

www.konferenciaonline.org.ua

Міжнародна наукова
інтернет-конференція

**Інформаційне суспільство:
технологічні, економічні
та технічні аспекти становлення**

Випуск 92

ISSN 2522-932X

Google Scholar

 **AKADEMIA NAUK STOSOWANYCH**
WYŻSZA SZKOŁA ZARZĄDZANIA I ADMINISTRACJI
W OPOLU

8-9 жовтня 2024 р.

м. Тернопіль, Україна – м. Ополе, Польща
2024

УДК 001 (063)

Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення (випуск 92): матеріали Міжнародної наукової інтернет-конференції, (м. Тернопіль, Україна, м. Ополе, Польща, 8-9 жовтня 2024 р.) / редкол. : О. Патряк та ін. ГО “Наукова спільнота”, WSZIA w Opolu. Тернопіль : ФО-П Шпак В.Б. 2023. 78 с. – ISSN 2522-932X

Збірник доповідей підготовлено за матеріалами Міжнародної наукової інтернет-конференції (випуск 92) 8-9 жовтня 2024 р. на сайті www.konferenciaonline.org.ua

Оргкомітет ГО Наукова спільнота:

Патряк Олександра Тарасівна, кандидат економічних наук, ЗУНУ;

Шевченко (Огінська) Анастасія Юріївна, кандидат економічних наук, директор ТОВ «Школа для майбутнього» (ThinkGlobal Ternopil);

Назарчук Оксана Михайлівна, доктор філософії (Ph.D.), ДВНЗ «Київський національний економічний університет імені Вадима Гетьмана»;

Гомотюк Оксана Євгенівна, доктор історичних наук, професор, ЗУНУ;

Біловус Леся Іванівна, доктор історичних наук, кандидат філологічних наук, професор, ЗУНУ;

Ребуха Лілія Зіновіївна, доктор педагогічних наук, кандидат психологічних наук, професор, ЗУНУ;

Недошитко Ірина Романівна, кандидат історичних наук, доцент, ЗУНУ;

Стефанишин Олена Василівна, кандидат історичних наук, доцент, ЗУНУ;

Яблонська Наталія Мирославівна, кандидат філологічних наук, старший викладач, ЗУНУ;

Рудакевич Оксана Мирославівна, кандидат філософських наук, ЗУНУ;

Русенко Святослав Ярославович, аспірант, Тернопільський національний педагогічний університет імені Володимира Гнатюка.

Тексти матеріалів конференції подаються в авторській редакції. Відповідальність за точність, достовірність і зміст поданих матеріалів несуть автори. Всі роботи ліцензуються відповідно до Creative Commons Attribution 4.0 International License.

Автори зберігають авторське право, а також надають збірнику право першого опублікування оригінальних наукових статей на умовах ліцензії Creative Commons Attribution 4.0 International License, що дозволяє іншим розповсюджувати роботу з визнанням авторства твору та першої публікації в цьому збірнику.

Наша адреса: Оргкомітет МНІК "Конференція онлайн"

а/с 797, м. Тернопіль 46005

тел. моб. 068 366 0 525

e-mail: inetkonf@ukr.net

URL Інтернет-конференції: <http://www.konferenciaonline.org.ua/>

ISSN 2522-932X

© ГО “Наукова спільнота” 2024

© Автори статей 2024



Секція 1. Інформаційні системи і технології

Величківський Ілля Олегович, здобувач вищої освіти освітнього ступеня «Магістр», 2 курс, Національний авіаційний університет, м. Київ, Україна

Льєнко Анна Вадимівна, кандидат технічних наук, доцент, доцент кафедри комп'ютеризованих систем захисту інформації, Національний авіаційний університет, м. Київ, Україна

Галата Лілія Павлівна, доктор філософії, доцент, Національний авіаційний університет, м. Київ, Україна

ПРОГРАМНИЙ МОДУЛЬ ЗАХИСТУ ІНФОРМАЦІЇ В ХМАРНИХ ОБЧИСЛЕННЯХ НА ОСНОВІ МАШИННОГО НАВЧАННЯ

Інтернет-адреса публікації на сайті:

<http://www.konferenciaonline.org.ua/ua/article/id-1924/>

Вступ./Introduction. У сучасну епоху цифрових технологій забезпечення безпеки даних у хмарних обчисленнях стає критично важливим завданням. З розвитком обсягу даних та збільшенням кількості кіберзагроз традиційні методи захисту вже не можуть повністю забезпечити належний рівень безпеки. У цьому контексті використання методів машинного навчання, зокрема навчання з підкріпленням (Reinforcement Learning, RL), є перспективним підходом. RL дозволяє створювати інтелектуальні системи захисту, які здатні адаптуватися до нових загроз і самостійно навчатися оптимальним діям на основі аналізу поведінки атак та дій користувачів. Це дозволяє не тільки своєчасно виявляти аномалії, але й ефективно реагувати на них, запобігаючи несанкціонованому доступу до даних у хмарних середовищах. Впровадження таких технологій може значно підвищити рівень кібербезпеки, забезпечуючи надійний захист інформаційних систем у складних і мінливих умовах.

Мета роботи. / Aim. Детальний огляд сучасних технологій захисту даних у хмарних обчисленнях. Дослідити існуючі можливості застосування алгоритмів машинного навчання для захисту інформації, розглянути їх переваги та недоліки, та провести порівняльний аналіз.

Матеріали та методи./Materials and methods. Навчання з підкріпленням (Reinforcement Learning, RL) є одним із найважливіших підходів у машинному навчанні. У цьому підході агент (суб'єкт, який приймає рішення) взаємодіє з середовищем, виконуючи певні дії, і отримує винагороду (або штраф) за кожну дію. Метою агента є максимізація накопиченої винагороди, знаходячи оптимальну стратегію дій у середовищі. Цей тип навчання використовується в ситуаціях, де складно побудувати явну модель середовища або визначити правильні дії заздалегідь. Найбільш популярними алгоритмами навчання з підкріпленням є Q-Learning та Deep Q-Learning.

1. Q-Learning є одним із популярних методів навчання з підкріпленням. Це модель, що дозволяє агенту вивчати оптимальну стратегію шляхом взаємодії із середовищем і отримання винагороди за кожну дію. Агент намагається максимізувати сумарну винагороду, поступово визначаючи найкращі дії в кожній ситуації. Однак Q-Learning потребує багато часу для навчання в складних середовищах, і його ефективність знижується у випадках із великою кількістю станів або дій. Крім того, якщо модель недостатньо навчена, вона може виконувати субоптимальні дії, що призводить до низької ефективності та неправильних висновків.

2. Deep Q-Learning – це розширення класичного Q-Learning, яке використовує нейронну мережу для оцінки значень Q-функції, що дозволяє ефективно працювати з великими й складними середовищами. Нейронна мережа допомагає обробляти дані з багатовимірними вхідними даними, що робить цей метод ефективним для задач з високою розмірністю станів, таких як відеоігри або робототехніка. Проте, Deep Q-Learning може бути нестабільним і потребує великих обчислювальних ресурсів для навчання. Крім того, він вразливий до переобучення та може здійснювати некоректні дії, якщо навчальні дані є неповними або нерепрезентативними.

Ключові переваги навчання з підкріпленням:

1. Адаптивне прийняття рішень. Системи, побудовані на основі навчання з підкріпленням, можуть навчатися на основі власного досвіду взаємодії зі середовищем, коригуючи свою стратегію для досягнення максимальної винагороди. Це дозволяє створювати моделі, здатні приймати оптимальні рішення навіть у невідомих або динамічних умовах.

2. Можливість роботи у невизначених середовищах. Навчання з підкріпленням особливо корисне у випадках, коли середовище є складним, змінюваним або не має повної інформації про стани й дії. Алгоритми RL дозволяють агентам адаптувати свою поведінку без повного знання правил або моделей середовища.

3. Ефективне використання досвіду. Агент зберігає інформацію про свій попередній досвід (історію дій та отриманих винагород), що дозволяє йому покращувати свої стратегії з часом, враховуючи попередні помилки і успіхи. Це призводить до поступового вдосконалення поведінки й підвищення ефективності.

4. Вирішення складних послідовних завдань. RL ефективний для задач, де необхідно приймати серії рішень, кожне з яких впливає на кінцевий результат (наприклад, у робототехніці, управлінні або іграх). Агент може навчитися планувати свої дії, щоб досягти довгострокових цілей.

5. Гнучкість і генералізація. Алгоритми RL можуть використовуватися для вирішення різних типів завдань без значних змін у своїй структурі. Вони здатні до узагальнення знань і можуть застосовувати накопичений досвід для вирішення нових, схожих завдань.

Результати та обговорення. / Results and discussion.

Таблиця 1. Зведена таблиця порівняння алгоритмів машинного навчання для захисту інформації

Особливість	Q-Learning	Deep Q-Learning
Представлення станів	Використовує таблицю для збереження всіх значень Q для кожного стану і дії. Підходить для малих і простих середовищ.	Використовує нейронну мережу для представлення станів, що дозволяє працювати з великими та складними середовищами.
Масштабованість	Обмежена масштабованість: не підходить для великих середовищ через експоненційне зростання таблиці станів.	Висока масштабованість: завдяки нейронним мережам здатний працювати з великими і складними середовищами.
Час навчання	Повільне навчання в середовищах з великою кількістю станів і дій.	Навчання може бути швидшим завдяки використанню нейронних мереж, але потребує більше обчислювальних ресурсів.
Потреба у пам'яті	Вимагає великої пам'яті для зберігання таблиці Q, особливо в середовищах з великою кількістю станів.	Менша потреба в пам'яті порівняно з Q-Learning, оскільки нейронна мережа узагальнює значення Q-функції.
Обчислювальна складність	Невелика обчислювальна складність для простих задач. Може легко впоратися зі завданнями невеликих розмірів.	Висока обчислювальна складність через використання нейронних мереж, що потребує GPU для ефективного навчання.
Узагальнення	Не здатний до узагальнення: кожен стан має окреме значення Q.	Вміє узагальнювати: здатний використовувати набуті знання для нових, схожих станів завдяки навчанню нейронної мережі.
Використання у складних середовищах	Ефективний для простих середовищ з обмеженою кількістю станів і дій.	Здатний працювати у складних середовищах, де багато можливих станів і дій (ігри, робототехніка).

Висновки. / Conclusions. Підсумовуючи можна зробити висновок, що розробка та реалізація програмного модуля захисту інформації в хмарних обчисленнях на основі методів навчання з підкріпленням відкриває нові горизонти у сфері кібербезпеки. Використання алгоритмів RL для динамічного виявлення загроз та адаптивного реагування на них дозволяє створювати системи, здатні ефективно захищати дані в умовах складних і мінливих

середовищ. Завдяки здатності агентів самостійно навчатися оптимальним діям і стратегічно реагувати на атаки, такі системи забезпечують більш високий рівень безпеки і надійності.

Проте, як і будь-які інші технології, використання навчання з підкріпленням у хмарних обчисленнях має свої виклики. Зокрема, значні обчислювальні ресурси, необхідні для навчання та роботи агентів, можуть створювати додаткові навантаження на інфраструктуру, особливо в реальних умовах. Крім того, нестабільність моделей RL і ризик переобучення можуть призвести до неправильної оцінки загроз або неефективної поведінки у невідомих ситуаціях.

Оскільки обсяги та складність кіберзагроз постійно зростають, необхідність у розробці більш досконалих і гнучких рішень стає все більш актуальною. Програмні модулі на основі навчання з підкріпленням є перспективним напрямком для забезпечення безпеки даних у хмарних обчисленнях, що дозволяє не тільки ефективно виявляти і реагувати на загрози, а й прогнозувати потенційні атаки на основі аналізу поведінки зловмисників.

*Гомель Ілля Олександрович, магістрант,
Національний авіаційний університет, м. Київ*

НЕБЕЗПЕКА TELEGRAM ЯК МЕСЕНДЖЕРА ДЛЯ ОБМІНУ ДАНИМИ

Інтернет-адреса публікації на сайті:

<http://www.konferenciaonline.org.ua/ua/article/id-1918/>

В останні роки месенджер Telegram здобув значну популярність серед українців завдяки своїй зручності, швидкості передачі повідомлень та широкому набору функцій. Однак, разом із зростанням його використання, постає питання про безпеку цього інструменту для обміну даними. Telegram позиціонується як захищена платформа, що використовує шифрування для забезпечення конфіденційності інформації. Проте, з огляду на специфіку його архітектури та певні особливості роботи з даними, виникають загрози як для приватності користувачів, так і для їх інформаційної безпеки.

У цій статті ми розглянемо основні небезпеки використання Telegram як месенджера для обміну даними, звертаючи увагу на вразливості, пов'язані з архітектурою системи, питаннями зберігання даних, шифрування, а також потенційні ризики, які виникають через широке використання Telegram у різних сферах, включаючи бізнес, журналістику та політичну активність.

У жовтні 2023 року Національний координаційний центр кібербезпеки (НКЦК) ухвалив рішення обмежити використання месенджера Telegram у державних установах України, зокрема в органах влади, військових формуваннях та на об'єктах критичної інфраструктури. Основною причиною такого рішення стали підтверджені дані про те, що російські спецслужби отримали доступ до інформації користувачів Telegram, включно з видаленими

повідомленнями. Це відкриває можливості для витоку важливих державних даних та компрометації службових осіб.

Крім того, Telegram широко використовується ворожими силами для проведення кібероперацій проти України. Серед основних загроз виділяють фішингові атаки та розповсюдження шкідливого програмного забезпечення через платформи Telegram-каналів та ботів. Ці інструменти дозволяють ворогу отримувати доступ до конфіденційної інформації, інфікувати пристрої співробітників державних органів та військових, а також коригувати ракетні удари по критичній інфраструктурі України. У такий спосіб Telegram стає не лише засобом комунікації, але й інструментом для проведення широкомасштабних кібератак.

Окремо про загрози, пов'язані з Telegram, згадав начальник Головного управління розвідки (ГУР) Міністерства оборони України Кирило Буданов. Він зазначив, що використання Telegram активно підтримується російськими спецслужбами, оскільки дає можливість реалізовувати інформаційно-психологічні операції та контроль за комунікацією в межах українського інформаційного простору. За словами Буданова, Telegram також використовується для поширення дезінформації, яка спрямована на підрив морального духу українських військових та мирного населення, а також для збору розвідувальних даних в реальному часі.

Обмеження використання Telegram стосується службових пристроїв державних органів, включаючи військових і об'єкти критичної інфраструктури. Винятки можливі лише в разі, коли це є необхідністю для виконання службових обов'язків. Це рішення є частиною ширшої стратегії протидії інформаційно-психологічним атакам і забезпечення безпеки національних комунікацій, яка націлена на зниження кіберзагроз і мінімізацію ризиків для державної безпеки.

Telegram дедалі частіше розглядається як серйозна загроза безпеці даних через його зв'язки з російськими спецслужбами, такими як ФСБ та Роскомнагляд. Як повідомляє СБУ, Telegram фактично став інструментом, що активно використовується російською державою для контролю та дезінформаційних кампаній. Співпраця месенджера з російськими державними структурами передбачає можливість блокування небажаних каналів і допуск до інформації користувачів, що зберігається на серверах, потенційно розташованих у Росії. Ця взаємодія ставить під загрозу конфіденційність даних мільйонів користувачів.

Telegram також використовується для просування російської пропаганди та поширення інформаційно-психологічного впливу на суспільство в умовах війни. Російські державні органи, зокрема ФСБ, отримують доступ до повідомлень і даних користувачів, що створює серйозні загрози для національної безпеки України. У той же час, адміністрація Telegram відмовляється блокувати проросійські канали, які активно поширюють пропаганду, що дестабілізує ситуацію в Україні та сприяє дезінформаційним кампаніям ворога.

Функціонування Telegram як інформаційної платформи для проведення кібератак і розвідувальних операцій посилює небезпеку цього месенджера. В умовах конфлікту між Україною та Росією, Telegram використовується для поширення неправдивої інформації, що негативно впливає на моральний стан населення і військових. Російські хакери використовують месенджер для поширення фішингових атак та шкідливого програмного забезпечення, яке дозволяє отримувати доступ до чутливої інформації та контролювати пристрої користувачів.

Особливо небезпечним є використання Telegram для коригування ракетних ударів. За допомогою каналів та груп, ворог може отримувати дані про місця розташування військових об'єктів та цивільної інфраструктури, що стають цілями для ракетних атак. Таким чином, месенджер перетворюється не лише на засіб комунікації, але й на інструмент для ведення активних військових операцій.

Також варто зазначити, що російські інформаційно-психологічні операції (ІПСО) у Telegram є важливим елементом дезінформаційної війни, спрямованої на підрив національної безпеки України. Через цей месенджер поширюються фейкові новини, маніпулятивні матеріали, а також пропаганда, яка має на меті створення паніки, формування негативних суспільних настроїв та підрив довіри до державних інституцій. ІПСО у Telegram часто включають спеціально створені групи та канали для координації інформаційних атак, спрямованих на виклик емоційної реакції та дестабілізацію ситуації в українському суспільстві, особливо під час війни.

Telegram, попри свою популярність як зручний месенджер для обміну даними, становить серйозну загрозу для безпеки. Основні ризики полягають у потенційній співпраці платформи з російськими спецслужбами, такими як ФСБ та Роскомнадзор, які можуть отримати доступ до конфіденційної інформації користувачів. Крім того, Telegram активно використовується для поширення російських інформаційно-психологічних операцій (ІПСО), дезінформаційних кампаній та кібератак, що сприяють дестабілізації ситуації в Україні, підриву довіри до державних органів і коригування військових операцій ворога.

Завдяки архітектурі месенджера та особливостям його функціонування, російські спецслужби мають можливість отримувати доступ до повідомлень користувачів, зокрема видалених, що створює ризик витоку критично важливих даних. Це особливо небезпечно в умовах воєнного конфлікту, коли зловмисники можуть використовувати отриману інформацію для розвідки або стратегічних атак. Telegram також є важливим інструментом для проведення кібератак, спрямованих на державні установи та військові структури.

Крім цього, на платформі поширюється шкідливе програмне забезпечення через боти та канали, які ворог використовує для збору інформації та коригування ракетних ударів. Ворог також активно використовує месенджер для фішингових атак, що призводять до викрадення особистих даних та зараження пристроїв шкідливими програмами.

Серед загроз також є використання Telegram для поширення російської пропаганди та дезінформації через спеціально створені канали та групи. Пропагандистські матеріали спрямовані на піддрив морального духу населення, деморалізацію українських військових та створення паніки серед мирних жителів. Інформаційно-психологічні операції (ІПСО), що здійснюються через Telegram, впливають на суспільні настрої, маніпулюють громадською думкою та сприяють поширенню недостовірної інформації.

Список використаних джерел:

1. НКЦК прийняв рішення обмежити використання Telegram в органах державної влади, військових формуваннях, на об'єктах критичної інфраструктури, Режим доступу: <https://www.rnbo.gov.ua/ua/Diialnist/6994.html> (Дата звернення: 01.10.2024)
2. Telegram співпрацює з Роскомнадзором та ФСБ, – СБУ, режим доступу <https://www.unian.ua/techno/communications/telegram-spivpracyuye-iz-roskomnadzorom-ta-fsb-sbu-12587346.html> (Дата звернення: 01.10.2024)

*Єрмоленко Микола Володимирович, аспірант
факультету інформаційних систем та технологій,
Приватний вищий навчальний заклад «Європейський університет»*

*Науковий керівник: Склярєнко Олена Володимирівна,
кандидат фізико-математичних наук, доцент, завідувач кафедри
математичних дисциплін та інноваційного проектування,
Приватний вищий навчальний заклад «Європейський університет»*

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ АВТОМАТИЗАЦІЇ БУХГАЛТЕРСЬКОГО ОБЛІКУ

Інтернет-адреса публікації на сайті:

<http://www.konferenciaonline.org.ua/ua/article/id-1906/>

Інформаційні технології автоматизації підвищують точність та зменшують вартість бухгалтерського обліку. Бухгалтерський облік утворює необхідну ланку макроекономіки, що забезпечує наповнення макроекономіки вхідними даними. Отже автоматизація бухгалтерського обліку покращує як процеси на рівні підприємства так і на рівні країни в цілому.

Інформаційні технології автоматизації бухгалтерського обліку, включають в себе програми для взаємодії користувачів із системами обліку, сховища зберігання даних, прикладні програмні сервери для обробки облікових даних та їх взаємодію. Для вдосконалення автоматизації бухгалтерського обліку використане порівняння наявних програм бухгалтерського обліку, аналіз переваг та недоліків, шляхи покращення наявних програм [1].

Моделювання програми бухгалтерського обліку забезпечило:

- Проектування, аналіз, моделювання, прототипування, дизайн та розробку інформаційних систем.
- Аналіз та вдосконалення організаційних процесів та проектного управління.
- Створення регламентів, документації до програмних продуктів, інструкцій користувачів.
- Розробку тестів програмних продуктів.

Особлива увага привернута до універсальних технологій повторного використання. OLE (Object Linking and Embedding) – це технологія, що дозволяє об'єднувати інформацію з різних додатків в одному документі або програмі. СОМ-компоненти – це об'єкти, які можуть бути вбудовані або пов'язані з іншими додатками або документами. Мови програмування, які використовують СОМ-об'єкти:

- Microsoft Visual Basic: Visual Basic має підтримку СОМ і легко інтегрується з СОМ-компонентами.
- C++: За допомогою Microsoft's Active Template Library (ATL) або Microsoft Foundation Classes (MFC) можна створювати СОМ-компоненти в C++.
- C#: З використанням бібліотеки InteropServices, C# може взаємодіяти з СОМ-компонентами.
- Delphi: Delphi також має підтримку СОМ та може створювати СОМ-компоненти.
- Python: Модуль win32com надає можливість взаємодії з СОМ-об'єктами в Python. Це частина бібліотеки pywin32, яка забезпечує доступ до функцій Win32 API, включаючи СОМ [2].
- PHP: Клас com дозволяє створювати екземпляри OLE-сумісного СОМ-об'єкта, викликати його методи та отримувати доступ до його властивостей [3].
- VAF: За допомогою Менеджера СОМ-з'єднань.

Розробки СОМ-компонентів може реалізовуватися мовою програмування Python із використанням бібліотеки win32com у середовищі LiClipse.

Оглядаючи наявні програми бухгалтерського обліку увагу привертають програми Tryton та BAS Бухгалтерія КОПІ.

Tryton – програма бухгалтерського обліку, ідеальна для компаній різного розміру, легка у використанні, із доступними на 100% джерельними кодами. Tryton складається із наступних модулів: фінансового обліку, продажів, складського обліку, аналітичної звітності, керуванням відносинами із покупцями, закупівель, ланцюгом постачань, виробництва, доставки [4].

"BAS Бухгалтерія КОПІ" є професійним інструментом бухгалтера для ведення бухгалтерського і податкового обліку, підготовки та реєстрації податкових документів, а також підготовки та здачі обов'язкової

регламентованої звітності з розширеними можливостями обліку. Рішення має розширений функціонал в частині розрахунку заробітної плати, що дозволяє використовувати його на підприємствах зі складним розрахунком заробітної плати [5].

Список використаної літератури:

1. Букало Н. А. Автоматизація обліку в сучасних умовах [Електронний ресурс]: <https://evnuir.vnu.edu.ua/bitstream/123456789/8522/1/automation.pdf>
2. Вікіпедія. [Електронний ресурс]: https://en.wikipedia.org/wiki/Component_Object_Model
3. PHP Documentation. [Електронний ресурс]: <https://www.php.net/manual/ru/class.com.php>
4. [Електронний ресурс]: Tryton.org
5. [Електронний ресурс]: Vas-soft.eu

Журавель Андрій Петрович, здобувач вищої освіти освітнього ступеня «Магістр», 2 курс, Національний авіаційний університет, м. Київ, Україна

Браїловський Микола Миколайович, кандидат технічних наук, доцент, Київський національний економічний університет імені Тараса Шевченка

СИСТЕМА БЕЗПЕКИ ЕЛЕКТРОННИХ ПЛАТЕЖІВ

Інтернет-адреса публікації на сайті:

<http://www.konferenciaonline.org.ua/ua/article/id-1926/>

Вступ. Система безпеки електронних платежів є ключовим елементом у сучасному фінансовому середовищі, де цифрові транзакції стали повсякденною практикою. З розвитком технологій та поширенням онлайн-платежів виникають нові загрози, що вимагають підвищеної уваги до захисту фінансових даних. Фішинг, кібератаки, шахрайські транзакції та ненадійні методи аутентифікації – це лише деякі з викликів, які стоять перед користувачами та платіжними системами. У зв'язку з цим розробка ефективних методів безпеки, зокрема, використання багатофакторної аутентифікації, шифрування та блокчейн-технологій, стає першочерговим завданням для запобігання кібератакам і забезпечення захисту електронних платежів.

Мета роботи. Мета полягає в аналізі системи безпеки електронних платежів, виявленні основних загроз, а також у вивченні сучасних технологій і методів захисту, які сприяють безпеці фінансових транзакцій.

Матеріали та методи. Для досягнення мети даної роботи, в рамках дослідження системи безпеки електронних платежів, були використані наступні матеріали та методи: літературний, статистичний, аналітичний, індукції та дедукції.

Результати та обговорення.

Електронні платежі – це процес здійснення фінансових операцій за допомогою електронних засобів, без використання готівки. Вони дозволяють перевести кошти з одного рахунку на інший за допомогою інтернету, мобільних додатків, платіжних карток, або інших цифрових інструментів.

