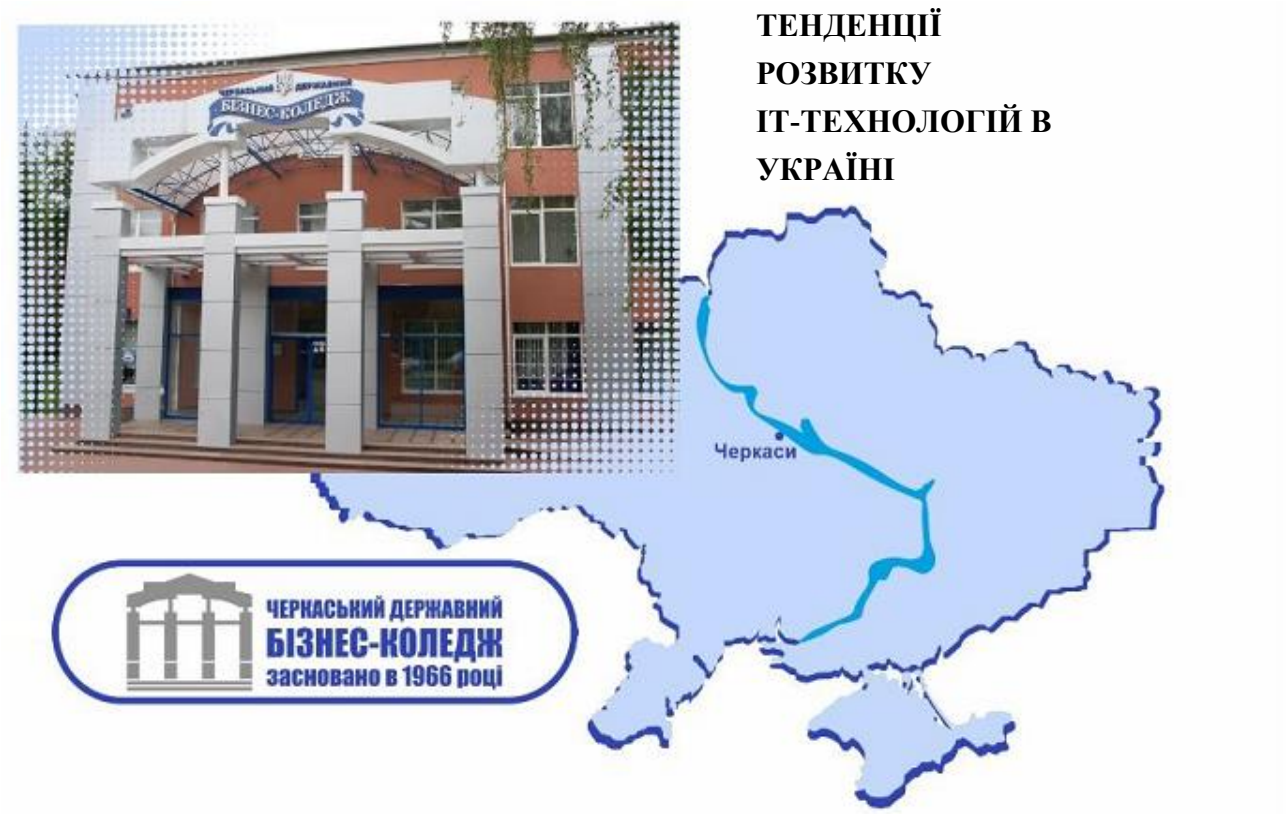



# МАТЕРІАЛИ

## XV Студентської

## науково-практичної конференції

## студентів, аспірантів та молодих вчених

**за тематикою**
**«Тенденції розвитку**
**ІТ-технологій в Україні»**

**15-16 березня 2023 р.**
**м. Черкаси**

**Міністерство освіти і науки України**
**Черкаський державний бізнес-коледж**

# МАТЕРІАЛИ

## XV Студентської

## науково-практичної конференції

## студентів, аспірантів та молодих вчених

**за тематикою**

## «Тенденції розвитку ІТ-технологій в Україні»

**15-16 березня 2023 р.**
**м. Черкаси**

УДК 004.7+00.5

Матеріали XV Студентської науково-практичної конференції студентів, аспірантів та молодих вчених за тематикою «Тенденції розвитку ІТ-технологій в Україні»: збірка наукових праць. Черкаси, 2023, 101 с.

**ISBN 777-777-7777-77-7 (електронне видання)**

Доповіді наукової конференції містять результати досліджень за наступними напрямками: обробка та захист інформації; інженерні підходи до розробки програмного забезпечення; інформаційні технології в галузевих рішеннях; робототехніка та адміністрування комп'ютерних систем.

Роботи друкуються в авторській редакції. В збірці максимально зменшено втручання в обсяг та структуру відібраних до друку матеріалів. Редакційна колегія не несе відповідальності за достовірність досліджень, матеріалів та результатів досліджень, що надано в рукописах, та залишає за собою право не поділяти погляди деяких авторів на ті чи інші питання, висвітлені в роботах.

Збірник становить інтерес для студентів, аспірантів, викладачів та наукових працівників.

## *Оргкомітет конференції*

**Азьмук Н.А.** – заступник директора з навчально-методичної роботи ЧДБК, д-р екон. наук – голова оргкомітету;

**Заболотній С.В.** - професор кафедри комп'ютерної інженерії та інформаційних технологій ЧДБК, д-р тех. наук;

**Хотунов В.І**. – завідувач кафедри комп'ютерної інженерії та інформаційних технологій ЧДБК, канд.. пед. наук;

**Захарова М.В**. – доцент кафедри комп'ютерної інженерії та інформаційних технологій ЧДБК, канд. тех. наук;

**Бурмістров С.В.** – доцент кафедри комп'ютерної інженерії та інформаційних технологій ЧДБК, канд. тех. наук;

**Михайлюта С.Л.** – доцент кафедри комп'ютерної інженерії та інформаційних технологій ЧДБК, канд. техн. наук;

**Музиченко В.М.** – завідувач відділенням дизайну ЧДБК;

**Марченко С.В.** – відповідальний секретар.

УДК 004.7+00.5

ISBN 777-777-7777-77-7

# ЗМІСТ

# Секція 1.

# ОБРОБКА ТА ЗАХИСТ ІНФОРМАЦІЇ

# ВПЛИВ ІНФОРМАЦІЇ НА ЛЮДИНУ

*Васильченко Ю. В.*
*vasilchenko496@gmail.com*
*Черкаський державний бізнес-коледж*
*Науковий керівник: Захарова М. В.*
*м. Черкаси, Україна*

**Актуальність теми.** «Вплив інформації на людину» є дуже актуальною в наш час темою, оскільки ми живемо в епоху інформаційного вибуху, коли інформація оточує нас з усіх боків. Інформація впливає на наше сприйняття світу, наше розуміння подій, віру в політичних лідерів, сприйняття нашого місця в соціумі та інше. Завдяки широкому розповсюдженню соціальних мереж та швидкому поширенню новин, ми отримуємо доступ до більшої кількості інформації, ніж будь-коли раніше. Однак, разом з цим, також стикаємося з проблемою поширення фейкової та неправдивої інформації, яка може вплинути на наше сприйняття світу та призвести до неправильних рішень. Тому, тема «Вплив інформації на людину» є дуже важливою і потребує уваги та досліджень.

**Мета** даної роботи спрямована на покращення розуміння впливу інформації на людину та розробку заходів для зменшення негативних наслідків від її неправильного сприйняття.

**Об’єктом вивчення** є загальнодоступна інформація в мережі Інтернет.

**Предметом роботи** є дослідження та аналіз знайденої інформації.

Агітація - найважливіший засіб впливу на свідомість та настрій широких мас, з метою спонукати їх до політичної чи іншої активності, ідеологічна зброя боротьби партій [1].

Агітація може використовувати різні методи, такі як емоційний тиск, застосування схем та стереотипів мислення, використання ефектів соціального впливу та ін. Таким чином, люди можуть бути переконані у правильності певної ідеї або проблеми, не здійснюючи об’єктивний аналіз інформації.

Інструменти впливу медіа [2]:

1) Переконання. Мета переконування досягається не тільки завдяки

самому повідомленню, а й залежить від розумової активності аудиторії. Під переконуванням розуміють такий вплив на свідомість, який за допомогою логічно впорядкованих аргументів (доказів, фактів) і обґрунтованих висновків підтверджує, формує або змінює ставлення реципієнта до когось або чогось, веде до прийняття ним зваженого рішення, до осмисленої дії.

2) Навіювання - це спроба вплинути на психіку людини, щоб вона вірила у щось, не маючи для цього доказів. Цей інструмент використовується, коли потрібно вплинути на емоції та почуття людини.

3) Наслідування. За об`єкт наслідування аудиторія бере моделі поведінки, звички, манери спілкування, ідеали, матеріальні і духовні цінності, естетичні смаки тощо. Наслідування важливий елемент соціалізації людини, набуття нею соціокультурного досвіду

4) Маніпулювання. На відміну під переконування, маніпуляція завжди прихована. В її основі лежить цілеспрямована дія на масову аудиторію, щоб скерувати її в потрібне русло, викликати в неї бажані настрої і поведінку. При цьому сама мета замаскована від аудиторії, а повідомлення, за допомогою якого досягається вплив, ретельно планується.

Фейк – спеціально поширювана в мас-медіа соціальних мережах відверто неправдива інформація, фальсифікація, підробки. Фейк використовують у пропаганді, для того, щоб дезінформувати, ввести в оману, залякати, деморалізувати аудиторію, викликати агресію, посіяти в паніку. Сфери поширення фейків – ЗМІ та соціальні мережі [3].

ІПСО – інформаційно-психологічна операція. ІПСО може бути використаний в різних сферах, таких як політика, масові засоби масової інформації, реклама та інше. Цей спосіб використання інформації дуже ефективний, оскільки люди мають тенденцію реагувати на емоції та відчуття, а не на логіку.

ІПСО може мати негативні наслідки, такі як створення паніки, страху, сприяння формуванню стереотипів та несприятливого сприйняття дійсності [4].

Отже, в сучасному світі через високий розвиток сучасних технологій

активно використовується маніпуляція суспільною думкою використовуючи засоби масової інформації. Особливо активно це проявляється під час російсько-української війни, де російська сторона використовує пропаганду для створення електорату путінського режиму, а також для пропаганди війни, національної, расової, релігійної ненависті, що підбурює до дискримінації, ворожості, насилля. Потрібно завжди критично обробляти інформацію та довіряти лише офіційним джерелам.

**Список використаних джерел**


1. Агітація — [Електронний ресурс]. Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/%D0%90%D0%B3%D1%96%D1%82%D0%B0%D1%86%D1%96%D1%8F
2. Інструменти впливу медіа— [Електронний ресурс]. Режим доступу до ресурсу: https://jarch.donnu.edu.ua/article/view/11693/11568
3. Фейки — [Електронний ресурс]. Режим доступу до ресурсу: http://surl.li/kvjk
4. ІПСО — [Електронний ресурс]. Режим доступу до ресурсу: https://tyzhden.ua/shcho-take-ipso-chomu-vazhlyvo-tse-znaty-i-iaki-operatsii-zaraz-provodyt-rosiia-proty-ukrainy/


## СОЦІАЛЬНА ІНЖЕНЕРІЯ


*Колісник М. М.*
*maksimkolisnuk7@gmail.com*
*Черкаський державний бізнес-коледж*
*Науковий керівник: Захарова М. В.*
*м. Черкаси, Україна*


**Актуальність теми.** Соціальна інженерія – це мистецтво маніпулювання людською поведінкою з метою отримання доступу до конфіденційної інформації або впливу на дії цільової особи. Це може включати в себе використання психологічних методів, інформації з соціальних мереж, маскування та імітацію іншої особи або організації, щоб створити довіру та

отримати доступ до важливої інформації або системи. Також соціальна інженерія може використовуватися в контексті кібербезпеки для виявлення та запобігання соціальним інженерним атакам.

**Метою роботи** є дослідження методів соціальної інженерії, яка може бути використана як для позитивних, так і для негативних цілей, і є потужним інструментом в кіберпросторі.

Соціальна інженерія може стати засобом здійснення кібератак, крадіжки особистих даних та інших злочинів. Ключова роль соціальної інженерії полягає в знаходженні інформації про жертв в мережі та її використанні в користь атакувачів, і способи її використання включають підставлення невинних осіб і створення підставних скарг. Наприклад, фейковий акаунт є дієвим методом маніпулювання, і негативні наслідки соціальної інженерії можуть включати блокування акаунту та виключення з гри. Однак соціальна інженерія також може бути важливим інструментом забезпечення кіберзахисту.

Таким чином, для забезпечення безпеки користувачів мережі необхідно проводити аналіз кожного з випадків впливу, а також підвищувати рівень кібербезпеки з метою запобігання використання методів, інструментів та засобів соціальної інженерії для шкоди, що дозволить використовувати навички протидії для підвищення безпеки в IT-галузі та зменшення ризиків витоку конфіденційної інформації. Узагальнюючи, соціальна інженерія є важливою проблемою в сучасному цифровому світі, і потребує постійного вивчення та контролю для забезпечення безпеки та захисту від кіберзлочинності.

## Список використаних джерел


1. HitOk [Електронний ресурс]. Режим доступу: https://www.youtube.com/channel/UCwrNkeWwahveYd-osLhATMQ (дата звернення: 21.11.2022р.).
2. "Social Engineering" від Pluralsight [Електронний ресурс]. Режим доступу https://www.pluralsight.com (дата звернення: 21.01.2023р.).

# ОСОБЛИВОСТІ СИСТЕМ АУТЕНТИФІКАЦІЇ ІНФОРМАЦІЇ

*Парфенюк І. О.*
*il228best@gmail.com*
*Черкаський державний бізнес-коледж*
*Науковий керівник: Захарова М. В.*
*м. Черкаси, Україна*

Дані, інформація, повноваження – найбільші цінності для будь-якої сучасної компанії після людських ресурсів, звичайно. Все частіше ми чуємо новини про несанкціонований доступ до тих чи інших ресурсів. Причому жертвами зловмисників можуть стати як комерційні організації, чи банки, і уряди держав. Плата за незабезпечену безпеку ресурсів може виявитися катастрофічною для комерційних компаній та вкрай високою для державних. Починаючи від прямих збитків і закінчуючи банальною втратою лояльності клієнтів та втратою конкурентних переваг [5].

