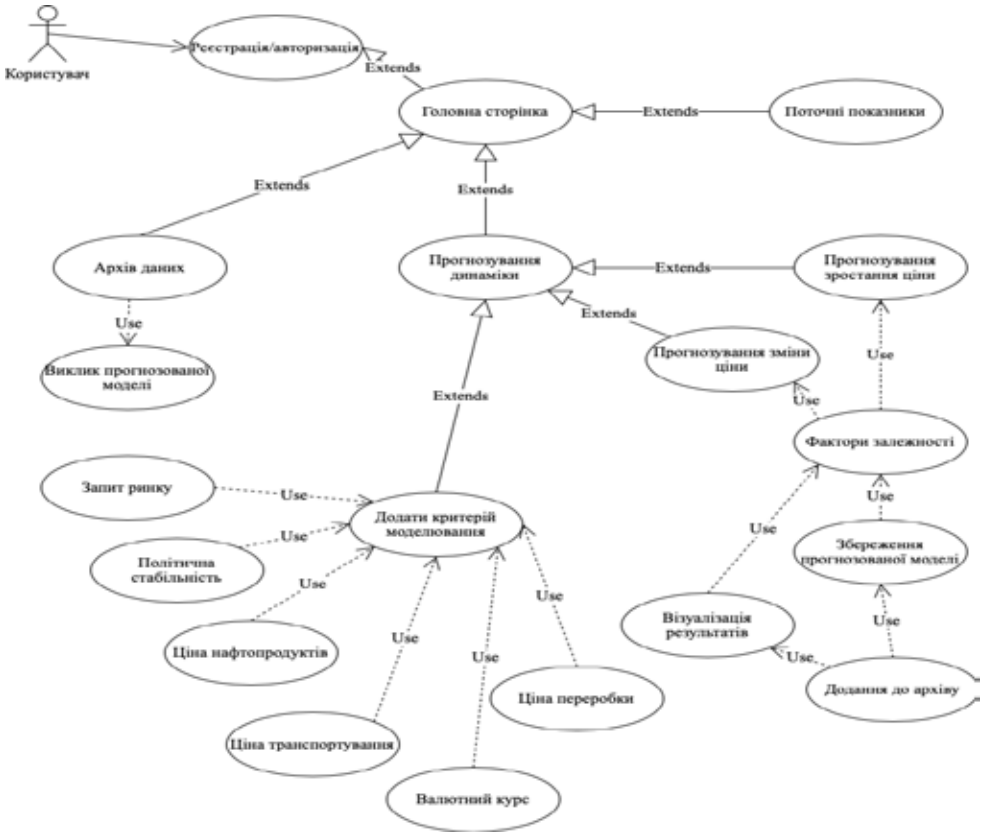


Рис. 1. Діаграма варіантів використання інформаційної системи

– Візуалізація результатів. Варіант використання який відповідає за виклик спеціалізованих бібліотек та компонентів візуалізації прогнозованих даних та взаємодії з ними.

– Додавання до архіву. Можливість архівування усіх даних використаних при прогнозуванні, а також збереження додаткових факторів впливу на результат.

– Додати критерій моделювання. Можливість власноруч додавати критерії, які мають вплив на паливний ринок, або на динаміку поведінки вартості на нафтопродукти. Початково використовується автоматизована система пошуку зовнішніх факторів та додання їх до моделювання.

Інші можливості системи мають додаткові функції, та використовуються для корегування точності прогнозованої моделі чи є необхідними для організації функціонування інформаційної системи із зовнішніми функціональними компонентами.

Робота системи побудована таким чином, що першим етапом є пошук та оновлення діагностичної інформації. Це є необхідним для побудови якісного прогнозу та формування динаміки поведінки вартості. Система використовує розроблений функціональний модуль парсингу, який дозволяє зберігати великі обсяги даних. Наступним етапом є побудова прогнозу та формування візуальної моделі. Це дозволяє аналітику визначати поведінку паливних ринків. Також є можливість додавати зовнішні фактори які можуть використовуватися як корегуючи коефіцієнти для більш якісної оцінки та побудови прогнозу. Такий процес візуалізується завдяки побудові діаграми станів, рис. 2.

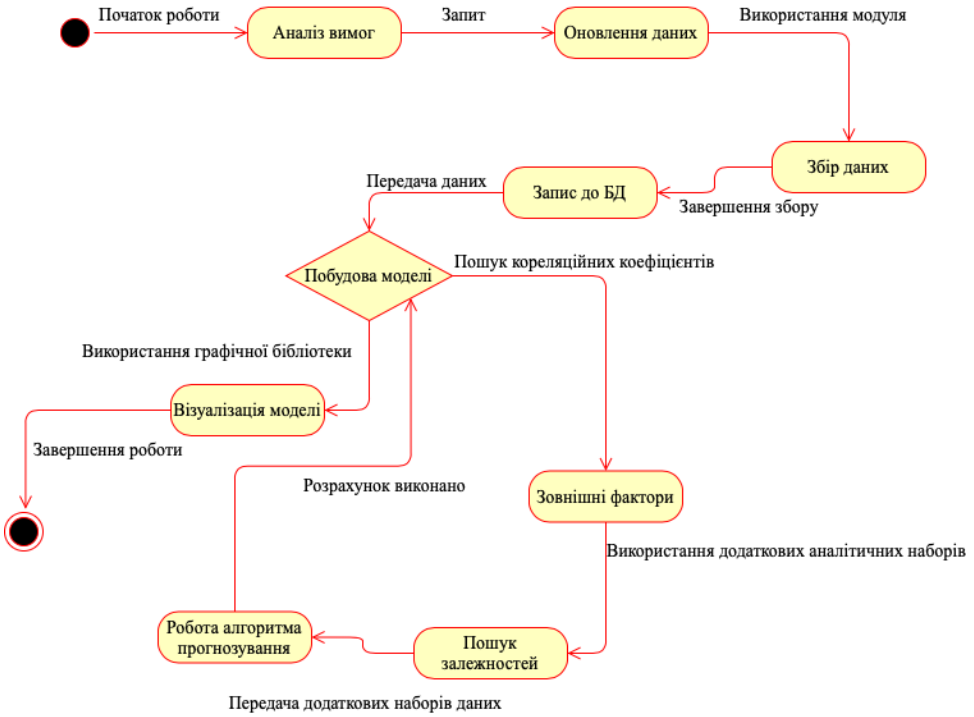


Рис. 2. Діаграма станів інформаційної системи

Реалізацію системи виконано засобами мови програмування GoLang для серверної частини та з використанням ReactJS для графічного інтерфейсу. Для забезпечення більш якісної візуалізації прогнозованих даних, застосовуються спеціалізовані бібліотеки візуалізації графіків. Для роботи з базами даних використано PostgresSQL, яке дозволяє зберігати та оброблювати великий обсяг інформації.