Електронні платежі можуть включати оплату товарів та послуг онлайн через платіжні системи (наприклад, PayPal, Google Pay, Apple Pay); банківські перекази через системи онлайн-банкінгу; мобільні платежі за допомогою смартфонів через спеціальні додатки; оплату комунальних послуг, штрафів, податків тощо через цифрові платформи а також криптовалютні транзакції через блокчейн [4; 5].

Згідно даних НБУ кількість операцій з використанням платіжних карток, емітованих українськими банками та фінансовими установами, за 2023 рік становила 7 912,5 млн, а їхня загальна сума – 6 140,8 млрд грн [1].

Системи електронних платежів є інструментами, що дозволяють здійснювати безготівкові фінансові операції за допомогою електронних пристроїв і технологій. Ці системи забезпечують швидку, зручну та безпечну передачу коштів між учасниками фінансових операцій (табл.1) [3].

Таблиця 1.

Переваги та недоліки основних платіжних систем

Система	Тип системи	Основні переваги	Основні недоліки
Visa/Master Card	Платіжні картки	Глобальне покриття, висока безпека	Залежність від банківської системи
PayPal	Електронний гаманець	Зручність, можливість здійснення міжнародних переказів	Високі комісії за деякі операції
Google Pay	Мобільні платежі	Безконтактні платежі, швидкість	Залежність від наявності NFC та підтримки на стороні продавця
Apple Pay	Мобільні платежі	Безконтактні платежі, інтеграція з Apple пристроями	Обмежено лише Apple пристроями
Bitcoin	Криптовалюта	Анонімність, децентралізація	Велика волатильність
Ethereum	Криптовалюта	Підтримка смарт-контрактів, децентралізація	Складність розробки та використання
SWIFT	Міжбанківські перекази	Глобальна система міжбанківських переказів	Висока вартість транзакцій
SEPA	Міжбанківські перекази (ЄС)	Стандартизація платежів у євро	Підтримує лише євро
Приват24	Інтернет-банкінг	Зручність для українських користувачів	Обмеження на використання за межами України
Payoneer	Міжнародні перекази	Зручні міжнародні платежі, особливо для фрілансерів	Обмежені функції для особистих користувачів

Загалом, основні системи електронних платежів на сьогодні забезпечують зручність, швидкість та безпеку проведення фінансових операцій. Вибір системи залежить від вимог користувача, таких як глобальність операцій, анонімність, можливість проведення великих транзакцій або інтеграція з мобільними пристроями. Сучасні системи постійно вдосконалюються, пропонуючи нові функціональні можливості та підвищуючи рівень захисту від загроз.

Безпека електронних платежів є критичним аспектом сучасної фінансової системи, що гарантує захист користувачів від шахрайства, крадіжки даних та несанкціонованого доступу до їх фінансових коштів. Вона охоплює технології, процеси та політики, які спрямовані на захист конфіденційної інформації, а також забезпечення надійності та довіри до платіжних систем. Основні компоненти безпеки електронних платежів включають: шифрування даних, аутентифікація та двофакторна аутентифікація користувачів, системи виявлення шахрайства, сертифікати безпеки та захист від фішингу та шкідливих програм. Це в комплексі дозволяє мінімізувати ризики та забезпечувати стабільне і захищене проведення фінансових операцій в інтернеті [2].

З розвитком цифрових технологій з'являються нові загрози для безпеки фінансових транзакцій, тому захист від цих загроз є пріоритетом для користувачів і платіжних систем (табл. 2).

Таблиця 2

Основні загрози безпеці електронних платежів

Загроза	Опис
Фішинг	Використання підроблених вебсайтів або електронних листів для отримання конфіденційної інформації (логіни, паролі, платіжні дані) від користувачів.
Кібератаки на платіжні системи	Злом серверів або баз даних платіжних систем для незаконного доступу до фінансової інформації користувачів.
Перехоплення даних	Використання шкідливих технологій для перехоплення даних, які передаються через мережу, з метою доступу до платіжної інформації.
Шахрайські транзакції	Несанкціоноване використання платіжних карток або електронних гаманців для проведення фінансових операцій без згоди власника.

Загалом, безпека електронних платежів стикається з багатьма викликами, серед яких шахрайство, кібератаки, недостатня захищеність даних, а також відсутність єдиних стандартів і складність інтеграції різних систем. Основні проблеми включають людський фактор, ненадійну аутентифікацію, та повільну реакцію на нові загрози. Для забезпечення безпеки платіжних операцій необхідно постійно вдосконалювати системи захисту, впроваджувати новітні технології шифрування, багатофакторну аутентифікацію та забезпечувати обізнаність користувачів щодо безпеки їх фінансових даних.

Висновки. У сучасному фінансовому середовищі система безпеки електронних платежів відіграє надзвичайно важливу роль у забезпеченні

безпеки та довіри користувачів до фінансових транзакцій. З розвитком технологій і зростанням популярності онлайн-платежів з'являються нові виклики, які вимагають комплексного підходу до захисту інформації та фінансових даних. Встановлено, що основні загрози, з якими стикаються платіжні системи, включають фішинг, кібератаки, шахрайські транзакції та перехоплення даних. Для ефективної боротьби з цими загрозами необхідно використовувати сучасні технології, такі як шифрування, багатофакторна аутентифікація та системи виявлення шахрайства. Також важливим аспектом є підвищення обізнаності користувачів щодо ризиків, пов'язаних з електронними платежами, та навчання їх використанню безпечних методів онлайн-транзакцій. Впровадження сучасних технологій безпеки та відповідні політики можуть суттєво знизити ризики і сприяти розвитку безпечного та надійного фінансового середовища для всіх учасників.

Список використаних джерел:

1. Другий рік повномасштабної війни: обсяги безготівкових розрахунків зростають. URL: <https://bank.gov.ua/ua/news/all/drugiy-rik-povnomasshtabnoyi-viyni-obsyagi-bezgotivkovih-rozrahunkiv-zrostayut>
2. Золотухін О., Лановий О. Метод ідентифікації в безконтактних платежах. *Інформаційні системи та технології. Секція 6. Програмна інженерія*, 2018. С. 305-307.
3. Іванишин М. Р., Паламарчук Є. А. Існуючі рішення платіжних систем та принципи їх роботи. ВНТУ, 2023. С. 1-7.
4. Сердюк К. В. Аналіз та застосування сучасних платіжних систем. Суми : Сумський державний університет, 2024. 74 с.
5. Туржанський А. Аналіз сучасного стану та перспективи розвитку інтернет торгівлі в Україні. *Кваліфікаційна робота на здобуття освітнього ступеня магістра спеціальності «Економіка»*. Національний авіаційний університет. Київ, 2023. – 87 с.

*Кацман Віта Юріївна, кандидат технічних наук,
доцент, Національний технічний університет
«Дніпровська політехніка», м. Дніпро
ORCID: 0000-0002-0395-5895*

МЕТОДИКА ВИДІЛЕННЯ СІЛЬСЬКОГОСПОДАРСЬКИХ КУЛЬТУР НА БАГАТОСПЕКТРАЛЬНИХ ЦИФРОВИХ СУПУТНОВИХ ЗНІМКАХ

Інтернет-адреса публікації на сайті:

<http://www.konferenciaonline.org.ua/ua/article/id-1930/>

Карти землекористування або ґрунтово-рослинного покриву є основним інструментом управління інформацією про поверхню землі. Вони відображають взаємодію між різними типами ґрунтово-рослинного покриву, надаючи важливі дані для управління земельними ресурсами, а також для екологічних цілей,

таких як землекористування, зміна землекористування та лісове господарство [1, с. 240]. Основною метою цього дослідження є розробка методики виділення сільськогосподарських культур на супутникових зображеннях з використанням вегетаційних індексів та архітектури VGG19 для точного виділення основних типів зрошуваних культур.

Дослідження базується на використанні супутникових даних Sentinel-2 і Landsat 8, які є джерелом багатоспектральних зображень з необхідною роздільною здатністю для обчислення вегетаційних індексів, таких як NDVI, EVI, NDWI і SAVI [2, с. 410]. Ці індекси широко використовуються в аграрних дослідженнях для оцінки стану рослинності.

Для досягнення точних результатів виділення сільськогосподарських культур було виконано наступні кроки:

- канали SWIR 1 і SWIR 2 зображень Sentinel-2 були передискретизовані до роздільної здатності 10 м, щоб забезпечити однаковий масштаб із іншими каналами;

- дані Sentinel-2 і Landsat 8 були скориговані з урахуванням атмосферних впливів від верхньої частини атмосфери до поверхневої відбивної здатності, що було виконано за допомогою програми Sen2Core, доступної через пакет Sentinel Hub [3 с.41, 4 с.457];

- усі зображення були згруповані за місяцями для відповідного регіону дослідження;

- архітектура VGG19 була застосована для сегментації зображень і класифікації сільськогосподарських культур на основі попередньо обчислених вегетаційних індексів.

Після підготовки даних були розраховані вегетаційні індекси NDVI (Normalized Difference Vegetation Index), EVI (Enhanced Vegetation Index), NDWI (Normalized Difference Water Index) та SAVI (Soil Adjusted Vegetation Index). Ці індекси допомагають виділяти різні типи рослинності і є важливими для класифікації сільськогосподарських культур.

Для тестування використовувалися вхідні дані у вигляді багатоспектральних зображень та вегетаційних індексів. Після попередньої обробки, що включала корекцію атмосферних впливів та дискретизацію каналів, зображення були сегментовані, а потім класифіковані за типами культур. Для забезпечення високої точності результатів було проведено порівняння ефективності алгоритмів на різних комбінаціях вегетаційних індексів. Для сегментації сільськогосподарських земель використано архітектуру VGG19, яка продемонструвала точність класифікації на рівні 88,7% для пшениці та 85,2% для кукурудзи. Найкращі результати були досягнуті при використанні комбінації NDVI та EVI, при цьому точність класифікації пшениці збільшилася на 2,8% при поєднанні обох індексів у порівнянні з використанням лише NDVI.

На рис. 1 представлені графіки результатів навчання нейронної мережі VGG19 протягом 50 епох, де відображено динаміку точності та втрат моделі.

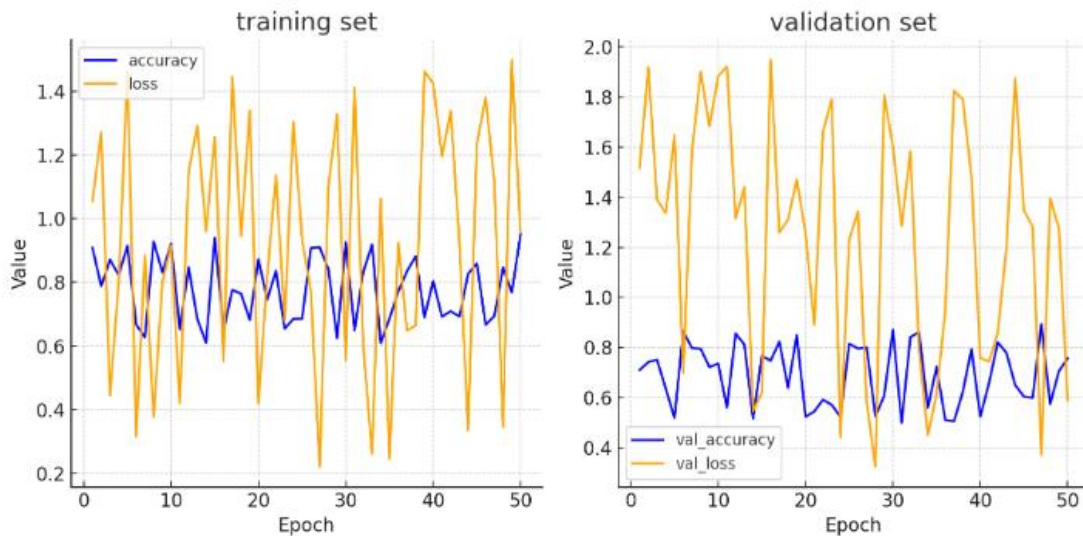


Рисунок 1 – Навчання мережі VGG19

Синя лінія відображає точність моделі на тренувальному наборі, а помаранчева лінія показує втрати. Видно, що точність поступово зростає, а втрати зменшуються, що свідчить про ефективне навчання моделі з часом.

Дослідження показало, що комплексне використання вегетаційних індексів NDVI та EVI в поєднанні з архітектурою VGG19 дає значно кращі результати у порівнянні з використанням одного індексу. Такий підхід дозволяє отримати більш повну інформацію про рослинність, оскільки NDVI більше чутливий до загального стану рослинності, а EVI враховує атмосферні впливи та оптичну густину. Завдяки цьому, точність класифікації підвищується, що було продемонстровано на прикладі пшениці та кукурудзи. Зокрема, точність класифікації пшениці збільшилася на 2,8% при використанні обох індексів, що свідчить про ефективність комплексного підходу для точного картування сільськогосподарських культур.

Література:

1. Jones, J. W.; Antle, J. M.; Basso, B.; Boote, K. J.; Conant, R.T. ; Foster, I.; Godfray, H. C. J.; Herrero, M.; Howitt, R. E.; Janssen, S.; et al. Brief History of Agricultural Systems Modeling. *Agric. Syst.* 2017, 155, 240-254.
2. Lee, K.; Kyung, D.; Park, C.-W.; Ho, S. K.; Na, S.-I. Selection of Optimal Vegetation Indices and Regression Model for Estimation of Rice Growth Using UAV Aerial Images. *Korean J. Soil Sci. Fertil.* 2017, 50, 409-421.
3. Comba, L.; Biglia, A.; Riccauda Aimonino, D.; Tortia, C.; Mania, E.; Guidoni, S.; Gay, P. Leaf Area Index Evaluation in Vineyards Using 3D Point Clouds from UAV Imagery. *Precis. Agric.* 2020, 21, 881-896.

4. Каштан В.Ю., Шевцова О.С. Інформаційна технологія попередньої обробки супутникових зображень з використанням згорткової нейронної мережі. Системні технології. Регіональний міжвузівський збірник наукових робіт. – Випуск 1 (150). – Дніпро, 2024. С. 36-50. DOI: <https://doi.org/10.34185/1562-9945-1-150-2024-04>

5. Gascon, F.; Cadau, E.; Colin, O.; Hoersch, B.; Isola, C.; Fernández, B. L.; Martimort, P. Copernicus Sentinel-2 Mission: Products, Algorithms and Cal/Val. In Proceedings of the Earth Observing Systems XIX, San Diego, CA, USA, 17-21 August 2014; SPIE: Bellingham, WA, USA, 2014; Volume 9218, pp. 455-463.

***Кіш Віктор Вікторович**, магістр,
кафедра системного аналізу і теорії оптимізації,
факультет математики та цифрових технологій,
Державний вищий навчальний заклад Ужгородський
національний університет, м. Ужгород*

***Йовбак Ніка Ігорівна**, студентка,
кафедра системного аналізу і теорії оптимізації,
факультет математики та цифрових технологій,
Державний вищий навчальний заклад Ужгородський
національний університет, м. Ужгород*

***Науковий керівник: Кіш Надія Василівна**,
доцент кафедри прикладної лінгвістики,
Державний вищий навчальний заклад Ужгородський
національний університет, м. Ужгород*

УПРАВЛІННЯ БІЗНЕС ПРОЦЕСАМИ В ІТ ПРОЄКТАХ

Інтернет-адреса публікації на сайті:

<http://www.konferenciaonline.org.ua/ua/article/id-1932/>

Управління бізнес-процесами в ІТ-проєктах – це не просто сукупність дій, а стратегічний підхід, який пронизує весь життєвий цикл проєкту від зародження ідеї до запуску продукту та його подальшої підтримки. Це систематичний аналіз, моделювання, оптимізація та автоматизація всіх дій, що виконуються в рамках проєкту, забезпечуючи ефективність, прозорість та адаптивність.

Ефективне управління бізнес-процесами дозволяє досягти значних результатів. Воно підвищує продуктивність, знижує витрати, покращує якість продуктів і послуг, збільшує задоволеність клієнтів та зменшує ризики провалу проєкту. За рахунок усунення неефективних дій, дублювання функцій та оптимізації послідовності виконання завдань, ми досягаємо значного підвищення ефективності. Автоматизація рутинних операцій скорочує час виконання проєктів та зменшує кількість помилок. А підвищення контролю

над процесами забезпечує дотримання стандартів та зниження кількості дефектів.

Процес управління бізнес-процесами включає в себе кілька послідовних етапів. Все починається з моделювання. Використовуючи спеціальні нотації, такі як BPMN, ми візуалізуємо та формалізуємо існуючі процеси, отримуючи чітке уявлення про їх структуру та взаємозв'язки. Наступним етапом є аналіз. Глибокий аналіз дозволяє виявити вузькі місця, дублювання функцій та інші неефективності. Далі проводиться оптимізація, яка може включати реінжиніринг процесів, автоматизацію рутинних задач, делегування повноважень та стандартизацію. Після оптимізації здійснюється автоматизація процесів за допомогою систем управління бізнес-процесами (BPMS). І, нарешті, проводиться моніторинг та контроль виконання процесів, збір даних та аналіз результатів.

Для ефективного управління бізнес-процесами використовується широкий спектр інструментів та технологій. BPMN – це стандартна мова для моделювання бізнес-процесів, яка дозволяє візуалізувати та формалізувати процеси. BPMS – це системи управління бізнес-процесами, які забезпечують автоматизацію виконання процесів, контроль та аналіз. RPA (роботизована автоматизація процесів) дозволяє автоматизувати рутинні завдання. Штучний інтелект використовується для аналізу великих обсягів даних, прогнозування та прийняття рішень. А хмарні технології забезпечують гнучкість і масштабованість систем управління бізнес-процесами.

Поверхнєве розуміння управління бізнес-процесами може призвести до частикових покращень, але не дозволить досягти максимального потенціалу. Глибоке занурення дозволяє:

- Поняти кореневі причини проблем: Аналіз процесів на рівні деталей дозволяє виявити приховані проблеми та розробити ефективні рішення.
- Оптимізувати процеси під конкретні потреби бізнесу: Індивідуальний підхід до кожного процесу дозволяє досягти максимальної ефективності.
- Використовувати весь потенціал сучасних технологій: Розуміння можливостей штучного інтелекту, машинного навчання та інших технологій дозволяє створювати інноваційні рішення.
- Сформувати культуру безперервного покращення: Постійний аналіз та оптимізація процесів стають невід'ємною частиною корпоративної культури.

Отже, управління бізнес-процесами в IT-проектах – це не просто модний тренд, а необхідність для досягнення успіху в сучасному динамічному бізнес-середовищі. Це комплексний підхід, який дозволяє підвищити ефективність, знизити витрати та поліпшити якість продуктів і послуг. Завдяки використанню сучасних технологій та інструментів, управління бізнес-процесами стає все більш доступним і ефективним.

Список використаних джерел:

1. <https://kissflow.com/workflow/bpm/business-process/>
2. <https://www.it.ua/knowledge-base/technology-innovation/business-process-management-bpm>
3. <https://www.villanovau.com/articles/bpm/what-is-a-business-process/>
4. <https://flokzu.com/bpm/the-complete-guide-of-business-processes/>

*Колодій Роман Ігорович, аспірант (здобувач),
Національний університет "Львівська політехніка", Львів
ORCID: 0009-0002-4628-6422*

*Науковий керівник: Виклюк Ярослав Ігорович,
професор, доктор технічних наук*

ДОСЛІДЖЕННЯ ВЗАЄМОДІЇ ПОЯСНЮВАНОВОГО ШТУЧНОГО ІНТЕЛЕКТУ (ХАІ) ТА ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ (LLM)

Інтернет-адреса публікації на сайті:

<http://www.konferenciaonline.org.ua/ua/article/id-1916/>

Сучасний розвиток штучного інтелекту характеризується стрімким зростанням можливостей та складності моделей, зокрема великих мовних моделей (LLM), таких як GPT-3 та GPT-4 [5]. Вони демонструють високі результати в обробці природної мови, генерації тексту та розв'язанні складних завдань у різних сферах, включаючи медицину та фінанси [4]. Проте їхня непрозорість та складність призводять до виникнення "чорної скриньки", що ускладнює розуміння процесів прийняття рішень цими моделями [1]. Це викликає питання до довіри, відповідальності та етичності використання таких систем, особливо в критично важливих галузях.

Пояснювальний штучний інтелект (ХАІ) стає все більш актуальним, оскільки забезпечує прозорість та інтерпретованість моделей ШІ [2]. Інтеграція ХАІ з LLM відкриває нові можливості для підвищення довіри користувачів та забезпечення відповідального використання ШІ. Зокрема, LLM можуть сприяти розвитку ХАІ через:

- Переклад складних технічних пояснень у природну мову, що робить результати ХАІ доступними для широкого кола користувачів, включаючи неекспертів.
- Надання контексту та додаткової інформації, збагачуючи та уточнюючи пояснення за допомогою власної бази знань.
- Генерацію прикладів, допомагаючи користувачам зрозуміти альтернативні сценарії та фактори, що впливають на рішення моделі.

Retrieval-Augmented Generation (RAG) моделі є інноваційним підходом, який об'єднує можливості великих мовних моделей з динамічним доступом до

зовнішніх джерел інформації під час генерації відповідей [3]. На відміну від традиційних LLM, які покладаються виключно на внутрішні знання, RAG моделі можуть використовувати актуальні дані з баз знань, документів або Інтернету. Це дозволяє:

- Підвищити точність та актуальність відповідей, оскільки модель має доступ до найсвіжшої інформації.
- Зменшити ймовірність генерування некоректної або застарілої інформації, що є особливо важливим у швидкоплинних галузях, таких як медицина чи право.
- Включати посилання на джерела інформації, що підвищує прозорість та довіру користувачів до результатів. Користувачі можуть самостійно перевірити джерела та впевнитися у достовірності наданої інформації.
- Адаптувати відповіді до специфічних запитів, враховуючи контекст та потреби користувача.

Впровадження RAG підходу сприяє розвитку більш надійних та відповідальних ШІ-систем, які можуть ефективно поєднувати генеративні можливості LLM з перевагами структурованих та достовірних даних. Це особливо корисно в освітніх платформах, де важливо надавати точні та підтвержені знання, а також у професійних середовищах, де помилки можуть мати серйозні наслідки.

Інтеграція ХАІ та LLM, включаючи RAG моделі, супроводжується низкою викликів:

- Оцінка якості пояснень: Необхідно розробити стандартизовані метрики для оцінки пояснень, згенерованих LLM. Це включає обґрунтованість (наскільки пояснення логічно підтримує рішення), повноту (наскільки пояснення охоплює всі важливі аспекти), контекстну обізнаність (відповідність пояснення специфічному контексту запиту) та стислість (лаконічність без втрати змісту). Відсутність таких метрик ускладнює порівняння та вдосконалення моделей, а також може призвести до надання користувачам неповних або некоректних пояснень.
- Адаптація пояснень для різних аудиторій: Різні користувачі мають різний рівень знань та різні потреби. Кінцеві споживачі можуть потребувати простих та зрозумілих пояснень без технічних деталей, тоді як розробники або регулятори можуть вимагати більш глибокого аналізу та технічної інформації. Важливо розробити методи, які дозволять динамічно налаштовувати пояснення відповідно до профілю користувача, забезпечуючи релевантність та корисність інформації для кожної групи.
- Вирішення проблем упередженості: LLM, навчені на великих обсягах даних з Інтернету, можуть успадковувати та посилювати існуючі соціальні та культурні упередження. Це може призвести до надання некоректних або дискримінаційних пояснень. Необхідно розробити методи

виявлення упередженості в моделях та їх поясненнях, а також стратегії пом'якшення, такі як коригування навчальних даних, використання технік постобробки або впровадження спеціальних алгоритмів, що контролюють генерацію відповідей.

Отже, підсумовуючи, варто відмітити значний потенціал взаємодії між ХАІ та LLM для підвищення прозорості та довіри до ШІ-систем. Проте, щоб реалізувати цей потенціал, необхідно зосередитися на вирішенні вищезгаданих викликів. Розробка ефективних метрик оцінки пояснень дозволить стандартизувати підхід до оцінювання якості та порівняння різних моделей. Адаптивні методи представлення інформації забезпечать релевантність пояснень для різних аудиторій, підвищуючи їх корисність та ефективність. Техніки пом'якшення упередженості сприятимуть створенню більш етичних та справедливих ШІ-систем, що особливо важливо в контексті соціальної відповідальності та дотримання прав людини.

Узагальнюючи, цей напрямок досліджень відображає важливий зсув у сфері ШІ: прагнення до прозорості та пояснюваності стає фундаментальною вимогою для побудови довіри та забезпечення етичного та відповідального розвитку ШІ-систем [5]. Взаємодія між ХАІ та LLM має потенціал не лише покращити технічні аспекти моделей, але й вплинути на те, як ШІ-системи сприймаються та використовуються суспільством. Це відкриває шлях до більш тісної інтеграції ШІ в повсякденне життя, де користувачі можуть взаємодіяти з технологіями на основі взаємної довіри та розуміння.