Метою даної роботи є аналіз методів аутентифікації, розгляд її видів та виявлення найбільш ефективного способу для забезпечення захисту інформації.

Аутентифікація (англ. authentication) – це основа безпеки будь-якої системи, яка полягає у перевірці аутентичності даних про користувача сервером. Вона не тотожна ідентифікації та авторизації. Ці три терміни є елементами захисту. Перша стадія – ідентифікація. На ній відбувається розпізнавання інформації про користувача, наприклад, логін та пароль. Друга стадія – аутентифікація. Тобто, процес перевірки інформації про користувача. Третя стадія – авторизація, на якій відбувається перевірка прав користувача та визначається можливість доступу [1].

Методи аутентифікації:

1) Парольний. Найпоширеніший метод, в якому аутентифікація може відбуватися за одноразовими та багаторазовими паролями. Багаторазовий пароль задає користувач, а система зберігає їх у базі даних. Він є однаковим для кожної сесії. До них відносяться PIN-коди, слова, цифри, графічні ключі. Одноразові паролі – різні для кожної сесії. Це може бути SMS із кодом.

2) Комбінований. Аутентифікація відбувається з використанням кількох методів, наприклад, парольних та криптографічних сертифікатів. Він потребує спеціального пристрою для зчитування інформації.
3) Біометричний. Це найдорожчий метод аутентифікації. Він запобігає витоку або крадіжці персональної інформації. Перевірка проходить за фізіологічними характеристиками користувача, наприклад, по відбитку пальця, сітківці ока, тембру голосу і навіть ДНК [1].

Види аутентифікації:

1. Однофакторна аутентифікація. Це найпоширеніший варіант. Приклад – аутентифікація за допомогою пароля. Сприяє достатній простоті доступу до програм та сервісів. Останніми роками однофакторний тип почав втрачати свою актуальність. Підібрати пароль до логін з кожним роком стає все простіше. Особливо це стосується ситуацій, коли клієнт (користувач) не генерує password, а вигадує його один для всіх акаунтів.

Для захисту даних користувача деякі системи використовують «тимчасові паролі». При вході в обліковий запис щоразу відвідувач отримуватиме на телефон або електронну пошту «таємну комбінацію». Цей пароль одноразовий, діє деякий час (сильно обмежений) [2].

2. Двофакторна аутентифікація – це додатковий рівень захисту облікового запису. Крім введення пароля, потрібно також ввести одноразовий код, який надходить на пошту або телефон, або відбиток пальця. Цим ви підтверджуєте свою особистість. Коли ви активуєте цю опцію, окрім пароля хакеру потрібно також ввести код, щоб зайти у ваш обліковий запис. Ви також отримаєте повідомлення, якщо хтось спробує отримати доступ до вашого обліку. Одноразовий код діє лише кілька хвилин або годин, після чого він самознищується. Таким чином, завдяки двофакторній аутентифікації ваші онлайн-акаунти стають невразливими для кіберзлочинців [3].

3. Багатофакторна аутентифікація (MFA) – це процес входу в систему, який складається з кількох кроків і вимагає від користувача вказати більше інформації, а не пароль. Наприклад, крім пароля, система може попросити

користувача вказати код, надісланий на електронну пошту, відповісти на секретне запитання або сканувати відбитки пальців. Друга форма аутентифікації може допомогти запобігти несанкціонованому доступу до облікового запису, якщо системний пароль було зламано.

1) Знижує ризики безпеки. Багатофакторна автентифікація мінімізує ризики, пов’язані з людським фактором, неправильними паролями та втраченими пристроями.
2) Забезпечує реалізацію цифрових ініціатив. Організації можуть впевнено робити цифрові ініціативи. Підприємства використовують багатофакторну автентифікацію для захисту даних організації та користувачів, щоб вони могли безпечно здійснювати онлайн-взаємодію та транзакції.
3) Підвищення ефективності реагування системи безпеки. Компанії можуть налаштувати систему багатофакторної автентифікації на активне надсилання попереджень при виявленні підозрілих спроб входу до системи. Це допомагає як компаніям, так і приватним особам швидше реагувати на кібератаки, що зводить до мінімуму будь-які потенційні збитки [4].

Таким чином, проаналізувавши види аутентифікації, приходимо до висновку, що найбільш ефективним є багатофакторна аутентифікація, яка дозволяє знизити ризики втрати інформації, забезпечити стабільний шлях для здійснення взаємодій у мережі та покращити ефективність систем захисту для непередбачених атак.

## Список використаних джерел


1. Techtarget [Електронний ресурс] – Режим доступу до ресурсу: https://www.techtarget.com/searchsecurity/definition/authentication.
2. Strongdm [Електронний ресурс] – Режим доступу до ресурсу: https://www.strongdm.com/authentication.
3. N-able [Електронний ресурс] – Режим доступу до ресурсу: https://www.n-able.com/blog/network-authentication-methods.

4. Freecodecamp [Електронний ресурс] – Режим доступу до ресурсу: https://www.freecodecamp.org/news/user-authentication-methods-explained/.
5. IBM [Електронний ресурс] – Режим доступу до ресурсу: https://www.ibm.com/topics/multi-factor-authentication.

# ДОСЛІДЖЕННЯ СУЧАСНОГО «ШТУЧНОГО ІНТЕЛЕКТУ ТА НЕЙРОМЕРЕЖ». ТЕХНОЛОГІЯ, ЗАСТОСУВАННЯ ТА ПЕРСПЕКТИВИ

*Новіков О. С.*
*alexnovikov847@gmail.com*
*Черкаський державний бізнес-коледж*
*Науковий керівник: Люта М.В.*
*м. Черкаси, Україна*

Штучний інтелект – це комп’ютерна технологія, яка може навчитися вирішувати складні завдання, такі як розпізнавання образів, розуміння мови та прийняття рішень. ШІ використовує методи навчання, які дозволяють йому збирати та аналізувати велику кількість даних, щоб зробити висновки та прийняти рішення на основі цих даних.

Штучний інтелект (ШІ) є однією з найбільш перспективних технологій нашого часу. За допомогою машинного навчання, глибинного навчання та інших методів комп’ютерна технологія може навчитися розв’язувати складні завдання, які раніше вважалися неможливими для автоматизації. ШІ здатен розв’язувати задачі від найпростіших до найскладніших, від розпізнавання образів до розуміння мови та прийняття рішень. Проте, зростаюча потужність і розповсюдження ШІ необхідно супроводжувати обов’язковими етичними і правовими засадами. У цьому звіті ми розглянемо потенціал та ризики ШІ, а також важливість його розвитку у збалансованому та відповідальному напрямку.

Штучний інтелект використовується в багатьох галузях, які можуть вирішувати проблеми та поліпшувати процеси. Ось кілька прикладів використання ШІ:

1) **Розпізнавання образів**: ШІ може розпізнавати обличчя, автомобілі, птахів, тварин та інших об’єктів на зображеннях та відео.
2) **Розпізнавання мови**: ШІ може розпізнавати та перекладати мову на різні мови, допомагаючи людям спілкуватися в різних культурах та мовних середовищах.
3) **Медицина**: ШІ може діагностувати та лікувати різні хвороби шляхом аналізу даних та інформації про пацієнтів.
4) **Автономні транспортні засоби**: ШІ може допомогти автомобілям, літакам та іншим транспортним засобам рухатися без водія та пілота, розпізнавати перешкоди та уникати їх.
5) **Фінанси**: ШІ може аналізувати ринки та прогнозувати тенденції, допомагаючи інвесторам приймати рішення про вкладення коштів.
6) **Комп’ютерні ігри**: ШІ може стати опонентом гравців у різних іграх, від шахів до відеоігор, забезпечуючи високий рівень виклику та інтелектуальної складності.
7) **Політика**: ШІ може аналізувати даний та інформацію про виборців та кандидатів, допомагаючи політичним кампаніям краще спілкуватися зі своїми виборцями та формувати свою стратегію.

Прикладом першого є Google Lens, додаток який у червні 2018 року став доступним у Google Play. Це один з конкретних прикладів використання ШІ в розпізнаванні образів. Ця система дозволяє використовувати камеру смартфона для розпізнавання різних об’єктів, тварин, рослин, товарів в магазинах та інших елементів. Наприклад, якщо ви спрямуєте камеру на цінник товару в магазині, Google Lens може розпізнати його та надати додаткову інформацію про товар, таку як ціна, відгуки та рейтинг.

Один з конкретних прикладів використання ШІ в розпізнаванні мови - це система голосового помічника Amazon Alexa (2014). Alexa використовується у різних пристроях, таких як Amazon Echo та Echo Dot, і дозволяє користувачам контролювати свої пристрої та виконувати інші завдання голосом. Alexa використовує глибинне навчання для розпізнавання різних мов та акцентів.

Система збирає дані про голосові команди, які користувачі вимовляють, і використовує ці дані, щоб навчитися розпізнавати різні голосові команди та аналізувати їх контекст. Крім того, Alexa також використовує систему природної мови (Natural Language Processing, NLP) для розуміння різних мовних конструкцій, таких як запитання, заперечення та інші. Це дозволяє системі розуміти користувача, навіть якщо він використовує нестандартну фразеологію або мовні вирази.

Один з конкретних прикладів застосування ШІ у медицині - це розвиток комп'ютерної томографії (CT) та магнітно-резонансної томографії (MRI). ШІ допомагає аналізувати велику кількість даних, що отримуються під час проведення CT та MRI сканування, та генерувати докладні тридименсійні зображення внутрішніх органів людини. Крім того, ШІ також використовується у діагностиці та лікуванні онкологічних захворювань. Наприклад, системи ШІ можуть аналізувати зображення з CT та MRI сканувань та допомагати ідентифікувати ознаки ракових захворювань в ранніх стадіях розвитку. Крім того, ШІ можуть бути використані для розробки індивідуальних планів лікування, враховуючи унікальні особливості та потреби кожного пацієнта.

Один з конкретних прикладів ШІ в автономних транспортних засобах – це система «Tesla Autopilot» (2021), яка використовує глибинне навчання та нейронні мережі для автоматизації керування автомобілем. Система вміє розпізнавати дорожні знаки, розмітку, перешкоди та інші об'єкти на дорозі, щоб допомогти водієві уникнути небезпек та допомогти збільшити безпеку на дорогах. Крім того, система вміє підлаштовувати швидкість та відстань до інших транспортних засобів, щоб зменшити ризик зіткнення та забезпечити комфортну поїздку. Штучний інтелект також використовується в інших автономних транспортних засобах, таких як літаки, дрони та судна.

Один з конкретних прикладів застосування штучного інтелекту в фінансовій галузі – це системи автоматизованого трейдингу. Системи автоматизованого трейдингу можуть приймати рішення про купівлю та продаж акцій та інших фінансових інструментів на основі аналізу даних та

прогнозування тенденцій. Вони можуть адаптуватися до змін ринку та удосконалювати свої алгоритми навчання, щоб підвищити ефективність та точність прийнятих рішень. Ці системи забезпечують швидкість та точність прийнятих рішень, що дозволяє трейдерам отримувати прибуток та знижувати ризики в процесі торгівлі. Вони також можуть допомогти в зменшенні впливу емоцій та людських помилок на прийняття рішень у фінансових операціях.

Один з прикладів використання ШІ у комп'ютерних іграх – це глибинне навчання (deep learning), яке використовується для покращення поведінки інтелектуальних агентів у грі. Наприклад, в грі Starcraft II використовується система AlphaStar, що використовує глибинне навчання для створення штучного інтелекту, який може змагатися з гравцями на професійному рівні. AlphaStar здатний адаптуватися до різних стратегій гравців та навчатися новим технікам та стратегіям в грі. Інший приклад – це використання ШІ в іграх, які розвиваються в реальному часі, наприклад, в грі Dota 2. Тут інтелектуальні агенти використовують глибинне навчання та інші методи машинного навчання, щоб навчитися приймати рішення та прогнозувати поведінку гравців. Це допомагає створювати більш складні та високорівневі ігри, які створюють більш реалістичну та цікаву геймплей досвід для гравців.

Один з прикладів використання ШІ у політиці – це аналіз даних та прогнозування результатів виборів. Компанії, що займаються політичним маркетингом, використовують методи ШІ, такі як машинне навчання та аналітику даних, щоб дізнатися про поведінку виборців, їхні погляди на політичні питання, та відповідно до цього створювати стратегії для залучення голосів.

Але ШІ у наш час також доступний і звичайним людям, у 2022 році був «БУМ» різних ШІ, наприклад на сайті https://www.futurepedia.io/ зібрано більш ніж 1000 різних ШІ, найвідоміші з них – це ChatGPT, Midjourney, Pixai, Codeium, Dalle і т. д.

Наприклад, ChatGPT – це велика мовна модель, розроблена компанією OpenAI. Він здатен розуміти і генерувати тексти на різні теми. Його база знань

охоплює різні галузі знань, такі як наука, технології, культура та бізнес. Він може допомогти вам знайти відповіді на запитання, надати поради та виконувати інші завдання, що пов’язані з мовою та текстом. Зараз деякі студенти за допомогою його пишуть есе, реферати і т. д.

Midjourney, Pixai та DALL-E – це ШІ, які створюють цифрові зображення з описів природною мовою. Вводячи prompt (підказки), ШІ розуміє, що треба генерувати.

Character.AI втілює в життя мрію наукової фантастики про відкриті бесіди та співпрацю з комп’ютерами. На цьому сайті можна спілкуватись з персонажами з відеоігор, фільмів, аніме.

Недоліками штучного інтелекту в сучасному його розвитку є:

1) **Недостатня здатність до загальної розуміння**: Незважаючи на значний прогрес у розвитку ШІ, він все ще має деякі обмеження в розумінні тонких моментів та контекстуальних відтінків, що можуть викликати помилки та неправильні висновки.
2) **Проблеми з етикою та безпекою**: У зв’язку зі збільшенням використання ШІ у різних галузях, виникають етичні та безпечні проблеми, такі як порушення приватності, зловживання даними, та несумісність з міжнародними нормами.
3) **Висока вартість та складність**: ШІ є досить складною технологією, що потребує значних інвестицій у дослідження та розробку. Окрім того, використання ШІ також може вимагати додаткової інфраструктури та спеціалізованого обладнання, що може бути досить дорогим.
4) **Потенційна загроза для робочих місць**: Розвиток ШІ може призвести до автоматизації багатьох видів робіт, що може призвести до зниження попиту на робочу силу та загрози для економічної стабільності.
5) **Проблеми з надійністю та непередбачуваність**: Незважаючи на великий потенціал ШІ, він все ще може бути досить непередбачуваним та нестабільним, що може призвести до помилок та втрати даних.