Розробка системи виконана за модульною архітектурою, та більшість робочих модулів виконується на сервері обробки даних. Складовою системи є розробка спеціалізованого парсеру, який автоматизовано під'єднується до різних фондових бірж за рахунок використання відкритих API на стороні бірж. Ґрунтуючись на принциповому алгоритмі роботи інформаційної системи, можливо сформувати логіку роботи системи на архітектурно-програмному рівні. Більшість процесів виконується на backend-рівні, отже система має загально-серверну оптимізацію. За рахунок використання REST.API є можливість сформувати роботу окремих модулів, рис. 3. Такий тип розробки має спеціалізований характер за рахунок можливості впровадження розробленої інформаційної системи, як компонента до будь-якого іншого web-рішення.

Це дозволить використовувати систему прогнозування та застосування отриманих даних як вхідну інформацію до різних напрямків ведення бізнесу, орієнтованого на паливних ринках, придбанні палива, чи переробці палива на інші матеріали.

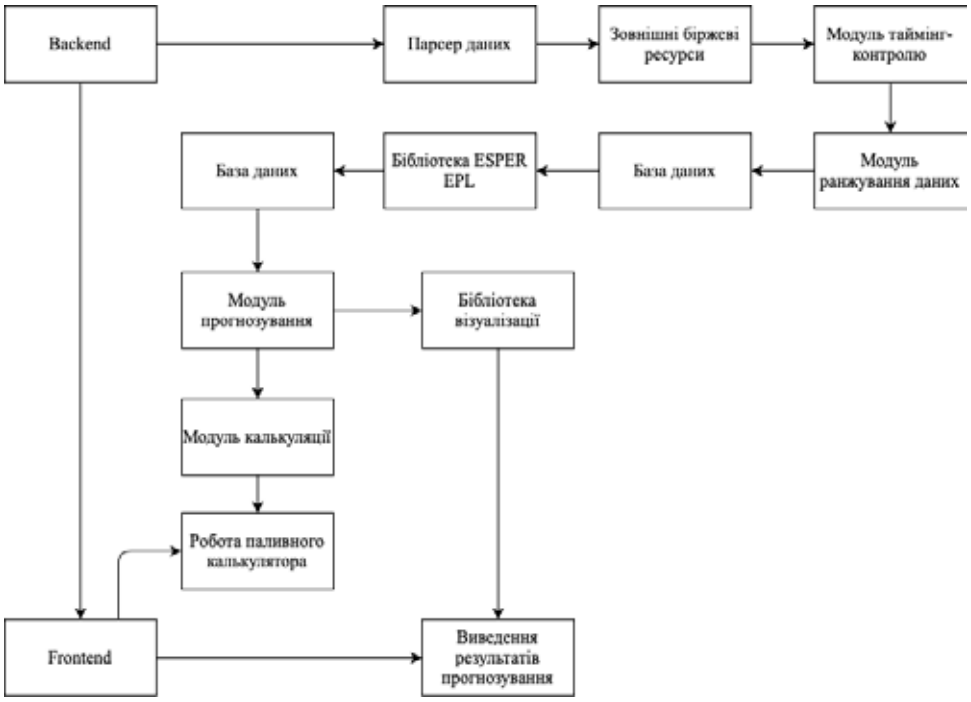


Рис. 3. Архітектурна схема роботи інформаційної системи

Web-платформа є оптимальним рішенням, за рахунок того, що не використовується прив'язування до апаратної платформи, а для роботи системи необхідно тільки наявність Інтернет-з'єднання та web-браузер для роботи.

Інтерфейсна частина системи включає в себе виведення прогнозованої динаміки на завтрашній день з урахуванням сьогоднішніх показників вартості, рис. 4. Прогноз будується та виводиться для:

- Нафти.
- Бензину марки А92.
- Бензину марки А95.
- Дизельного палива.
- Зріджений газ.

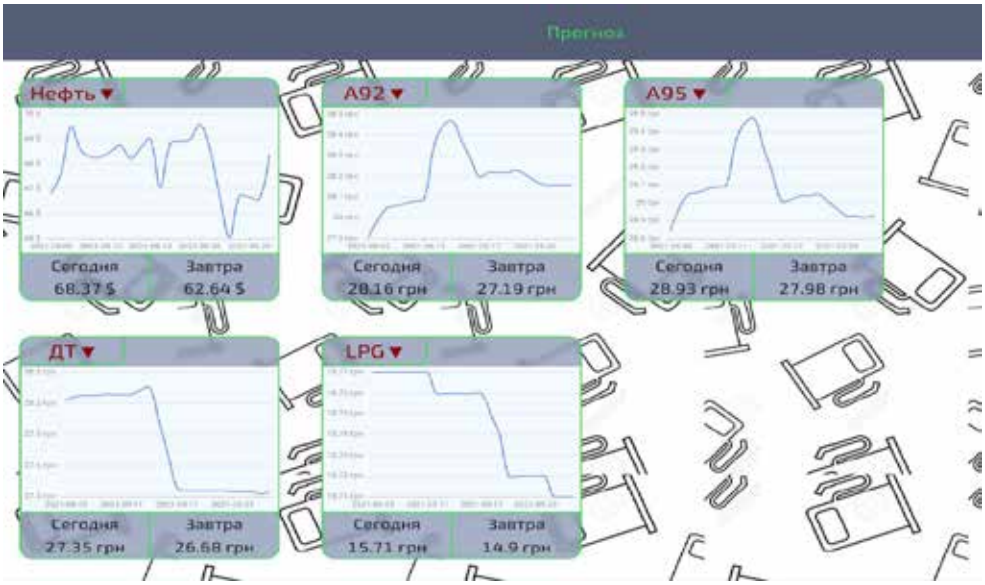


Рис. 4. Сторінка виведення прогнозованих даних

Для кожної окремої категорії можливо переглянути динамічний графік змін вартості, який зберігається та оновлюється завдяки постійній процедурі збору нових даних та оновленню розрахованої моделі, рис. 5. За рахунок використання великої кількості зовнішніх факторів, які прямим чи опосередкованим чином впливають на фінальну вартість нафтопродуктів, то допустима похибка системи прогнозування зумовлена 10% відсотками на 100 прогнозованих випадків. Тим самим можливо досить точно визначати динамічний коефіцієнт зміни вартості на наступний день, тиждень та навіть місяць.