Література:

1. Mavrepis, P. XAI for All: Can Large Language Models Simplify Explainable AI? [Електронний ресурс] / P. Mavrepis // arXiv preprint arXiv:2401.13110, 2024. – Режим доступу: <https://arxiv.org/pdf/2401.13110>.
2. Zyteck, A. LLMs for XAI: Future Directions for Explaining Explanations [Електронний ресурс] / Zyteck, A. // arXiv preprint arXiv:2405.06064, 2024. – Режим доступу: <https://arxiv.org/abs/2405.06064>.
3. Exploring AI in Search: An Introduction to RAG Models [Електронний ресурс] // Perplexity.ai, 2023. – Режим доступу: https://www.perplexity.ai/page/exploring-ai-in-search-an-intr-jBULt6_mSB2yAV8b17WLDA.
4. Weidinger, L., Mellor, J., Rauh, M., et al Ethical and Social Risks of Harm from Language Models [Електронний ресурс] / L. Weidinger, J. Mellor, M. Rauh, et al. // arXiv preprint arXiv:2112.04359, 2021. – Режим доступу: <https://arxiv.org/abs/2112.04359>.
5. Zhao, W. X., Zhou, K., Li, J., et al. Огляд великих мовних моделей [Електронний ресурс] / W. X. Zhao, K. Zhou, J. Li, et al // arXiv preprint arXiv:2303.18223, 2023. – Режим доступу: <https://arxiv.org/abs/2303.18223>.

МЕТОД ВИЯВЛЕННЯ ВТОРГНЕНЬ

Інтернет-адреса публікації на сайті:

<http://www.konferenciaonline.org.ua/ua/article/id-1925/>

Abstract

Method of detection of invaders

This paper presents an advanced intrusion detection method for computer systems and networks. The proposed approach combines signature-based techniques, anomaly detection, and neural network technologies with machine learning algorithms. The method incorporates multi-stage analysis, including data preprocessing, neural network-based anomaly detection, signature analysis, and adaptive detector generation. Key features include the integration of machine learning classifiers with neural networks and a continuous adaptation mechanism. The paper discusses the method's effectiveness in detecting both known and novel attacks while minimizing false positives. It also addresses implementation challenges and the method's applicability across various network environments. The research emphasizes the importance of adaptive security measures in the face of evolving cyber threats.

Вступ

У сучасному світі одним з найбільш пріоритетних напрямків кібербезпеки є розробка ефективних систем виявлення вторгнень, які забезпечують захист комп'ютерних мереж та інформаційних систем від зловмисних атак. Виявлення вторгнень є критично важливим компонентом загальної стратегії безпеки, що дозволяє своєчасно ідентифікувати та реагувати на потенційні загрози.

Щодня кількість та складність кібератак зростає: їх використовують не лише для крадіжки даних, але й для промислового шпіонажу, порушення роботи критичної інфраструктури і навіть для впливу на політичні процеси. В цьому контексті, розробка передових методів виявлення вторгнень стає все більш актуальною.

Стаття присвячена аналізу відомих підходів до виявлення вторгнень на основі машинного навчання на великих обсягах мережевого трафіку.

Постановка задачі

Задача полягає у визначенні недоліків відомих методів виявлення вторгнень у комп'ютерні системи та мережі, а також обґрунтуванні підходів до їх виправлення.

Термінологія

Система виявлення вторгнень (IDS) – це програмне або апаратне забезпечення, яке автоматично виявляє і попереджає про несанкціоновані спроби доступу, атаки або порушення безпеки в комп'ютерній мережі або системі.

Сигнатурний аналіз – метод виявлення вторгнень, що базується на порівнянні шаблонів відомих атак з поточною активністю в мережі.

Виявлення аномалій – підхід до ідентифікації вторгнень, який фокусується на виявленні відхилень від нормальної поведінки системи або мережі.

Машинне навчання в кібербезпеці – застосування алгоритмів, які дозволяють комп'ютерним системам автоматично вдосконалювати свою здатність виявляти загрози на основі аналізу даних без явного програмування.

Опис методу

Системи виявлення вторгнень (СВВ) поділяються на два основні типи: локальні та мережеві [1]. Локальні СВВ встановлюються на кожному окремому комп'ютері, тоді як мережеві СВВ аналізують пакети, що надходять в мережу через один пристрій, перш ніж пересилати їх заданим вузлам. Мережеві СВВ стають менш ефективними зі збільшенням кількості вузлів у мережі, оскільки забезпечення надійної фільтрації пакетів ускладнюється.

Методи виявлення атак можна розділити на три основні групи:

1. Сигнатурні методи.
2. Методи виявлення аномалій.
3. Комбіновані методи.

Сигнатурні методи описують кожну атаку особливою моделлю або сигнатурою. Ці методи мають високу точність визначення факту атаки, але не здатні виявляти атаки, сигнатури яких ще не визначені. Найпоширенішим серед сигнатурних методів є метод контекстного пошуку, який полягає у виявленні у вихідній інформації певної множини символів.

Пропонований метод виявлення вторгнень базується на комбінованому підході, що поєднує переваги сигнатурних методів, методів виявлення аномалій та нейромережових технологій. Цей інтегрований підхід дозволяє ефективно виявляти як відомі, так і нові типи атак, одночасно знижуючи кількість помилкових спрацьовувань [2].

Метод починається з етапу попередньої обробки мережевого трафіку. На цьому етапі сенсорна система отримує трафік від датчиків мережі, здійснюється збір та нормалізація даних, а також виділення ключових ознак пакетів. Отриманий набір даних нормалізується і перетворюється на масштабований вектор даних, що забезпечує якісну підготовку для подальшого аналізу та підвищує ефективність роботи системи в цілому.

Наступним кроком є аналіз даних за допомогою першої нейронної мережі. Цей етап передбачає подачу нормалізованого вектора даних на обробку нейронній мережі, яка навчена виявляти аномалії у мережевому трафіку. Якщо нейромережа не виявляє ознак аномалій, система повертається до початкового етапу збору даних. У випадку виявлення аномалій, система переходить до наступного етапу аналізу.

Паралельно з нейромережевим аналізом проводиться сигнатурний аналіз, який передбачає порівняння вхідних даних з базою відомих сигнатур атак. Цей етап дозволяє швидко виявляти відомі загрози, що є особливо важливим для захисту від поширених типів атак.

У разі виявлення потенційної загрози, система генерує набір спеціалізованих детекторів з різними параметрами та структурою. Ці детектори навчаються розпізнавати специфічні ознаки мережевої атаки, що дозволяє більш точно ідентифікувати характер загрози. Вектор вхідних даних досліджується цими детекторами для підтвердження наявності вторгнення.

Ключовою особливістю запропонованого методу є застосування алгоритмів машинного навчання, зокрема, методів класифікації, таких як Random Forest, у поєднанні з нейронними мережами. Модель машинного навчання тренується на історичних даних про атаки та нормальний трафік, що дозволяє їй ефективно розрізняти легітимну та зловмисну активність. Використання машинного навчання значно підвищує адаптивність системи до змін у мережевому середовищі та покращує її здатність виявляти складні та раніше невідомі типи атак.

Після проведення всіх етапів аналізу відбувається агрегація результатів. На цьому етапі комбінуються результати сигнатурного аналізу, виявлення аномалій та машинного навчання. На основі цієї агрегованої інформації приймається остаточне рішення про наявність або відсутність вторгнення. У разі підтвердження вторгнення, система генерує сигнал тривоги [3].

Важливою складовою методу є постійне оновлення та адаптація. Це включає регулярне оновлення бази сигнатур для виявлення нових відомих атак, а також періодичне перенавчання моделей машинного навчання та нейронних мереж на нових даних. Крім того, система має механізм "мутації" детекторів, які поглинають інформацію про виявлене втручання, що дозволяє системі постійно вдосконалюватися та адаптуватися до нових загроз.

Запропонований метод демонструє високу ефективність у виявленні широкого спектру атак, від добре відомих до нових та складних. Його гнучкість та адаптивність роблять його придатним для застосування в різноманітних мережевих середовищах, від невеликих локальних мереж до великих корпоративних інфраструктур. Крім того, інтеграція машинного навчання та нейронних мереж дозволяє системі постійно вдосконалюватися, покращуючи свою точність та ефективність з часом.

Література:

1. Аналіз та класифікація методів виявлення вторгнень в інформаційну систему | Системи управління, навігації та зв'язку. Збірник наукових праць. *Open Journal Systems*. URL: <https://journals.nupp.edu.ua/sunz/article/view/323> (дата звернення: 29.09.2024).

2. Учасники проектів Вікімедіа. Система виявлення вторгнень – Вікіпедія. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/Система_виявлення_вторгнень (дата звернення: 29.09.2024).
3. Лукова-Чуйко Н. Методи виявлення вторгнень у сучасних системах іds. *Інформаційна та кібернетична безпека*. С. 19-26. URL: [https://moodle.znu.edu.ua/pluginfile.php/598874/mod_folder/content/0/03-BIST_No+1\(5\)_2021+Lukova+19-26.pdf?forcedownload=1](https://moodle.znu.edu.ua/pluginfile.php/598874/mod_folder/content/0/03-BIST_No+1(5)_2021+Lukova+19-26.pdf?forcedownload=1).

Моргаль Олег Михайлович, старший викладач,
Київський політехнічний інститут ім. Ігоря Сікорського
ORCID: 0000-0003-4654-9499

Савчук Олена Володимирівна,
кандидат технічних наук, старший науковий співробітник,
Київський політехнічний інститут ім. Ігоря Сікорського
ORCID: 0000-0003-3176-7952

Турок Вадим Васильович, студент,
Київський політехнічний інститут ім. Ігоря Сікорського

ІНТЕЛЕКТУАЛЬНИЙ ЗАСТОСУНОК РОЗПІЗНАВАННЯ ЗАБАРВЛЕНОСТІ ТЕКСТОВИХ ПОВІДОМЛЕНЬ УКРАЇНСЬКОЮ МОВОЮ

Інтернет-адреса публікації на сайті:

<http://www.konferenciaonline.org.ua/ua/article/id-1915/>

Проблема загрозової чи емоційної забарвленості у текстових повідомленнях є особливо актуальною, оскільки вона може мати серйозні соціальні наслідки, від особистісних конфліктів до масових деструктивних взаємодій у віртуальному середовищі [1].

Метою роботи є розробка та валідація інтелектуального застосунку, який спроможен ефективно виявляти емоційне забарвлення у текстових повідомленнях, написаних українською мовою (унікальні мовні та культурні особливості), забезпечуючи високу точність та надійність виявлення агресивного контенту [2].

Основні задачі роботи: 1. Розробка моделі виявлення емоцій. 2. Валідація та тестування системи. 3. Аналіз результатів та розробка рекомендацій для покращення системи.

Особливості задачі: 1. Мовні та культурні особливості. 2. Різноманітність форм вираження емоцій. 3. Неоднозначність контексту. 4. Висока точність та надійність.

Формалізація задачі: 1. Визначення емоцій. 2. Створення датасету повідомлень, які включають приклади агресивного та неагресивного контенту. 3. Вибір методології. 4. Розробка алгоритму. 5. Тестування та оцінка ефективності (оцінка та швидкість обробки).

Тип навчання: наглядове навчання (supervised learning) з позначенням емоцій позитивне (1) або негативне (-1); встановлення кореляції між вхідними та вихідними даними, що передбачають невідомі раніше вхідні дані. Тип нейронної моделі: рекурентна нейронна мережа (RNN) з використанням архітектури LSTM (Long Short-Term Memory) [3].

Оцінка якості: за допомогою метрик точності (accuracy) та втрати (loss).

Мова програмування: Python, середовище – Visual Studio Code.

Вибір нейронної мережі та її параметрів

Вибір моделі: Sequential з бібліотеки Keras.

Перший шар – Embedding: input_dim=5000, output_dim=128, input_length=100. LSTM шар: кількість вузлів – 128, dropout=0.2 і recurrent_dropout=0.2 (20%). Вихідний шар – Dense: 1 вузол, activation='sigmoid', для бінарної класифікації.

Компіляція моделі: loss='binary_crossentropy' (бінарна класифікація). optimizer='adam' (метод оптимізації).

Тренування моделі: batch_size=32, epochs=25.

Оцінка точності моделі: тестові дані типового приклада LSTM.

Навчання мережі

Ключові етапи навчання мережі:

1. Підготовка даних – embedding, padding:
2. Створення моделі: шари – Embedding (обробка входів), Dense (класифікація).
3. Навчання моделі: 1. Пряме поширення (Forward Propagation).
2. Обчислення втрати (Loss Calculation).
3. Зворотне поширення (Backpropagation).
4. Оптимізація параметрів – алгоритм Adam.
5. Валідація та тестування.

Результати навчання та роботи мережі

Точність (accuracy) на тестовому наборі даних склала 83.48%, що є досить високим показником для багатьох застосувань на 25-ій епосі.

Планування експерименту.

1. Зміна архітектури мережі. 2. Гіперпараметри навчання. 3. Регуляризація та уникнення перенавчання: збільшення обсягу даних, застосування попередньо навчених ваг.

Результати експериментів:

1. При зміні кількості LSTM шарів досягнуто збалансованість втрат та точності на тренуванні та валідації, що свідчить про адекватну складність моделі. 2. Зміна функцій активації виявилася невдалою. 3. Зміна гіперпараметрів навчання – це важливий процес для досягнення *оптимальної продуктивності* моделі, залежить від апріорного налаштування. 4. Використання регуляризації. Застосування dropout-шару допомагає зменшити перенавчання і давати кращі результати на тестовому наборі даних та узагальнювати свої знання краще на нових даних. 5. Використання попередньо.

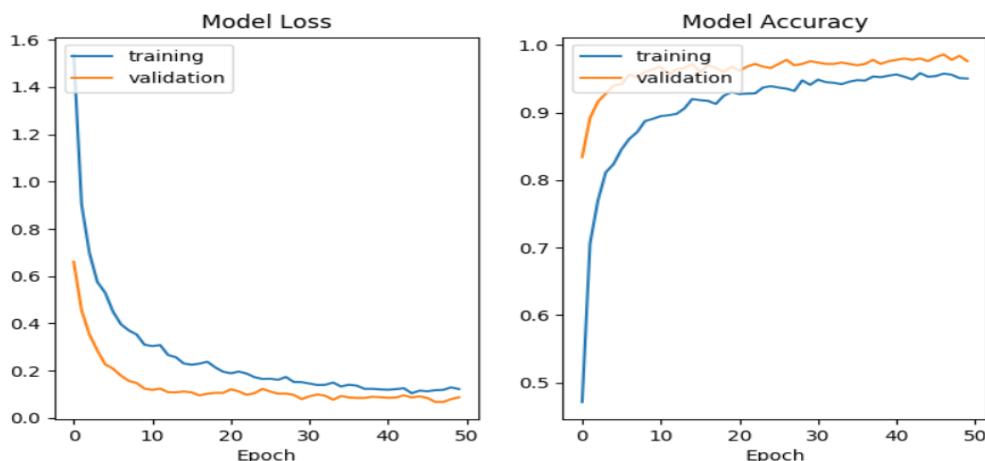


Рисунок 1 – Вплив регуляризації на втрати моделі та перенавчання

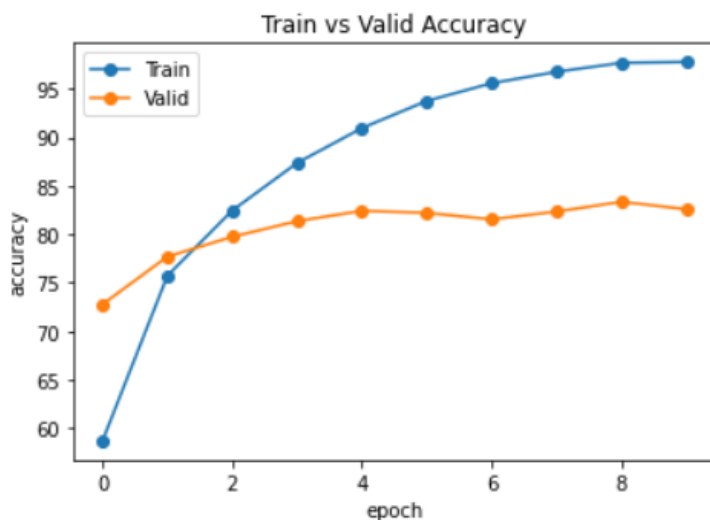


Рисунок 2 – Використання попередньо навчених векторів слів навчених векторів слів є ефективним підходом для аналізу текстів. Вектори слів будуть оновлюватися під час процесу навчання, допомагаючи моделі налаштувати їх під конкретну задачу.

Точність на тестовій вибірці: 87,6 %

Ймовірність негативного забарвлення в тексті: 0.2

Текст містить позитивне емоційне забарвлення

Рисунок 3 – Приклад передбачення

Використання попередньо навчених векторів слів допомагає моделі швидше знаходити семантичні зв'язки у тексті та розпізнавати важливі слова та фрази. Однак для роботи з природними мовами необхідно вирішити багато проблем по удосконаленню моделі [4].

Висновки

Модель показала добрі результати на тренувальному, валідаційному та тестовому наборах даних, з точністю близько 83.48% на тестовому наборі. ROC AUC (коефіцієнт χ^2 Пірсона) вказує на здатність моделі розрізняти класи, і значення 0,76 свідчить про досить хорошу здатність. Важливо слідкувати за динамікою навчання та уникати перенавчання, оцінюючи якість моделі на

валідаційних та тестових даних. Загальною важливістю є те, що навчання нейронних мереж вимагає належного розуміння та налаштування параметрів, а також аналізу результатів для досягнення ефективних рішень в завданнях обробки тексту та класифікації.

Розроблений застосунок може бути використаний в різних сферах життя, таких як маркетинг, медицина та кібербезпека.

Література:

1. Basyuk, T., & Vasyliuk, A. Peculiarities of an Information System Development for Studying Ukrainian Language and Carrying out an Emotional and Content Analysis. *CEUR Workshop Proceedings*, 3396, 2023, 279-294.
2. Lomovatskyi Anton , Basyuk Taras. Methods of Machine Learning and Design of a System for Determining the Emotional Coloring of Ukrainian-language Content / *SISN*, Vol. 15, 2024, 74-86. <https://doi.org/10.23939/sisn2024.15.074>
3. Mathieu Cliché. 2017. BB twtr at SemEval-2017 Task 4: Twitter Sentiment Analysis with CNNs and LSTMs.
4. Дерев'янюк С. П. Психологія емоційного інтелекту: Навчально-методичні рекомендації. Чернігів : НУЧК ім. Т. Г. Шевченка, 2023.

*Токарєв Володимир Володимирович, кандидат технічних наук,
доцент, доцент кафедри Інформаційних систем,
Харківський національний економічний
університет імені Семена Кузнеця
ORCID:0000-0002-7143-6165*

*Маламуж Олексій Петрович, магістрант
кафедри Інформаційних систем,
Харківський національний економічний
університет імені Семена Кузнеця*

ІНТЕГРАЦІЯ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМИ МОДЕЛЮВАННЯ БІЗНЕС-ПРОЦЕСІВ (BPM)

Інтернет-адреса публікації на сайті:

<http://www.konferenciaonline.org.ua/ua/article/id-1908/>

У сучасному динамічному світі ключ до успіху будь-якої організації полягає в її здатності швидко адаптуватися до змін та ефективно управляти своїми бізнес-процесами. З розвитком технологій, особливо штучного інтелекту (ШІ), відкриваються нові можливості для оптимізації та автоматизації бізнес-процесів, що значно підвищує ефективність і гнучкість діяльності компаній. Інтеграція ШІ у системи моделювання бізнес-процесів (BPM) є одним із напрямків, що може кардинально трансформувати методи управління проектами та розробки програмного забезпечення. Використання штучного інтелекту в BPM не лише підвищує ефективність існуючих процесів, але й

сприяє адаптації до змінних умов діяльності з мінімальними затратами часу та ресурсів. Ця інтеграція включає впровадження машинного навчання для автоматизації рутинних завдань, використання алгоритмів обробки природної мови для покращення комунікацій та розуміння документів, а також розробку інтелектуальних систем для стратегічного планування та аналізу великих обсягів даних. Основна мета даного дослідження полягає в детальному аналізі та розробці методів інтеграції алгоритмів ШІ у процесі BPM для оптимізації проектування та розробки програмного забезпечення. Специфічні завдання включають вивчення поточного стану технологій BPM та ШІ, аналіз можливостей їх інтеграції, та розробку конкретних рекомендацій і моделей для ефективного впровадження ШІ у бізнес-процеси. Дослідження базується на комплексному аналізі літературних джерел, кейс-стадії реальних компаній та теоретичних методів моделювання бізнес-процесів. Основний акцент робиться на аналізі можливостей машинного навчання та обробки природної мови в контексті BPM. Використовуються дані з відкритих джерел, наукових публікацій, а також результати опитувань та інтерв'ю з експертами у цій галузі.

Дослідження має на меті виявити основні переваги та можливі виклики інтеграції ШІ в BPM, визначити найефективніші стратегії та технології для їх впровадження, і зрештою, розробити методичні рекомендації для компаній, що планують використовувати ШІ для оптимізації своїх бізнес-процесів. Окрім того, дослідження сприятиме формуванню стратегічного розуміння ролі ШІ в майбутньому розвитку бізнес-моделювання та управління проектами. Інтеграція штучного інтелекту в системи моделювання бізнес-процесів (BPM) стає важливим напрямком у розвитку сучасних інформаційних технологій. Завдяки ШІ, BPM перетворюється, набуваючи нових властивостей, таких як адаптивність, прогнозування та автоматизація, що робить управління бізнес-процесами більш ефективним та еластичним. Цей розділ має на меті проаналізувати сучасний стан інтеграції ШІ в BPM, виділити основні тенденції, переваги, виклики та перспективи. Бізнес-процеси (BPM) – це систематичне управління процесами в організації для покращення їх ефективності. BPM використовує різноманітні методи та технології для візуалізації, аналізу, вимірювання, контролю та оптимізації ключових бізнес-процесів. Штучний інтелект (ШІ) описує галузь комп'ютерних наук, що займається створенням машин, здатних виконувати завдання, які зазвичай потребують людського інтелекту. Це включає машинне навчання, обробку природної мови та робототехніку.



Рис.1. Вплив штучного інтелекту на BPM

Вище представлена діаграма, яка наглядно показує вплив штучного інтелекту на три ключові аспекти управління бізнес-процесами: автоматизація процесів, покращення прийняття рішень та адаптивність. Кожен сектор діаграми представляє один з цих аспектів, показуючи їх рівнозначну важливість у використанні ШІ для оптимізації BPM.

Незважаючи на значні переваги, інтеграція ШІ в BPM також стикається з низкою викликів:

Складність інтеграції: Інтеграція ШІ в існуючі системи BPM може бути технічно складною, вимагаючи значних модифікацій архітектури та інтерфейсів.

Великі обсяги даних: Ефективне використання ШІ вимагає великих обсягів даних для навчання алгоритмів, що може викликати проблеми зі зберіганням та обробкою даних.

Етичні та правові питання: Використання ШІ порушує питання про конфіденційність, безпеку даних та етику, особливо коли йдеться про автоматизацію рішень, які можуть впливати на людські життя.

Попри існуючі виклики, перспективи інтеграції ШІ в BPM виглядають оптимістично. Подальші дослідження та розвиток технологій можуть допомогти подолати технічні та етичні перепони, відкриваючи нові можливості для підвищення ефективності, гнучкості та адаптивності бізнес-процесів.

Література:

1. Токарев В., Ільїна І., Шевченко І., Гриценко І. Про один підхід до рішення асиметричної TSP – задачі при B2C доставках за допомогою платформи "Swarm-bot" – system у фізичному неорганізованому середовищі. Системи управління, навігації та зв'язку, 2023. – №4 (74), с. 110-113.
2. Gryzun L, Tokariev V. Mobile applications design for digital education: IT-students' engagement experience on conditions of online learning the course "Mobile technologies". Proceedings of the 2nd Workshop on Digital Transformation

of Education, co-located with the 18th International Conference on ICT in Education, Research, and Industrial Applications: (ICTERI 2023). CEUR Workshop Proceedings, 2023. Ivano-Frankivsk. Ukraine, pp. 110-123.

3. Koshovyi M. D., Pylypenko O. T., Ilyina I. V., Tokarev V. V. Growing tree method for optimization of multifactorial experiments, Radio Electronics, Computer Science, Control, 2023. – № 3, pp. 55-61.

4. Koshevoy N., Iina I., Tokariev V., Malkova A., Muratov V. Implementation Of The Gravity Search Method For Optimization By Cost Expenses Of Plans For Multifactorial Experiments. Radioelectronic and Computer Systems, 2023. – Vol. 1(105), pp. 23-32.

5. Ільїна І. В., Токареєв В. В., Яковлєв А. В., Шевченко І. І. Використання системи підтримки прийняття рішень для організації гуманітарної логістики, Системи управління, навігації та зв'язку, 2024, №1(75), с. 88-91.

*Чепис Олександр Вікторович, аспірант,
Тернопільський національний технічний
університет імені Івана Пулюя, м. Тернопіль
ORCID: 0009-0001-4480-5877*

*Науковий керівник: Приймак Микола Володимирович,
доктор технічних наук, професор,
Тернопільський національний технічний
університет імені Івана Пулюя, м. Тернопіль*

ЕНЕРГОЕФЕКТИВНІСТЬ В БЕЗПЛОТНИХ ЛІТАЛЬНИХ АПАРАТАХ

Інтернет-адреса публікації на сайті:

<http://www.konferenciaonline.org.ua/ua/article/id-1927/>

Безпілотні літальні апарати (БПЛА) стрімко розвиваються та набувають дедалі більшої актуальності у всіх сферах життя. Їх використовують у промисловості, побуті та у військовій сфері. Одним з ключових факторів є час автономної роботи без необхідності підзаряджання, оскільки в більшості випадків це потребує використання людського ресурсу, як у випадку безпілотних літальних апаратів, тому оптимізація енергоефективності є актуальним питанням.