Підводячи підсумки, то стає зрозумілим, що у майбутньому, розвиток ШІ,

має потенціал розширити наші знання про світ, вирішити складні проблеми та створити нові можливості для людства. Однак, ми повинні залишатися свідомими та обачними щодо наслідків використання ШІ і продовжувати дослідження та розуміння цієї технології, щоб забезпечити її безпеку та використання для блага людства.

**Список використаних джерел**


1. Welcome to ChatGPT. URL: https://chat.openai.com/chat (дата звернення: 05.03.2023).
2. URL: https://www.youtube.com/watch?v=csIxOuVNf3s (дата звернення: 05.03.2023).
3. URL:https://www.youtube.com/watch?v=OQGdrezi0Y4&list=RDFGeaG4eL4OY&index=2 (дата звернення: 05.03.2023).


## ШАХРАЙСТВО В ІНТЕРНЕТІ


*Андріуца М. М.*
*wipietrampit813@gmail.com*
*Черкаський державний бізнес-коледж*
*Науковий керівник: Захарова М. В.*
*м. Черкаси, Україна*


Шахрайство в інтернеті – це заволодіння чужим майном за допомогою введення в оману або зловживання довірою іншої людини. Цей вид шахрайства відрізняється тим, що особа, яка заволодіває чужим майном, використовує підроблені документи або імітує чиїсь повноваження або довіру. Це може включати підроблення підписів, використання скомпрометованих аккаунтів електронної пошти або соціальних мереж, а також імітацію чужої особистості за допомогою інтернет-шахрайства або фішингу. Відмінністю цього виду шахрайства є те, що заволодіння майном відбувається без примусу або насильства, а шахраї використовують довіру інших людей для досягнення своєї мети.

Види шахрайства в інтернеті п’ять найпоширеніших схем:

1) Фішинг;
2) Шахрайство з кредитними картами;
3) Фіктивні інтернет-магазини;
4) Пропозиції допомоги в погашенні боргу;
5) Пропозиції швидкого заробітку;

**Фішинг.** Є одним з найпоширеніших видів шахрайства в Інтернеті. Це підробка веб-сторінок, електронних листів або повідомлень з метою шахрайського заволодіння особистою інформацією користувачів. Найчастіше фішинг використовують для крадіжки логінів та паролів, банківських реквізитів, номерів кредитних карток тощо.

Зазвичай фішинг-атаки відбуваються через електронну пошту, де відправники надсилають листи від імені відомих компаній або сервісів, запрошуючи користувачів перейти за посиланням на підроблену сторінку, де їх просять ввести свої дані. Іноді фішери використовують соціальну інженерію, щоб переконати користувачів у необхідності надати свої дані.

Щоб запобігти стати жертвою фішингу, необхідно бути дуже уважним під час відкриття пошти від незнайомих відправників, особливо якщо вона містить посилання. Також варто перевірити, чи відповідає адреса електронної пошти або URL-адреса веб-сайту дійсному домену компанії. Якщо користувач отримав підозрілий лист або повідомлення, ні в якому разі не слід надавати свої особисті дані або виконувати будь-які дії, краще повідомити про це відповідним органам.

**Шахрайство з кредитними картами**. Форма злочинної діяльності, яка полягає у використанні чужої кредитної картки без дозволу власника з метою отримання користі.

Існують різні способи шахрайства з кредитними картками в Інтернеті. Один з найпоширеніших - це крадіжка кредитної картки або її даних, наприклад, номеру картки, терміну дії та коду CVV2. Зловмисники можуть отримати доступ до цих даних через атаки на сайти, які зберігають інформацію про кредитні картки, або через відправлення шахрайських електронних листів,

що містять посилання на фіктивні вебсайти, які виглядають як офіційні сайти банків або інших фінансових установ.

Інший спосіб шахрайства з кредитними картами - це крадіжка фізичної картки. Це може статися через викрадення картки або зловмисники можуть отримати доступ до неї через крадіжку пошти або крадіжку даних зі смітників, де вони можуть знайти відомості про кредитні картки.

Після отримання даних про кредитну картку або самої картки, зловмисники можуть використовувати її для здійснення покупок в Інтернеті або для зняття грошей з банкоматів. Щоб запобігти шахрайству з кредитними картками, важливо виконувати певні заходи безпеки, такі як збереження своїх кредитних карток в безпечному місці, ніколи не розкривати свої дані кредитної картки в Інтернеті, не використовувати прості паролі, і вчасно сповіщати свій банк у разі крадіжки кредитної картки.

**Фіктивні інтернет-магазини.** Це сайти, що не мають реального товару або послуги, які пропонуються на сайті, і призначені для шахрайства та обману споживачів. Такі сайти часто створюються з метою збору особистої інформації про користувачів, крадіжки коштів з кредитних карток, розсилання спаму або вірусів, а також для продажу фальшивих або низькоякісних товарів.

Шахраї можуть створювати фіктивні магазини з виглядом реального бізнесу, з використанням знайомих брендів і логотипів, щоб привернути увагу споживачів. Для цього вони створюють професійно виглядаючий сайт з каталогом товарів, детальним описом і фотографіями товарів, підтвердженнями оплати та доставки. Однак, коли споживач робить замовлення і оплачує його, він не отримує товар або отримує товар низької якості, а свої кошти втрачає.

**Пропозиції допомоги в погашенні боргу**. Також відоме як «скам з боргами», це один з популярних видів шахрайства в Інтернеті. У цьому виді шахрайства злочинці під видом допомоги у погашенні боргів шукають людей, які перебувають у фінансовій скруті.

Шахраї зазвичай звертаються до людей, які взяли кредити або мають інші види боргу, з обіцянкою допомогти їм знайти спосіб погашення боргу за менші

гроші або уникнути сплати боргу взагалі. Шахраї можуть пропонувати різні послуги, такі як реструктуризація боргу, об’єднання боргів, зниження відсотків по кредитах і т. д.

Щоб привернути увагу потенційних жертв, шахраї можуть використовувати підроблені логотипи і назви відомих компаній, фальшиві рецензії та інші методи обману. Зазвичай злочинці просять жертв перерахувати гроші на їх банківський рахунок як забезпечення для отримання послуги, пропонованої шахраями.

Однак, після отримання грошей, шахраї можуть зникнути, залишивши своїх жертв зі значними фінансовими втратами. Крім того, жертви можуть втратити свої особисті та фінансові дані, що може призвести до подальшої крадіжки особистої інформації та шахрайства з їхнім ім’ям.

Щоб уникнути стати жертвою шахраїв, важливо бути обачними при отриманні пропозицій допомоги в погашенні боргів, особливо якщо вони надходять з незапрошених чи з невідомих джерел

**Пропозиції швидкого заробітку.** Є дуже поширеними в інтернеті, шахраї можуть використовувати різні схеми, щоб залучити людей до цих пропозицій.

Одна з найпоширеніших схем – це схема «піраміди», коли люди набираються до програми, яка пропонує заробляти гроші, рекрутуючи нових учасників. Зазвичай для того, щоб приєднатися до такої програми, людина повинна спочатку зробити платіж. Дана схема шахрайства працює, доки є нові учасники, які приєднуються і платять, але коли потік нових учасників вичерпуэться, схема розпадається, а ті, хто залишився останнім, втрачають свої гроші.

Інша поширена схема - обман з приводу роботи з дому. Шахраї можуть обіцяти легку роботу з високою оплатою, проте, зазвичай, людина повинна спочатку заплатити за «навчання» або «стартовий пакет». Після того, як людина заплатила, вона може отримати якісь документи або посилання на роботу, але це зазвичай не дає жодних реальних можливостей заробити гроші, або ж робота не відповідає тому, що обіцяли на початку.

Ще один тип шахрайства пов’язаний з онлайн-гральними сайтами, де шахраї обіцяють високі виплати від гри або виграші, які насправді не існують. Ця схема шахрайства може включати в себе вимоги оплати для отримання виграшів або запити особистої інформації та банківських даних, які можуть бути використані для викрадення грошей.

У результаті аналізу видів шахрайства в Internet можна виділити основні принципи запобігання шахрайству, а саме:

1) Не надавати особисті дані на незнайомих сайтах. Паспортні і платіжні дані, телефон, логін і пароль в інтернеті надавати тільки в разі 100% впевненості, що перебуваєте на офіційних сайтах. Наприклад, якщо оформляєте кредит онлайн на сайті Credit365, варто переконатися, що в адресі сайту немає помилок, а всі адреси і контакти збігаються з інформацією в інших джерелах.
2) Не робити великих передоплат при покупці в інтернет-магазині. Краще використовувати спосіб покупки – накладений платіж. Тоді можна отримати товар, оглянути його і після цього оплатити.
3) Не користуватися підозрілими сервісами або пропозиціями інших людей. Люди або сервіси, що пропонують швидкий заробіток або допомогу в рішенні кредитних труднощів часто виявляються шахраями.

**Список використаних джерел**


1. Western Union [Електронний ресурс]. Режим доступу: https://www.westernunion.com/ua/ua/fraud-awareness/fraud-types.html (дата звернення: 01.03.2023р.).
2. Volyn News [Електронний ресурс]. Режим доступу: https://www.volynnews.com/news/all/internet-shakhraystvo-iak-unyknuty-i-shcho-robyty-iakshcho-staly-zhertvoiu/ (дата звернення: 01.03.2023р.).
3. EMA [Електронний ресурс]. Режим доступу: https://www.ema.com.ua/citizens/cyber-safety-school/frend-frod/ (дата звернення: 01.03.2023р.).

4. Міністерство Юстиції України [Електронний ресурс]. Режим доступу: https://minjust.gov.ua/m/yak-ne-stati-jertvoyu-shahraiv-v-interneti-ta-scho-robiti-yakscho-vi-potrapili-u-pastku (дата звернення: 01.03.2023р.).

## РОЗВИТОК ШТУЧНОГО ІНТЕЛЕКТУ В УКРАЇНІ

*Литовченко В. О.*
*lytovchenko15@gmail.com*
*Черкаський державний бізнес-коледж*
*Науковий керівник: Фальченко Н. Г.*
*м. Черкаси, Україна*

Під штучним інтелектом розуміють галузь інформатики, одним із завдань якої є моделювання інтелекту людини штучним способом – за допомогою комп'ютера.

*Штучний інтелект* — дуже перспективна область досліджень, розвиток якої зумовлений досягненнями в комп'ютерній сфері. Можна вважати, що розповсюдження комп'ютерів та кібернетичних приладів, їх застосування для людських потреб будуть визначати рівень життя в наступному столітті. Висока продуктивність нових технологій значною мірою залежить від використання в них засобів штучного інтелекту.

Значний внесок у розвиток систем штучного інтелекту зробили В.М. Глушков, М.М. Амосов, О.Г. Івахненко, Л.А. Калужнін, О.І. Кухтенко, В.І. Скурихін та інші українські вчені.

Найперші винаходи українських вчених, які містили штучний інтелект:

1) *комп'ютерна система "Редактор формул із голосовим уведенням"*, яка дозволяє здійснювати комп'ютерний набір математичних формул без використання клавіатури і "миші". Користувач уводить інформацію за допомогою голосу.
2) *комп'ютерна система "Телефон із голосовим номеронабирачем"*, що дозволяє зв`язатися з абонентом шляхом вимовляння голосом його номера або імені – пароля, яке складається з одного слова.
3) *автономний робот «ІНТЕЛЕКТ-10»,* є прообразом майбутнього

автономного багатофункціонального робототехнічного пристрою, що використовувався головним чином, при виконанні рутинних, втомлюючих і не привабливих для людини робіт.

4) *робот «Інтелект-12»* призначений для заміни людини при виконанні небезпечної або рутинної роботи. Міг бути використаним у хімічно, радіаційно або бактеріологічне небезпечному середовищі, для роботи з вибухонебезпечними речами, для охорони тощо.
5) *комп'ютерна система автоматичного розпізнавання зон ультразвукової луногенності «КРУЇЗ»*. Головне призначення – підвищення якості діагностики в ультразвуковій медицині.
6) *крокуючий робот і системи керування* можуть слугували основою для побудови багатоагентної системи для проведення розвідки при рятувальних операціях.

Наразі, в світі є дуже поширеними різні чат-боти, чи програми з використанням штучного інтелекту. Одним з таких чат-ботів є *ChatGPT*, але мала кількість людей знає про його український аналог *Idearium.*

Idearium – це чат-бот зі штучним інтелектом для мобільних пристроїв. Його інтерфейс зручний та лаконічний. Чат-бот може спілкуватися з користувачами українською та ще 12 мовами. Але хоч застосунок доступний безкоштовно, на день надається тільки певна кількість спроб на те, щоб поставити питання і щось дізнатись від Idearium. В описі застосунку вказано, що це інструмент для натхнення та ідей. Але він підійде не тільки для мозкового штурму, але й для будь-яких інших питань.

Застосунок працює дуже просто: ставите питання – він знаходить відповідь. Чим більш розгорнуте питання, тим чіткіша відповідь. До прикладу, якщо запитати в цього застосунку – "що таке Idearium?". То можна дізнатися про етимологію слова "Ідеарій". Даний чат-бот з'явився в мережі інтернет 18 січня 2022 року.

Україна тісно пов'язана з розробками штучного інтелекту по всьому світі. Прикладом для цього став робот Макс, якого спроектували в Південній Кореї.

У вересні 2017 року на саміті IBM в Києві було представлено робота Макса, який міг підтримувати розмову, відповідати на питання та виконувати команди, задані у довільній формі. Усе це завдяки використанню суперкомп'ютера фірми IBM – Watson з когнітивною системою штучного інтелекту, основне завдання якої – розуміти питання, сформульовані природною мовою, і знаходити на них відповіді в базі даних.

На даний час штучний інтелект в Україні стрімко розвивається. Компанія Deep Knowledge Analytics склала рейтинг Artificial Intelligence Industry in Eastern Europe 2022 за кількістю компаній, що працюють у сфері штучного інтелекту. Україна входить до трійки лідерів серед країн Східної Європи. В Україні працює 57 компаній в галузі штучного інтелекту. Наша країна налічує 26 аутсорсинг-компаній, а у світі їх лише 226. Згідно з даними ресурсу LinkedIn, в країні понад 2 тис компаній-розробників у сфері штучного інтелекту. Більша частка розробок відведена на програмне забезпечення, інформаційні технології, чат-боти та розважальні продукти тощо.