Для нормально розподіленої випадкової величини при оцінці на грубі помилки часто використовують критерій Н.В. Смірнова (інші назви – критерій Граббса, критерій Смірнова-Граббса).

При відомої генеральної дисперсії *σ2* (наприклад, коли генеральна дисперсія досить точно відома за поточними вимірам) використовують статистику критерію *Tα*. Для цього будують варіаційний ряд результатів випробувань (тобто мають у своєму розпорядженні їх по зростанню) і, якщо одне з крайніх значень ряду сумнівно, обчислюють критерій для сумнівного значення *x* за формулою (1):

$$T = \frac{|x_i - \bar{x}|}{\sigma} \tag{1}$$

де *xi* – крайній (мінімальний чи максимальний) елемент варіаційного ряду;

$\bar{x}$ – середнє вибіркове;

σ – стандартне (середньоквадратичне) відхилення.

Рис. 5. Графік динамічної зміни вартості для обраної категорії

Стандартне відхилення визначається за формулою (2):

$$\sigma = \sqrt{\frac{\sum_{i=1}^{n}(x_i - \bar{x})^2}{n-1}}, \tag{2}$$

де *xi* – крайній (мінімальний чи максимальний) елемент варіаційного ряду;

$\bar{x}$ – середнє вибіркове;

n – число спостережнь.

Значення $T_{(min)}$ та $T_{(max)}$ порівнюються з критичним значенням *Cα* метода Смірнова-Граббса. Вибірка не містить грубих похибок, якщо $T_{(i)} \le C_{\alpha}$ [11–13].

Спроектована інформаційна система може використовуватися як самостійний програмний інструмент для збору, оцінки та прогнозування динаміки даних, так і в якості функціонального модуля, який інтегровано до інших програмних систем.

Висновки та перспективи подальших досліджень. Спроектована та розроблена система є універсальним математичним засобом, який може використовуватися в якості інструмента з прогнозуван-

ня для будь-якого напрямку, так як використовуються математичні алгоритми в яких є фактор подій. Додатковим компонентом системи було спроектовано та розроблено спеціалізований програмний модуль аналізу великого обсягу вхідних даних та додаткових факторів, які мають вплив на точність результатів прогнозування. Розроблена система є практичним інструментом та потужним рішенням в області прогнозування даних. Подальшим розвитком інформаційної системи є підвищення точності прогнозованих даних та мінімізація значення похибок процесу прогнозування та відбору достовірних даних. Додання додаткових методів перевірки якості даних та аналітично-корегуючі компоненти дозволять збільшити напрямки застосування інформаційної системи.

Список використаних джерел:

1. Агеев, А.Н. Стратегия развития ТЭК и механизмы ее реализации. *Нефть. Газ и бизнес*. 2013. № 5. С. 7–9.
2. Байков, Н. Мировая нефтяная промышленность: прогнозы развития до 2035 г. *Мировая экономика и международные отношения*. 2013. № 3. С. 54–61.
3. Васильева, Н.С. Формирование цены в рыночных условиях. М. : Бизнес. 2015. 620 с.
4. Калита, Н. Ценообразование в условиях рынка. Киев : УкрНИИТИ. 2014. С. 22.
5. Фадєєва, І.Г. Методологічні засади моделювання і прогнозування діяльності та фінансово-економічних показників об'єктів управління НГК. *Ефективна економіка*. 2015. № 1. URL: http://www.economy.nayka.com.ua/?op=1&z=3713
6. Трофимчук, Т.С. Моделирование тенденций добычи нефти, цены их взаимосвязей с факторами. *Проблемы экономики и управления нефтегазовым комплексом*. 2013. № 2. С. 45–49.
7. Бакулін, Є.М., Шелудченко, В.І., Єгер, Д.О. Основні напрямки розвитку нафтової і газової промисловості України. *Розвідка та розробка нафтових і газових родовищ*. 2007. № 4(25). С. 5–13.
8. Шибаева, Н.О., Шибаев, Д.С., Рудниченко, Н.Д, Вычужанин, В.В. Разработка модели решающего дерева для когнитивного представления метаданных о больших объемах информации. *Сборник материалов XXVI Международной научно-технической конференции. Нижегородский государственный технический университет им. Р.Е. Алексеева. 2020.* Нижний Новгород, 2020. С. 684–690.
9. Світлицький, В.М. Геологічні основи та теорія пошуків і розвідки нафти і газу : навч. посібник для ВНЗ. Київ : Інтерпрес ЛТД, 2010. 390 с.
10. Суярко, В.Г. Загальна та нафтогазова геологія. Харків : ХНУ імені В.Н. Каразіна, 2013. 212 с.
11. Frank, E. Grubbs. Sample Criteria for Testing Outlying observations. 1950. Vol. 21. No. 1. P. 27–58.
12. Frank, E. Grubbs. Procedures for Detecting Outlying Observations in Samples. *Technometrics*. 1969. Vol. 11. No. 1. P. 1–21.
13. СТ СЭВ 545-77. Прикладная статистика. Правила оценки анормальности результатов наблюдений. М. : Изд-во стандартов. 1978. 26 с.

References:

1. Ageev, A.N. (2013). Development strategy of the fuel and energy complex and mechanisms for its implementation. *Oil. Gas and business*, no. 5, p. 7–9. [in Russian].
2. Baykov, N. (2013). World oil industry: development forecasts up to 2035. *World economy and international relations*, no. 3, p. 54–61. [in Russian].
3. Vasilieva, N.S. (2015). Price formation in market conditions. M.: Business, 620 p. [in Russian].
4. Kalita, N. (2014). Pricing in market conditions. Kiev: UkrNIITI, p. 22. [in Russian].
5. Fadova, I.G. (2015). Methodological ambush of modeling and forecasting the performance and financial and economic indicators of oil and gas complex management. *The economy is effective*, no 1. URL: http://www.economy.nayka.com.ua/?op=1&z=3713. [in Ukrainian].
6. Trofimchuk, T. S. (2013). Modeling trends in oil production, prices of their relationships with factors. *Problems of economics and management of the oil and gas complex*, no 2, p. 45–49. [in Russian].
7. Bakulin, Y.M., Sheludchenko, V.I., Eger, D.O. (2007). The main directions of development of the naphtha and gas industry of Ukraine. *Development and distribution of naphtha and gas genera*, no 4 (25), p. 5–13. [in Ukrainian].
8. Shibaeva, N.O., Shibaev, D.S., Rudnichenko, N.D, Vychuzhanin, V.V. (2020). Development of a decision tree model for the cognitive representation of metadata about large amounts of information. *Collection of materials of the XXVI International Scientific and Technical Conference. Nizhny Novgorod State Technical University named after R.E. Alekseeva*. Nizhny Novgorod, p. 684–690. [in Russian].
9. Svitlitskiy, V.M. (2010). Geological bases and theory of production and development of oil and gas: Navch. checklist for VNZ. K.: Interpress LTD, 390 p. [in Ukrainian].
10. Suyarko, V.G. (2013). The geology of the Naftogaz. Kharkiv: KhNU imeni V.N. Karazina, 212 p. [in Ukrainian].
11. Frank, E. (1950). Grubbs. Sample Criteria for Testing Outlying observations, vol. 21, no. 1, p. 27–58. [in English].
12. Frank, E. (1969). Grubbs. Procedures for Detecting Outlying Observations in Samples. *Technometrics*, vol. 11, no. 1, p. 1–21. [in English].
13. ST SEV 545-77. (1978). Applied statistics. Rules for assessing the abnormality of observation results. M.: Publishing house of standards, 26 p. [in Russian].