Тривалість польоту дрона залежить від багатьох факторів таких як: акумулятор, що характеризується ємністю – чим більша ємність тим більший час польоту, проте варто враховувати вагу батареї, оскільки збільшення маси збільшує споживання енергії, хімічний склад що забезпечує різну максимальну ємність при однаковій вазі та стан акумулятора; вага дрону і корисне навантаження (додаткові компоненти, камери, давачі тощо): чим більша вага дрону тим більше енергії необхідно забезпечити для того щоб залишатися повітрі; умови навколишнього середовища: вітер – чим більший вітер тим

більше енергії потрібно для підтримки стабільного положення (не враховуючи випадків, коли вітер допомагає зберегти заряд батареї), екстремальні температури, що можуть негативно вплинути на продуктивність акумулятора; щільність повітря, що характеризується висотою польоту (чим вище, тим більше енергії потрібно для утримання в повітрі); стиль польоту: швидкі маневрені рухи споживаються значно більше енергії в порівнянні з плавними поворотами [4]. Також одним з ключових факторів є дизайн та компоненти дрона: обтічна конструкція з ефективними пропелерами і двигунами буде зменшувати опір та підвищить енергоефективність, також це стосується використання якісних двигунів та програмного забезпечення [2]. На енергоефективність дрону впливають також і інші фактори такі як: використання GPS, відеозапис і робота датчиків, технічний стан дрону тощо. Тому дрон з більш ємним акумулятором та обтічною конструкцією, що летить в безвітряну погоду з помірною швидкістю, зможе пробути в повітрі довше, ніж важкий дрон зі зношеним акумулятором, який виконує складні маневри при сильному вітрі.

Розглянувши фактори, що впливають на ефективність використання енергії при польоті, можна підбирати та оптимізувати необхідні параметри, щоб забезпечити найбільшу ефективність під конкретні задачі.

Виконуючи розробку або вдосконалення БПЛА для забезпечення необхідної енергоефективності потрібно звертати увагу на матеріали з якого він виготовляється, звертаючи увагу на різні композитні матеріали, та матеріали з вуглеволокна, які мають меншу вагу при забезпеченні оптимальної міцності. За їх допомогою досягається оптимізація конструкції дрону, яка спрямована на покращення аеродинамічних характеристик: зменшення опору при польоті, збільшення підйомної сили. Також на зменшення споживання енергії впливає використання енергоефективної електроніки та оптимізованого програмного забезпечення, що дозволяє не тільки зменшити базові енергозатрати на обробку інформації, а й оптимізувати параметри польоту [1].

Майбутніми тенденціями в розвитку БПЛА є впровадження технологій гібридного живлення наприклад поєднання акумуляторів з паливними елементами або збір енергії під час польоту використовуючи сонячні панелі для підзаряджання акумулятору [3], використання штучного інтелекту для побудови конструкцій та оптимізації аеродинамічних характеристик; побудови більш точних комп'ютерних симуляцій, що максимально наближені до реальних умов польоту, що дозволить краще оцінити можливості дрону без фізичних тестів.

Отже, забезпечення максимальної енергоефективності у БПЛА – це завдання, що включає в собі безліч аспектів потрібних для врахування починаючи від конструкції дрону, завершуючи умовами в яких буде проводитись його експлуатація і це питання вимагає комплексного підходу. Зосередившись на легких матеріалах, аеродинамічному дизайні, доповненні дронів ефективними алгоритмами обробки даних та оптимізації процесів

ми зможемо виготовляти БПЛА, які будуть не лише ефективно виконувати місії, але й зберігати максимальну енергоефективність. А оскільки технології продовжують розвиватися, ми можемо очікувати на появу ще більш інноваційних рішень, які підвищать енергоефективність і стійкість БПЛА в найближчому майбутньому.

Література:

1. Денисов, Ю. О., Шаповалов, О. Л., Серeda, О. В., & Куц, Є. В. (2021). ОПТИМІЗАЦІЯ ЕНЕРГОДИНАМІЧНИХ ПРОЦЕСІВ У СИСТЕМІ КЕРУВАННЯ ПРИВОДОМ СТАБІЛІЗАЦІЇ ПОЛЬОТУ БЕЗПІЛОТНОГО ЛІТАЛЬНОГО АПАРАТА. Технічні науки та технології, (3(13)), 187-195. [https://doi.org/10.25140/2411-5363-2018-3\(13\)-187-195](https://doi.org/10.25140/2411-5363-2018-3(13)-187-195)
2. Driving Aerodynamic Drone Design with Advanced Simulation. URL: <https://enterprise.trimech.com/driving-aerodynamic-drone-design-with-advanced-simulation/> (дата звернення: 08.10.2024).
3. What Affects the Range of a Drone? URL: <https://amprius.com/drone-range/#:~:text=A%20heavier%20drone%20requires%20more,with%20a%20similar%20battery%20capacity.> (дата звернення: 07.10.2024).
4. What are the factors that affect the flight time and range of drone? URL: <https://www.droneassemble.com/what-are-the-factors-that-affect-the-flight-time-and-range-of-drone?/> (дата звернення: 07.10.2024).

Шафрай Ілля Юрійович, здобувач вищої освіти освітнього ступеня «Магістр», 2 курс, Національний авіаційний університет, м. Київ, Україна

МЕТОД ПРОТИДІЇ КІБЕРАТАКАМ В КОРПОРАТИВНИХ МЕРЕЖАХ

Інтернет-адреса публікації на сайті:

<http://www.konferenciaonline.org.ua/ua/article/id-1929/>

Вступ. У наші часи обмін даними між учасниками є важливим аспектом процесів обробки та зберігання інформації. Локальні та глобальні мережі розвиваються з впровадженням нових протоколів передачі даних, вдосконаленням апаратних можливостей мережевого обладнання, зростанням кількості підключених користувачів і збільшенням загального обсягу трафіку. Інтенсивний розвиток цієї галузі супроводжується низкою проблем. Такими як: зростання кількості користувачів інформаційних послуг та проблема захисту інформації, яка передається через мережу.

Класифікація систем виявлення вторгнень. Системи виявлення вторгнень можна класифікувати за різними ознаками. Одним із ключових факторів є розташування системного агента.

- Системи виявлення вторгнень на основі хостів (HIDS);
- Мережеві системи виявлення вторгнень (NIDS);

- Гібридні системи виявлення вторгнень.

HIDS – це система виявлення вторгнень, яка працює на окремому хості і моніторить його внутрішні події для виявлення загроз.

NIDS – це система виявлення вторгнень, яка аналізує мережевий трафік у реальному часі для виявлення підозрілих або шкідливих дій. Вона розташовується в ключових точках мережі, перехоплює пакети і перевіряє їх на наявність відомих атак або аномалій.

Гібридні – поєднують в собі можливості як HIDS, так і NIDS для забезпечення комплексного захисту на рівні хостів і мережі.

Аналіз методів раннього виявлення вторгнень. Методології, що застосовуються сучасними системами виявлення вторгнень, можна поділити на три основні категорії:

- **Сигнатурні** – метод виявлення на основі сигнатур функціонує через аналіз шаблонів раніше виявлених загроз. Він дозволяє швидко та точно ідентифікувати відомі атаки. Проте цей метод залежить від постійного оновлення бази даних сигнатур і не здатний розпізнавати невідомі загрози, відсутні в базі даних, або нові види атак.

- **Орієнтовані на аномалії** - ґрунтується на припущенні, що всі атаки відрізняються від типової поведінки системи. Цей метод базується на розділенні мережевої активності на нормальні та ненормальні стани, що здійснюється за допомогою правил або евристик, а не шаблонів або сигнатур.

- **Гібридні** – поєднують у собі як сигнатурні методи, так і методи виявлення аномалій, забезпечуючи таким чином більш комплексний підхід до виявлення вторгнень.

Класифікація основних загроз у вигляді аномальної поведінки.

Атака на інформаційну систему визначається як цілеспрямована дія зловмисника, яка використовує вразливості системи, що призводить до порушення доступності, цілісності та конфіденційності оброблюваної інформації. Усунення цих вразливостей може запобігти здійсненню атаки.

Якщо атаки розглядати як аномалії в комп'ютерних мережах, то:

1. **Розвідка** класифікується як **контекстна аномалія**, оскільки ця атака спрямована на отримання специфічної інформації та розвідувальних даних.

2. **Експлойти** типу R2U і U2R є **точковими аномаліями** через їхню специфічну та складну природу, яка залежить від контексту.

3. **DoS і DDoS**-атаки характеризуються як **колективні аномалії**, оскільки велика кількість запитів надходить одночасно, намагаючись підключитися до сервера, хоча жоден окремий запит не є дійсним.

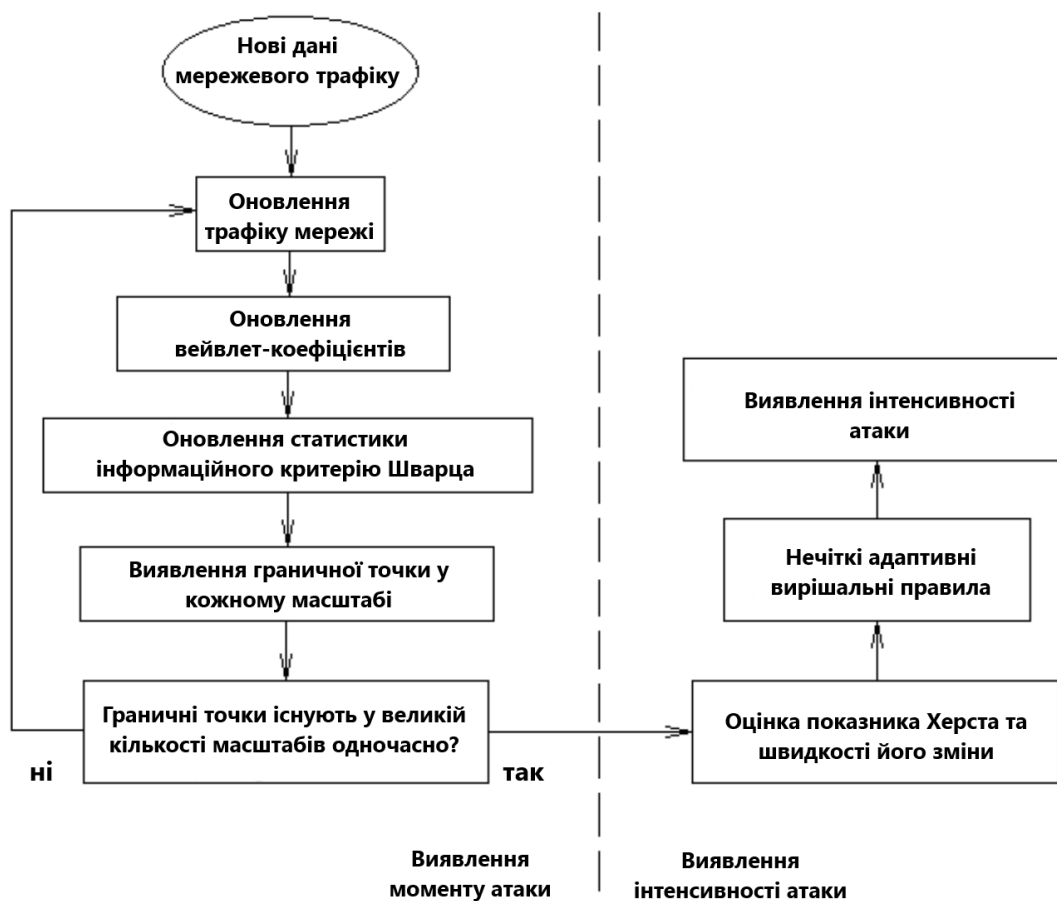


Рис. 1.1. Загальна схема виявлення атаки

Основні етапи виконання атаки. Процес здійснення атаки можна поділити на кілька основних етапів:

1. Збір інформації перед атакою;
2. Безпосереднє виконання атаки;
3. Завершення атаки.

Часто, коли йдеться про атаку, акцент робиться лише на другій фазі, нехтуючи початковою та завершальною стадіями. Проте збір інформації та дії з приховування слідів також є невід'ємними частинами атаки й можуть бути поділені на кілька підетапів.

Виявлення аномально-шкідливої поведінки. Методи виявлення зловживань базуються на припущенні, що характеристики, які визначають поведінку зловмисника, є заздалегідь встановленими. Технології виявлення зловживань здебільшого реалізуються за допомогою експертних систем, таких як Snort, RealSecure IDS та Enterasys Advanced Dragon IDS.

Нижче розглянемо технології, що використовуються в цих системах (рис. 1.2).

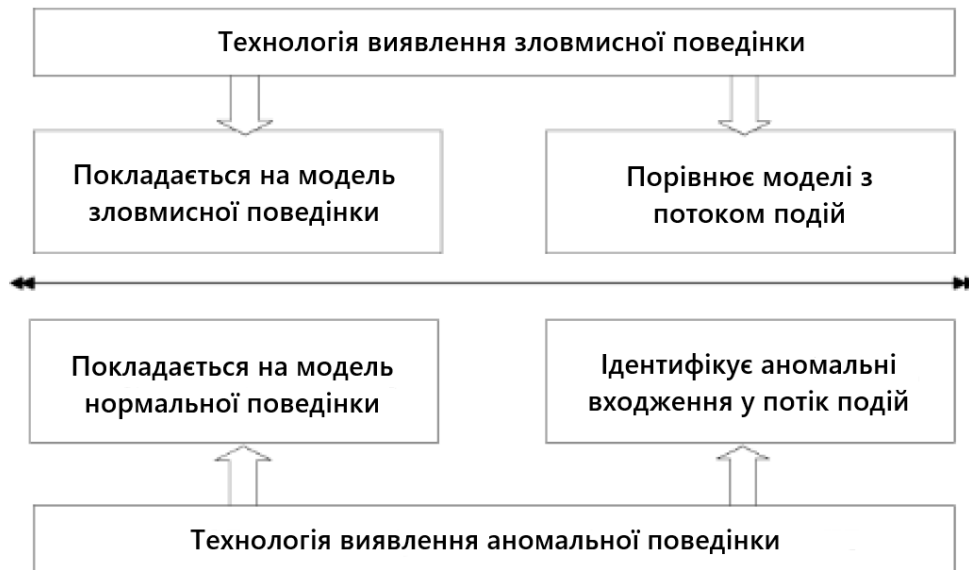


Рис. 1.2. Сучасні технології СВВ

Датчики аномалій виявляють нетипову поведінку, або аномалії, в роботі окремого об'єкта. Основною проблемою їх практичного застосування є нестабільність як захищених об'єктів, так і зовнішніх елементів, які з ними взаємодіють. Об'єктом спостереження може бути як уся мережа, так і окремий комп'ютер або мережевий сервіс.

Головні недоліки у сучасних СВВ. У сучасних системах домінує підхід, заснований або виключно на ідентифікації зловмисників за сигнатурами, або на виявленні аномалій у роботі мережі, що моніториться. До експлуатаційних недоліків належить високий обсяг обчислювальних завдань, необхідних для базової категоризації подій як "свої" або "чужі". Крім того, більшість існуючих систем не здатні обробляти весь обсяг вхідних даних у режимі реального часу на звичайних персональних комп'ютерах. Швидкість обробки мережевого або іншого трафіку подій часто відстає від реального часу в 1,5-2 рази. Це призводить до того, що в деяких системах аналіз проводиться із затримкою, що означає, що атака на інформаційно-обчислювальні ресурси може не бути вчасно виявлена і не буде нейтралізована існуючими засобами захисту.

Більшість сучасних сервіс-орієнтованих архітектур спочатку не призначені для роботи з різними операційними системами та апаратними обчислювальними платформами. Як наслідок, більшість продуктів, як західних, так і вітчизняних, не можуть функціонувати на кількох операційних системах одночасно.

Крім того, жоден програмний або апаратний комплекс не підтримує функцію "гарячої заміни", яка дозволила б негайно активувати резервну систему у разі відмови основної, тим самим відновлюючи скомпрометовану лінію захисту мережевого периметра.

Висновки

У роботі було здійснено огляд, аналіз і класифікацію сучасних систем виявлення вторгнень (СВВ). Розглянуто різні підходи до виявлення загроз, зокрема сигнатурний та поведінковий аналіз, також класифікували основні типи загроз, що проявляються у вигляді аномальної поведінки в мережах. Важливим аспектом стало виявлення недоліків сучасних СВВ, таких як обмеженість у виявленні нових загроз та кросс-платформеність. Задача підвищення ефективності СВВ в умовах зростаючих обсягів трафіку й кількості користувачів залишається актуальною, що потребує вдосконалення як методів, так і інструментів захисту.

Список використаних джерел:

1. Цмоць І. Г., Теслюк С. В. Моделі та засоби автоматизованої системи дослідження трафіку комп'ютерних мереж з використанням фільтра пакетів Берклі. Інтелектуальна система моніторингу та аналізу трафіку для виявлення атак в програмно-конфігурованих мережах // Наукові журнали та конференції Львівської політехніки. – 2022. – №2(1). – С. 1-11.
2. Наталенко М. М., Корецька В. О. Ефективність класифікації додатків аналізу мережевого трафіку комп'ютерних мереж методами машинного навчання // Телекомунікаційні та інформаційні технології. – 2022. – №4(72). – С. 46-53.

***Шестак Ярослав Іванович**, аспірант, старший викладач кафедри інженерії програмного забезпечення та кібербезпеки, Державний торговельно-економічний університет, Київ
ORCID: 0000-0002-5102-9642*

***Завгородня Єлизавета Олександрівна**, аспірант, асистент кафедри інженерії програмного забезпечення та кібербезпеки, Державний торговельно економічний університет, Київ
ORCID: 0000-0003-0549-7020*

***Науковий керівник: Криворучко Олена Володимирівна**, доктор технічних наук, професор, завідувач кафедри інженерії програмного забезпечення та кібербезпеки, Державний торговельно-економічний університет, Київ*

ЗАХИСТ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ЗВО

Інтернет-адреса публікації на сайті:

<http://www.konferenciaonline.org.ua/ua/article/id-1928/>

***Abstract.** The information systems of higher education institutions are constantly undergoing transformations, and there is a coordination between the information systems of the digital state, including applications and systems: DIIA,*

EDEBO, education quality assessment systems, NAQA. Given the constant addition of services to electronic information resources, there is a need to build secure communication channels and ensure the protection of local networks and infrastructure in general

Keywords: *information, protection, HEI, infrastructure, system.*

Анотація. *В інформаційних системах закладів вищої освіти постійно тривають трансформації, відбуваються узгодження між інформаційними системами цифрової держави, зокрема із застосунками і системами: ДІЯ, ЄДЕБО, системи оцінювання якості освіти, НАЗЯВО. З огляду на постійне додавання сервісів до інформаційних електронних ресурсів, постає необхідність у побудові захищених каналів зв'язку та забезпеченні захисту локальних мереж та інфраструктури в цілому.*

Ключові слова: *інформація, захист, ЗВО, інфраструктура, система.*

В період воєнного стану дуже актуальним є проблема побудови інформаційних систем, розвитку та впливу на інфраструктуру різних зовнішніх систем до яких будуть підключатися зовнішні канали зв'язку для передачі даних. кіберризика, які утворилися внаслідок воєнних дій проти України, впливають на ймовірне використання інформаційних систем та на стійкість інфраструктури ЗВО у кіберпросторі. Впродовж багатьох років інформаційні технології та інформаційні системи входили у повсякденне життя людей, давали багато зручних сервісів, спрощення процедур та отримання позитивних відгуків на всі надані чи отримані послуги. Наша держава постійно розвивається і тому збільшуються сфери надання цифрових послуг у державному секторі, бізнес секторі тощо. Інформаційна інфраструктура ЗВО в процесі цифровізації освіти, бізнесу, державних установ, установ спеціального призначення постійно оновлювалася, модернізувалася, удосконалювалася та трансформувалася відповідно до їх потреб і виконуваних задач. Сьогодні немає жодного процесу, який не був би охоплений інформаційними системами, які розвиваються паралельно з розвитком апаратного забезпечення та інформаційних технологій. Так дедалі більше інформації користувачі можуть отримати не виходячи з дому, ефективно і швидко вирішувати багато питань стосовно отримання освіти, вибору курсів, закладів, отримання підтвердження кваліфікації онлайн тощо.

Інформаційна інфраструктура ЗВО дає можливість підключатися, брати, формувати та надавати інформацію за запитами глобальної інфраструктури Smart-міста, цифрової держави, що полегшує роботу самих систем, зменшує ризики надання не достовірної, не коректної інформації, не актуальної інформації чи не правдивої інформації (фейків).

Споживачами цифрової інформації ЗВО наразі є інформаційні системи Smart-міста та зовнішні інфраструктури: підрозділи міністерств, електронні

майданчики для проведення тендерів, системи для звітування, єдина державна електронна база з питань освіти, система для учнів закладів середньої освіти, які обирають напрям та спеціальність для навчання у ЗВО. Здобувачі вищої освіти отримують з інформаційних систем ЗВО всю необхідну інформацію, визначену їм правами доступу, у процесі навчання, підтвердження наукових досягнень, рівню знань, план проведення наукових заходів, участь у заходах та результати їх проведення, отримання відповідної кваліфікації у процесі навчання, можливість працевлаштування та реалізації своїх прав. В свою чергу стейкхолдери отримують права доступу до інформаційних систем інфраструктури ЗВО, зокрема до робочих програм, силабусів, дискутують та беруть участь у погодженні запропонованих набуття компетентностей здобувачів вищої освіти, підготовці майбутніх фахівців відтворення у їх документах підтвердження набутих знань і умінь дипломом, відомствами чи сертифікатами відповідних органів чи іншими документами. Тому, від правильності побудови інформаційної інфраструктури ЗВО, кібернетичного захисту та продуманості каналів зв'язку (API) залежить ефективне функціонування ЗВО, його місце у інформаційному просторі міста, у інформаційному просторі наукового середовища країни та світу.

Для позиціонування ЗВО як наукової світової ланки необхідно розвивати належним чином свою інформаційну інфраструктуру, розвивати інтерфейси відповідно до досягнень власних науковців та залучених ззовні, персоналізувати їх, демонструвати, пропонувати власні розробки, курси, займатися науковими розробками спільно із фахівцями інших ЗВО, наукових інституцій, тим самим піднімаючи власні рейтинги. Додатково, важливим є постійний розвиток і підтримка всіх зовнішніх зв'язків з впливовими інформаційними інфраструктурами регіонального, державного, наукового та світового сектору. Тому інформаційна інфраструктура дуже важлива для всіх ЗВО, навчальних закладів, державних органів і комерційних установ, оскільки має надавати інформацію, з її подальшою верифікацією, без окремого керування фізично окремими особами, що в свою чергу підтвердить прозорість системи та унеможливить вплив корупційних складових на процеси в освітньому середовищі. Таким чином, для забезпечення виконання цих завдань для інформаційної інфраструктури має бути застосована система збереження конфіденційності інформації та захисту персональної інформації на основі критеріїв прозорості та відкритості. Крім того, має бути організована та застосована система кіберзахисту, що наразі, в період воєнного стану в Україні є актуальною і важливою.

Розвиток Smart-міста та цифрової держави не можливий без цифровізації всіх ділових, державних, цивільних та інших процесів в установах, а саме всіх етапів навчання людини, її соціалізації, розвитку на всіх етапах її становлення. Також розвиток особистості залежить від розвитку інфраструктури міста, регіону та всієї держави, всіх сфер обслуговування. Відповідно, важливим

є інформування про можливість у цифровому просторі відобразити, надати доступ до ресурсів всіх відкритих і закритих інформаційних систем інфраструктури. Від розвитку інфраструктури залежить обізнаність людей у недоліках і перевагах систем та їх місце у розвитку регіону держави, важливість вкладу кожного громадянина відповідно до своєї діяльності – реалізації проектів з розбудови держави. Інформаційна інфраструктура закладів вищої освіти залежить від всіх ланок міської, регіональної та державної інфраструктури, вона не може існувати окремо, не може самостійно розвиватися чи впливати на будь які процеси. Тому інформаційна інфраструктура ЗВО має багатогранну структуру з великою кількістю зав'язків, системою кіберзахисту та зовнішніми інформаційними системами інформаційних структур цифрового міста, держави.

Застосування бази знань у інформаційній інфраструктурі ЗВО дає позитивні зрушення через глибокий аналіз всіх процесів управління освітнім процесом. Так використання інтелектуальних систем у вирішенні задач з керування освітнім процесом, дають можливість охопити всі інформаційні системи, аналізувати та надавати рекомендації чи пропозиції з керування всіма процесами у ЗВО, структурувати інформацію з різних інформаційних систем, накопичувати її, з подальшою обробкою масивів цифрової інформації, надавати пропозиції стосовно побудови кібернетичного захисту інформаційних систем та інформаційної інфраструктури ЗВО, надавати прогнози стосовно траєкторії розвитку ЗВО та напрямів затребуваних спеціальностей, коригувати навчальні плани відповідно до потреб стейкхолдерів тощо. Для цього необхідно сформувати базу знань, яка постійно через нейронні мережі буде навчатися, удосконалюватися та видавати необхідну інформацію залежно від потреб внутрішніх та зовнішніх запитів користувачів системи. База знань дозволить оптимізувати керування освітнім процесом, виявляти недоліки інформаційних систем та інформувати відповідальних фахівців для їх усунення, коригувати параметри, трансформувати бази даних та канали зв'язку, а також виявляти потребу в модифікації системи кібернетичного захисту інформаційної інфраструктури ЗВО. Нейронна мережа з алгоритмами дозволяє у скорочені терміни переформатовувати цифрову інформацію, перетворювати та концентрувати всю важливу для ЗВО інформацію, організувати архівування та подальше накопичення для аналізу, трансформації та прогнозування. Також є можливість шифрування інформації з постійними і тимчасовими ключами, які система генерує і використовує для захисту. Таким чином інфраструктура закладу вищої освіти потребує детального вивчення, та побудови захисту відповідних інформаційних систем. Суттєвим є і будуть важливі системи кіберзахисту та системи подвійної ідентифікації користувачів для автентифікації у інформаційних системах.