Висновок: штучний інтелект – це наше майбутнє! І як би людство не старалося залишатися на першому місці, інноваційні технології постійно будуть випереджати його.

**Список використаних джерел**


1. Розвиток штучного інтелекту в Україні [Електронний ресурс].–Режим доступу: https://elartu.tntu.edu.ua/bitstream
2. Idearium [Електронний ресурс]. – Режим доступу: https://corgit.xyz/software/idearium-ukrainskyi-analoh-chatgpt
3. Форум Робототехніка[Електронний ресурс]. – Режим доступу: ck-oda.gov.ua/forum-robototehnika-v-nashomu-zhytti/
4. Вікіпедія [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/

# АНАЛІЗ РЕАЛІЗАЦІЇ ПРИСТРОЇВ ПЕРЕШКОДОСТІЙКОГО КОНТРОЛЮ НА ОСНОВІ ПРИНЦИПУ ПАРНОСТІ

*Олексієнко Т. О., Уперяка Р. А.*
*sergii.vl.burmistrov@ukr.net*
*Черкаський державний бізнес-коледж*
*Науковий керівник: Бурмістров С. В.*
*м. Черкаси, Україна*

Сучасні цифрові системи обчислювальних машин, як правило, є швидкодіючими і високопродуктивними. Швидкості їх роботи досягають нині десятків і сотень мільйонів операцій на секунду. Завдання, які вони виконують, можуть реалізуватись протягом кількох годин і навіть діб. У процесі вирішення завдань цифрові системи можуть виконувати мільярди операцій. Результат роботи може стати хибним, якщо в результаті хоча б однієї операції допущена помилка.

Помилка в роботі системи може носити або систематичний характер, що виникає внаслідок відмови, або випадковий, що виникає внаслідок збою – короткочасного порушення правильної роботи цифрової системи, що відбуваються, як правило, внаслідок перешкод, внутрішніх (флуктуації) та зовнішніх (електричні поля від іскріння, вібрації). Збої існують у будь-якій радіоелектронній апаратурі, але в деяких галузях техніки, таких як телебачення, радіомовлення, ними часто нехтують. В обчислювальній техніці треба боротися з помилками будь-якого виду, особливо в машинах, що забезпечують правильне функціонування пов’язаних з ними технічних пристроїв (космічних апаратів, ракет, технологічних установок, верстатів) і людських колективів (військових з’єднань, заводських підрозділів).

Таким чином, виникає актуальне завдання підвищення надійності роботи цифрових обчислювальних пристроїв в умовах практично неминучої появи відмов та збоїв. Як правило завдання вирішують двома шляхами:

Перший шлях – збільшення надійності окремих елементів вузлів та пристроїв машини. Даний шлях є досить ефективним, але він обмежується можливостями технології на даному етапі розвитку техніки, і не може

гарантувати абсолютну достовірність інформації, що передається.

Другий шлях – за допомогою виявлення та виправлення помилок, що виникають внаслідок збоїв. Цей шлях пов’язаний із введенням надлишковості в інформацію, що переробляється. Надлишковість може бути або тимчасовою, пов’язаною зі збільшенням часу вирішення задачі (у окремому випадку завдання може бути вирішено, наприклад, двічі) і вводиться програмним шляхом, будучи основою програмного контролю цифрових систем, або просторовою (структурною), що полягає у подовженні кодів чисел, в які вводяться додаткові (контрольні) розряди, та є основою апаратурного контролю цифрових систем. В першому випадку при збереженні розрядності відбувається затримка в часі при передачі інформації, а в другому випадку при збільшенні розрядності зберігається швидкість передачі інформації.

Завдання розробника, який визначив необхідність усунення помилок апаратним методом, зводиться до вибору такого коду, який за можливо меншої надлишковості забезпечує потрібну коригуючу здатність.

Щоб спростити вирішення поставленого завдання, потрібно накласти одне суттєве обмеження: вважати, що в кодових комбінаціях (машинних словах) можливі лише поодинокі помилки та неможливі помилки вищої кратності. В результаті отримано мінімальну кількість контрольних розрядів *n*-розрядних слів певної довжини (див. табл.1).

Таблиця 1. **Оптимальний розмір надлишкових машинних слів.**

| № пп | Розрядність машинного слова | Кількість контрольних розрядів | Розрядність надлишкового машинного слова | Відсоток контрольних розрядів машинного слова |
|---|---|---|---|---|
| 1 | 4 | 3 | 7 | 42,8 |
| 2 | 8 | 4 | 12 | 33,3 |
| 3 | 16 | 5 | 21 | 23,8 |
| 4 | 32 | 6 | 38 | 15,8 |
| 5 | 64 | 7 | 71 | 9,9 |

З аналізу таблиці видно, що із зростанням розрядності машинного слова

відсоток контрольних розрядів суттєво зменшується, але залишається складовою частиною надлишкового машинного слова (див. рис. 1). Вже при розрядності 1024 біти відсоток становить в районі 1%

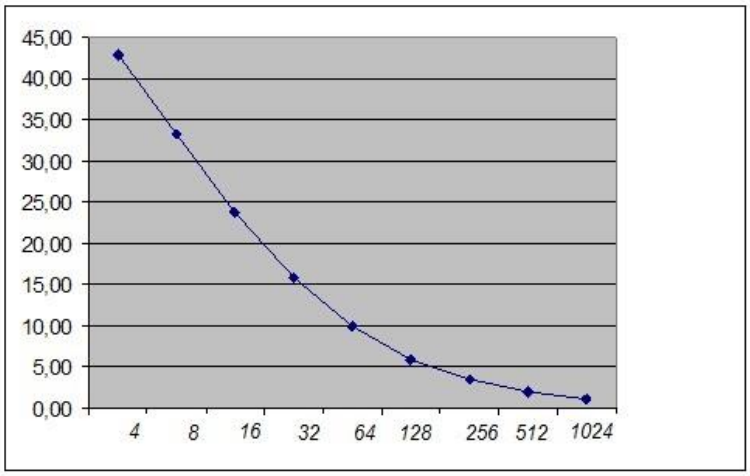



Рисунок 1. – Відсоток кількості розрядів контрольних сум в залежності від розрядності шини

Проаналізувавши теоретичні дані, що лежить в основі пристрою, визначено і обґрунтовано постановку задачі роботи.

Використовуючи коди Хемінга для виправлення помилок, що можуть виникнути при передачі інформації внаслідок зовнішніх впливів або флуктуацій, побудувати принципову схему пристрою для автоматичного виправлення помилок у восьмирозрядній шині цифрового пристрою.

Пристрій перешкодостійкого кодування восьмирозрядної шини на основі логічних елементів І-НЕ повинен складатись з двох складових частин: блоку передаючої частини та блоку прийомної частини (див. рис. 1).

Так як розрядність машинного слова становить 8 розрядів, розрядність відповідного надлишкового машинного слова повинна становить 12 розрядів. Причому контрольними розрядами є 1-ий, 2-ий, 4-ий та 8-ий розряди.

Передаюча частина добавляє в початкове вхідне слово

$$A_1(a_{1.1}, a_{1.2}, a_{1.3}, a_{1.4}, a_{1.5}, a_{1.6}, a_{1.7}, a_{1.8}),$$

що надходить із восьмирозрядної вхідної шини (інформаційні розряди), контрольні розряди $\boldsymbol{b_{1.01}}, \boldsymbol{b_{1.02}}, \boldsymbol{b_{1.04}}, \boldsymbol{b_{1.08}}$. Утворене надлишкове слово

$$B_1(\boldsymbol{b_{1.01}}, \boldsymbol{b_{1.02}}, b_{1.03}, \boldsymbol{b_{1.04}}, b_{1.05}, b_{1.06}, b_{1.07}, \boldsymbol{b_{1.08}}, b_{1.09}, b_{1.10}, b_{1.11}, b_{1.12})$$

передається по дванадцятирозрядній шині передачі інформації.

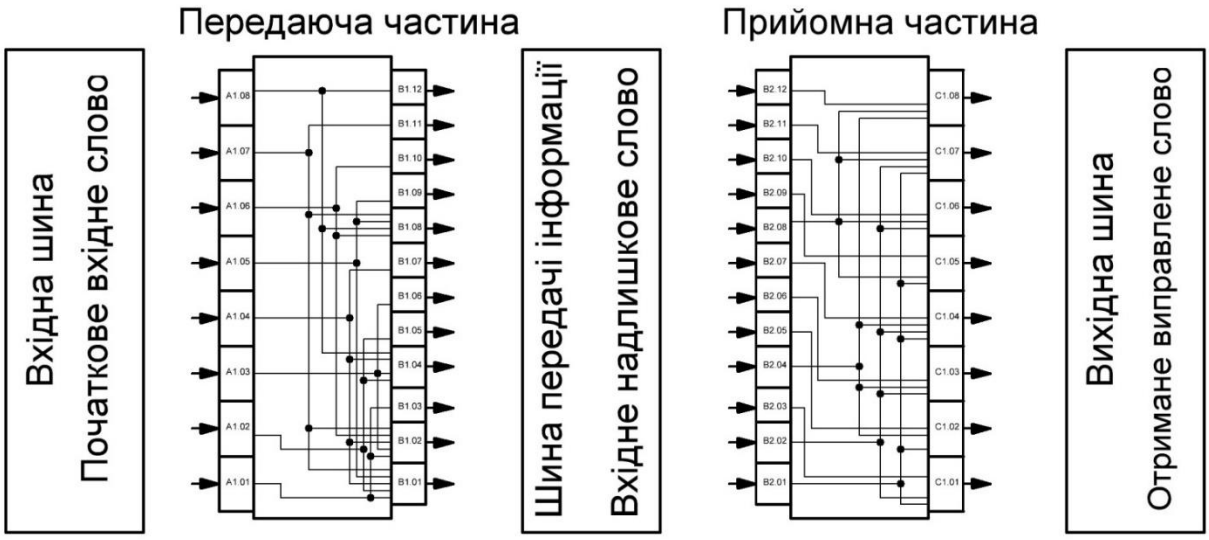



Рисунок 1. – Загальна структура пристрою

Прийомна частина отримує надлишкове слово

$$B_2(\boldsymbol{b_{2.01}}, \boldsymbol{b_{2.02}}, b_{2.03}, \boldsymbol{b_{2.04}}, b_{2.05}, b_{2.06}, b_{2.07}, \boldsymbol{b_{2.08}}, b_{2.09}, b_{2.10}, b_{2.11}, b_{2.12})$$

з дванадцятирозрядної шини передачі інформації, перераховує контрольні розряди $\boldsymbol{b_{2.01}}$, $\boldsymbol{b_{2.02}}$, $\boldsymbol{b_{2.04}}$, $\boldsymbol{b_{2.08}}$ і попарно порівнює їх з отриманими контрольними розрядами

$$b_{1.01} \overset{?}{=} b_{2.01}, b_{1.02} \overset{?}{=} b_{2.02}, b_{1.04} \overset{?}{=} b_{2.04}, b_{1.08} \overset{?}{=} b_{2.08}$$

і, при потребі у випадку виявлення одиничної помилки, відновлює початкове слово

$$C_1(c_{1.1}, c_{1.2}, c_{1.3}, c_{1.4}, c_{1.5}, c_{1.6}, c_{1.7}, c_{1.8}).$$

$A_1=C_1$ – основна умова передачі машинного слова – повне збереження інформації.

В результаті отримано принципову схему пристрою вказаної конструкції. Блок передаючої частини складається з 12 модулів. Схема містить 8 входів і 12 виходів. Кожний вихід має свою комбінаційну схему. Всі схеми об’єднані в 3 уніфіковані схеми.

Блок прийомної частини складається з 28 модулів. Схема містить 12 входів і 8 виходів. Кожний вихід має свою комбінаційну схему. Всі схеми об’єднані в 8 уніфікованих схем.

Характеристики блоку: Склад ІМС: К561ЛА7 – 602, К561ЛА9 – 92 штуки, К561ЛА8 – 85 штук. Кількість умовних транзисторів – 1520. Час затримки сигналу в пристрої 60 мкс при передачі сигналу і 120 мкс при прийомі сигналу.

**Висновки.** Розрахунки показують, що із зростанням розрядності шини цифрового пристрою для забезпечення такого ж часу затримки сигналу, що і у восьмирозрядній шині, кількість умовних транзисторів зростає в геометричній прогресії. Тому, незважаючи на зменшення долі контрольних сум при зростанні розряду шини, застосування методу парності контрольних сум не є перспективним.

## Список використаних джерел


1. Шило В. Л. Популярні цифрові мікросхеми. Довідник. Третє видання, виправлене. Київ: «Металургія». 1989. 352 с.: іл. (Масова радіо бібліотека. Вип.1112)
2. Рябенький В. М., Жуйков В. Я., Гулий В. Д. Цифрова схемотехніка. Львів: «Новий Світ-2000». 2009. 736 с.
3. Жабін В. І., Жуков І. А., Клименко І. А., Ткаченко В. В. Прикладна теорія цифрових автоматів. К.: НАУ. 2007. 364 с.