УДК 004.9
DOI https://doi.org/10.32689/maup.it.2021.1.10

Денис ШИБАЄВ
аспірант кафедри технічної кібернетики та інформаційних технологій, Одеський національний морський університет, вул. Мечникова, 34, м. Одеса, Україна, індекс 65029 (denscreamer@gmail.com)

ORCID: https://orcid.org/0000-0002-3260-5843

Наталя ШИБАЄВА
кандидат технічних наук, доцент кафедри інформаційних технологій, Державний університет «Одеська політехніка», просп. Шевченко, 1, м. Одеса, Україна, індекс 65001 (nati.shibaeva@gmail.com)

ORCID: https://orcid.org/0000-0002-7869-9953

Микола РУДНІЧЕНКО
кандидат технічних наук, доцент кафедри інформаційних технологій, Державний університет «Одеська політехніка», просп. Шевченко, 1, м. Одеса, Україна, індекс 65001 (nickolay.rud@gmail.com)

ORCID: https://orcid.org/0000-0002-7343-8076

Володимир НІКІФОРОВ
студент, ПрАТ «ВНЗ «Міжрегіональна Академія управління персоналом», вул. Фрометівська, 2, м. Київ, Україна, індекс 03039 (nikifvova@gmail.com)

ORCID: https://orcid.org/0000-0001-6241-1516

Denis SHIBAYEV
Graduate student of the Department of Technical Cybernetics and Information Technologies, Odessa National Maritime University, str. Mechnikova, 34, Odessa, Ukraine, postal code 65029 (denscreamer@gmail.com)

Natalia SHIBAYEVA
Candidate of Technical Sciences, Associate Professor of Information Technology, Odessa Polytechnic State University, ave. Shevchenko, 1, Odessa, Ukraine, postal code 65001 (nati.shibaeva@gmail.com)

Mykola RUDNICHENKO
PhD in Technical Sciences, Associate Professor of Information Technology, Odessa Polytechnic State University, ave. Shevchenko, 1, Odessa, Ukraine, postal code 65001 (nickolay.rud@gmail.com)

Volodymyr NIKIFOROV
Student, Interregional Academy of Personnel Management, str. Frometivska, 2, Kyiv, Ukraine, postal code 03039 (nikifvova@gmail.com)

Бібліографічний опис статті: Шибаєв Д., Шибаєва Н., Рудніченко М., Нікіфоров В. Проектування гнучкої системи тестування web-ресурсів. *Інформаційні технології та суспільство*. 2021. Вип. 1. С. 85–91. DOI: https://doi.org/10.32689/maup.it.2021.1.10

Bibliographic description of the article: Shybaiev, D., Shybaieva, N., Rudnichenko, M., Nikiforov, V. (2021). Proektuvannia hnuchkoi systemy testuvannia web-resursiv [Design of a flexible web-resource testing system]. *Informatsiini tekhnolohii ta suspilstvo – Information technology and society*, 1, 85–91. DOI: https://doi.org/10.32689/maup.it.2021.1.10

ПРОЕКТУВАННЯ ГНУЧКОЇ СИСТЕМИ ТЕСТУВАННЯ WEB-РЕСУРСІВ

Анотація. *Роль тестування є невід'ємною частиною в сучасних процесах розробки, більш того, ця роль суттєво збільшується. Це пов'язано зі зростанням складності програмного продукту і збільшення вимог до його якості. З'являються нові способи і методи розробки програмного забезпечення та його підтримки. Одним з таких підходів є впровадження різних видів тестування під час етапу розробки продукту для виявлення і мінімізації програмних і логічних помилок, та підвищення якості програмного коду і продукту взагалі. Існує безліч методологій і типів тестування відмінності яких знаходиться в цілях і об'єктах тестування. Регресійне тестування, яке направлено на виявлення*

дефектів у вже протестованих ділянках коду, в основному проводять автоматизованим тестуванням. Для цього використовують системи з тестування програмного коду і пошуку помилок, які є програмними драйверами. Вони дозволяють аналізувати інформацію яка використовується в системі та методом перегляду програмного коду виконувати аналіз його працездатності. ***Метою*** *статті є розробка проекту системи тестування web-ресурсів в реальному часі із застосуванням гнучкого редактора тестових сценаріїв та системи масштабування функціональних можливостей системи. Реалізація поставленої мети передбачає вирішення низки* ***завдань****: 1) проектування системи обробки тестових сценаріїв; 2) формування системної логіки та поведінки програмної системи; 3) проектування аналітичного модуля візуалізації результатів тестування.* ***Наукова новизна.*** *Спроектоване рішення є спеціалізованим драйвером до системи тестування та перевірки якості Selenium. Таке рішення дозволяє тестувати web-ресурси із спеціалізовано-спроектованого тестового простору та аналізувати отримані результати із застосуванням спеціалізованого аналітичного модуля із візуалізацією графічних компонентів. Як* ***висновок****, у статті наголошується, що розробка сучасного програмного засобу, який дозволить верифікувати, аналізувати та перевіряти програмний код на наявність помилок для використання з прикладним програмуванням є актуальною та сучасною задачею, яка суттєвим чином підвищить якість розробки програмних продуктів та забезпечить можливість зберігати робочу документацію в єдиному вигляді. Подальшим розвитком є інтеграція окремого редактора тестових сценаріїв та додання можливостей проведення різних типів тестування програмних систем.*

Ключові слова: *тестування, selenium, якість програмних рішень, аналіз якості, web-системи.*