Висновки: Аналізуючи різні інформаційні системи, їх розвиток, стратегічного підходу до формування інформаційної інфраструктури в Україні та за кордоном, було виявлено загальний підхід до опису функціональних характеристик загальної побудови інформаційної інфраструктури ЗВО, каналів зв'язку (API), ідентифікації та передачі даних у зашифрованому вигляді. Для структуровання вхідної та вихідної інформації, ресурсів, процесів вибору каналів зв'язку підбираються системи кібербезпеки, ключів шифрування, методів ідентифікації тощо. Отже необхідно це питання розглядати, обговорювати та приймати рішення по оптимізації інфраструктури, застосуванні нових методів захисту у кібернетичному просторі та побудови безпечних інтерфейсів зв'язку між загально-державними електронними системами.

Список використаних джерел:

1. Шестак Я. І. Моделювання єдиного інформаційного простору закладу вищої освіти. Управління розвитком складних систем. 2022. №. 49. С. 81-89. URL: <https://doi.org/10.32347/2412-9933.2022.49.81-89>
2. Шестак Я., Чубаєвський В. Моделювання інформаційної інфраструктури ЗВО. Кібербезпека: освіта, наука, техніка. 2023. Т. 1, № 21. С. 121-135. URL: <https://doi.org/10.28925/2663-4023.2023.21.121135>
3. Моделювання інформаційної системи підприємства / О. В. Криворучко та ін. Комплексне забезпечення якості технологічних процесів та систем : матеріали тез доп. XI Міжнар. науково-практ. конф., м. Чернігів, 26-27 трав. 2021 р. Чернігів, 2021. С. 190. URL: <https://drive.google.com/file/d/1NnRKAaOqZQUcu rDMuE5TXRfNyPYDyZX4/view>

*Якимів Тарас Вікторович, магістрант,
Чернівецький національний університет
імені Юрія Федьковича*

АНАЛІЗ САМОПОДІБНОГО ТРАФІКУ З МЕТОЮ ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ ВІД ПРИХОВАНИХ DDOS-АТАК

Інтернет-адреса публікації на сайті:

<http://www.konferenciaonline.org.ua/ua/article/id-1917/>

Анотація

У рамках цієї роботи розглядаються методи аналізу самоподібності трафіку з використанням математичних та статистичних інструментів, таких як фрактальний аналіз та методи дослідження кореляційної структури даних. Особлива увага приділяється застосуванню цих методів для захисту корпоративних мереж від прихованих DDoS-атак, які можуть маскуватися під легітимний трафік, що значно ускладнює їх виявлення традиційними методами.

Вступ

У сучасному цифровому світі корпоративні мережі відіграють важливу роль в економіці, бізнесі та технологіях. Проте вони постійно піддаються загрозам кібератак, серед яких особливе місце займають DDoS-атаки (розподілені атаки на відмову в обслуговуванні). Ці атаки спрямовані на перевантаження мережевих ресурсів, що призводить до їх відмови в наданні послуг. Однією з найбільш небезпечних форм цих атак є приховані DDoS-атаки, які можуть бути важко виявленими через схожість з нормальним трафіком. Тому захист корпоративних мереж від таких атак вимагає нових підходів, серед яких аналіз самоподібного трафіку є ефективним методом.

Мережевий трафік в реальних системах має властивість самоподібності, що означає схожість структури трафіку на різних часових масштабах. Самоподібність полягає в тому, що статистичні властивості трафіку, такі як частота передачі пакетів і розподіл затримок, можуть бути подібними незалежно від того, на якому часовому інтервалі вони розглядаються. Ця властивість дозволяє будувати моделі мережевого трафіку, що можуть допомогти у виявленні аномалій, таких як DDoS-атаки. Фрактальна природа трафіку робить його більш стійким до випадкових коливань і дозволяє виявляти відхилення, які можуть бути спричинені кібератаками. Відповідно, аналіз самоподібного трафіку стає ключовим інструментом для моніторингу корпоративних мереж з метою попередження та виявлення прихованих DDoS-атак.

Приховані DDoS-атаки відрізняються тим, що вони маскуються під легітимний трафік. Це робить їх особливо небезпечними для корпоративних мереж, оскільки традиційні системи захисту, які спираються на фіксовані шаблони або чітко виражені аномалії, можуть не виявити такі атаки. Зазвичай ці атаки використовують ботнети для генерування трафіку, що виглядає природно, проте їхня мета перевантажити ресурси мережі, що призводить до відмови в обслуговуванні.

Аналіз самоподібного трафіку ґрунтується на математичних і статистичних методах дослідження кореляційної структури трафіку. Одним із ключових інструментів є фрактальний аналіз, який дозволяє вимірювати самоподібність трафіку. Найчастіше використовують такі методи, як:

1. **Масштабно-інваріантні методи** – вони допомагають визначити самоподібність на різних часових масштабах. Для цього використовують параметр Херста, який показує ступінь довгострокової залежності у часовому ряду.

2. **Мультифрактальний аналіз** – досліджує різні фрактальні властивості мережевого трафіку і дозволяє виявляти складніші патерни аномалій.

3. **Кореляційний аналіз** – визначає зв'язок між різними часовими інтервалами трафіку, що дозволяє ідентифікувати приховані DDoS-атаки через зміну кореляційних властивостей.

Самоподібність забезпечує можливість відстежувати структуру трафіку на різних масштабах часу. Якщо в певний момент з'являються порушення в характері самоподібності, це може свідчити про приховані DDoS-атаки. Такі порушення важко помітити в короткострокових часових інтервалах, але їх можна зафіксувати при аналізі на довготривалій основі.

Аналіз самоподібного трафіку є потужним інструментом для захисту корпоративних мереж від прихованих DDoS-атак. Використання математичних і статистичних методів дозволяє виявляти відхилення в поведінці мережевого трафіку, які можуть бути наслідком кіберзагроз. Це забезпечує можливість своєчасного попередження про потенційні атаки та підвищує ефективність захисту корпоративної інфраструктури.

Однак слід зазначити, що використання цього підходу потребує глибокого розуміння мережевої архітектури та доступу до інструментів аналізу великих обсягів даних. Поєднання фрактального аналізу з іншими методами кіберзахисту створює потужну систему захисту від кібератак, яка може забезпечити надійність і безпеку корпоративних мереж.

Список використаних джерел:

- [1] S. Sengupta, A. Greenberg, P. Patel, R. Chaiken, The nature of data center traffic: Measurements & analysis.
- [2] A. Lara, A. Kolasani, B. Ramamurthy, Network innovation using openflow.
- [3] H. Lai, S. Cai, H. Huang, J. Xie, H. Li, A parallel intrusion detection system for high-speed networks.

Секція 2. Економічні науки

*Polina Vitalyivna Tymofieieva, Master's student
in the field of Accounting and Taxation,
Vadym Hetman Kyiv National Economic University, Kyiv*

TAX MANAGEMENT AS AN INSTRUMENT OF ECONOMIC SECURITY OF THE ENTERPRISE

Internet address of the article on web-site:

<http://www.konferenciaonline.org.ua/ua/article/id-1914/>

The relevance of tax management as an instrument of economic security of an enterprise is determined by the current business environment, when companies face a high level of tax risks and complexity of tax legislation. Frequent changes in the legislative framework, globalization of economic processes and increased government control over tax revenues require companies to take a thorough approach to managing tax issues. Effective tax management allows businesses not only to reduce tax costs, but also to ensure financial stability and avoid potential legal conflicts with regulatory authorities. In the context of modern challenges to economic and financial security, the role of tax management is growing significantly, which makes this topic extremely relevant for research.

Many works of domestic and foreign scholars, including S. V. Barulin, E. O. Yermakova, Y. B. Ivanov, V. V. Stepanenko, A.F. Tsymbalyuk, have been devoted to tax management issues, confirming the importance of integrating tax management into the overall strategy of enterprises to maintain their economic security. However, there is a need for further research on the development of effective tools to minimize tax risks in the modern economy.

The purpose of this study is to examine the role of tax management as a tool for ensuring economic security of an enterprise, as well as to study methods and strategies for optimizing the tax burden.

Tax management is an important component of the overall enterprise management system, in particular in the context of ensuring economic security. Effective management of tax liabilities allows a company to minimize costs, reduce risks associated with non-compliance with tax laws and improve financial results. Tax management includes both strategic planning of tax policy and day-to-day administration of tax payments and tax risk management.

Tax management consists of several key elements, each of which has its own importance for the effective operation of the company.

First of all, tax planning is an important element. This is a set of measures aimed at reducing tax pressure by optimizing the structure of tax payments. The

planning process takes into account the current economic situation and forecasts future changes by analyzing tax legislation and possible modifications. Tax planning allows the company to avoid unnecessary financial expenses on taxes, ensuring the preservation of capital for further investment and development, thereby increasing its competitiveness.

The second important component is tax control, which covers the ongoing supervision of tax compliance. This includes analyzing tax reports, checking the correctness of tax payments and compliance with legal requirements. The tax control system allows detecting errors in reporting at an early stage, which helps to avoid financial penalties and reduces the risk of tax disputes with regulatory authorities.

Another important aspect is tax risk management. It involves analyzing and identifying potential threats that may arise as a result of changes in tax legislation or its ambiguous interpretation. Businesses create reserves to cover possible expenses during tax audits and develop strategies for dealing with controversial situations with the tax authorities.

An important factor of economic security is the ability of a company to adapt to changes in tax legislation. Tax reforms and new regulations can have a significant impact on business operations, especially if the company is not ready to adapt quickly.

Thus, tax management is an important tool for ensuring the economic security of an enterprise. It helps to mitigate risks, optimize financial resources and increase resilience to external threats. In the context of globalization and increased competition, effective tax management is becoming an important prerequisite for the long-term development and preservation of the company's competitiveness.

References:

1. Ivanov Y. B. Tax management: textbook / Y. B. Ivanov, A. I. Krysovaty, A. Ch: Znanie 2008, – 525 p.
2. Tax management: a textbook. O. O. Klockar, S. V. Boyko, I. G. Kemenyash, N. M. Rushchyshyn – Lviv: SPOLOM 2017. – 320 p.
3. Tarasyuk M. V. Theoretical foundations of state tax management / M. V. Tarasyuk // Sustainable development of economy. – 2013. – №3 – C. 3-8.
4. Levytska, S. O., Tsymbaliuk, A. F. (2011). Podatkovyi menedzhment na makrorivni: vitchyzniana ta mizhnarodna praktyky vprovadzhennia [Tax management at the macro level: national and international implementation practices]. Naukovi zapysky [Natsionalnoho universytetu «Ostrozka akademiia»]. Ser.: Ekonomika. – The National University of Ostroh Academy Proceedings. Ser.: Economy, 16, 69-76 [in Ukrainian].

ОПТИМІЗАЦІЯ МАРКЕТИНГОВОГО БЮДЖЕТУ ПІДПРИЄМСТВА В УМОВАХ ЗРОСТАЮЧОЇ КОНКУРЕНЦІЇ В ІНТЕРНЕТ-СЕРЕДОВИЩІ

Інтернет-адреса публікації на сайті:

<http://www.konferenciaonline.org.ua/ua/article/id-1922/>

В умовах цифровізації економіки та стрімкого зростання конкуренції в інтернет-середовищі підприємства змушені адаптуватися до нових реалій ринку. Важливим аспектом успішного просування стає ефективне планування та оптимізація маркетингового бюджету. Компанії стикаються з проблемою раціонального розподілу ресурсів серед безлічі маркетингових каналів, що в кінцевому підсумку впливає на рентабельність бізнесу. Мета цих тез – запропонувати модель оптимізації маркетингового бюджету, що ґрунтується на сучасних підходах до управління маркетингом в умовах конкуренції, і дати практичні рекомендації щодо її застосування на підприємствах.

Актуальні виклики для підприємств в інтернет-середовищі.

Сучасні підприємства стикаються з кількома ключовими викликами:

- **Зростання конкуренції.** Коли посилення конкуренції в більшості сегментів ринку вимагає збільшення рекламних бюджетів для залучення цільової аудиторії.
- **Зміна споживчої поведінки.** Споживачі стають більш вимогливими, і їх уподобання швидко змінюються. Відповідно, маркетинговим стратегіям необхідно бути гнучкими та адаптивними.
- **Різноманіття маркетингових каналів.** Поява нових рекламних платформ і каналів ускладнює процес бюджетування та контролю ефективності кампаній.

Модель оптимізації маркетингового бюджету.

Для розв'язання перелічених вище проблем запропоновано модель, яка включає такі ключові компоненти:

- **Аналіз поточної ефективності каналів.** Кожен канал (контекстна реклама, SEO, SMM, e-mail маркетинг тощо) оцінюється за показниками ROI, конверсії (їх кількість та коефіцієнт) та вартості залучення клієнта. На основі цих даних ухвалюються рішення про перерозподіл бюджету на користь більш ефективних каналів.
- **Прогнозування в аналітиці.** Використання технологій штучного інтелекту (ШІ) і машинного навчання для прогнозування майбутніх змін у поведінці споживачів і адаптації маркетингової стратегії під ці зміни.
- **Життєвий цикл клієнта (CLV, LTV).** Фокус на довгострокову цінність клієнта дає змогу компанії не тільки залучати нових клієнтів, а й ефективно утримувати наявних, перерозподіляючи бюджет на програми лояльності та ретаргетинг.

- **Гнучке бюджетування в реальному часі.** Впровадження інструментів (Google Analytics, CRM-системи) для оперативного коригування розподілу бюджету на основі поточних даних і змін у ринковій кон'юнктурі. Це дає змогу компаніям миттєво реагувати на зміни попиту та конкуренції.

Кейс

Спрогнозуємо кейс з урахуванням запропонованої моделі оптимізації маркетингового бюджету. Ми зробимо акцент на коректному відображенні всіх компонентів моделі.

Компанія займається продажем товарів для сну та відпочинку через інтернет. В умовах зростаючої конкуренції на ринку інтернет-торгівлі, компанія прагне збільшити ефективність використання маркетингового бюджету і підвищити кількість конверсій. Бюджет компанії на маркетинг становить 200 000 грн на місяць.

Модель оптимізації маркетингового бюджету передбачає такі компоненти:

- Аналіз поточної ефективності каналів
- Прогностична аналітика
- Облік життєвого циклу клієнта (CLV/LTV)
- Гнучке бюджетування в реальному часі

Аналіз поточної ефективності каналів.

Компанія використовує 4 основні маркетингові канали:

- Контекстна реклама (Google Ads) з показником конверсії 2% і ROI 120%.
- SEO, який дає конверсію 3% і ROI 300%.
- SMM з конверсією 1.5% і ROI 100%.
- E-mail маркетинг з конверсією 6% і ROI 400%.

Розподіл бюджету на момент аналізу:

Канали	Бюджет, грн	Конверсія, %	CPC, грн	Кількість покупок
Контекстна реклама	80 000	2%	25	64
SEO	40 000	3%	15	80
SMM	40 000	1,5%	20	30
E-mail	40 000	6%	5	480

Всього покупок до оптимізації = 654.

Прогностична аналітика.

Компанія прогнозує, що в наступні три місяці відбудуться такі зміни:

- Конкуренція в контекстній рекламі збільшиться, що може знизити ефективність цього каналу.

- Продовжується зростання популярності e-mail маркетингу, особливо серед постійних клієнтів.
- Зростання органічного трафіку за рахунок збільшення обсягів пошукових запитів, що збільшить ефективність SEO.
- Активність у соціальних мережах зросте, проте це зростання буде повільним.

Облік життєвого циклу клієнта (CLV/LTV).

Середня довгострокова цінність клієнта становить 15 000 грн. У зв'язку з цим, важливо не тільки залучати нових клієнтів, а й утримувати вже наявних. Програми лояльності, ретаргетинг і поліпшення роботи з постійними клієнтами стають пріоритетом, особливо через e-mail маркетинг, який демонструє високу конверсію і повернення інвестицій.

Гнучке бюджетування в реальному часі.

Компанія впроваджує інструменти для динамічної зміни бюджету залежно від актуальних даних. У процесі прогнозування та аналізу компанія вирішує перерозподілити маркетинговий бюджет таким чином:

- Контекстна реклама: зменшення бюджету з 80 000 грн до 40 000 грн, оскільки прогнозується зниження ефективності цього каналу.
- SEO: збільшення бюджету з 40 000 грн до 60 000 грн, оскільки прогнозується зростання органічного трафіку.
- SMM: збереження бюджету на рівні 40 000 грн, оскільки очікується невелике зростання.
- E-mail маркетинг: збільшення бюджету з 40 000 грн до 60 000 грн, оскільки цей канал показує високий ROI і відіграє важливу роль в утриманні клієнтів.

Прогноз результатів після оптимізації.

На основі прогностичної аналітики було перераховано конверсії:

Канали	Бюджет, грн	Конверсія, %	CPC, грн	Кількість покупок
Контекстна реклама	40 000	1,8%	25	29
SEO	60 000	3,5%	15	140
SMM	40 000	1,7%	20	34
E-mail	60 000	7%	5	840

Всього покупок після оптимізації = 1043.

Розрахунок і прогноз.

Після оптимізації бюджету компанія очікує збільшення загальної кількості покупок з 654 до 1 043, що являє собою приріст на 60%. Основний приріст досягається за рахунок перерозподілу бюджету в більш ефективні канали, такі як SEO та e-mail маркетинг.

Практичні рекомендації для підприємств.

На основі запропонованої моделі можна виділити такі практичні кроки для оптимізації маркетингового бюджету:

- **Інвестиції в аналітику і дані.** Регулярне використання інструментів аналітики (Google Analytics, CRM-системи) для оцінювання ефективності маркетингових кампаній і отримання актуальних даних для ухвалення рішень.
- **Тестування гіпотез.** Для мінімізації ризиків важливо проводити А/В-тестування різних рекламних стратегій і гіпотез перед їхнім масштабуванням.
- **Диверсифікація маркетингових каналів.** Використання багатоканальних стратегій, що включають контекстну рекламу, таргетовану рекламу в соцмережах, відеорекламу та e-mail маркетинг, дає змогу досягти ширшого охоплення аудиторії та підвищити ефективність кампаній.
- **Автоматизація процесів.** Впровадження сучасних інструментів для автоматизації маркетингових завдань (Google Ads Automation або Facebook Ads Manager) допомагає скоротити тимчасові витрати і підвищити точність виконання завдань.
- **Постійна адаптація до змін ринку.** Гнучкість і оперативність у зміні маркетингової стратегії на основі отриманих даних про поведінку споживачів і зміни на ринку.

Оптимізація маркетингового бюджету в умовах зростаючої конкуренції в інтернет-середовищі вимагає комплексного і гнучкого підходу. Застосування запропонованої моделі дає змогу не тільки ефективно розподіляти бюджет, а й адаптуватися до динаміки ринку і змін споживчих переваг. Впровадження автоматизованих рішень та аналітичних інструментів забезпечує компанії конкурентні переваги та сприяє зростанню рентабельності маркетингових інвестицій. Дотримання практичних рекомендацій допоможе підприємствам досягти кращих результатів і поліпшити свої позиції на ринку.

Література:

1. Барден, Ф. Код зламано, або Наука про те, що змушує купувати / Переклад з англ. Ю. Кузьменко. Книжковий клуб Клуб Сімейного Дозвілля, 2017. 304 с.
2. Остервальдер, А., Піньє, І. Створення бізнес-моделей. Посібник з візуалізації ідей / Пер. з англ. Р. Корнута. Київ: Наш Формат, 2017. 288 с.
3. Годін, С. Це маркетинг! Ви не зможете бути побаченими, поки не навчитеся бачити / Пер. з англ. С. Ведмідь. Київ: ArtHuss, 2024. 210 с.

*Олійник Ольга Степанівна,
кандидат економічних наук, доцент,
Кам'янець-Подільський національний університет
ім. Івана Огієнка, м. Кам'янець-Подільський
ORCID: 0000-0003-2370-3211*

СТАЛИЙ РОЗВИТОК РЕГІОНАЛЬНОГО РИНКУ ТУРИСТИЧНО-РЕКРЕАЦІЙНИХ ПОСЛУГ

Інтернет-адреса публікації на сайті:

<http://www.konferenciaonline.org.ua/ua/article/id-1912/>

Сталий розвиток туризму та рекреації будь-якого регіону є досить складним багатоплановим процесом, який потребує ефективного використання та раціонального поєднання інфраструктурного, фінансово-економічного, кадрового та інноваційного потенціалу. Промоція місцевих туристично-рекреаційних та курортних територій спрямована на вирішення стратегічних завдань: створення сучасного конкурентоспроможного туристсько-рекреаційного комплексу (далі ТРК), що забезпечує соціально-економічний розвиток регіону, а тим більше підвищення якості життя населення та зміцнення здоров'я населення. Сучасний рівень розвитку ТРК України вимагає формування ефективної системи управління її розвитком, яка б визначала мету, завдання, принципи та інструменти ринкового та державного регулювання.

Незважаючи на наявний багатий туристсько-рекреаційний потенціал, Україна мало відома на світовому ринку туристично-рекреаційних послуг і займає малий процент від світового обсягу послуг. Сталий розвиток туризму став можливим завдяки сучасним технологіям ефективної організації туристично-рекреаційного простору. Світовий досвід показує, що до найпрогресивніших технологій відносяться створення спеціальних економічних зон туристсько-рекреаційного типу; туристично-рекреаційні кластери муніципального, міждержавного, регіонального, міжрегіонального (національного) та транскордонного (міжнародного) рівнів; інноваційні технології просування регіонів і країн на національному та міжнародному туристичних ринках; технологія наукового забезпечення та кадрового забезпечення індустрії туризму.

Україна має всі необхідні умови для ефективного функціонування туризму. Проте слід виділити низку актуальних проблем, які перешкоджають його постійному розвитку та виходу на міжнародний ринок туристично-рекреаційних послуг: по-перше, воєнний час; по-друге, нерозвинена інфраструктура курортних зон; по-третє, високий рівень зношеності матеріально-технічної бази підприємств; по-четверте, недостатня кількість

кваліфікованих кадрів; по-п'яте, нерівномірність розвитку туристично-рекреаційного потенціалу; по-шосте, сезонність функціонування засобів розміщення; по-сьоме, висока частка нелегальних послуг розміщення відпочиваючих тощо.

На території України в даний час функціонує низка колективних санаторно-курортних організацій і готелів, з них частина надають спеціалізоване санаторно-курортне лікування, або надають оздоровчі послуги, а також надають послуги з тимчасового проживання. За останні роки модернізовано частина санаторно-курортних і готельних організацій. Основний потік туристів припадає на 3-зіркові готелі та приватний сектор.

До перспектив розвитку ТРК України відносяться: збільшення частки короткострокових турів; зростання попиту на індивідуальні тури; попит на сімейні готелі, зростання сегментів ринку для осіб «третього, четвертого віку» та людей з обмеженими можливостями; інтерес до медичних послуг та охорони здоров'я під час подорожей тощо.

Одним із найбільш швидкозростаючих сегментів туристичного ринку є доступний туризм. Доступність гарантується у всій індустрії туризму на національному та місцевому рівнях, починаючи зі створення умов для трансферу, проживання, харчування та дозвілля для людей з обмеженими можливостями, людей з дієтичними обмеженнями тощо. Сьогодні до десяти процентів усіх туристів у світі – це люди з особливими потребами, які часто подорожують із родичами чи друзями. Слід зазначити, що метою доступного туризму є не лише залучення людей з інвалідністю до туристичних подорожей. Потенційними споживачами цієї частини туристичного ринку також є люди похилого віку та молодь, студенти та сім'ї з маленькими дітьми, які потребують особливого ставлення з різних соціально-економічних причин.

Політика доступності даного виду туризму повинна бути орієнтована на вік, фізичні характеристики та обмежені можливості (пандуси, широкі двері, ліфти та підйомники, покажчики) і передбачати відповідно до них засоби розміщення (готелі), транспорт та його інфраструктуру (аеропорт, вокзал, дорожні служби). Регіони для розвитку цього виду туризму повинні бути доступними для всіх видів транспорту, а об'єкти, розташовані в цих регіонах, повинні бути фінансово доступними. Туристам повинна бути забезпечена можливість пересування незалежно від фізичних чи соціальних умов і людських можливостей (соціальний туризм, літній туризм, туризм четвертого віку).

Для такої диверсифікації туристичних послуг необхідно стимулювати інвестиційну діяльність в регіоні. Для розвитку ТРК України необхідна ефективна робота її фінансового механізму, тобто оптимізація податкового, митного, валютного регулювання. Це забезпечить державне стимулювання припливу іноземних і вітчизняних туристів, розвиток депресивних курортних

територій і соціального туризму; стимулювання надходження інвестицій до України, активізація середнього та малого підприємництва, розвиток системи їх мікрокредитування, субсидування заходів для реалізації інвестиційних проектів.