# ЗАГРОЗА ДЛЯ ПРИСТРОЇВ IoT


*Корнієнко А. Я.*
*nastykorni@gmail.com*
*Черкаський державний бізнес-коледж*
*Науковий керівник: Люта М. В.*
*м. Черкаси, Україна*


**Актуальність теми роботи.** На даний час світ інтернет речей постійно розвивається, та набуває популярності у використанні в побуті звичайних людей. Але окрім зручності у використанні потрібно тверезо оцінювати ризики та загрози, пов’язані з використанням цих технологій

**Метою** даної роботи є ознайомлення з ризиками та загрозами інтернет речей, зокрема з технологією Розумний будинок.

Пристрої IoT (Інтернет речей) стають все більш поширеними в нашому повсякденному житті, і хоча вони пропонують багато зручності та функціональності, вони також представляють значні проблеми з безпекою та загрози. Ось деякі з найпоширеніших:

1) Слабка автентифікація та авторизація: багато пристроїв IoT постачаються з іменами користувачів і паролями за замовчуванням, які широко відомі, що робить їх легкою мішенню для кіберзлочинців. У деяких випадках користувачі не змінюють ці облікові дані за замовчуванням, залишаючи свої пристрої вразливими для атак.
2) Уразливе програмне забезпечення та мікропрограми: пристрої IoT часто працюють із застарілим програмним забезпеченням і мікропрограмами, які можуть містити вразливості, якими можуть скористатися хакери. Виробники можуть не випускати оновлення та виправлення вчасно, залишаючи пристрої під загрозами протягом тривалого часу.
3) Відсутність шифрування: пристрої IoT можуть передавати дані через незашифровані канали, залишаючи конфіденційну інформацію вразливою для перехоплення та підслуховування хакерами.
4) Незахищені протоколи зв’язку: багато пристроїв Інтернету речей використовують незахищені протоколи зв’язку, такі як HTTP або FTP, які можуть перехоплюватися та маніпулювати зловмисниками.
5) Фізичні атаки: до пристроїв IoT можна отримати фізичний доступ і втрутитися в них, особливо якщо вони не захищені належним чином або розташовані в незахищених зонах.
6) Зловмисне програмне забезпечення та програми-вимагачі: пристрої IoT все частіше піддаються атакам зловмисного програмного забезпечення та програм-вимагачів, які можуть завдати значної шкоди як пристрою, так і мережі користувача.
7) Ботнети: пристрої IoT можна використовувати як частину ботнетів, які можуть запускати розподілені атаки на відмову в обслуговуванні (DDoS) або використовуватися для майнінгу криптовалюти.

Загалом зростаюча кількість пристроїв Інтернету речей та їх уразливості створили значні проблеми безпеці, які необхідно вирішити, щоб забезпечити безпеку та конфіденційність користувачів.

Розумні будинки – це системи підключених до Інтернету пристроїв, які дозволяють керувати різними аспектами домашнього життя, такими як освітлення, опалення, безпека тощо. Однак з'явилося багато вразливостей, якими можуть скористатися зловмисники, щоб зламати ці системи.

Деякі з найнебезпечніших вразливостей розумного будинку включають:

1) Неадекватна автентифікація та авторизація: багато пристроїв Інтернету речей мають слабкі або легко скомпрометовані паролі, які можуть дозволити зловмисникам отримати доступ до системи.
2) Програмне забезпечення, яке не підлягає виправленню: багато пристроїв IoT використовують застаріле програмне забезпечення, яке може містити вразливості, якими можуть скористатися зловмисники. Деякі виробники можуть не надавати оновлення чи виправлення, залишаючи пристрої під загрозами протягом тривалого часу.
3) Відсутність шифрування: пристрої IoT можуть передавати дані через незашифровані канали, залишаючи конфіденційну інформацію вразливою для перехоплення та підслуховування хакерами.
4) Незахищені протоколи зв'язку: багато пристроїв Інтернету речей, що використовуються в розумних будинках, використовують незахищені протоколи зв'язку, такі як HTTP або FTP, які можуть бути перехоплені зловмисниками та маніпулювати ними.
5) Фізичні атаки: до розумних домашніх пристроїв можна отримати фізичний доступ і змінити їх,особливо якщо вони не захищені належним чином або розташовані в незахищених зонах. Наприклад, хакер може отримати доступ до розумного замку, фізично маніпулюючи його проводкою або схемами.
6) Зловмисне програмне забезпечення та програми-вимагачі. Розумні домашні пристрої все частіше піддаються атакам зловмисного

програмного забезпечення та програм-вимагачів, які можуть завдати значної шкоди як пристрою, так і мережі користувача. Наприклад, атака програми-вимагача може заблокувати користувача в системі розумного дому, доки не буде сплачено викуп.

7) Бот-мережі: пристрої розумного дому можна використовувати як частину бот-мереж, які можуть запускати розподілені атаки на відмову в обслуговуванні (DDoS) або використовуватися для майнінгу криптовалюти.

**Висновки.** Загалом уразливості в пристроях розумного дому є значними ризиками, як для окремих користувачів, так і для великих мереж, оскільки вони можуть використовуватися як точки входу для зловмисників, щоб отримати доступ до конфіденційних даних або розпочати атаки на інші пристрої чи системи. Щоб зменшити ці ризики, виробникам важливо віддавати пріоритет безпеці при проектуванні та розробці пристроїв Інтернету речей, а користувачам – вживати заходів для захисту своїх пристроїв, регулярно оновлюючи програмне забезпечення та мікропрограми, використовуючи надійні паролі та вмикаючи шифрування, де це можливо. Крім того, заходи безпеки мережі, такі як брандмауери та системи виявлення вторгнень, можуть допомогти виявити та запобігти атакам на пристрої IoT. Ризик для конфіденційності та безпеки користувачів, а також для безпеки їхніх мереж і пристроїв. Оскільки розумні домашні пристрої стають все більш повсюдними та взаємопов’язаними, зростає ймовірність широкомасштабних атак. Щоб зменшити ці ризики, важливо, щоб користувачі дотримувалися найкращих практик, таких як зміна паролів за умовчанням, оновлення пристроїв за допомогою виправлень безпеки, використання шифрування та безпечних протоколів зв’язку та обмеження доступу до фізичних пристроїв. Виробники також зобов’язані віддавати пріоритет безпеці та конфіденційності користувачів. Зламаний розумний домашній пристрій може не тільки поставити під загрозу конфіденційність і безпеку будинку користувача, але також використовуватися як шлюз для доступу хакерів до інших пристроїв у мережі

користувача. Крім того, розумні домашні пристрої можуть збирати та передавати конфіденційні особисті дані, такі як місцезнаходження користувача та моделі активності, які можуть бути використані для зловмисних цілей, якщо їх перехоплять хакери.

Щоб усунути ці загрози, виробники пристроїв Інтернету речей повинні впровадити потужні заходи безпеки, включаючи безпечну автентифікацію, шифрування та протоколи зв'язку. Вони також повинні надавати регулярні оновлення програмного забезпечення та виправлення для усунення відомих вразливостей і дозволяти користувачам легко змінювати імена користувачів і паролі за умовчанням. Користувачі також можуть вживати заходів для захисту своїх розумних домашніх пристроїв, оновлюючи їх, використовуючи надійні паролі та мінімізуючи кількість особистих даних, які передаються через ці пристрої.

**Список використаних джерел:**


1. Internet of Things: A survey on the security of IoT frameworks.(2018) – [Електронний ресурс]. Режим доступу до ресурсу: https://www.scopus.com/record/display.uri?eid=2-s2.0-85034956984&origin=inward&txGid=37c46c8a89ed3b875d1535151abfcd20.
2. Серйозні недоліки, виявлені в кількох концентраторах розумного будинку: ваш пристрій серед них? – [Електронний ресурс]. Режим доступу до ресурсу: https://www.welivesecurity.com/2020/04/22/serious-flaws-smart-home-hubs-is-your-device-among-them/
3. Counting Down the Top Ten IoT Security Threats. IoT Evolution World. – [Електронний ресурс]. Режим доступу до ресурсу: https://www.iotevolutionworld.com/iot/articles/445972-counting-down-top-ten-iot-security-threats.htm

# Секція 2.

# ІНЖЕНЕРНІ ПІДХОДИ ДО РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

# ТЕХНІКИ ТА СТРАТЕГІЇ МОНЕТИЗАЦІЇ ІГОР

*Борозенець Д. А.*
*danyaborozenets2006@gmail.com*
*Черкаський державний бізнес-коледж*
*Науковий керівник: Марченко С. В.*
*м. Черкаси, Україна*

Монетизація та створення працездатної ігрової економіки нині є одним з ключових та пріоритетних напрямків у ході розробки ігрових додатків. Підходи до монетизації еволюціонують разом із засобами розповсюдження ігрових додатків до кінцевих гравців: багато нових ігор вимагають постійного підключення до мережі Інтернет або надаються за моделлю підписки, що вплинуло й на модель оплати. Таким чином, збалансована система монетизації є важливим інструментом залучення та утримання гравців, і протягом останніх десятиліть подібні системи постійно вдосконалювались, адаптувались під реалії ринку та задіювали новітні технології. У сучасні проєкти часто впроваджуються комплексні та неінтуїтивні системи монетизації, які використовують одразу декілька моделей. Звідси, окремий інтерес становить розгляд еволюції моделей монетизації та визначення ключових напрямків їх розвитку.

Традиційний метод монетизації – це отримання всього контенту гри шляхом єдиноразової оплати. Нині процес покупок відбувається на онлайн-платформах на кшталт Steam та Epic Games Store [1]. Недоліки даної моделі монетизації:

1) з високою ймовірністю пік доходу з гри прийдеться на перші місяці від релізу, після чого про неї забудуть, тобто проект не буде стабільно приносити гроші в далекій перспективі. Якщо компанія-розробник фокусується на розробці ігор саме з такою моделлю, то вона має постійно випускати нові проекти, щоб просто не стати банкрутом.
2) частина грошей втрачається через поширеність піратства, особливо у пострадянських країнах.

3) усі платять однакову ціну, тому люди, які потенційно витратили би на гру більше, не мають змоги це робити.

**DLC.** З часом розробники вирішили третю проблему за допомогою механізму DLC – додаткового контенту, який гравці можуть придбати після покупки основної гри. У більшості випадків DLC коштують менше, ніж, власне, гра, тим самим мотивуючи зацікавлених людей провести в ній ще більше часу. Деякі розробники зловживають цим: продають в DLC кінцівку сюжетної гри чи окремі ігрові механіки, що гравцями сприймається виключно негативно. Чим більш глибокий та реіграбельний проєкт, тим більш доречним та вдалим буде розробити під нього DLC. Тобто, DLC до одноразової сюжетної гри без великої кількості пов'язаних між собою геймплейних механік навряд чи зацікавлять гравців.

**Мікротранзакції.** Як правило, це маленькі за ціною покупки, які гравець може робити у грі для розблокування певного контенту. Ці покупки можуть бути як косметичними, не впливаючи на геймплей та прогрес гравця, так і навпаки [2]. Приклади косметичних мікротранзакцій: образи (скіни) для ігрових персонажів, емодзі, візуальні ефекти тощо. Однією з найпопулярніших практик у розробників мобільних ігор є так звані розхідні предмети (consumables). Це ресурси, які гравець постійно витрачає і які напряму впливають на швидкість його прогресу. Наприклад, у деяких іграх кожна дія витрачає енергію, відновлення якої треба або довго чекати, або заплатити. Дана система монетизації нині вважається застарілою [3]. Ще одним прикладом розхідних предметів у мобільних іграх є система прискорювачів, або ж бустерів. Гра навмисно змушує гравця чекати, поки, наприклад, необхідна будівля не добудується чи не зійде урожай, стимулюючи купити прискорювач, який скоротить нудний процес очікування у кілька разів. Дана система не блокує геймплей повністю – у цей час гравець все ще може займатися іншими ігровими активностями.

Головна перевага мікротранзакцій полягає в тому, що вони дуже дешеві та їх можна купляти постійно. Більшість людей, граючи в мобільну гру,

думають, що ніколи нічого в ній не придбають, проте вже після першої покупки для мозку така поведінка стане цілком нормальною, а зробити наступну покупку, навіть дорожчу, буде набагато легше. Саме цього добиваються розробники мобільних ігор.

**Лутбокси.** Є результатом еволюції мікротранзакцій та зараз інтегровані практично в будь-яку мобільну гру. Їх суть полягає в тому, що покупець не знає, що отримає – віртуальна винагорода визначається випадковим чином. У більшості ігор з даною системою є можливість відкривати лутбокси і за віртуальну валюту, щоб гра відчувалась більш чесною. Щоб мотивувати гравців купувати лутбокси, розробники розподіляють предмети, персонажів, картки чи будь-що інше, що випадає, на так звані типи рідкості, за якими визначається шанс на випадіння N-ого предмету [1]. Цілком справедливим є порівняння лутбоксів з казино, що дозволяє урядам країн на законодавчому рівні вважати даний метод монетизації гемблінгом.

Серед сучасних засобів монетизації ігор у мобільному геймінгу найбільш популярні техніки стосуються перегляду реклами. Зокрема, про це говорить відносно свіжа статистика щодо відповідних методів монетизації [4].

Додаткову цінність мають дослідження в галузі машинного навчання стосовно підходів до монетизації та залучення гравців. Ігрові додатки можуть збирати велику кількість інформації щодо своїх користувачів та прогнозувати на основі поведінки гравців ймовірність здійснення внутрішньоігрових платежів, припинення відвідування гри та ін. [5] Блокчейн-технології, зокрема модель розповсюдження NFT, можуть у перспективі теж суттєво вплинути на монетизацію сучасних ігор, оскільки розширюють товарно-грошові відносини на віртуальні об’єкти, у т. ч., створені для ігор чи згенеровані в них [6].

Розповсюдження та розвиток методів монетизації вже досить довгий час піднімає питання ігрової залежності та психології залучення гравців. Зокрема, протягом останніх років напрацьовується таксономія технологічних засобів, що призводять до адиктивних розладів поведінки у користувачів онлайн-сервісів [7]. Таким чином, монетизація ігор зачіпає широке коло питання у

галузі інформаційних технологій, економіки, юриспруденції та психології, що підкреслює значимість та перспективність досліджень у даному напрямку.

## Список використаних джерел


1. 7 Examples of Gaming Microtransactions – From Acceptable to Evil [Електронний ресурс]. Режим доступу: https://www.makeuseof.com/examples-of-gaming-microtransactions/ (дата звернення: 01.03.2023р.).
2. Video Game Monetization Models Overview [Електронний ресурс]. Режим доступу: https://rocketbrush.com/blog/game-monetization-models-overview (дата звернення: 01.03.2023р.).
3. How to set up Consumable and Non-consumable In-App Purchases [Електронний ресурс]. Режим доступу: https://qonversion.io/blog/setting-up-consumable-and-non-consumable-in-app-purchases/ (дата звернення: 01.03.2023р.).
4. Most used monetization methods for mobile gaming and non-gaming apps according to mobile publishers worldwide in 2021 [Електронний ресурс]. Режим доступу: https://www.statista.com/statistics/384215/app-developer-monetization-mix/ (дата звернення: 01.03.2023р.)
5. Mustac K. et al. Predicting Player Churn of a Free-to-Play Mobile Video Game Using Supervised Machine Learning // Applied Sciences, MDPI. 2022. Vol. 12. pp. 2795.
6. The Evolution of Gaming Monetization Models [Електронний ресурс]. Режим доступу: https://ancient8.gg/research/en/articles/the-evolution-of-gaming-monetization-models (дата звернення: 01.03.2023р.).
7. Flayelle M. et al. A taxonomy of technology design features that promote potentially addictive online behaviours // Nature Reviews Psychology. 2023. Vol. 2. pp. 136-150.