DESIGN OF A FLEXIBLE WEB-RESOURCE TESTING SYSTEM

Abstract. *The role of testing is an integral part of modern development processes, moreover, this role is significantly increasing. This is due to the increasing complexity of the software product and increasing requirements for its quality. New ways and methods of software development and support appear. One such approach is the introduction of various types of testing during the product development phase to detect and minimize software and logical errors, and improve the quality of software code and the product in general. There are many methodologies and types of testing, the differences of which are in the goals and objects of testing. Regression testing, which aims to detect defects in already tested areas of the code, is mainly performed by automated testing. To do this, use systems for testing software code and debugging, which are software drivers. They allow you to analyze the information used in the system and the method of viewing the program code to analyze its performance.* ***The aim.*** *The aim of the article is to develop a project of a system for testing web-resources in real time using a flexible test script editor and a system for scaling the functionality of the system. Realization of the set purpose provides the decision of a number of tasks: 1) designing of system of processing of test scenarios; 2) the formation of system logic and behavior of the software system; 3) design of an analytical module for visualization of test results.* ***Scientific novelty.*** *The designed solution is a specialized driver for the Selenium testing and quality control system. This solution allows you to test web-resources from a specialized-designed test space and analyze the results using a specialized analytical module with visualization of graphical components. In* ***conclusion,*** *the article emphasizes that the development of modern software that will verify, analyze and verify the program code for errors for use with application programming is an urgent and modern task that will significantly improve the quality of software development and ensure the ability to store working documentation in a single form. Further development is the integration of a separate test script editor and the ability to conduct various types of software testing.*

Key words: *testing, selenium, quality of software solutions, quality analysis, web-systems.*

Актуальність проблеми. Інформаційні системи з точки зору системного аналізу є складними системами, оскільки складаються з безлічі різних частин: функціональні модулі, сервера різного напрямку, бази даних, методів передачі даних і іншого. В спроектованих системах з безліччю взаємозв'язків між різними компонентами, інформаційних систем (ІС) один з одним і інших взаємних інтеграцій підвищується шанс виходу з ладу одного або декількох модулів. Це може привести до виходу з ладу інших модулів, або повне руйнування всієї ІС та припинення її роботи. ІС повинна складатися та містить в собі методи обробки позапланових ситуацій, щоб бути більш стійкою до помилок і гарантувати відмовостійкість по технічнім умовам під час виконання роботи і виникнення передбачених і непередбачених помилок. Але обробка непередбачених ситуацій це лише один з безлічі методів, які підвищують відмовостійкість системи. Будь-яка ІС покривається тестуванням, будь це мануальне або автоматизоване тестування.

З цієї причини розробка тестових сценаріїв за різними методиками для ІС є актуальною протягом усього життєвого циклу розробки. Тестування програмного забезпечення (STLC) [1] – це систематичне тестування різними діями, яке проводитиметься в плановому порядку для підвищення якості продукту.

В життєвому циклі програмного продукту передбачено тестування програмного забезпечення (STLC) наступними етапами зі своїми результатами і критеріями входу:

– Аналіз вимог – без специфікації неможливо правильно протестувати ІС, оскільки вони містять в собі перелік того, що треба продукту для поставленої мети проекту. Команда забезпечення якості (QA) ознайомлюється з цими вимогами, та приходять до розуміння, що повинні тестувати і як повинен ввести себе продукт. Вимоги можуть бути функціональні, які описують поводження системи, або нефункціональні які описують експлуатаційну характеристику системи, наприклад вимоги до безпеки.

– Планування тестування – на цьому етапі QA планує будь використовувати методи і стратегії для тестування, оцінюючи витрати ресурсів і можливе покриття тестами. Зазвичай на цьому етапі створюється тест план, який описує обсяг робіт з тестування [2].

– Проектування тест-кейсів – процес проектування і створення тест-кейсів, відповідно до визначених раніше критеріями якості, цілями тестування, критеріями приймання.

– Налаштування тестового середовища – тестові кейси готуються до інтегрування в життєвий цикл проекту, вбудовуються під необхідні вимоги.

– Виконання тесту – на цьому етапі QA починає виконання тестових кейсів, які були підготовлені на попередньому етапі. Спрямований на пошук помилок і можливих проблем ІС. Якщо один з тестових кейсів буде заблокований через дефект або іншої причини, такий тест кейс називається заблокованим. Такі тест-кейси повторно виконуються після усунення блокуючого фактора.

– Закриття тесту – на останньому етапі аналізується результат. Створюється звіт, документація, якщо необхідно – дефекти / баги, помилки за рівнем їх складності.

Комплексне тестування обернено на пошук невідповідність системи її вихідними цілям, а не для тестування функцій остаточно зібраної ІС. Тому, в комплексному тестуванні бере участь ІС, а саме опис її вихідних цілей, вимоги та вся інша документація, яка буде поставлятися з системою. З такими цілями використовується тестування чорній коробки [3–5].

Методологія тестування припускає цілі стратегії та підходи до тестування ІС для гарантування того, що продукт відповідає технічним завданням і готовий до експлуатації.

Методики тестування включають тестування того, що ІС працює відповідно до вимог, та не має небажаних сторонніх ефектів при використанні способами, що виходять за межі проектних параметрів, і в гіршому випадку буде відмовостійкою.

Для того щоб ІС була протестована в більшому обсязі необхідно використовувати різні підходи й способи методології тестування. Методології тестування охоплюють багато що: від модульного тестування окремих функцій, інтеграційного тестування різних модулів, до спеціалізованих форм тестування, які є такими як продуктивність та безпека [6].

Аналіз останніх досліджень і публікацій. Завдяки веб-платформам не тільки створюється перше враження про компанію або продукт у відвідувачів, але ще може відбуватися безліч важливих дій, таких як покупки продуктів або управління об'єктами в режимі реального часу. Саме тому в веб платформах величезне значення має надійність, функціональність і зручність сайту.

Проаналізувавши предметну область використання програмних засобів для проведення тестування програмного коду і робот інформаційних систем, було визначено, що веб платформи з тривалим життєвим циклом потребують тестування функціоналу та коду, щоб домогтися надійності системи і правильного функціонування всіх модулів.

Також можна прийти до висновку, що автоматизація тестування істотно зберігає витрати на завданнях такого плану. Адже з'являється можливість заощадити ресурси на відсутності дублювання ручного тестування при постійно зростаючому функціонал і релізів [7–8].

Можна суттєво зменшити витрати на додаткових фахівців якщо забезпечити можливість написання коду на зручному для тестувальника мовою програмування. Для цього необхідно забезпечити і синхронізувати роботу з системою на основі розробленого драйвера до чинного способу управління веб-браузера через методи запитів. Така система дозволить не витрачати безліч фінансових ресурсів на розробку всієї бібліотеки автоматизованого тестування куди входить управління браузером. Так само, залишається можливість розробити систему модульної, що істотно чином дозволить застосувати будь-яке програмне рішення до програмного коду. Реалізацію програмного засобу слід організувати з використанням сучасних технологічних рішень та алгоритмів [9–15].