Література:

1. Жук П. В. Оцінювання конкурентоспроможності туристично-рекреаційної сфери регіону: наукові підходи. Соціально-економічні проблеми сучасного періоду України. 2022. Вип. 4 (156). С. 22-28. <https://doi.org/10.36818/2071-4653-2022-4-4>
2. Михайличенко Х. І. Інноваційний розвиток туризму: монографія. / Х. І. Михайличенко – Київ: Київ. нац. торг.-екон. ун-ту. 2012. 608 с.
3. Роїк О. Р., Копичинська М. Ю. Дослідження привабливості туристично-рекреаційного комплексу на прикладі курорту Трускавець. Держава та регіони. Серія: Економіка та підприємництво. 2021. No 4 (121). С. 36-42. URL: http://www.econom.stateandregions.zp.ua/journal/2021/4_2021/8.pdf

Секція 3. Технічні науки

*Olena V. Bohoiavlenska, candidate of technical science,
National Technical University "Kharkiv
Polytechnic Institute", Kharkiv
ORCID: 0000-0002-7710-8939*

*Pavlo P. Karnozhytskyi, PhD Candidate,
National Technical University "Kharkiv
Polytechnic Institute", Kharkiv
ORCID: 0000-0003-4740-1971*

*Pavlo V. Karnozhytskyi, PhD, Assoc. Prof.,
National Technical University "Kharkiv
Polytechnic Institute", Kharkiv
ORCID: 0000-0001-6019-8432*

*Svitlana G. Deribo, candidate of technical science,
National Technical University "Kharkiv
Polytechnic Institute", Kharkiv
ORCID: 0000-0002-1790-9857*

STUDY OF HUMIC SUBSTANCES AS REAGENTS FOR THE PURIFICATION OF CONTAMINATED WATER

Internet address of the article on web-site:

<http://www.konferenciaonline.org.ua/ua/article/id-1909/>

Efficient complex use of coal resources requires knowledge of their raw material capabilities and properties. Every year, the scope of lignite application is growing due to its low cost and significant reserves [1]. Lignite can be transformed into valuable components for the chemical industry through the processes of extraction, oxidation, semi-coking, coking, gasification, thermal dissolution, hydrogenation, etc [2-4].

One of the main areas of non-traditional use of lignite is production of humic acids (HAs) [5-7]. Their group composition includes bituminoids, humic substances and residual coal. They belong to the high-molecular aromatic oxycarboxylic acids by chemical composition. HAs are of practical interest as selective sorbents due to their properties as good complexing agents.

Given the significant deposits of lignite in Ukraine, innovative technologies for its use are promising [8-10]. One of the methods could be the production of water-soluble sorbents from lignite to absorb heavy metal ions, which are becoming a dangerous source of pollution. They cannot be removed from water by mechanical means, biological treatment and traditional methods such as coagulation and flotation. This makes it necessary to control their release into the environment and requires the use of relatively inexpensive, accessible means of capturing them.

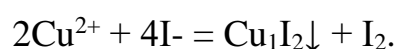
To solve this issue, barometric methods such as ultrafiltration are used [11]. The effectiveness of ultrafiltration membranes is ensured by reagents capable of binding heavy metal ions into complexes and concentrating them on the membrane surface. This makes it possible to purify water from traces of metals to maximal accepted concentrations and isolate them using conventional, cost-effective methods. To implement the method, synthetic water-soluble products are currently used as complexing agents [12, 13]. The disadvantage of synthetic complexing agents is their transformation into filtrate and entering natural water sources as well as their high cost. Complexing agents derived from natural raw materials, humic acids derived from lignite in particular, do not have such disadvantages.

HAs are anionic polyelectrolytes and belong to the natural absorbers of numerous pollutants [14-16] due to the presence of oxygen-containing functional groups and nitrogen-containing heterocycles, which can selectively bind to metal ions, forming strong complexes.

Thus, the discovery and development of non-energy methods of lignite use is a very promising scientific and practical task.

The study was conducted on a batch of lignite from the Oleksandriya deposit in Ukraine. The following values were determined: moisture content – 10.54 %, volatile-matter yield – 31.08 %, ash content – 39.51 %, total sulphur content – 0.74 %. The quantitative content of HA, which is 38.67 % mass, was determined by the Erdman's method. The content of fulvic acids was determined by the photometric method with pH = 2. For the comparison, a 0.01 n aqueous solution of H₂SO₄ was used. The content of fulvic acids, which is 0.21 %, was determined according to the calibration dependence.

The content of copper ions in water was determined in the initial solution and after the addition of HA using the iodometric method of analysis:



To a sample of the original aqueous solution (20 ml), 2 ml of H₂SO₄ (1:4) and 10 ml of KCl+KI were added and the released iodine was titrated with sodium thiosulfate (Na₂S₂O₃) with the addition of starch (2-5 ml). The starch is added when the solution becomes straw-coloured and titrated to a fuzzy purple colour. The calculated copper content amounted to 0.110 mg/l. The determined degree of purification was 86.36%.

The analysis of the data demonstrates that humic substances can provide a high level of water purification from copper ions and are promising for the production of water-soluble sorbents based on them.

Reference list:

1. Miszkiewicz H., Bielecki S., Kadłubowski S. Biouplynnianie polskiego chemicznie utlenionego węgla brunatnego (2016). Inżynieria i Ochrona Środowiska, 2016, Vol.19, No 1, s. 97-108. URL: <https://bibliotekanauki.pl/articles/297561>
2. A. Starzycka, J. Kasiński, A. Saternus, P. Urbański. Węgiel brunatny = Lignite – Wydanie II, zaktualizowane. – Warszawa : Państwowy Instytut Geologiczny –

- Państwowy Instytut Badawczy, [2020]. – 24 s. URL: https://www.pgi.gov.pl/images/muzeum/kopalnia_wiedzy/surowce/foldery/wegiel_brunatny.pdf
3. Bucha M., Jędrysek M. O.: Nowoczesne technologie zagospodarowania złóż węgla brunatnego. Mat. V Międzynarodowej Konf. Naukowej „Homo Naturalis” – Człowiek, przyroda, przestrzeń w myśl rozwoju zrównoważonego. Wyd. Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2010, s. 129-134.
 4. Ding, M.; Zhao, Y.-P.; Dou, Y.-Q.; Wei, X.-Y.; Fan, X.; Cao, J.-P.; Wang, Y.-L.; Zong, Z.-M. Sequential extraction and thermal dissolution of Shengli lignite. *Fuel Process. Technol.* 2015, 135, 20-24. <https://doi.org/10.1016/j.fuproc.2014.09.031>
 5. Олександрійське буре вугілля як джерело гумінових речовин / А. О. Сініцина, П. В. Карножицький // Сучасні технології переробки паливних копалин: тези доповідей V міжнародної науково-технічної конференції, 14-15 квітня 2022 року: укл. Мірошниченко Д. В. – Харків-Тернопіль: НТУ «ХП», Видавництво «Крок», 2022. – сс. 39-43.
 6. Verrillo M, Parisi M, Savy D, Caiazzo G, Di Caprio R, Luciano MA, Cacciapuoti S, Fabbrocini G, Piccolo A. Antiflammatory activity and potential dermatological applications of characterized humic acids from a lignite and a green compost. *Sci Rep.* 2022 Feb 9;12(1):2152. <https://doi.org/10.1038/s41598-022-06251-2>
 7. E. Sarlaki, A. Sh. Paghaleh, M. H. Kianmehr, K. A. Vakilian. Valorization of lignite wastes into humic acids: Process optimization, energy efficiency and structural features analysis, *Renewable Energy*, Volume 163, 2021, Pages 105-122. <https://doi.org/10.1016/j.renene.2020.08.096>
 8. Собко Б. Е. Потенциальная роль бурого угля в энергетическом балансе страны / Б. Е. Собко, А. А. Шустов., А. П. Белов // Национальный горный университет, Интехпроект. – Днепр. – 2018. – С. 42. URL: <https://repository.kpi.kharkov.ua/server/api/core/bitstreams/4e981b56-9e7a-42dc-9778-269d7ab76ad2/content>
 9. D. V. Miroshnichenko, S. V. Pyshyev, V. V. Lebedev, D. Yu. Bilets. Deposits and quality indicators of brown coal in Ukraine *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu.* 2022, (3): 005 – 010. <https://doi.org/10.33271/nvngu/2022-3/005>
 10. Сініцина А. О. Буре вугілля – сировина для отримання водорозчинних сорбентів / А. О. Сініцина, П. П. Карножицький // Інтегровані технології та енергозбереження. – 2023. – № 3. – С. 67-77. <http://doi.org/10.20998/2078-5364.2023.3.06>
 11. Брик М. Т., Цапюк О. А. Ультрафільтрація. Київ : Наукова думка, 1989. С. 288.
 12. Дюжев, В., Сініцина, А., Карножицький, П., & Карножицький, П. (2022). Соціально-економічні, екологічні проблеми збільшення стандартів життєдіяльності населення із застосуванням інноваційних технологій очищення водних ресурсів на основі водорозчинних сорбентів отриманих з українського бурого вугілля. *Вісник Національного технічного університету "Харківський політехнічний інститут" (економічні науки)*, (4), 88-92. <https://doi.org/10.20998/2519-4461.2022.4.88>

13. A. O. Sinitsyna, P. V. Karnozhytskyi, D. Yu. Bilets Modernization of the Complexation-Ultrafiltration Process for Removal of Copper Ions From Water. *Pet Coal* (2021); 63(4): 1065-1069 URL: <https://www.vurup.sk/petroleum/2021/volume-63/>
14. Zhou P., Yan H., Gu B. Competitive complexation of metal ions with humic substances. *Chemosphere*. 2005, Vol. 58. P. 1327-1337.
15. Leboeuf E. J., Weber JR W. Macromolecular Characteristics of Natural Organic Matter. 2. Sorption and Desorption Behavior. *Environ. Sci. Technol*, 2000. Vol. 34. P. 3632–3640.
16. Hanke D., Dick P. D. Organic Matter Stocks and the Interactions of Humic Substances with Metals in Araucaria Moist Forest Soil with Humic and Histic Horizons. Division – Soil Processes and Properties Commission. *Soil Chemistry*. 2017. Vol. 41. P. 1-20. <https://doi.org/10.1590/18069657rbcs20160368>

Воробйов Юрій Анатолійович, доктор технічних наук, професор,
Національний аерокосмічний університет ім. М.Є. Жуковського
«Харківський авіаційний інститут», м. Харків
ORCID: 0000-0001-6401-7790

Богач Олексій Анатолійович, аспірант,
Національний аерокосмічний університет ім. М.Є. Жуковського
«Харківський авіаційний інститут», м. Харків

ТЕХНІЧНА ПІДГОТОВКА ВИРОБНИЦТВА ЛЕГКОГО ЛІТАКА

Інтернет-адреса публікації на сайті:

<http://www.konferenciaonline.org.ua/ua/article/id-1919/>

Під легкими літаками Федеральна авіаційна адміністрація США (FAA) і авіаційна адміністрація Євросоюзу (ЕАА), і Державна авіаційна служба України розуміє літаки з максимальною злітною масою не більше 5700 кг і числом пасажирів (без урахування екіпажу) не більше 9 осіб [1, 2]. Зазвичай екіпаж включає 1–2 пілоти, таким чином загальна місткість літака не перевищує 11 осіб.

Технічна підготовка виробництва літаків являє собою єдину систему, яка включає в себе конструкторську, технологічну й організаційну підготовки виробництва та діє до зняття літака з виробництва [3].

Основним завданням конструкторської підготовки виробництва (далі – КПВ) є створення комплексу креслярської (електронної) документації для виготовлення й випробування макетів, дослідних зразків (дослідної партії), установлювальної серії і документації для сталого серійного виробництва нових виробів з використанням результатів прикладних науково-дослідних і дослідно-конструкторських робіт (далі – НДР і ДКР) відповідно до вимог технічного завдання (далі – ТЗ).

Зміст і порядок виконання робіт на цій стадії системи створення й освоєння нової техніки регламентуються державним стандартом про єдину систему конструкторської документації, якій визначає такі стадії КПВ, як ТЗ, технічна пропозиція, ескізний, технічний та робочий проекти.

ТЗ є вихідним документом, на основі якого здійснюється вся робота з проектування нового виробу. Воно розробляється на проектування нового виробу за дорученням або підприємства-виробника продукції і погоджується з замовником (основним споживачем), або замовника. У ТЗ визначається призначення майбутнього виробу, ретельно описуються його технічні й експлуатаційні параметри і характеристики: продуктивність, габарити, швидкість, надійність, довговічність й інші показники, обумовлені характером роботи майбутнього виробу. У ньому також містяться відомості про характер виробництва, умови транспортування, зберігання і ремонту; рекомендації з виконання необхідних стадій розробки конструкторської документації та її складові; техніко-економічного обґрунтування й інші вимоги.

На основі виконаних авторами НДР і ДКР, результатів вивчення патентної інформації, маркетингових досліджень, аналізу наявних аналогічних моделей і умов їхньої експлуатації було розроблено наступне ТЗ на проектування двомісного легкого літака [4].

Основні льотно-технічні характеристики літака: довжина літака – 6,36 м; висота літака – 2,66 м; розмах крила літака – 9,5 м; максимальна злітна вага – 600 кг; крейсерська швидкість – 160 км/год.; максимальна швидкість польоту – 185 км/год.; мінімальна швидкість горизонтального польоту – 100 км/год.; максимальна висота польоту – 3 000 м; практична дальність польоту – 300 км; максимальна тривалість польоту – 60 хв.

Очікувані умови експлуатації: температура повітря біля землі: $-25...+50$ °С; максимальні складові швидкості вітру біля землі при зльоті та посадці: зустрічна складова – 10 м/с; попутна складова – 5 м/с; бічна складова (ІВПШ, $\mu \geq 0,6$) – 6 м/с; бічний порив вітру – 7,5 м/с; експлуатаційний мінімуми погоди: мінімум для зльоту – дальність видимості на злітно-посадкових смугах (далі – ЗПС) щонайменше 200 м; мінімум для посадки – дальність видимості на ЗПС щонайменше 2000 м, висота хмарності щонайменше – 200 м.

Експлуатаційні фактори: максимальна висота аеродрому над рівнем моря – 800 м; типи ЗПС: ЗПС зі штучним та ґрунтовим покриттям; міцність ґрунту ЗПС не нижче 0,4 МПа; мінімальні розміри ЗПС 15×250 м.

Особливості застосування літака: дозволяється виконання польотів вдень, за правилами візуального польоту, над рівнинною та гірською місцевістю місцевих повітряних ліній.

Виходячи з тактико-технічних вимог до літака, що проектується, і аналізу статистичних даних, обрано схему вільнонесучого моноплана з низькорозташованим, прямим крилом (рис. 1).

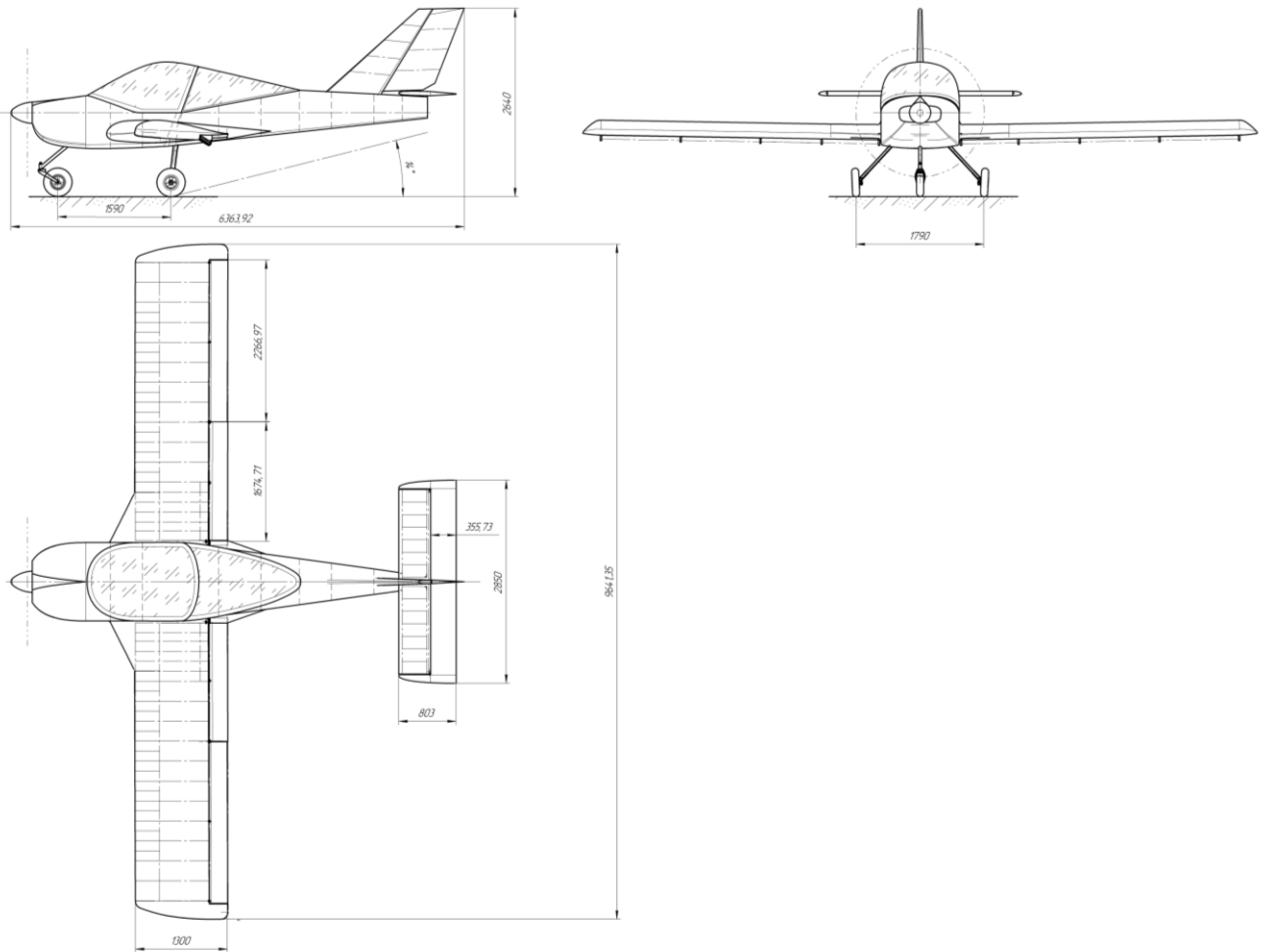


Рисунок 1 – Схема літака

Аеродинамічна схема літака, що проектується – класична, тобто, горизонтальне оперення (далі – ГО) знаходиться позаду крила. Перевагою даної схеми є те, що крило працює в чистому незбуреному потоці, який плавно обтікає його. До недоліків можна віднести роботу ГО у скошеному потоці, внаслідок чого знижується його ефективність [5].

Двигун поршневий. Він дозволяє отримати найменші питомі витрати палива та найбільшу тягу в заданому діапазоні швидкостей та висот польоту, володіючи при цьому меншими рівнями шуму та вібрацій. Кількість двигунів на літаку – один, розташований він у носовій частині фюзеляжу.

ГО розташоване на фюзеляжі. Це призводить до погіршення бічної стійкості літака за великих кутів атаки, оскільки оперення потраплятиме в супутній струмінь від крила. У зв'язку з цим площу вертикального оперення (далі – ВО) було збільшено.

Уздовж задньої кромки крила встановлена механізація (закрылки).

Схема шасі – триопорна з носовою опорою. Воно забезпечує більш ефективне гальмування при пробігу, суттєво зменшується можливість «козління» та повністю виключається явище капотування літака, покращує огляд при зльоті-посадці для пілотів. Крім цього схема шасі з носовою опорою має кращу стійкість при русі по аеродрому. Але з'являється можливість

виникнення коливань, що самозбуджуються, «шимі». Однак шасі, виконане за такою схемою, має більшу масу.

Розраховано злітна маса літака у трьох наближеннях. Обрано двигун Rotax 912IS2 за найближчою більшою потужністю до розрахункової потужності, а також за використанням у деяких літаках-аналогах.

КПВ – це дуже трудомісткий процес. Тому для зменшення її трудомісткості та циклу виконання використано сучасна САД-система. При цьому трудомісткість КПВ склала 14 169,7 люд.×год. [4].

Розроблено у системі CATIA V5R18 майстер-геометрії а також моделі розподілу простору основних агрегатів літака: фюзеляжу, крила, ГО, ВО.

На рис. 2 як приклад надано майстер-геометрія фюзеляжу.

Розраховано навантаження, що діють на агрегати літака та геометричні параметри конструктивних елементів, підібрано матеріали для їх виготовлення.

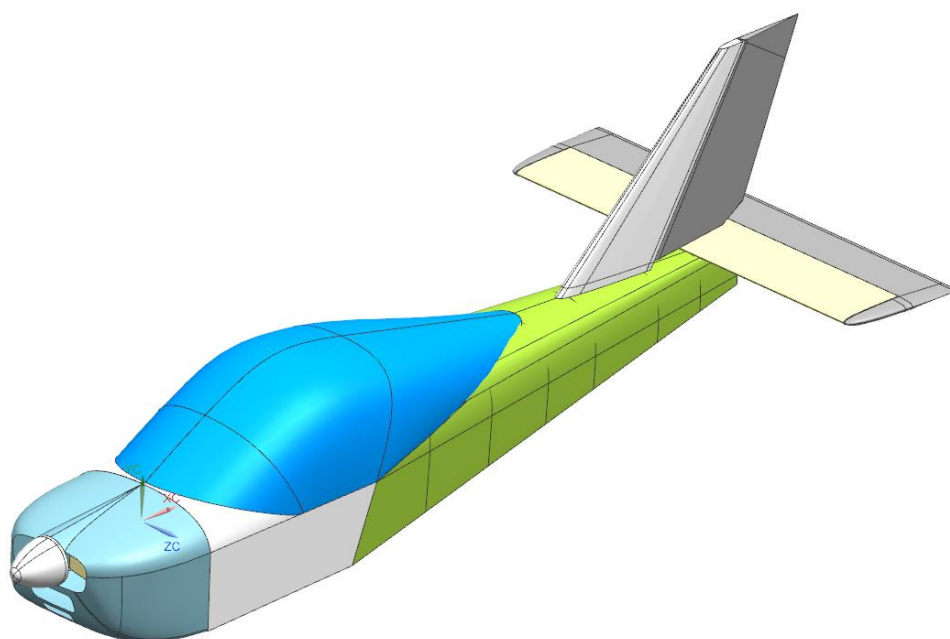


Рисунок 2 – Майстер-геометрія фюзеляжу літака

Технологічна підготовка виробництва (далі – ТПВ) починається лише трохи пізніше, ніж КПВ, за паралельно-послідовною схемою, коли можна говорити про етапи, де превалує КПВ, і про етапи, де більшу частину займає ТПВ.

ТПВ включає наступні роботи.

1. Відпрацювання конструкції на технологічність при проектуванні літака, виготовленні його дослідних зразків та перших серій. Внаслідок виконання цих робіт забезпечується серійний рівень технологічності конструкції з прийнятними техніко-економічними показниками виробництва.

2. Розроблення директивних технологічних матеріалів (далі – ДТМ): схеми членування літака, характеристику основних технологічних процесів (далі – ТП) за видами робіт, а також відомості про унікальні об'єкти конструкції, для яких потрібні нові ТП, обладнання, оснащення; рекомендації

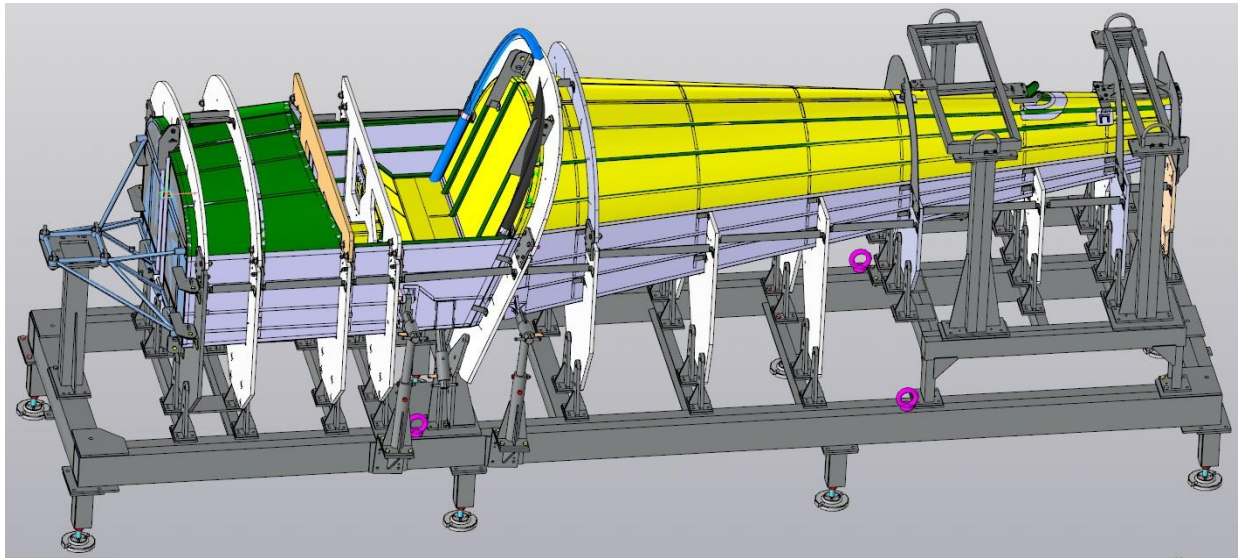
щодо схем ув'язування оснащення, схем і методів складання, з реконструкції цехів заводу та деякі інші технологічні відомості.