# СИСТЕМА АНАЛІЗУ МЕТЕОРОЛОГІЧНИХ ПОКАЗНИКІВ З АДАПТИВНИМ АЛГОРИТМОМ ПІДБОРУ ОПТИМАЛЬНОГО ВБРАННЯ ДЛЯ КОРИСТУВАЧА

*Драченко В. В.*
*valeradracenko418@gmail.com*
*Черкаський державний бізнес-коледж,*
*Науковий керівник: Захарова М. В.*
*м. Черкаси, Україна*

**Актуальність теми**. За останні роки активно зростає інтерес до розробки систем, які допомагають людям вирішувати повсякденні проблеми швидко та ефективно. Однією з таких проблем є вибір та підбір одягу, що підходить під метеорологічні умови. Метеорологічні умови можуть змінюватись протягом дня, що може ставити людей перед дилемою вибору між комфортом та стилем. У даній роботі досліджується вплив метеорологічних показників на вибір та підбір одягу.

**Мета** даної роботи полягає в розробці системи, яка б допомагала користувачам вибирати та підбирати одяг в залежності від метеорологічних показників, забезпечуючи комфорт та стиль.

Об’єктом дослідження є система, що допомагає вибирати та підбирати одяг в залежності від метеорологічних показників.

Предметом дослідження є алгоритми аналізу метеорологічних показників та підбору оптимального вбрання для користувача. Методи дослідження включають аналіз літературних джерел, розробку та тестування програмної системи.

Основна ідея розробленої системи полягає у підборі оптимального вбрання для користувача з урахуванням метеорологічних показників та чутливості користувача до змін температури. Система працює за принципом взаємодії з погодним API та адаптивним алгоритмом, який базується на особливостях користувача та показниках погоди. Після реєстрації та заповнення відповідної інформації, користувач отримує поради щодо вибору оптимального вбрання на

поточний день, що робить процес підготовки до виходу на вулицю більш зручним та ефективним.

Всередині програми відбувається запит на API (Application Programming Interface) погодного сайту, що дозволяє отримувати метеорологічні дані на поточний день [1]. На основі цих даних, а також інформації про користувача, в програмі застосовується адаптивний алгоритм підбору оптимального вбрання для користувача.

Розробка даної системи була здійснена з використанням фреймворку Ruby on Rails (RoR). RoR є відкритим програмним забезпеченням, яке дозволяє швидко створювати веб-додатки з використанням патерну Model-View-Controller (MVC). Цей фреймворк підтримує різноманітні бази даних та допомагає забезпечити безпеку додатків та оптимізувати їх продуктивність [2].

Розроблена система може бути корисною для широкого кола користувачів, які бажають підвищити комфорт свого перебування на вулиці та зменшити ризик захворювання, пов’язаного з некоректним вибором вбрання.

## *Висновки*

В роботі проведено аналіз технологій та алгоритмів, що використовуються для обробки та аналізу даних та досліджено особливості роботи з великими обсягами даних, що вимагають використання спеціалізованих інструментів та методів для їх оптимізації та ефективної обробки.

Результатом дослідження стали практичні рекомендації та розроблені моделі алгоритмів для обробки та аналізу даних. Виявлено, що використання стохастичних алгоритмів забезпечує ефективність та швидкість обробки великих обсягів даних, що є особливо важливим для сучасних досліджень.

Також, було проаналізовано технології, що використовуються для розробки програмного забезпечення для обробки даних, такі як Ruby on Rails та Sinatra. Результатом роботи стала реалізація веб-додатку на фреймворку Ruby on Rails для ефективної обробки та аналізу даних. Виявлено, що використання цієї технології дозволяє створювати ефективні та швидкі програмні продукти для обробки та аналізу даних.

Таким чином, використання стохастичних алгоритмів та технології розробки програмного забезпечення, такої як Ruby on Rails, є важливим для оптимізації та ефективної обробки великих обсягів даних. Результати даної роботи можуть бути корисні для дослідників та фахівців, які займаються аналізом даних та розробкою програмного забезпечення для їх обробки.

**Список використаних джерел**


1. Офіційна документація Ruby on Rails - Електронний ресурс. Доступ за посиланням: https://rubyonrails.org/
2. What Is an API? Definition and Examples - Електронний ресурс. Доступ за посиланням: https://www.howtogeek.com/343877/what-is-an-api/


## РОЗРОБКА ІНТЕРНЕТ-РЕСУРСУ ДЛЯ ОРГАНІЗАЦІЇ ТРАНСПОРТУВАННЯ ТВАРИН ЗАКОРДОН ДЛЯ ГО «КОТИКИ МУРКОТИКИ»


*Дудник В. Р.*
*dydvitrom@gmail.com*
*Черкаський державний бізнес-коледж*
*Науковий керівник: Хотунов В. І.*
*м. Черкаси, Україна*


**Актуальність теми** розробки інтернет-ресурсу для організації транспортування тварин за кордон для ГО «Котики муркотики» полягає в необхідності покращення інформування іноземних громадян про безпритульних домашніх тварин України, кількість яких стає більшою з кожним днем. На жаль, не кожна людина може знайти достатньо інформації про процедуру перевезення тварин за кордон, знайти надійного перевізника та забезпечити комфортні умови для тварини в процесі перевезення, ГО «Котики муркотики» прагне допомогти цим тваринам, забезпечуючи їм можливість знайти нові родини в інших країнах. Розробка інтернет-ресурсу для організації процесу транспортування тварин за кордон є важливим кроком у досягненні цієї мети.

**Метою даної роботи** є розробка інтернет-ресурсу, який надасть інформацію про безпритульних домашніх тварин України та процес їх

транспортування за кордон. Цей сайт допоможе залучити іноземних громадян до прийняття участі у рятуванні тварин.

**Об'єктом аналізу** є процес транспортування безпритульних домашніх тварин за кордон та розробка інтернет-ресурсу, який забезпечить організацію цього процесу. Аналіз також включає дослідження потенційної аудиторії сайту та її потреб у домашніх тваринах.

**Предметом роботи** є розробка інтернет-ресурсу, який буде інформувати іноземних громадян про безпритульних домашніх тварин України та процес їх транспортування за кордон.

**Основною метою** цього ресурсу є забезпечення можливості для іноземних громадян придбати домашню тварину з України та забезпечення безпечного процесу транспортування її до нового місця проживання

Проведена робота виконана кількома етапами, розглянутими далі:

1. Був здійснений аналіз потреб та вимог користувача.
2. Була розроблена архітектура системи і були визначені потрібні інструменти та технології, які були використані, а також був створений детальний план роботи.
3. Система була реалізована розробниками, використовуючи обрані інструменти та технології, та були створені необхідні скрипти та конфігураційні файли, які допомогли згенерувати статичний веб-додаток.
4. Система була протестована та налагоджена розробниками, були перевірені всі вимоги та потреби користувача, та були виправлені будь-які помилки та недоліки.
5. Система була впроваджена на живому вебсайті розробниками.
6. Система підтримувалася та розвивалася розробниками.

Розробка системи відбувалась за методологією Scrum з спринтами довжиною в 1 тиждень, що дозволило максимально ефективно і швидко надати замовнику результат і отримати від нього зворотній зв'язок. Для розробки було вирішено використати наступний стек технологій: React, Next.js, Storyblok та Vercel, які є досить актуальним для розробки сучасних вебдодатків.

Основні переваги використання Storyblok полягають у тому, що це headless CMS з відкритим кодом, що дає можливість розробникам зосередитись на фронтенді додатку та отримати потужний інструмент для керування контентом.

React, з свого боку, є однією з найпопулярніших технологій для фронтенд-розробки, яка дозволяє розробникам створювати ефективні та гнучкі інтерфейси.

Next.js – це фреймворк на основі React, який дозволяє розробникам створювати високопродуктивні, SEO-оптимізовані та масштабовані веб-додатки, що є дуже важливим для великих та складних проектів, таких як інтернет-ресурс для транспортування тварин.

Нарешті, Vercel є хмарним сервісом розгортання та хостингу веб-додатків, який має дуже швидку швидкість розгортання та надійність, що дозволяє розробникам легко підтримувати та масштабувати свій проект. Використання Vercel дозволяє зосередитись на розробці проекту, не витрачаючи час на налаштування та управління серверами.

## *Висновки*

Розробка інтернет-ресурсу для організації процесу транспортування тварин за кордон для ГО "Котики муркотики" є важливим кроком у реалізації мети забезпечення безпритульним домашнім тваринам можливості знайти нову родину за межами України. Сайт допоможе залучити іноземних громадян до рятування тварин та забезпечить їм можливість придбати домашню тварину з України. Крім того, інформація, що міститься на сайті, сприятиме безпечному та відповідному процесу транспортування тварин закордон.

## *Список використаних джерел*


1. Офіційна документація React [Електронний ресурс] – Режим доступу до ресурсу: https://bit.ly/2QIv46G.
2. Офіційна документація Node.js. [Електронний ресурс] – Режим доступу до ресурсу: https://bit.ly/3ZMswb5

3. Офіційна документація Next.js [Електронний ресурс] – Режим доступу до ресурсу: https://bit.ly/3lbHBUz.
4. Офіційна документація Vercel [Електронний ресурс] – Режим доступу до ресурсу: https://bit.ly/3J9CD2A.
5. Офіційна документація Storyblock [Електронний ресурс] – Режим доступу до ресурсу: https://bit.ly/3T6BPjL.

# РОЗРОБКА СИСТЕМИ ГЕНЕРУВАННЯ СТАТИЧНОГО ВЕБДОДАТКУ ДЛЯ ОРГАНІЗАЦІЇ ТРАНСПОРТУВАННЯ ТВАРИН ЗАКОРДОН ДЛЯ ГО «КОТИКИ МУРКОТИКИ»

*Бесєдовський. Н. О.*
*besedovskiy7@gmail.com*
*Черкаський державний бізнес-коледж*
*Науковий керівник: Хотунов В. І.*
*м. Черкаси, Україна*

**Актуальність теми.** Розробка систем генерування статичного вебдодатку стає все більш актуальною в останні роки. Однією з причин є зростання обсягу даних, що обробляються вебдодатками. Статичний вебдодаток може допомогти зменшити навантаження на сервер та покращити продуктивність вебсайту.

**Метою проекту** є створення системи генерування статичного вебдодатку для організації, яка дозволяє автоматизувати процес створення вебсторінок та забезпечити їх швидку та надійну роботу. Основні завдання проекту включають:

1.Розробка скриптів для отримання даних з джерел зберігання даних.

2.Розробка системи шаблонів для генерування вебсторінок.

3.Розробка скриптів для генерування статичних файлів вебсайту на основі даних та шаблонів.

**Об’єктом аналізу та дослідження у ході проведеної роботи** став процес генерування HTML коду на основі БД.

**Предметом роботи с**тала систем генерування статичного вебдодатку.

Проведена робота виконана кількома етапами, розглянутими далі.

Був проведений аналіз потреб та вимог користувача шляхом дослідження документації та інформації про організацію, що надавала основний контекст проекту. Після збору всієї необхідної інформації, вимоги були узагальнені та відсортовані з метою виділення ключових потреб та вимог, що були необхідні для реалізації проекту. Далі, на основі цих вимог, була розроблена стратегія проекту та визначено основні функціональні вимог.

Була розроблена архітектура системи, яка передбачала логічне розбиття функцій та даних на компоненти, що відповідали за різні аспекти функціонування системи. Для цього були використані різноманітні підходи до проектування, включаючи об’єктно-орієнтований та функціональний підходи.

Далі, були визначені потрібні інструменти та технології, які необхідні для реалізації проекту, такі як мови програмування, фреймворки, сервіси баз даних, сервіси хостингу та інші. Для вибору цих інструментів та технологій, було проведено дослідження, яке базувалось на потребах та вимогах користувача, а також на попередніх досвіді розробки схожих систем. Були розглянуті різні варіанти технологій та інструментів, що відповідали вимогам проекту, та здійснено вибір тих, які найкраще відповідали вимогам проект.

Це технічний стек для розробки веб-додатку. Основні компоненти:

- JS: JavaScript – це мова програмування, яка використовується для створення динамічних вебсторінок та вебдодатків.
- Storyblok: це головним чином CMS (Content Management System), яка дозволяє розробникам та контент-менеджерам легко керувати та публікувати контент в реальному часі.
- React: це JavaScript-бібліотека, яка використовується для створення користувацьких інтерфейсів, основаних на компонентах. Вона забезпечує ефективне відображення та взаємодію з даними.
- Next.js: це фреймворк для рендерингу на стороні сервера, який побудований на основі React. Він дозволяє створювати швидкі та ефективні веб-додатки з підтримкою серверного рендерингу.

– SCSS: це мова стилів на основі CSS, яка містить додаткові функції та можливості, такі як змінні, вкладені селектори та міксіни.
– HTML: HTML (HyperText Markup Language) – це мова розмітки, яка використовується для створення веб-сторінок та їх структури.
– CSS: CSS (Cascading Style Sheets) – це мова стилів, яка використовується для опису зовнішнього вигляду вебсторінок.
– Vercel: це платформа для розгортання та хостингу веб-додатків, яка забезпечує швидку та легку розгортання на основі Git.

Були створені необхідні скрипти та конфігураційні файли, які допомогли згенерувати статичний веб-додаток. Цей етап включає в себе кодування та тестування функціональності системи, а також налагодження її роботи, щоб забезпечити правильну генерацію статичного вебдодатку. Результатом цього етапу є готовий статичний вебдодаток, який був розгорнутий на Vercel.

Система була протестована та налагоджена, були перевірені всі вимоги та потреби користувача та були виправлені будь-які помилки та недоліки.

## *Висновки*

В результаті виконання роботи було розроблено систему генерації статичного веб-додатку для організації. Було проведено аналіз потреб та вимог користувача, розроблена архітектура системи, визначені необхідні інструменти та технології, створений детальний план роботи, а також реалізована система за допомогою створених скриптів та конфігураційних файлів. Отриманий статичний веб-додаток розроблений з використанням таких технологій, як JS, Storyblok, React, Next.js, SCSS, HTML, CSS та був розміщений на Vercel для публікації в Інтернеті. В ході виконання роботи були виконані поставлені завдання та досягнена мета роботи. Також були закріплені теоретичні знання та вдосконалені практичні навики.