Таким чином, при реалізованої системи автоматизованого тестування веб-додатків можна заощадити фінанси, якщо під час життєвого циклу інформаційної системи необхідно виконувати регресивні, димчаті тести раз по раз при кожному релізі. Або в ІС буде безліч модулів, які взаємодіють між собою, в такому випадку без автоматизованих тестів обійтися не вийде. Підкріплює це все можливість складання автоматичної звітності.

Метою статті є проектування інтерактивного драйверу для системи sileneum, яка дозволить проводити автоматизоване тестування web-ресурсів із збереженням результуючих звітів та можливістю аналізу протестованих фрагментів.

Виклад основного матеріалу. Концепція системи складається з необхідності виконувати велику кількість різних програмних тест-кейсів з web-контентом, що сприяє інтенсивному використанні браузера. Розробка має сугубо спеціалізований напрям, отже таке програмне рішення впроваджується тільки до спеціалізованих проектів та використовують його спеціалісти з забезпечення якості програмного коду та роботи системи. Таким чином, використання відбувається тільки персоналізовано без авторизації або реєстрації в системі.

Першим етапом є створення діаграми варіантів використання, завдяки якій, визначаються усі вимоги до кінцевої системи. Після виконання всіх етапів проектування, здійснюється перехід до стадії розробки програмного забезпечення.

Діаграма варіантів використання, рис. 1, охоплює частину наступних об'єктів:

– Написання автоматизованих тестів – додання до системи редактора та генератора автоматизованих тестових сценаріїв.

– Отримання звітності тестів – спеціалізований модуль електронного документообігу, який дозволяє користувачам системи документувати результати роботи системи.

– Закриття веб-браузера – функціональні відключення роботи браузера, який реалізуються завдяки прямих запитів.

– Споруда графіків – використання спеціалізованих бібліотек для візуалізації результатів тестування.

– Звернення до системи версій – можливість синхронізувати роботу розробленої програмної системи з зовнішніми системами контролю версій для більш надійної роботи програмного засобу.

– Збереження результатів тестів – можливість зберігати отримані тестові результати та тестові сценарії в окремій директорії системи чи в базі даних у вигляді звіту.

– Робота з веб-браузером – функціональне поєднання програмного засобу з роботою браузера для пошуку помилок.

– Драйвер веб-браузера – модуль синхронізації даних для забезпечення роботи з браузером.

– Ініціалізація веб-браузера – отримання зворотного зв'язку стосовно версії браузера та його розширень, які на поточний момент використовуються. А також можливість при запуску наладити систему під необхідність.

– Маніпуляції зі сторінкою – можливість проводити всебічне тестування web-сторінки.

– Отримання елементу – запит на пошук елементу в програмному коді web-сторінки.

– Парсинг сторінки – модуль автоматизованого збору інформації зі сторінки для можливості якісно взаємодіяти з веб-сторінкою та аналізувати вже існуючі компоненти.

– Отримання сторінки за URL – виконання переходу на сторінку з імітацією роботи реального web-сервера.

– Отримання поточної сторінки – швидкий виклик сторінки з виведенням інформації без додаткового завантаження.

– Використання клавіатури – можливість організовувати введення даних.

– Натискання на елемент – імітація натискання на об'єкт сторінки та виведення результату її реакції.

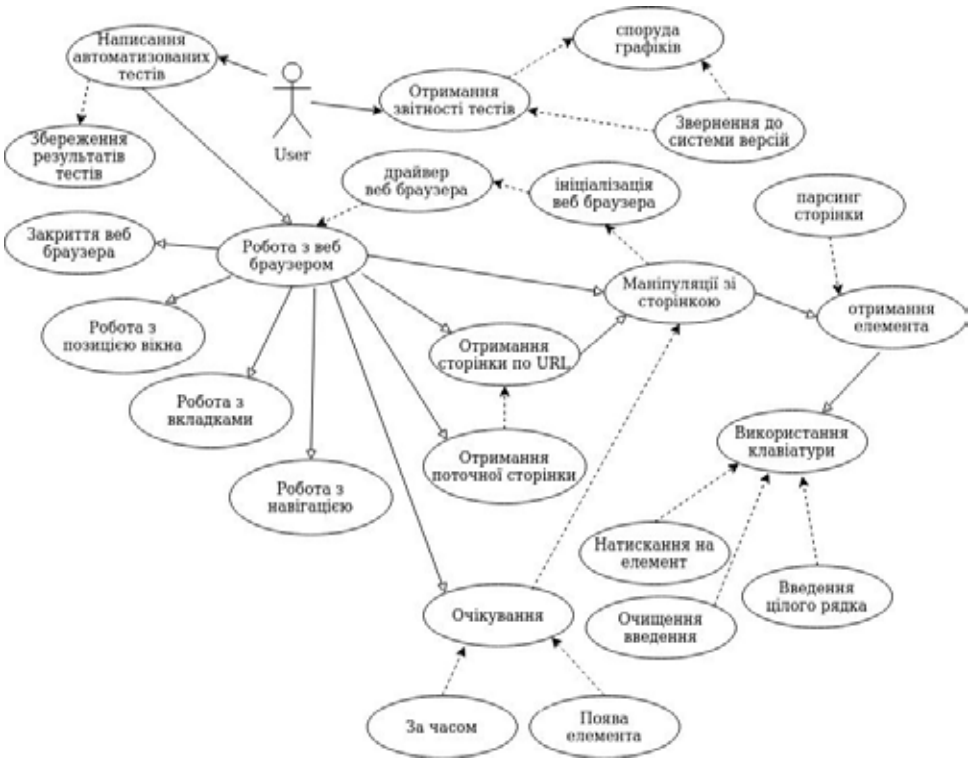


Рис. 1. Діаграма варіантів використання

– Очищення введення – можливість швидкого очищення усієї введеної інформації на сторінку.

– Введення цілого рядка – можливість додавати одночасно великі обсяги текстової інформації для перевірки розмірності рядків та їх реакції на додану інформацію.

Після визначення функціональної складової системи, виконується проектування логічних компонентів системи, а саме класів, які складають загальну концептуальну логіку системи, рис. 2.