3. Проектування та виготовлення контрольно-еталонного оснащення (шаблонів, макетів, еталонів, контретапонів, монтажних еталонів та ін.).

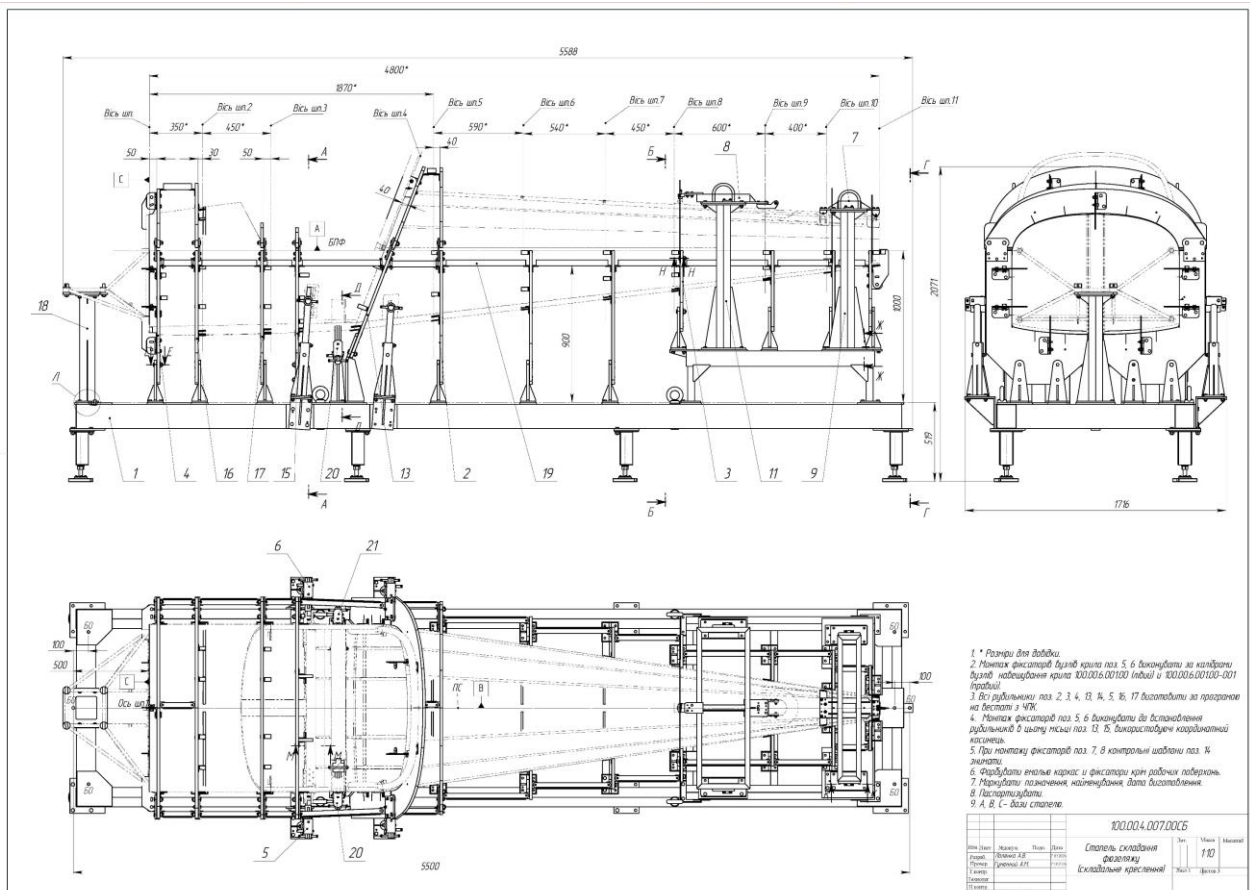
4. Проектування ТП, їх технічне нормування, визначення трудомісткості за видами робіт, агрегатів та літака в цілому.

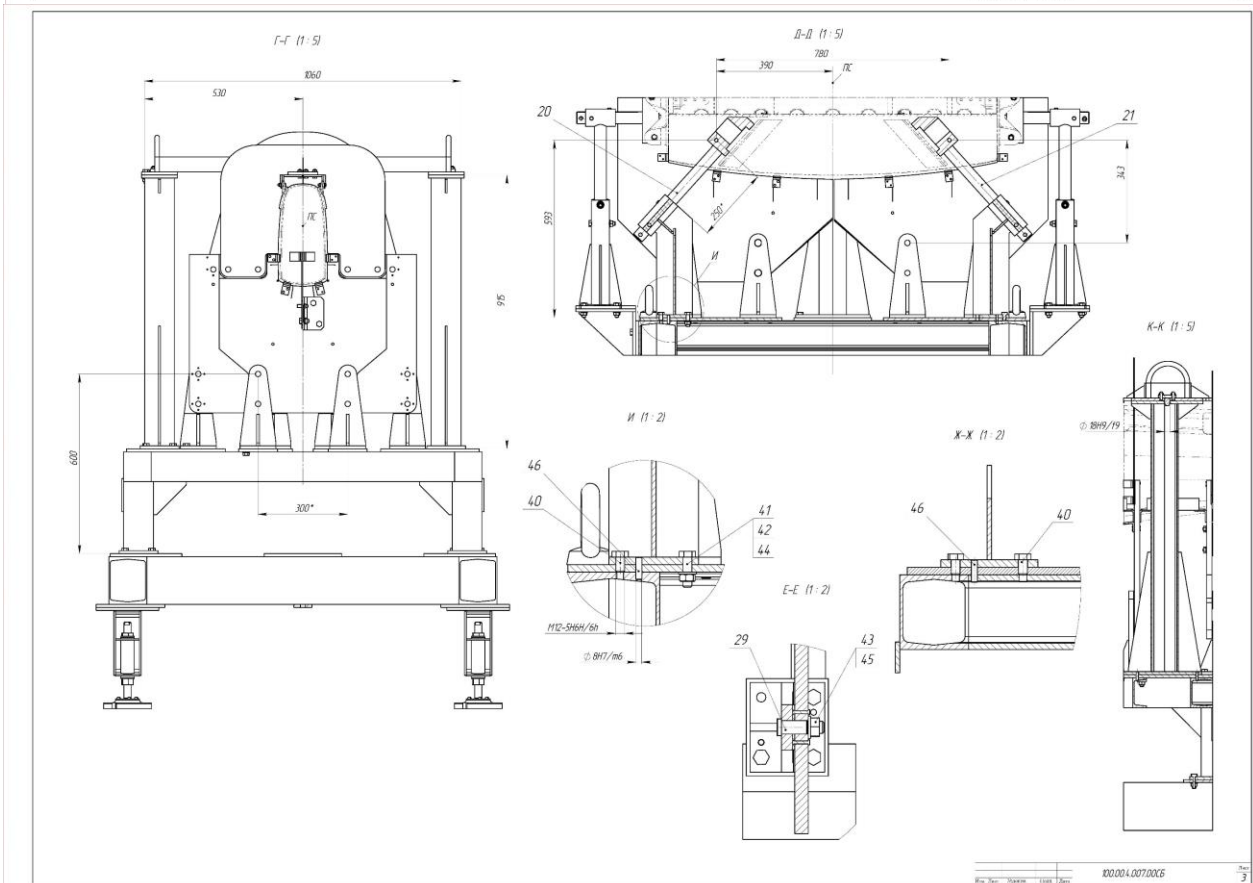
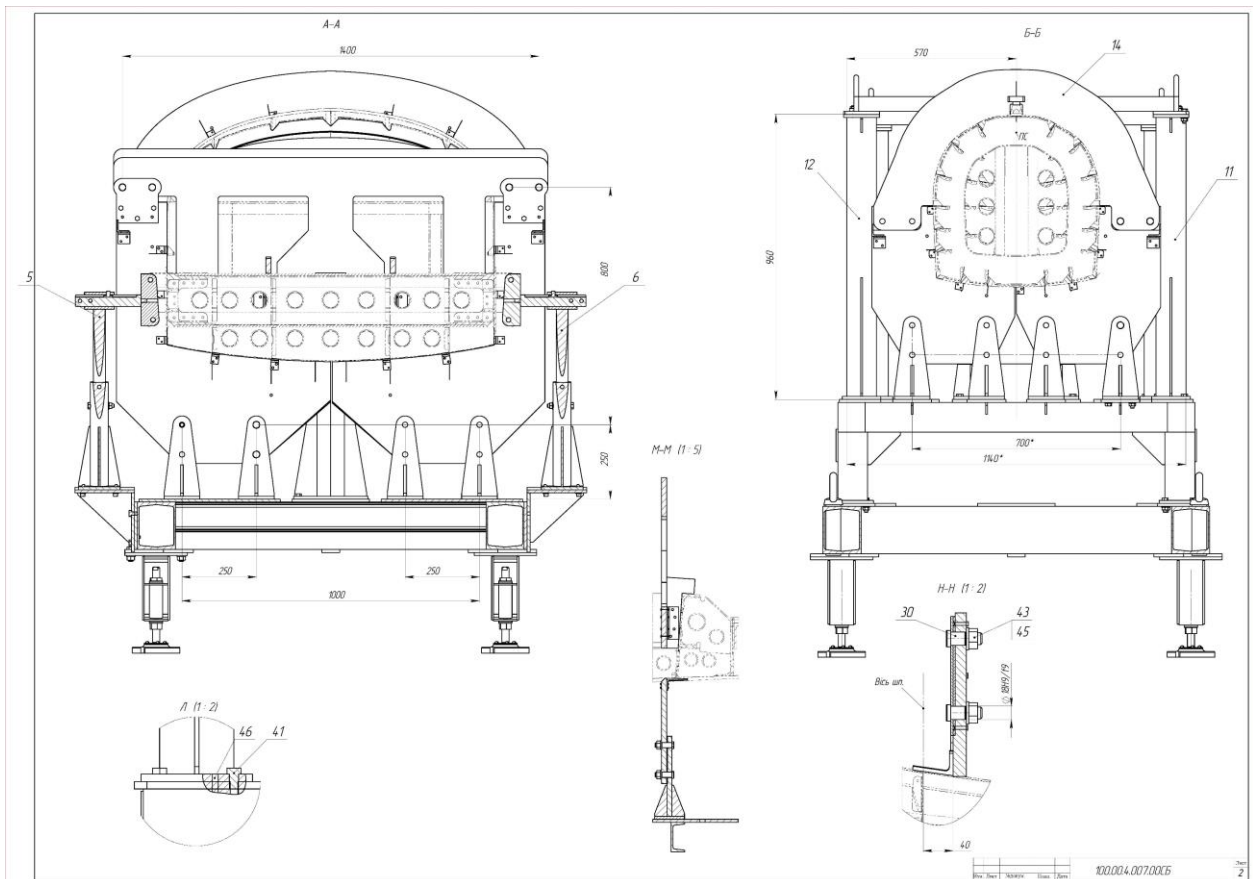
5. Проектування та виготовлення ЗТО та контролю.

На рис. 3 надано цифрова 3D-модель (а) та електронне складальне креслення (б) стапелю складання фюзеляжу.



а





б

Рисунок 3 – Цифрова 3D-модель (а) та електронні складальні креслення (б) стапелю складання фюзеляжу

Література:

1. Code of Federal Regulations 14 (14CFR). Part 23. (FAR-23) Airworthiness standards: normal, utility, acrobatic and commuter airplanes [Electronic resource]. – Available at: https://www.faa.gov/aircraft/air_cert/designapprovals/small_airplanes/small_airplanes_regs (accessed 2 October 2024).
2. Part 23 – Airworthiness standards: Normal category airplanes [Electronic resource]. – Available at: <https://aviation-regulations.com/part/23> (accessed 2 October 2024).
3. Технологія виробництва літальних апаратів: Підручник: у 2 кн. – Кн. 2. Технологія складання літальних апаратів [Текст] / Ю. М. Терещенко, Л. Г. Волянська, К. А. Животовська та ін. ; За ред. Ю. М. Терещенка. – К. : Книжкове вид-во НАУ, 2006. – 492 с.
4. Безплавовий метод конструкторської підготовки виробництва літаків авіації загального призначення [Текст] / Ю.А. Воробйов, А.М. Гуменний, О.А. Богач // Авіаційно-космічна техніка і технологія. – 2024. – № 5 (199). – С. 78-89.
5. McCormick B. W. Aerodynamics, Aeronautics and Flight Mechanics. New York : Wiley, 1995. 652 p.

***Клименко Олександр Володимирович,**
асистент кафедри тракторів і
сільськогосподарських машин, Дніпровський державний
аграрно-економічний університет, м. Дніпро
ORCID:0000-0003-3044-9135*

***Ковцун Андрій Ігорович,** здобувач, Дніпровський державний
аграрно-економічний університет, м. Дніпро*

***Акастьолов Олексій Володимирович,**
здобувач, Дніпровський державний
аграрно-економічний університет, м. Дніпро*

***Теслюк Геннадій Володимирович,**
кандидат технічних наук, доцент кафедри тракторів і
сільськогосподарських машин, Дніпровський державний
аграрно-економічний університет, м. Дніпро
ORCID:0000-0003-4541-5720*

ЗАСТОСУВАННЯ КОМБІНОВАНОГО КУЛЬТИВАТОРА ДЛЯ ПЕРЕДПОСІВНОГО ОБРОБІТКУ ҐРУНТУ

Інтернет-адреса публікації на сайті:

<http://www.konferenciaonline.org.ua/ua/article/id-1907/>

Метою сучасного сільськогосподарського виробництва є зниження витрат енергетичних ресурсів та впровадження нових методів у технологіях обробітку сільськогосподарських культур, орієнтованих на збереження родючості ґрунту та підвищення врожайності.

Урожайність сільськогосподарських культур багато в чому залежить від якості обробки ґрунту перед посівом. За агротехнічними вимогами передпосівна обробка ґрунту повинна забезпечити вирівняну поверхню поля, знищення бур'янів, збереження ґрунтової вологи, оптимальної щільності та структурного складу посівного шару ґрунту [2]. Виконання цих вимог особливо важливо для дрібнонасіньових культур, мала глибина закладення насіння яких вимагає застосування спеціальної техніки [5].

Визнаючи високий рівень конструктивної розробки робочих органів і машин для передпосівної обробки ґрунту, слід відзначити недоліки, що мають місце в показниках якості підготовки ґрунту до посіву. Конструктивні особливості лапових робочих органів культиваторів, особливості стрілочастих універсальних і розпушувальних лап, не дозволяють виконувати обробку ґрунту без винесення вологих шарів ґрунту на поверхню поля. Традиційні культиватори не забезпечують необхідної диференціації ґрунтової структури в посівному шарі, має місце приживання зрізаних бур'янів після обробки. Тому виникає необхідність у розробці нових робочих органів, що забезпечують виконання вимог до передпосівної обробки ґрунту, зокрема для дрібнонасіньових культур.

В останні роки все частіше на полях нашої країни і за кордоном для передпосівної обробки ґрунту застосовуються комбіновані машини, які на практиці довели свою економічну ефективність. Вони здатні за рахунок зменшення кількості проходів агрегату по полю забезпечити різке скорочення термінів весняно-польових робіт, зменшити ущільнення ґрунту колесами агрегатів, а також суттєво знизити витрати на паливо та підвищити продуктивність праці. Традиційно застосовують робочі органи у наступних комбінаціях: пружинні розпушувальні лапи, вирівнювальний брус, котки (РВК-3,6, РВК-5,4); голчаста ротаційна борона, вирівнююча дошка, коток зубчасто-кільчастий (КЗК-5,6); дискова борона, універсальні стрілочасті лапи, котки, що прикочують (АКП-3,6, АКП-5,4, АКП-7,2) та інші [3].

Комбіновані культиватори забезпечують передпосівну обробку відповідно до агротехнічних вимог вони гарантують відсутність брил і гребенів з мульчованим поверхневим шаром, ущільнення посівного шару ґрунту, повне підрізання бур'янів, що забезпечує сприятливі умови для швидких і гарних сходів, зростання та розвитку культурних рослин. Поєднання технологічних операцій забезпечує покращення термінів весняно-польових робіт.

Таким чином, перспективним напрямком у розвитку механізації передпосівної обробки ґрунту є застосування комбінованих машин, що дозволяють в одному технологічному процесі виконувати кілька операцій із точним дотриманням агротехнічних вимог.

Література:

1. Бондаренко М. Г., Демещук В. А. Комплектування і використання машинно-тракторного парку в рослинництві. – К.: „Вища школа”, 1995, с. 236.
2. Демидко О. О. та ін. "Шляхи економічного використання енергоносіїв на механізованих роботах". Вісник аграрної науки. № 7. 1998 р.

3. Погорілий Л. та ін. Перспективи конструкції ґрунтообробних машин: тенденції та еволюції". – К.: 1998р.
4. Кобець А. С. "Основи теорії робочих органів сільськогосподарських машин" Дніпропетровськ – 1999 р.
5. Шевченко І. А. Обґрунтування технологій та технічних засобів для обробітку ґрунтів на базі їх агрофізичних показників: Дис... докт. техн. наук: 05.05.11. – Мелітополь, 2003. – 403 с.

Коляда Оксана Юрївна, кандидат технічних наук,
доцент, Полтавський політехнічний фаховий
коледж Національного технічного університету
«Харківський політехнічний інститут», місто Полтава
ORCID: 0000-0003-3925-0499

Поліщук Валентина Миколаївна,
кандидат технічних наук, доцент,
Харківський національний університет міського
господарства ім. О.М. Бекетова, місто Харків
ORCID.0000-0002-7059-1454

Чепела Станіслав Олександрович,
Харківський національний університет міського
господарства ім. О.М. Бекетова, місто Харків
ORCID.0009-0007-2585-5506

ДІАГНОСТИКА СВІТЛОВИХ ПАРАМЕТРІВ СВІТЛОСИГНАЛЬНИХ ВОГНІВ

Інтернет-адреса публікації на сайті:

<http://www.konferenciaonline.org.ua/ua/article/id-1913/>

За допомогою зорового апарата людина отримує понад 80% інформації необхідної для успішного виконання завдання.

Для світлової системи ефективних величин основною характеристикою зразкового приймача є відносна спектральна світлова ефективність випромінення для стандартного фотометричного спостерігача $V(\lambda)$, яка дозволяє визначити основні світлотехнічні параметри, до яких відносяться світловий потік, сила світла, освітленість, яскравість, світимість тощо. Кожен з цих параметрів важливий з точки зору визначення застосування обраного типу джерела світла, прийнятої системи освітлення, методів розрахунку та їх контролю в процесі експлуатації.

Світлосигнальна система застосовується, як правило, для візуального спостереження світлового сигналу на деякому фоні. При візуальних вимірюваннях або спостереженнях основною характеристикою випромінювання є яскравість, бо саме на яскравість реагує око людини, яка

в свою чергу створює освітленість сітківки ока. Відповідно до фізіологічних властивостей ока зараз пропонується враховувати різницю між яскравістю об'єкта L та її суб'єктивним світловим відчуттям. Аналіз показує, що зорове відчуття визначається яскравістю світної поверхні L і не залежить від відстані до неї, а є функцією розкриття зіниці ока. Дальність видимості світлових сигналів визначається мінімальною яскравістю, нижче якої людське око не реагує на світло (гранична або порогова яскравість). Також дальність видимості світлових сигналів залежить від стану атмосфери, бо поглинання й розсіяння нею світлових променів є одним із чинників, що впливають на видимість світлових сигналів [1, с. 77].

Сила світла, яка напряму пов'язана з яскравістю, визначає дальність видимості світлового сигналу. Чим більше сила світла джерела, тим більше дальність видимості ($I_t = \tau I_0$) з урахуванням коефіцієнта пропускання атмосфери τ . Отже, основними чинниками, що впливають на дальність видимості світлових сигналів, є сила світла джерела, стан атмосфери, величина граничної освітленості та яскравість фону, на якому спостерігається світловий сигнал. Вимірювання сила світла світлосигнальних вогнів та її кутовий розподіл визначаються за результатами гоніофотометричних вимірювань. Дистанція фотометрування приймається рівною дистанції формування пучка променів, яка може сягати понад 10 l [3].

Кольорові характеристики випромінювання світлосигнальних вогнів суворо регламентуються і цілком визначаються спектральними характеристиками абсорбційних світлофільтрів, що входять до їх складу та розподілом енергії у спектрі випромінювання джерела світла.

Застосування в світлосигнальних установках світлодіодних джерел світла визначеного кольору вимагає додаткового контролю колірних характеристик, з урахуванням атмосферних явищ [4].

В лабораторних умовах контроль кольоровості проводиться за допомогою колориметрів, а також шляхом розрахунку за результатами спектральних вимірювань. Лабораторні методи визначення колірних характеристик випромінювання світлосигнальних вогнів дозволяють виконати вимірювання з достатньою для експлуатації точністю.

Перевірка параметрів світлосигнального обладнання здійснюється зовнішнім оглядом, а також експлуатаційною перевіркою. На даний час відповідно до прописаних інструкцій перевці підлягають такі умовно світлотехнічні параметри – правильність регулювання сили світла вогнів підсистем за ступенями яскравості та відсутність темнових провалів у підсистемах вогнів. Система вважається працездатною і правильно відрегульованою, якщо відсутні вогні, які не працюють або надто відрізняються від інших за рівнем яскравості. Технічне діагностування світлосигнальних вогнів у процесі експлуатації являє собою комплекс лабораторно-стендових та натурно-польових досліджень світлотехнічних параметрів. За результатами перевірок та вимірювань надається висновок відповідно рівня працездатності системи та її подальшої експлуатації.

Роботи із аналізу існуючих методик технічного діагностування світлотехнічного обладнання світлосигнальних вогнів з урахуванням впровадження новітніх зразків освітлювальних приладів спеціального призначення дають можливість створенню нових науково обґрунтованих фотометричних методик, що дозволить підтримувати світлосигнальні установки у працездатному стані та забезпечить нормований рівень безпеки візуального спостереження об'єкту.

Література:

1. Поліщук В. М. Зорове сприйняття в умовах зовнішнього освітлення / В. М. Поліщук, О. Ю. Коляда Світлотехніка та електроенергетика. – 2021. – том 60 № 2. – С. 71-78.
2. Девяткіна С. С. Критерії відмови складних топологічних світлосигнальних систем / С. С. Девяткіна, С. О. Горлова. Інформаційні технології в освіті, техніці та промисловості – 2015. – № 1-2. – С. 202-203.
3. Установка для измерений силы света, пространственного распределения и цветовых характеристик светящихся объектов Гониофотометр X-RITE. [Електронний ресурс] – Режим доступу: <http://www.all-pribors.ru/opisanie/44305-10-goniefotometr-x-rite-46588>.
4. Світлодіоди: характеристики, маркування та види. [Електронний ресурс] – Режим доступу: <http://www.poradi.ru/budinok-i-rodina/12685-svitlodiodiharakteristiki-markuvannja-ta-vidi.html>.

*Корбан Віктор Харитонович, доктор технічних наук,
доцент, кафедра технічної експлуатації флоту,
Національний університет «Одеська морська академія», м. Одеса*

ЗАХИСТ МОРСЬКОГО СЕРЕДОВИЩА ВІД ЗАБРУДНЕНЬ ВИХЛОПНИМИ ГАЗАМИ СУДНОВИХ ЕНЕРГЕТИЧНИХ УСТАНОВОК

Інтернет-адреса публікації на сайті:

<http://www.konferenciaonline.org.ua/ua/article/id-1921/>

Розвиток суднових енергетичних установок (СЕУ) значною мірою визначається вимогами економічності та екологічної безпеки, які відображені в міжнародних і національних нормативних документах. У практиці, що склалася, процеси використання паливно-енергетичних ресурсів в елементах суднових енергетичних установок, як на морському транспорті, так і на суднах флоту рибної промисловості супроводжуються значним забрудненням навколишнього середовища. Екологічна безпека використання паливно-енергетичних ресурсів на суднах визначається раціональним використанням

потужностей за мінімізації або відсутності шкідливих чинників, що впливають на стан довкілля.

До теперішнього часу відбулося значне збільшення чисельності торгових суден, що призвело до забруднення морського середовища вихлопними газами суднових енергетичних установок. Виникла серйозна проблема щодо захисту морського середовища від забруднення. На міжнародному рівні розроблено та впроваджено програму ЮНЕП вивчення регіональних морів, що охоплює одинадцять регіонів: Середземного моря, Червоного моря та Аденської затоки, Кувейтської, Західної та Центральної Африки, Східної Африки, Карибського басейну, Східної Азії, Південної Азії, південно-східної та південної частин Тихого океану, Південно-Західної Атлантики, у реалізації якої беруть участь 120 прибережних держав [1]. Виникла необхідність у розробленні методів і технічних засобів захисту морського середовища від забруднення вихлопними газами суднових енергетичних установок морських суден, що містять оксиди азоту, діоксиди сірки, а також аерозолі.

Неповне згоряння палива в суднових енергетичних установках морських суден, окислення домішок і наявність присадок у дизельному паливі та мастилі призводить до того, що в складі вихлопних газів може перебувати до одного відсотка токсичних речовин, що включають CO , N_xO_y , SO_2 , незгорілі вуглеводні C_xH_y , твердий фільтрат вільного вуглецю, високотоксичний пірен $\text{C}_{16}\text{H}_{10}$ (природний компонент кам'яновугільної смоли, сирої нафти та викопного палива), у сполуці свинцю. За відомими даними, для очищення і нейтралізації газових викидів суднових дизелів можуть застосовуватися каталітичні плазмові та рідинні нейтралізатори, дія яких заснована на безполуменовому окисленні продуктів неповного згоряння дизельного палива CO та C_xH_y в CO_2 та H_2O , а також на розкладенні NO_x в O_2 та N_2 .