## *Список використаних джерел*

1. Офіційна документація React. [Електронний ресурс]. Доступно: https://reactjs.org/docs/getting-started.html

2. Офіційна документація Node.js. [Електронний ресурс]. Доступно: https://nodejs.org/en/docs/

# Секція 3.

# ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ГАЛУЗЕВИХ РІШЕННЯХ

# СУЧАСНІ ТЕХНОЛОГІЇ, ЯКІ МОЖУТЬ ВИРОБЛЯТИ ШТУЧНУ ЇЖУ. ЧОМУ ЦЕ ВАЖЛИВО ТА АКТУАЛЬНО ДЛЯ НАС?

*Кітораги В. О.*
*kitiv25@gmail.com*
*Черкаський державний бізнес-коледж*
*Наукові керівники:*
*Люта М. В., Житнич К. Г.*
*м. Черкаси, Україна*

Зважаючи на широке поняття теми «Сучасні технології», є багато галузей, які можуть бути включені в цю тему. Однією з них є біотехнологія, яка охоплює використання живих організмів та їх компонентів для вирішення проблем в різних сферах.

Біотехнології можуть вирішити багато сучасних проблем, таких як:

1) Використання генетичного інженерінгу для створення нових видів рослин і тварин з більш ефективними властивостями, такими як високий вміст білка або мінералів;
2) Використання біотехнології в сільському господарстві для поліпшення врожаїв, контролю шкідників та забезпечення безпеки харчових продуктів;
3) Вплив біотехнології на довкілля, зокрема на створення біорозкладаючих матеріалів та виробництво біопалива;
4) Використання біотехнології в космічних дослідженнях, зокрема вирощування рослин та проведення дослідів з бактерій на космічних станціях;
5) Використання мікроорганізмів для виробництва біопродуктів та штучної їжі.

Це лише деякі приклади, але біотехнології можуть включати багато інших аспектів, таких як клінічні дослідження, технології обробки води, тощо. І з усього вище написаного я хочу розповісти саме про використання біотехнологій для вироблення штучної їжі.

**Біотехнології створення їжі** – це галузь, що досліджує використання живих організмів та їх складових частин для створення нових продуктів харчування. Наприклад, генетично модифіковані організми використовують

для отримання більш стійких до хвороб та шкідників рослин, що забезпечує більший врожай та зменшення використання пестицидів. Також біотехнології дозволяють вирощувати штучне м’ясо та інші продукти, що може мати позитивний вплив на екологію та здоров’я людей.

Сучасні технології створення штучних продуктів харчування, таких як м’ясо та риба, базуються на використанні клітинної культури. Цей процес називається **«клітинна агрокультура»** і полягає в тому, що відбувається вирощування клітин на спеціальних середовищах, що містять необхідні харчові компоненти та інші речовини.

У випадку створення штучного м’яса, для отримання клітин використовуються зразки живої тканини тварин, зокрема корів та курей. Клітини зразків розмножуються в спеціальних умовах і переростають в шари м’якоті, що відповідають структурі натурального м’яса. Потім ці шари збираються та складаються в білкову гелеву матрицю, яка надає продукту вигляд та консистенцію м’яса.

Щодо створення штучної риби, то використовуються ті ж принципи. Клітини зразків риби вирощуються на спеціальних середовищах та переростають в різноманітні види тканин, що відповідають структурі риби. Однак, для отримання більш складних структур, таких як органи риби, потрібно використовувати більш складні технології, такі як біопринтинг, який дозволяє створювати тривимірні структури з клітин.

Інші штучні продукти харчування, такі як молочні продукти та яйця, можуть бути створені за допомогою генетичної інженерії. Наприклад, молоко може бути отримане зі спеціально модифікованих клітин грибів.

Процес створення штучного м’яса та інших продуктів зазвичай здійснюється за допомогою біотехнологій, таких як культивування клітин тварин у штучних умовах. Для цього звичайно використовуються спеціальні пристрої-біореактори або культиватори, які забезпечують оптимальні умови для розвитку клітин.

**Біореактор** – це пристрій для культивування клітин, мікроорганізмів або

тканин у контрольованих умовах. Він складається з різних компонентів, таких як резервуар для культивування, датчиків тиску, температури та pH, системи змішування, системи подачі поживних речовин та інших факторів.

Інші пристрої, такі як тканинні інженерні камери, також можуть використовуватися для створення штучних продуктів. Вони працюють на основі культивування тканин у контрольованих умовах і можуть відтворювати форму та структуру різних продуктів, таких як м’ясо, риба та інші продукти.

За допомогою цих технологій можна створювати продукти, що мають високу біологічну цінність та не містять шкідливих речовин, таких як антибіотики або гормони. Крім того, вони можуть бути створені без використання тварин та зменшити вплив людської діяльності на навколишнє середовище.

Хоча ці технології ще не повністю розвинуті, вони можуть бути важливим кроком у напрямку створення більш екологічно чистих та здорових продуктів для споживачів.

Чому це нам потрібно:

- Розвиток нових технологій у сфері створення штучних продуктів їжі дозволяє зменшити вплив на довкілля, збільшити доступність їжі та зменшити витрати на її виробництво.
- Створення штучних продуктів їжі на базі рослин, грибів та інших натуральних інгредієнтів дозволяє зменшити споживання м’яса, що може бути корисно для здоров’я людей та допомогти знизити витрати на виробництво м’яса.
- Штучне м’ясо та риба можуть бути створені з використанням стовбурових клітин тварин, що дозволяє зменшити кількість вбивства тварин та збільшити безпеку харчування.
- Сучасні технології створення штучних продуктів їжі можуть вирішити проблему дефіциту продуктів у важкодоступних районах, де традиційне виробництво їжі неможливе.

– Штучні продукти їжі можуть бути створені з використанням новітніх технологій, таких як 3D-друк, що дозволяє створювати продукти різної форми та текстури.

Підводячи підсумки, стає зрозумілим, що біотехнології стали необхідністю у сучасному світі, де стикаємося з проблемами як зміна клімату, перенаселення та інші. Ці технології допомагають покращувати життя людей, зменшувати негативний вплив на навколишнє середовище та підтримувати економічний розвиток. А біотехнології у створенні нових продуктів, зокрема штучного м’яса та риби, дозволяють зменшити негативний вплив тваринництва на навколишнє середовище та поліпшити глобальну екологічну ситуацію. Завдяки новим технологіям можна ефективно створювати більше продуктів з меншої кількості ресурсів, що сприяє збереженню природних ресурсів та зменшенню негативного впливу на довкілля. Усі ці технології потребують досліджень та розробок, а також етичного врахування можливих наслідків застосування. Однак, важливо розуміти, що біотехнології мають великий потенціал для покращення нашого світу та стануть ключовим фактором у подальшому розвитку технологій.

## Список використаних джерел


1. М’ясо з пробірки. Історія та перспективи вирощування м’яса в лабораторії URL: https://nauka.ua/amp/myaso-z-probirki-istoriya-ta-perspektivi-viroshchuvannya-myasa-v-laboratoriyi
2. Супер їжа – штучне м’ясо – Агробізнес сьогодні. URL: http://agro-business.com.ua/agro/idei-trendy/item/19217-superizha-shtuchne-miaso.html
3. М’ясо з пробірки – NiNa.Az URL: https://www.wiki-data.uk-ua.nina.az/%D0%9C%27%D1%8F%D1%81%D0%BE_%D0%B7_%D0%BF%D1%80%D0%BE%D0%B1%D1%96%D1%80%D0%BA%D0%B8.html

# ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У СФЕРІ ТУРИЗМУ. ЧОМУ ЦЕ ВАЖЛИВО ТА АКТУАЛЬНО ДЛЯ НАС?

*Поліщук О. В.*
*cukerochka07@gmail.com*
*Черкаський державний бізнес-коледж*
*Науковий керівник: Люта М. В.*
*м. Черкаси, Україна*

Створення нових інформаційних технологій має велике значення для розвитку суспільства. Вони активно перетворюють інші технології матеріального і нематеріального виробництва, в кінцевому підсумку формуючи новий стиль роботи, спосіб життя в цілому. ***Суть інформаційних технологій становлять методи і засоби формування та підтримки інформаційних потоків у системах управління об'єктами, у тому числі, підприємствами сфери туризму.***

Для успішної діяльності туристичної фірми необхідно використовувати постійний потік правдивої і своєчасної інформації для прийняття важливих управлінських рішень з метою досягнення очікуваного кінцевого результату - отримання прибутку. У зв'язку з тим, що інформацією учасники туристського ринку обмінюються протягом дня, виникає необхідність у вмінні збирати, опрацьовувати її. Внаслідок входження України до світової мережі інформаційних комунікацій поступово вдосконалюються умови функціонування інформаційних систем, зокрема, розроблена державна програма інформатизації, формується нормативно-правова база, збільшується кількість підприємств інформаційної інфраструктури, поліпшується якість каналів зв'язку, урізноманітнюються технічні засоби та інформаційні технології активізації інформаційних систем**. Індустрія туризму ідеально пристосована для впровадження сучасних ІТ**, тому за останні десятиліття зазнала значного впливу науково-технічного прогресу. Система ІТ у туризмі охоплює інформаційні системи менеджменту, глобальні системи бронювання, мультимедіа, інтегровані комунікаційні мережі.

Основними складовими розвитку інформаційних технологій в галузі

туризму є:

1. *Інформаційна інфраструктура.*
2. *Бази даних туристичного профілю.*
3. *Сайти і портали туристичного профілю в мережі Інтернет.*
4. *Електронний маркетинг.*
5. *Рекламна діяльність.*
6. *Автоматизація діяльності туристичних організацій.*
7. *Автоматизація керування діяльністю сфери туризму.*

Серед найважливіших досягнень сфери туризму стала її *комп'ютеризація.* Завдяки використанню ресурсів персонального комп'ютера та каналів зв'язку було дано перший поштовх до всесвітньої інтеграції баз даних та внутрішніх систем бронювання. Удосконалювалося і програмне забезпечення взаємодії між туроператором та турагентом. Така система зручна для зв'язку туристичних підприємств, що знаходяться в різних часових поясах, економить час та ресурси турагента.

Крім глобальних дистриб'юторських систем, отримати інформацію про послуги готелів, забронювати номери можна за допомогою *публічних інформаційних порталів та власних сторінок* в Інтернеті. Спеціалізовані web-сторінки містять інформацію про туристичні послуги, оформлення й відправлення замовлень, оформлення документів у режимі он-лайн для розрахунків традиційним шляхом з використанням стандартних засобів. Однією з новітніх технологій є використання *електронного довідника-каталогу,* до функцій якого входить вибір туристичного продукту, автоматизованих агентств, оформлення замовлення.

Для швидкого і безпомилкового контролю, повноцінного аналізу існуючої ситуації, швидкості і повноти обслуговування клієнта неминучим і незамінним стає *впровадження автоматизованих систем управління (АСУ)*.

*Системи управління продаж послуг* споживачу - це сучасний підхід до управління відділом реалізації і вирішення питань з організації і проведення заходів. Важливою тенденцією розвитку міжнародної туристичної індустрії

останніх років стало активне *використання систем оптимізації прибутку.* Ця система працює в реальному часі, аналізує отриману від системи управління туристичною фірмою інформацію, враховує специфіку сегментів ринку і проведені реконструкції по ціноутворенню та управлінню тарифами. Автоматизація управління діяльністю туристичної фірми тісно пов'язана із *системою збору та аналізу зовнішньої поточної інформації.* Ці процеси мають комплексний характер і охоплюють усі сторони функціонування туристичної фірми і взаємин з клієнтами.

В наш час, за яскраво вираженої невизначеності, стохастичності зовнішнього середовища необхідною властивістю туристичної фірми виступає її здатність до адаптації. Висока надійність і забезпечення стійкості - один із фундаментальних принципів її функціонування. *Позитивними* сторонами (перевагами) впровадження в практику роботи турфірми автоматизованої інформаційної системи з управління є:

- зниження тривалості операційного циклу;
- своєчасна корекція асортименту послуг, що надаються;
- скорочення витрат ресурсів та вирішення ряду інших завдань.

Одним з останніх досягнень у запровадженні інформаційних технологій в сферу туризму стало намагання створити в мережі Інтернет *єдиний інформаційний простір,* доступний як туристичним підприємствам, так і іншим організаціям, що беруть участь в забезпеченні туристичного процесу, а також і самим туристам. У зв'язку з цим створюються туристичні інформаційні системи, які відкривають безмежні можливості для взаємодії та ведення бізнесу в режимі реального часу. В Україні теж створено автоматизований інформаційно-рекламний центр "Українська туристична інформаційна система", що має вихід в Інтернет. Це – суттєвий крок у напрямку створення українського інформаційного туристичного простору та його інтеграції у світовий інформаційний туристичний простір.

**Висновки**

Туристичний бізнес остаточно переходить на технологічні методи роботи,

так як автоматизація дозволяє значно прискорити виконання багатьох завдань, що стоять перед турфірмою, економити грошові кошти, підвищити ефективність роботи як кожного туроператора окремо, так і усього туристичного бізнесу в цілому. Це прямо впливає на конкурентноздатність фірми на ринку послуг в наш час. Тому дані процеси є вкрай актуальними для українського туристичного бізнесу. Використання мережі Інтернет, Інтернет-технологій, програмних продуктів наскрізної автоматизації всіх бізнес-процесів туристичного бізнесу сьогодні не просто питання лідерства і створення конкурентних переваг, але і виживання на ринку послуг в найближчий час. Для прискорення впровадження новітніх інформаційних технологій у туризмі бажана державна фінансова підтримка науково-дослідних і практичних розробок.

**Список використаних джерел**


1. Інформаційні технології в туризмі. URL: https://tourlib.net/books_ukr/vt5-1.htm (дата звернення:05.03.2023)
2. Сучасні технології в туризмі. URL: https://tourlib.net/statti_ukr/kudinova2.htm (дата звернення:05.03.2023).