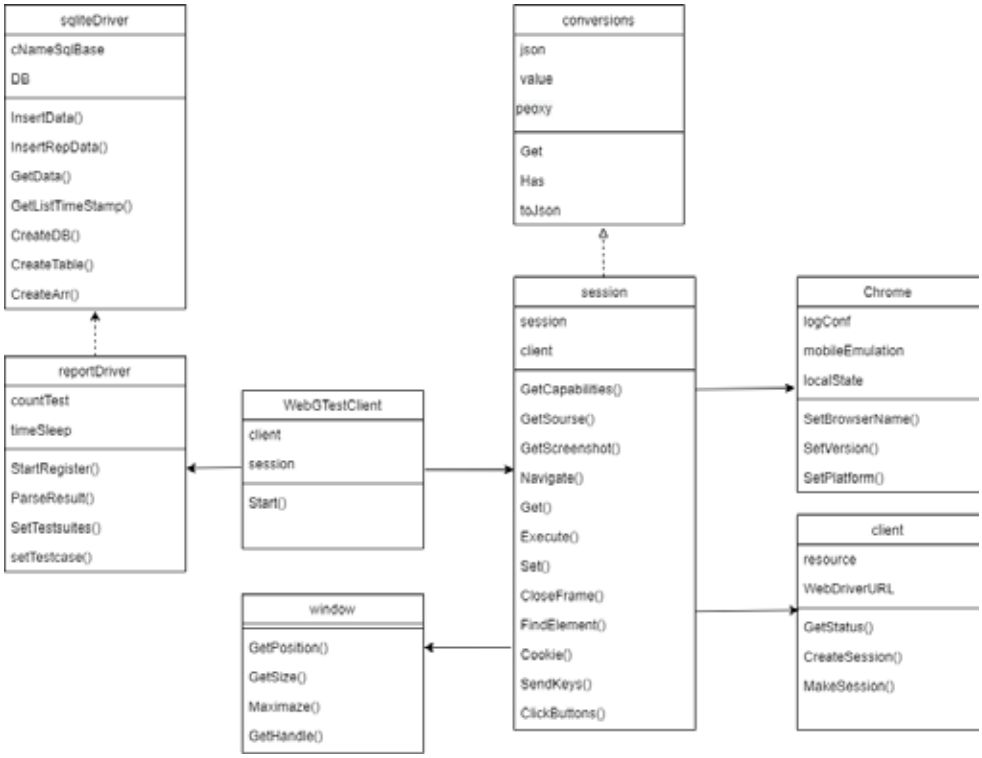


Рис. 2. Діаграма класів інформаційної системи

В процесі проектування програмної системи було визначено наступні класи:

– Клас reportDriver – відповідає за можливість роботи модуля звітування та формування подій, в результаті роботи системи тестування об'єктів.

– Клас conversions відповідає за перетворення рядків у json формат і навпаки. Необхідний для коректної передачі даних в Selenium.

– Клас sqliteDriver відповідає за підключення бази даних та синхронізації отриманих результатів тестування з різними функціональними модулями системи, а також з системою контроля за версіями.

– Клас WebGTestClient відповідає за початок роботи. Він запускає сесію яка відповідає за всю програму.

– Клас Chrome відповідає за підключення html сторінок для роботи в імітованому браузері Chrome.

– Клас session – відповідає за роботу з браузером та являє собою інтерфейс, який позволяє запускати та імітувати команди які були описані у тестовому сценарію.

Спроектована система має спеціалізоване призначення, яке дозволяє взаємодіяти з web-сторінками, та проводити автоматизоване тестування функціональних можливостей. Таке рішення є актуальною задачею для тестувальників-автоматизаторів, та потребує використання спеціалізованого програмного оточення. До такого оточення слід віднести функціональний сервер Selenium, який дозволяє проводити тестування на хості сайта чи додатка. Однак, Selenium не є досить гнучким рішенням для проведення тестування. Він орієнтований для використання виключно web-мов програмування, що суттєвим чином зменшує ефективність тестування. Автоматизовані та функціональні тестові сценарії ноебхідно розробляти виключно використовуючи мову програмування C++, оскільки вона має більший вплив на взаємодію зі структурними та функціональними компонентами.

Отже, для взаємодії мови програмування C++ та серверу тестування Selenium, необхідно розробити спеціалізований драйвер оточення, який дозволить поєднати функціональні можливості та зробити з цього єдине функціональне рішення.

Структурна взаємодія ґрунтується на поєднанні тестових сценаріїв, які написані мовою програмування C++ та їх взаємодії з спеціалізованим набором скриптів. Далі тестовий сценрій інтерпретується для виконання на сервері Selenium, який під'єднується до хосту сайту чи додатку. Це дозволяє провести процес тестування, та отримані результати зберегти в оточенні Selenium. Наступним етапом є трансляція результатів тестування в більш ефективну систему виведення інформації для тестувальника та для інших робітників з групи розробки. Для цього використовується журналізоване формування звіту.

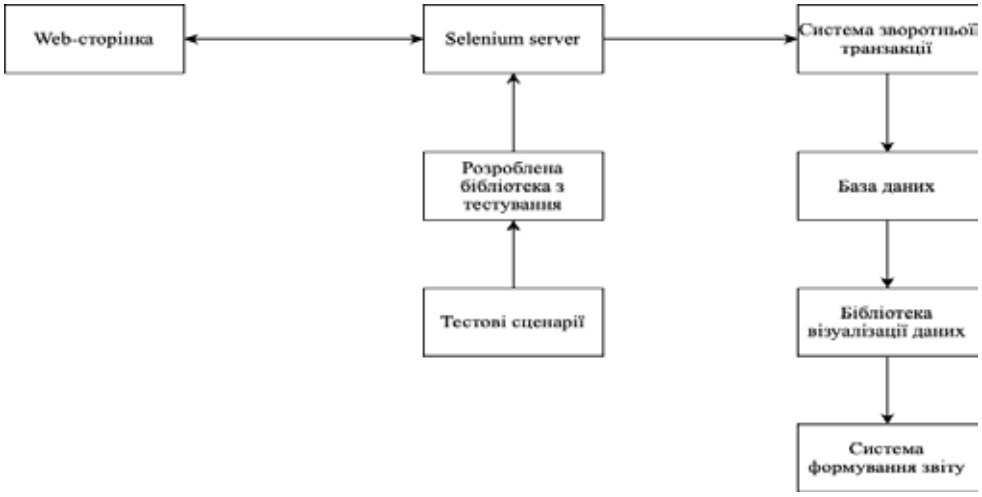


Рис. 3. Схема взаємодії спроектованих системних компонентів

Такий звіт має бути реалізовано в актуальному для перегляду вигляді. Для цього обрана система транслювання результатів в формат HTML і додаватиме до бази даних запис.