У низькотемпературних нейтралізаторах ($t \leq 150$ °C) можуть використовуватися оксидні каталізатори у вигляді гранульованої суміші Mn , CuO , Cr , Fe тощо. Нейтралізатори можуть бути розташовані у випускних колекторах або в трубопроводах. У плазмових нейтралізаторах можуть використовуватися спеціальні камери для допалювання горючих елементів відпрацьованих вихлопних газів за температури $t = (700-850)$ °C, у яких оксид вуглецю, альдегіди, суспензії пального й олій окислюються до CO_2 та H_2O , проте негорючі речовини, такі як твердий фільтрат вільного вуглецю, залишаються незмінними.

У рідинних нейтралізаторах відпрацьовані вихлопні газу суднових дизелів можуть пропускатися через шар рідини (води), в якій знешкоджуються розчинні речовини (альдегіди, оксиди сірки, вищі оксиди азоту), затримується твердий фільтрат вільного вуглецю, рідкі аерозолі мастила та дизельного пального, гасяться його розпалені частинки. Однак, за даними А. М. Владимірова без змін залишаються оксиди вуглецю та азоту [2].

Нейтралізація суднових стічних вод може вирішуватися обладнанням суден спеціальною цистерною достатнього об'єму для збирання та зберігання стічних вод із подальшим їхнім передаванням у позасудові приймальні пристрої або обладнанням суден системою для обробки стічних вод до потрібних норм безпосередньо на борту судна та подальшим їхнім скиданням згідно зі встановленими правилами з використанням біологічних, фізичних і фізико-хімічних методів очищення. Знезараження стічних вод після їх очищення може здійснюватися хлоруванням, озонуванням, електролізом або ультразвуковими впливами [3, 4].

З метою видалення нафтопродуктів зі скидних вод найчастіше застосовують системи грубого і тонкого очищення. Грубе очищення має виконуватися сепарувальними пристроями відстійного типу, в яких від води відокремлюються грубодисперсні частинки нафтопродуктів. Принцип дії сепараторів відстійного типу полягає в розділенні нафтоводяної суміші під впливом внутрішньої енергії дисперсної системи. Швидкість потоку води в сепараторі має бути меншою за швидкість підйому частинок нафти. Частинки діаметром 2-5 мм спливають зі швидкістю 100 мм/с, а частинки, менші за 0,8 мм, спливають так повільно, що несуться потоком води. Тому шлях рідини в сепараторі подовжується за рахунок лабіринту їхніх сіток, перегородок, сопел і гвинтоподібних поверхонь.

У сучасному морському флоті з урахуванням вимог захисту морського середовища виконується конструювання окремих елементів суднового обладнання, спрямоване на забезпечення повноти згоряння палива, що дає змогу зменшити забруднення морського середовища вихлопними газами дизелів. На сучасному рівні розвитку науки і техніки названі проблеми можуть бути вирішені вже найближчим часом.

Література:

1. Леонов В. Е. Основы экологии и охрана окружающей среды: Монография / В. Е. Леонов, В. Ф. Ходаковский, Л. Б. Куликова, под ред. д.т.н., проф. В. Е. Леонова. – Херсон: Издательство ХГМИ, 2010. – 352 с.
2. Владимиров А. М. Охрана окружающей среды / А. М. Владимиров, Ю. И. Ляхин, Л. Т. Матвеев, В. Г. Орлов. – Гидрометеиздат, 1991. – 423 с.
3. Abn-Jrai, A. The influence of H₂ and CO on diesel engine combustion characteristics, exhaust gas emissions and after treatment selective catalytic NO_x reduction / A. Tsolakakis, A. Megaritis // Int. J. Hydrogen Energy 2007. – 2007. – Vol. 32. – № 15. – P. 3565-3571.
4. Леонов В. Є. Технологія очищення стічних вод з метою захисту гідросфери. Монографія / В. Е. Леонов, В. Г. Шерстюк, А. П. Бень, за редакцією д.т.н., проф. В. Є. Леонова – Херсон: ПП Вишемирський В. С., 2008, – 152 с.

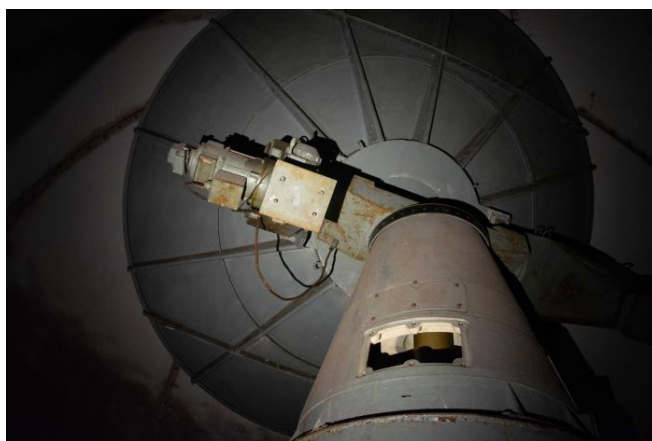
*Корбан Дмитро Вікторович, кандидат технічних наук,
доцент, кафедра управління судном,
Національний університет «Одеська морська академія», м. Одеса*

ВИКОРИСТАННЯ У РАДІОЛОКАЦІЙНІЙ ІНФОРМАЦІЇ МЕТЕОРОЛОГІЧНИХ РАДІОЛОКАТОРІВ ДЛЯ ВИРІШЕННЯ ЗАДАЧІ ПОЛЯРИЗАЦІЙНОЇ СЕЛЕКЦІЇ НАВІГАЦІЙНИХ ОБ'ЄКТІВ НА МОРСЬКИХ СУДНАХ

Інтернет-адреса публікації на сайті:

<http://www.konferenciaonline.org.ua/ua/article/id-1920/>

Мережевий метеорологічний радіолокатор МРЛ-5 п'ятого покоління складається з самого радіолокатора і автоматизованої системи обробки луна-сигналів «МЕТЕОКОМПРКА» (АМРК). Подання метеоданих на індикатори МРЛ-5 здійснюється у вигляді кольорових карт метеоявищ у дальній і ближній зонах радіолокаційного спостереження МРЛ-5. На рис.1 (а, б) надані антенний пристрій (а) та індикатори (б) МРЛ-5.



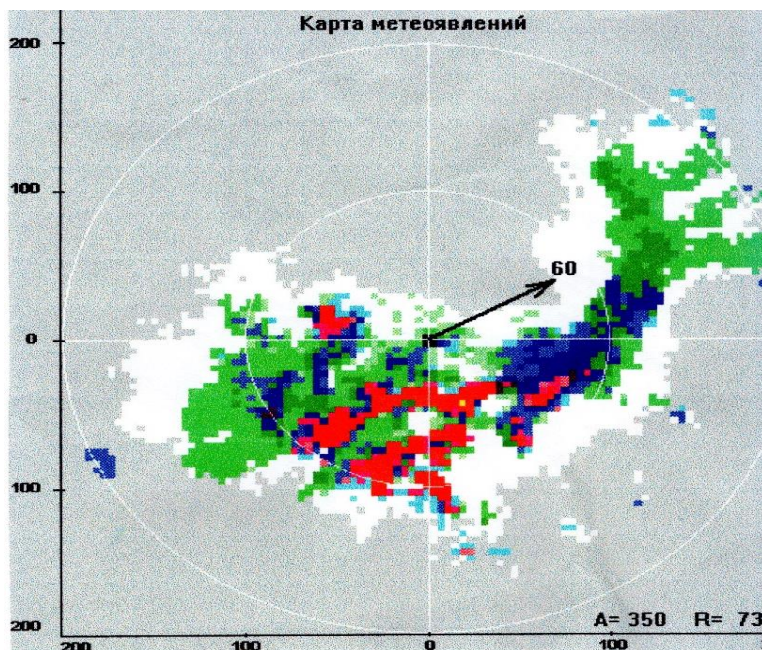
а



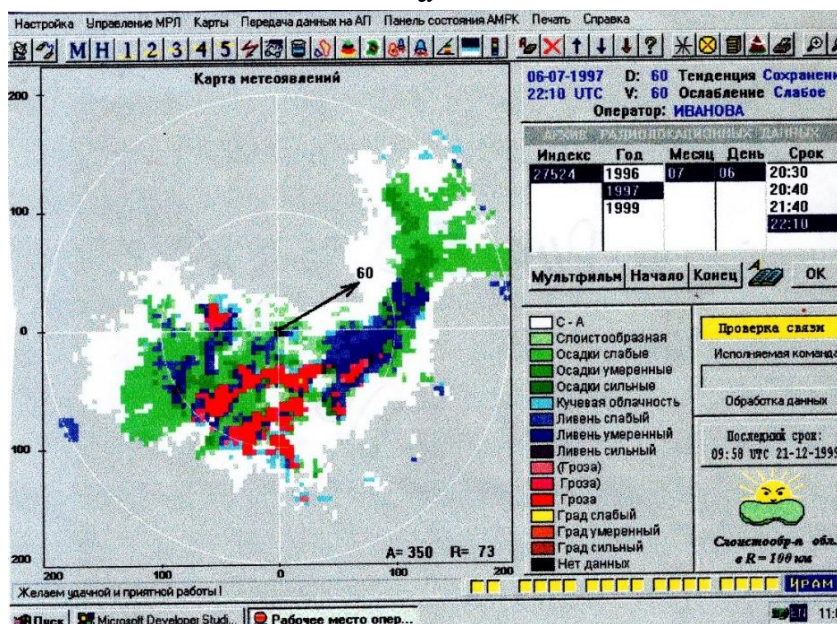
б

Рис.1 Антенний пристрій (а) та індикатори (б) МРЛ-5

На рис.2 (а, б) представлені види кольорових карт, які отримані щодо метеорологічних явища у дальній (40 -300 км) та ближній зонах (0 – 40 км) за допомогою МРЛ-5 і АМРК.



а



б

Рис.2. Кольорова карта метеорологічних явищ (а) та кольорова карта метеорологічних явищ з шкалою їх видів (б).

Особливу небезпеку для безпеки судноводіння мають випадні опади інтенсивністю від 25 мм/год до 300 мм/год за траєкторією руху судна, інформацію про які для екіпажу судна надає радіолокаційний комплекс МРЛ-5.

У табл.1 надані градації інтенсивності випадних опадів за даними МРЛ на європейській території та у табл.2 за територією США з урахуванням типів хмар.

Таблиця 1 – Градації інтенсивності випадних опадів за даними МРЛ на Європейській території

Номер градації	Оцінка інтенсивності	Інтенсивність, I , мм/год	Радіолокаційна відбиваність, Z , δBZ
1	слабкі	0.05 – 2,90	18 – 29
2	помірні	3,00 – 25,00	30 – 45
3	сильні	25,10 – 60,00	45 – 50
4	дуже сильні	60,00 – 150,00	Більше 51

Таблиця 2 – Градації інтенсивності випадних опадів за даними МРЛ на території США, з урахуванням типів хмар

Номер градації	Оцінка інтенсивності	Інтенсивність, випадних опадів I , мм/год	
		з шаруватоподібних хмар	з конвективних хмар
1	слабкі	< 2,5	< 5,0
2	помірні	2,5 – 5,0	5,0 – 27,5
3	сильні	12,5 – 25,0	27,5 – 55,0
4	дуже сильні	25,0 – 50,0	55,0 - 112,5
5	інтенсивні	50,0 - 125,0	112,5 – 177,5
6	екстремальні	> 125,0	> 177,5

Використовуючи відомості з МРЛ, щодо характеристики осередків опадів які випадають у різних районах земної кулі, де проходять траси морських суден, вирішується задача поляризаційної селекції навігаційних об'єктів, що знаходяться у випадних опадах великої інтенсивності.

Література:

1. Настанова з експлуатації АМРК " МЕТЕОКОМІРКА", ИТАВ. 416311.001 НЕ., 2000. 147 с.
2. Брильов Г. Б. Метеорологічні автоматизовані радіолокаційні мережі / Г. Б. Брильов, Т. А. Базлова та інші. / СПб: Інститут радарної метеорології, 2002. – 331 с.

*Лапчак Світлана Мирославівна, викладач спецдисциплін
легкої промисловості Відокремленого структурного
підрозділу «Одеський технічний фаховий коледж
Одеського національного технологічного університету»*

*Кузіна Наталя Володимирівна, викладач спецдисциплін
легкої промисловості Відокремленого структурного
підрозділу «Одеський технічний фаховий коледж
Одеського національного технологічного університету»,
аспірантка Київського національного
університету технологій та дизайну.*

ОПТИМІЗАЦІЯ ПРОЦЕСУ ВДЯГАННЯ І ЗНЯТТЯ ВЗУТТЯ: НОВІ ПІДХОДИ ТА ТЕХНОЛОГІЇ

Інтернет-адреса публікації на сайті:

<http://www.konferenciaonline.org.ua/ua/article/id-1910/>

Сучасний ритм життя характеризується неперервною руховою активністю. Люди більше не прив'язані до однієї локації, а постійно змінюють місце свого перебування, переміщуючись між роботою, заняттями та зустрічами. Такий ритм життя потребує не лише ефективності, але і комфорту, який напряму залежить від правильного вибору взуття. З огляду на динамічний життєвий стиль, взуття повинно відповідати певним вимогам та бути легким, зручним, мати можливість швидкого зняття та одягання, а також стійким до зношення. Зручне взуття не лише полегшує пересування, але й стає важливим елементом загального іміджу [1].

Перевагами адаптивного взуття є підтримка та фіксація стопи в різних умовах, можливість регулювання ширини та об'єму, а також використання дихаючих матеріалів. Це дозволяє комфортно почуватися впродовж дня, незалежно від навантаження. Нині одним із ключових факторів, які впливають на комфорт такого взуття є конструктивні рішення для полегшення вдягання та зняття взуття, які впроваджуються завдяки застосуванню технологічних інновацій. Застосування 3D-друку в дизайні взуття дозволяє створювати індивідуальні моделі, що точно відповідають анатомічній будові ноги, що суттєво спрощує їх носіння. Завдяки новим рішенням, взуття стало не лише привабливим, але і більш функціональним, що забезпечує безперешкодний процес взування. На сьогодні, більшість взуттєвих компаній, які виготовляють адаптивне взуття, привертають увагу інноваційним особливостям взуття, серед яких провідне місце займають механізми ковзання, що дозволяють легко взувати та знімати взуття, особливо для людей з обмеженою функцією руху та з певними фізіологічними вадами. Ці механізми представляють собою цілісну

конструкцію, яка усуває потребу в шнурках або ремінцях, пришвидшуючи час вдягання та знімання взуття. Приклад зазначеного дизайну можна побачити у спортивному та повсякденному взутті, де еластичні матеріали створюють щільну і разом з тим зручну посадку. Ці функції не тільки підвищують зручність, але й зберігають естетичну привабливість та довговічність взуття. Інтегрувавши такі інноваційні елементи дизайну, виробники успішно впоралися з повсякденною проблемою, зробивши взуття більш доступним для широкої аудиторії споживачів [2-3].

Адаптивні та регульовані застібки – ще одне важливе впровадження, спрямоване на спрощення процесу носіння взуття. Ці застібки, часто реалізовані за допомогою липучок, еластичних стрічок або регульованих пряжок, дозволяють користувачам налаштувати посадку взуття відповідно до фізіологічних змін стопи. Ця гнучкість особливо корисна для людей зі змінним розміром стопи через такі захворювання, як набряки, або для дітей, у яких стопи ще ростуть. Регульовані застібки забезпечують легке затягування або послаблення взуття, забезпечуючи надійну посадку без зав'язування шнурків. Ця конструкція не тільки підвищує комфорт користувача, але й збільшує зручність використання взуття з часом, роблячи його практичним рішенням для різних статево-вікових груп.

Петлі на п'яті та фіксатори – прості, але ефективні конструктивні елементи, які забезпечуючи зручну точку захоплення, щоб допомогти користувачам просунути або витягнути ноги докладаючи мінімум зусиль. Ця конструкція особливо корисна для людей з обмеженою силою або спритністю рук, наприклад для людей похилого віку або людей з артритом. Перелічені елементи: петлі на п'яті та фіксатори спрощують процес знімання та зменшують фізичне навантаження, пов'язане з носінням взуття. Це доповнення до дизайну взуття підкреслює важливість доступності та орієнтованих на користувача інноваційних елементів у адаптивних виробках.

Оптимізація елементів фурнітури адаптивного взуття для спрощення процесу взування і зняття значно впливають на загальний стан здоров'я користувачів. Це допомагає зменшити навантаження на суглоби, покращує кровообіг і підтримує природну форму стопи, що, в свою чергу, сприяє загальному фізіологічному стану активних людей [4-5].

На завершення, адаптивне взуття стає важливим атрибутом сучасного життя, яке відповідає на виклики сьогодення та підвищує комфорт споживачів. Інновації у цій сфері безумовно впливатимуть ритм життя, забезпечуючи стиль і зберігаючи зручність одночасно.

Література:

1. Dimou E., Manavis A., Papachristou E., Kyratsis P., A Conceptual Design of Intelligent Shoes for Pregnant Women. Business Models and ICT Technologies for the Fashion Supply Chain Proceedings of IT4Fashion 2016.200.69
2. Alvarez R., Stokes I.A.F. Dimensional changes of the feet in pregnancy, Journal of Bone and Joint Surgery – Series A, 1988, 70, 271-274.
3. Bertuit J., Leyh C. Plantar Pressure During Gait in Pregnant Women, Journal of the American Podiatric Medical Association, 2016, 106, 398-405.
4. Nyska M., Sofer D. Plantar foot pressures in pregnant women, Israel Journal of Medical Sciences, 2017, 33, 139-146.
5. Шубенок О.С., Омельченко, Н.М. Коновал, В.П. Ортопедичні пристосування до взуття вагітних жінок [Текст] / О. С. Шубенок, Н. М. Омельченко, В. П. Коновал // Легка промисловість. – 2005. – № 4. – С. 58-59.

Зміст

Секція 1. Інформаційні системи і технології

Величківський Ілля Олегович, Ільєнко Анна Вадимівна, Галата Лілія Павлівна ПРОГРАМНИЙ МОДУЛЬ ЗАХИСТУ ІНФОРМАЦІЇ В ХМАРНИХ ОБЧИСЛЕННЯХ НА ОСНОВІ МАШИННОГО НАВЧАННЯ.....	3
Гомель Ілля Олександрович НЕБЕЗПЕКА TELEGRAM ЯК МЕСЕНДЖЕРА ДЛЯ ОБМІНУ ДАНИМИ.....	6
Єрмоленко Микола Володимирович ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ АВТОМАТИЗАЦІЇ БУХГАЛТЕРСЬКОГО ОБЛІКУ	9
Журавель Андрій Петрович, Браїловський Микола Миколайович СИСТЕМА БЕЗПЕКИ ЕЛЕКТРОННИХ ПЛАТЕЖІВ.....	11
Каштан Віта Юріївна МЕТОДИКА ВИДІЛЕННЯ СІЛЬСЬКОГОСПОДАРСЬКИХ КУЛЬТУР НА БАГАТОСПЕКТРАЛЬНИХ ЦИФРОВИХ СУПУТНОВИХ ЗНІМКАХ.....	14
Кіш Віктор Вікторович, Йовбак Ніка Ігорівна УПРАВЛІННЯ БІЗНЕС ПРОЦЕСАМИ В ІТ ПРОЄКТАХ.....	17
Колодій Роман Ігорович ДОСЛІДЖЕННЯ ВЗАЄМОДІЇ ПОЯСНЮВАНОВОГО ШТУЧНОГО ІНТЕЛЕКТУ (ХАІ) ТА ВЕЛИКИХ МОВНИХ МОДЕЛЕЙ (LLM).....	19
Максютенко Микола Миколайович МЕТОД ВИЯВЛЕННЯ ВТОРГНЕНЬ.....	22
Моргаль Олег Михайлович, Савчук Олена Володимирівна, Турок Вадим Васильович ІНТЕЛЕКТУАЛЬНИЙ ЗАСТОСУНОК РОЗПІЗНАВАННЯ ЗАБАРВЛЕНОСТІ ТЕКСТОВИХ ПОВІДОМЛЕНЬ УКРАЇНСЬКОЮ МОВОЮ.....	25
Токарев Володимир Володимирович, Маламуж Олексій Петрович ІНТЕГРАЦІЯ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМИ МОДЕЛЮВАННЯ БІЗНЕС-ПРОЦЕСІВ (ВМР).....	28

Чепис Олександр Вікторович ЕНЕРГОЕФЕКТИВНІСТЬ В БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТАХ.....	31
Шафрай Ілля Юрійович МЕТОД ПРОТИДІЇ КІБЕРАТАКАМ В КОРПОРАТИВНИХ МЕРЕЖАХ.....	33
Шестак Ярослав Іванович, Завгородня Єлизавета Олександрівна ЗАХИСТ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ЗВО.....	37
Якимів Тарас Вікторович АНАЛІЗ САМОПОДІБНОГО ТРАФІКУ З МЕТОЮ ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ ВІД ПРИХОВАНИХ DDOS-АТАК.....	41

Секція 2. Економічні науки

Polina Vitalyivna Tymofieieva TAX MANAGEMENT AS AN INSTRUMENT OF ECONOMIC SECURITY OF THE ENTERPRISE.....	44
Кравець Олександр Володимирович ОПТИМІЗАЦІЯ МАРКЕТИНГОВОГО БЮДЖЕТУ ПІДПРИЄМСТВА В УМОВАХ ЗРОСТАЮЧОЇ КОНКУРЕНЦІЇ В ІНТЕРНЕТ-СЕРЕДОВИЩІ.....	46
Олійник Ольга Степанівна СТАЛІЙ РОЗВИТОК РЕГІОНАЛЬНОГО РИНКУ ТУРИСТИЧНО-РЕКРЕАЦІЙНИХ ПОСЛУГ.....	50

Секція 3. Технічні науки

Olena V. Bohoiavlenska, Pavlo P. Karnozhytskyi, Pavlo V. Karnozhytskyi, Svitlana G. Deribo STUDY OF HUMIC SUBSTANCES AS REAGENTS FOR THE PURIFICATION OF CONTAMINATED WATER.....	53
Воробйов Юрій Анатолійович, Богач Олексій Анатолійович ТЕХНІЧНА ПІДГОТОВКА ВИРОБНИЦТВА ЛЕГКОГО ЛІТАКА.....	56
Клименко Олександр Володимирович, Ковцун Андрій Ігорович, Акастьолов Олексій Володимирович, Теслюк Геннадій Володимирович ЗАСТОСУВАННЯ КОМБІНОВАНОГО КУЛЬТИВАТОРА ДЛЯ ПЕРЕДПОСІВНОГО ОБРОБІТКУ ҐРУНТУ.....	63

Коляда Оксана Юрїївна, Полїщук Валентина Миколаївна, Чепела Станїслав Олександрович ДІАГНОСТИКА СВІТЛОВИХ ПАРАМЕТРІВ СВІТЛОСИГНАЛЬНИХ ВОГНІВ.....	65
Корбан Віктор Харитонович ЗАХИСТ МОРСЬКОГО СЕРЕДОВИЩА ВІД ЗАБРУДНЕНЬ ВИХЛОПНИМИ ГАЗАМИ СУДНОВИХ ЕНЕРГЕТИЧНИХ УСТАНОВОК.....	67
Корбан Дмитро Вікторович ВИКОРИСТАННЯ У РАДІОЛОКАЦІЙНІЙ ІНФОРМАЦІЇ МЕТЕОРОЛОГІЧНИХ РАДІОЛОКАТОРІВ ДЛЯ ВИРІШЕННЯ ЗАДАЧІ ПОЛЯРИЗАЦІЙНОЇ СЕЛЕКЦІЇ НАВІГАЦІЙНИХ ОБ'ЄКТІВ НА МОРСЬКИХ СУДНАХ.....	70
Лапчак Світлана Мирославівна, Кузіна Наталя Володимирівна ОПТИМІЗАЦІЯ ПРОЦЕСУ ВДЯГАННЯ І ЗНЯТТЯ ВЗУТТЯ: НОВІ ПІДХОДИ ТА ТЕХНОЛОГІЇ.....	73

www.konferenciaonline.org.ua

Міжнародна наукова інтернет-конференція

**"Інформаційне суспільство:
технологічні, економічні та
технічні аспекти становлення"
(випуск 92)**

8-9 жовтня 2024 р.

Наукове видання

**«Інформаційне суспільство: технологічні, економічні
та технічні аспекти становлення»**

Рік заснування – 2011

Видання виходить 11 разів на рік

Відповідальний за випуск *У.О. Русенко*
Комп'ютерне верстання *О.В. Ковальський*

Підписано до друку 16.10.2024
Формат 60x84/16. Папір офсетний. Друк на дублікаторі.
Умов.-друк. арк. 4,5. Обл.-вид. Арк 4,95.
Тираж 50 прим.

Віддруковано ФО-П Шпак В.Б.
Свідоцтво про внесення суб'єкта видавничої справи до
Державного реєстру видавців, виготовлювачів і розповсюджувачів
видавничої продукції серія ДК№7599 від 10.02.2022р.
Тел. 097 299 38 99
E-mail: tooums@ukr.net