З метою більшої візуалізації роботи, виконано розробку спеціалізованої бібліотеки збереження результатів, яка трансює отримані результати до бази даних, після чого використовується бібліотека візуалізації графіки, яка будує діаграми та дозволяє структурувати інформацію в файлі. На рис. 3 зображено схему взаємодії системних компонентів в розробленій інформаційній системі.

Висновки та перспективи подальших досліджень. Результатом роботи є спроектоване спеціалізоване програмне оточення, яке включає в себе окрему функціональну бібліотеку та набір спеціалізованих автоматизованих тестових сценаріїв, які виконуються у взаємодії з Selenium Server. Також спроектовано гнучку та ефективну систему звітування за результатами тестів. На підставі аналізу структури традиційного звіту про дефекти програмних продуктів, які були виявлені при тестуванні, створена модифікована структура звіту про помилки. Запропонована структура звіту дозволяє не тільки поліпшити взаємодію розробників та тестувальників програмного забезпечення, а й використовується як засіб контролю за їх діяльністю. При цьому кожне поле звіту розглядається з точки зору його обліку для оцінки ефективності тестування. Розроблено методику кількісної оцінки ефективності тестування програмних продуктів на основі баг-репортів. Ефективність роботи інженера з оцінки якості оцінюється за формулою, яка отримана евристичним шляхом і враховує кількість і критичність помилок. Встановлено мінімальний достатній рівень ефективності тестування при використанні зазначеної методики. Надалі ефективним розвитком системи є впровадження самостійного платформного рішення з додання нових тестових сценаріїв та їх використанні при багаторазових перевірках ресурсів.

Список використаних джерел:

1. Принципи Software Testing Life Cycle (STLC). URL: https://softwaretestingfundamentals.com/software-testing-life-cycle.

2. Блєк Р. Ключевые процессы тестирования. Планирование, подготовка, проведение, совершенствование. М.: Лори. 2016. 537 с.

3. Эдгрен Р. The little black book on test design. NY : CreateSpace. 2011. 228 с.

4. Фаулер М., Райс Д., Фоммел М. Архитектура корпоративных программных приложений. М. : Вильямс. 2006. 544 с.

5. Бейзер Б. Тестирование черного ящика. Технологии функционального тестирования программного обеспечения и систем. М. : Вильямс. 2004. 320 с.

6. Криспин Л., Грегори Д. Agile-тестирование. Обучающий курс для всей команды. М. : Манн Иванов и Фербер. 2019. 528 с.

7. The ROI of Test Automation», Michael Kelly. URL: http://www.sqetraining.com/sites/default/files/articles/XDD8502filelistfilename1_0.pdf
8. Гленфорд М., Майерс Г., Баджетт Т., Сандлер К. Искусство тестирования программ. М. : Вильямс. 2012. 272 с.
9. Баранов С. Процесс разработки программных изделий. М. : ФИЗМАТЛИТ. 2000. 176 с.
10. Дастин Є. Автоматизоване тестування програмного забезпечення. впровадження, управління та експлуатація. М. : Лори. 2016. 592 с.
11. Джез Х., Хамбл Д., Фарли Д. Непрерывное развертывание ПО. Автоматизация процессов сборки, тестирования и внедрения новых версий программ. М. : Вильямс. 2011. 432 с.
12. Гленфорд М., Майерс Г., Баджетт Т. Искусство тестирования программ. М. : Вильямс, 2012. 272 с.
13. Мослей Д. Just Enough Software Test Automation. NY : CreateSpace. 2002. 260 с.
14. The Selenium Browser Automation Project documentation. URL: https://www.selenium.dev/documentation/en
15. Generic opensource Robot Framework for python. URL: https://robotframework.org/#introduction

References:

1. Principles of Software Testing Life Cycle (STLC). Access mode: https://softwaretestingfundamentals.com/software-testing-life-cycle. [in Ukrainian].
2. Blek, R. (2016). Key testing processes. Planning, preparation, implementation, improvement. M.: Laurie, 537 p. [in Russian].
3. Edgren, R. (2011). The little black book on test design. NY: CreateSpace, 228 p. [in English].
4. Fowler, M., Rice, D., Fommel, M. (2006). Architecture of corporate software applications. M.: Williams, 544 p. [in Russian].
5. Beizer, B. (2004). Black box testing. Functional testing technologies for software and systems. M.: Williams, 320 p. [in Russian].
6. Crispin, L., Gregory, D. (2019). Agile testing. Training course for the whole team. M.: Mann Ivanov and Ferber, 528 p. [in Russian].
7. The ROI of Test Automation, Michael Kelly. Access mode: http://www.sqetraining.com/sites/default/files/articles/XDD8502filelistfilename1_0.pdf [in English].
8. Glenford, M., Myers, G., Budgett, T., Sandler, K. (2012). The Art of Software Testing. M.: Williams, 272 p. [in Russian].
9. Baranov, S. (2000). Process of software products development. M.: FIZMATLIT, 176 p. [in Russian].
10. Dustin, Є. (2016). Automated software testing. vprovadzhennya, management and exploitation. M.: Lori, 592 p. [in Ukrainian].
11. Jez, H., Humble, D., Farley, D. (2011). Continuous software deployment. Automation of assembly, testing and implementation of new versions of programs. M.: Williams, 432 p. [in Russian].
12. Glenford, M., Myers, G., Budgett, T. (2012). The Art of Software Testing. M.: Williams, 272 p. [in Russian].
13. Mosley, D. (2002). Just Enough Software Test Automation. NY: CreateSpace, 260 p. [in English].
14. The Selenium Browser Automation Project documentation. Access mode: https://www.selenium.dev/documentation/en [in English].
15. Generic opensource Robot Framework for python. Access mode: https://robotframework.org/#introduction [in English].

НАУКОВЕ ВИДАННЯ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА СУСПІЛЬСТВО

INFORMATION TECHNOLOGY AND SOCIETY

ВИПУСК 1
ISSUE 1

2021

Коректура
Ірина Чудеснова

Комп'ютерна верстка
Наталія Кузнєцова

Формат 60x84/8. Гарнітура Cambria.
Папір офсет. Цифровий друк. Ум. друк. арк. 10,70. Замов. № 0821/293. Наклад 300 прим.

Видавництво і друкарня – Видавничий дім «Гельветика»
65101, Україна, м. Одеса, вул. Інглезі, 6/1
Телефон +38 (048) 709 38 69, +38 (095) 934 48 28, +38 (097) 723 06 08
E-mail: mailbox@helvetica.ua
Свідоцтво суб'єкта видавничої справи
ДК No 6424 від 04.10.2018 р.