## БЕЗПЕКА ІНТЕРНЕТ-БАНКІНГУ В УКРАЇНІ: ПРАКТИЧНІ АСПЕКТИ


*Скубій Є. В.*
*yevgeniyaskubiy@gmail.com*
*Черкаський державний бізнес-коледж*
*Науковий керівник: Люта М. В.*
*м. Черкаси, Україна*


**Вступ.** В останні роки банківська система нашої країни переживає бурхливий розвиток. Пройшли часи, коли можна було легко заробляти на спекулятивних операціях з валютою та шахрайстві. Сьогодні все більше банків робить ставку на професіоналізм своїх співробітників і нові інформаційні технології. За твердженнями експертів, основна і найголовніша загроза, яка чатує на будь-якого користувача Інтернет-банкінгу - це ризик шахрайського злому і несанкціонованого доступу до коштів на рахунку. «Єдиною істотною

небезпекою, яка може підстерігати користувачів цих систем, є ризик протиправного заволодіння їх коштами зловмисниками, з використанням можливостей систем «Інтернет-банкінгу».

**Системи дистанційного надання банківських послуг клієнтам**. Технологія дистанційного банківського обслуговування (ДБО) клієнтів.

*Види ДБО*:

- Система "Клієнт-банк" (структура файлів електронних платіжних документів, файлів-квитанцій, файлів-виписок з поточного рахунку клієнта; поняття статусу електронного платіжного документа і його зміна в процесі обробки на АРМ клієнт і АРМ-банк)
- Система "Інтернет-банкінг" (склад функціональних модулів та їх взаємодія; розвиток спектру послуг для клієнтів на прикладі системи "Приват24"; переваги для банків і клієнтів)
- Система "Мобільний банкінг" (характеристики систем мобільних платежів, використовуваних українськими банками; типи мобільних банківських послуг)

**Інформаційні технології, що використовуються в банківській діяльності.**

- Бази даних на основі моделі «клієнт-сервер» (характерне використання ОС Unix та БД Oracle).
- Засоби міжмережевої взаємодії для міжбанківських розрахунків.
- Служби розрахунків, повністю орієнтованих на Internet, або, так звані, віртуальні банки.
- Банківські експертно-аналітичні системи, що використовують принци штучного інтелекту і багато іншого

**Основні функції банківських систем.**

- Автоматизація всіх щоденних внутрішньобанківських операцій, ведення бухгалтерії та складання зведених звітів.
- Системи комунікацій з філіями та іногородніми відділеннями.

- Системи автоматизованого взаємодії з клієнтами (так звані системи "банк-клієнт").
- Аналітичні системи. Аналіз всієї діяльності банку та системи вибору оптимальних у даній ситуації рішень.
- Автоматизація роздрібних операцій - застосування банкоматів і кредитних карток.
- Системи міжбанківських розрахунків.
- Системи автоматизації роботи банку на ринку цінних паперів.
- Інформаційні системи. Можливість миттєвого отримання необхідної інформації, що впливає на фінансову ситуацію.

**Система захисту та безпеки інформації в банківській системі передбачає наявність:**

**Шифрування даних.** На сьогодні вже всіма банками, які надають послугу Інтернет-банкінгу, застосовується SSL-шифрування даних, що передаються від комп'ютера користувача в систему банку і назад. Цей захід безпеки дозволяє виключити поширений раніше вид шахрайства «man in the middle»: дані про платіж перехоплювалися на етапі, коли вони відправлені від клієнта, але ще не дійшли в банк, шахрай міняв дані і тільки після цього відправляв їх в банк. Щоб скористатися всіма перевагами захищеної передачі даних, слід дотримуватися елементарних заходів безпеки в Інтернеті - не реагувати на підозрілі повідомлення (отримані нібито від вашого банку) і не переходити з невідомих посиланнях.

**Одноразові паролі, одержувані в банкоматі.** При такій системі захисту, крім звичайного логіна і пароля, для входу в систему і підтвердження операцій користувач повинен ввести одноразовий пароль. З точки зору безпеки така система має перевагу - щоб здійснювати операції по картковому рахунку через інтернет-банкінг, особа повинна як мінімум мати в наявності безпосередньо саму карту, а також знати ПІН-код, щоб отримати список паролів в банкоматі. Разом з тим не можна не відзначити ряд недоліків такої системи захисту. По-перше, список паролів, роздрукований у вигляді чека з банкомату, вам

доведеться зберігати для підтвердження майбутніх операцій. А це означає, що якщо ви випадково втратите або викинете чек (або просто використовуєте всі паролі), вам доведеться йти за новим.

**Електронний цифровий підпис (ЕЦП).** Плюс ЕЦП в тому, що він дозволяє однозначно ідентифікувати користувача. Недолік же полягає в тому, що ЕЦП також може бути вразливим для шахраїв. Існують «трояни», які вміють знаходити і красти на зараженому комп'ютері аутентифікаційні дані (ідентифікатори, паролі і навіть ключі ЕЦП) користувачів для доступу до різних сервісів (в тому числі і серверів віддаленого обслуговування клієнтів банків. Якщо для підтвердження ваших фінансових операцій через інтернет ви використовуєте ЕЦП, не забувайте користуватися антивірусними програмами.

**Список використаних джерел**


1. Інформаційні системи і технології в банківських та фінансових установах. URL: p06_10.pdf (maup.com.ua)
2. Інформаційні системи і технології в банківській сфері. URL: 9363_Інформац сист в банківській справі - MP.doc (maup.com.ua)
3. Безпека Інтернет-банкінгу в Україні: практичні аспекти. URL: Безпека Інтернет-банкінгу в Україні в 2023 році (bankchart.com.ua)
4. Інформаційні технології (банки). URL: Інформаційні технології (банки) - Кафедра інформаційних технологій (udau.edu.ua)


## ДІЯ – БРЕНД ЦИФРОВОЇ ДЕРЖАВИ


*Васильченко Ю. В.*
*vasilchenko496@gmail.com*
*Черкаський державний бізнес-коледж*
*Науковий керівник: Захарова М. В.*
*м. Черкаси, Україна*


**Актуальність теми** "Дія – бренд цифрової держави" полягає в тому, що у сучасному світі цифрові технології стають все більш важливими для ефективного функціонування держави та надання послуг громадянам. Проект

"Дія" є важливим кроком в напрямку цифрової трансформації держави та забезпечення більш ефективної взаємодії між громадянами та державою.

**Метою** виконаної роботи є дослідження та інформування громадян про проект «Дія»

**Об'єктом вивчення** є платформа «Дія».

**Предметом роботи** є дослідження та аналіз проекту "Дія" як ключового інструменту цифрової трансформації держави.

Проект "Дія" - цифрова платформа для отримання державних послуг та підвищення ефективності управління державою. Він об'єднує різноманітні державні послуги в онлайн-режимі через вебсайт або мобільний додаток. "Дія" є зручним та доступним для всіх категорій громадян завдяки зрозумілому інтерфейсу. Проект є інструментом управління державою, оскільки дозволяє державним органам відслідковувати надходження звернень громадян та покращувати якість державних послуг, зменшувати бюрократію та забезпечувати прозорість та захист персональних даних громадян.[1]

Проект "Дія" є цифровою платформою, яка надає громадянам можливість отримувати різноманітні державні послуги в онлайн-режимі. Однак, при здійсненні таких операцій, існує певний ризик порушення інформаційної безпеки, так як громадяни надають свої персональні дані, які можуть бути скомпрометовані або використані несанкціонованою особою.

Однією з основних технологій шифрування, яку використовує проект "Дія", є шифрування трафіку за допомогою протоколу SSL / TLS. Цей протокол шифрує дані, які передаються між користувачем та сервером, щоб захистити їх від перехоплення та зловмисних дій. SSL / TLS також забезпечує перевірку автентичності сервера та встановлення безпечного з'єднання між ним та користувачем.[2]

Проект "Дія" є конкурентоспроможним на ринку державних електронних послуг в Україні. Його основна конкурентна перевага полягає у високому рівні зручності та доступності для громадян, а також в широкому спектрі державних послуг, які можна отримати в онлайн-режимі через цю платформу. Проектом

зацікавлені багато країн, а такі країни як США хочуть розробити власний аналог платформи. Естонія разом з Мінцифрою розробили власний проект під назвою «mRiik», що є аналогом Дії з меншим функціоналом.[3]

Розвиток цифрової інфраструктури та відкрите програмне забезпечення є важливими факторами успіху проекту "Дія". Ці два аспекти забезпечують стійкість та безпеку функціонування цифрової платформи, а також надають можливість забезпечувати її подальший розвиток та розширення функціоналу.

У випадку проекту "Дія", відкрите програмне забезпечення дозволяє розробникам з усього світу приєднатися до проекту та долучатися до його подальшого розвитку. Це забезпечує більшу кількість ідей та інновацій, а також дозволяє забезпечити більшу стійкість та безпеку проекту завдяки великій кількості розробників, які можуть виявляти та виправляти помилки в програмному коді.

## Висновки

Отже, розвиток проекту "Дія" та подальша цифрова трансформація держави можуть стати одними з ключових факторів, які забезпечать конкурентоспроможність України у світі та поліпшить якість життя громадян.

## Список використаних джерел


1. Інформація про проект «Дія» — [Електронний ресурс]. Режим доступу до ресурсу: https://plan2.diia.gov.ua/
2. Шифрування платформи — [Електронний ресурс]. Режим доступу до ресурсу: https://pingvin.pro/gadgets/news-gadgets/dodatok-diya-vykorystovuye-podvijne-shyfruvannya-i-gotuyetsya-do-zapusku-bug-bounty.html
3. Конкурентоспроможність проекту — [Електронний ресурс]. Режим доступу до ресурсу: https://www.bbc.com/ukrainian/features-59672498

# ЗАСТОСУВАННЯ БЛОКЧЕЙНУ В ЛОГІСТИЦІ ТА УПРАВЛІННІ ЛАНЦЮГАМИ ПОСТАВОК

*Гончарова А. А.*
*annaartemivna@gmail.com*
*Черкаський державний бізнес-коледж*
*Науковий керівник: Куцевський С. М.*
*м. Черкаси, Україна*

Блокчейн – це технологія зберігання та доступу до даних. Таким чином, кожен «блок» зберігає кінцевий набір даних і транзакцій, тоді як «ланцюжок» з'єднує всі блоки у фіксованому порядку. Поточний набір даних визначається шляхом відстеження ланцюга від першого до (наступного) останнього блоку та вирішення транзакцій у кожному блоці. У результаті блокчейн містить не тільки поточний набір даних, але і повну історію транзакцій [3]. Кожен блок містить часову позначку, хеш попереднього блоку та дані транзакцій, подані як хеш-дерево. Інформація про транзакції зазвичай надається відкритою, не шифрованою. Захистом від підробки та спотворення слугує включення хешу всього блоку у наступний блок. Тому внесення змін в один з блоків вимагає відповідних змін в усіх блоках після нього, що зазвичай виявляється або дуже складно, або дуже коштовно.

Технологія блокчейн містить три найважливіші характеристики: децентралізованість, надійність та незмінність.

Мережа децентралізована, оскільки повністю управляється учасниками процесу, не покладаючись на центральний орган влади або централізовану інфраструктуру, що встановлює довіру з усіма учасниками процесу. Децентралізація даних приводить до збільшення прозорості щодо історії транзакцій [3].

Технологія блокчейн базується на складній системі шифрування, в якій кожен блок має свій унікальний ключ. Використання шифру гарантує, що користувачі можуть змінювати тільки ті блоки ланцюга, до яких у них є доступ, тобто якими вони володіють, знаючи відповідний ключ, без якого запис у файл здійснити не можна [2]. Тобто щоб додати транзакцію до книги записів, вона

повинна бути спільною в межах однорангової мережі. Усі члени зберігають власну локальну копію документа, учасники підписують транзакції, використовуючи відкритий або приватний криптографічний ключ перед тим, як ділитися ним з мережею. Тому лише власник приватного ключ може ініціювати їх. Водночас учасники можуть залишатися анонімними, оскільки ключі не пов’язані з реальними особами. Він незмінний завдяки своєму алгоритму, одна або кілька транзакцій групуються разом, щоб сформувати новий блок. Усі учасники мережі можуть перевірити транзакції в блоці. Якщо учасники не досягнули консенсусу щодо дійсності нового блоку – блок відхиляється. Подібним чином, якщо існує консенсус щодо того, що транзакції в блоці є дійсними, блок додається до ланцюжка. Криптографічний хеш генерується для кожного блоку. Кожен блок не тільки зберігає записи транзакцій, але і хеш з попереднього блоку, це створює взаємозалежність блоку, що зв’язується з ланцюгом - блокчейном.

Ланцюг створення нового блоку є: надіслати нову транзакцію; надіслати блок, що відповідає запиту на нову транзакцію для всіх вузлів ланцюга; більшість вузлів схвалюють нову транзакцію; додається новий блок до ланцюжка; зберігається новий примірник книги, що містить усі блоки у мережі вузла [1].

Принципи функціонування блокчейн:

- Розподілена база даних. Кожна сторона в блокчейн має доступ до всієї бази даних та її повної історії, тобто жодна сторона не контролює дані або інформацію, і кожна сторона може перевіряти записи своїх партнерів по транзакціях безпосередньо, без посередника;
- Передача однорангових блоків. Зв’язок відбувається безпосередньо між одноранговими блоками, а не через центральний вузол, тобто кожен вузол зберігає та передає інформацію на всі інші вузли;
- Незворотність записів. Після введення транзакції в базу даних та оновлення облікових записів записи не можуть бути змінені, оскільки вони пов’язані з кожним попереднім записом транзакцій [3].

За допомогою розумних контрактів можна виконувати різні функції всередині мережі блокчейну, зокрема: дозвіл на транзакції з «кількома підписами», завдяки чому транзакція здійснюється лише тоді, коли більшість або коли необхідний відсоток учасників погоджується підписати його; увімкнення автоматизованих транзакцій, ініційованих для конкретної події. «Смарт-контракт» був введений Н. Сабо з метою забезпечення відносин у загальнодоступних мережах [1].

На ринку вже наявні компанії, які застосовують блокчейн. Прикладом такого продукту є Smart Containers, створено в Швейцарії, компанія використовує програмне забезпечення Ethereum. Smart Containers займається перевезенням в контейнерах продуктів, чутливих до температури та специфічних умов зберігань, відстеженням  та підтримкою умов зберігання і транспортування. У Сінгапурі використовують продукт Yojee для відстеження стану замовлень вантажу перевізниками в режимі реального часу, формування рахунків, диспетчеризація і автоматичний розподіл замовлень між водіями. В Україні також є компанії, які використовують технології блокчейн, зокрема A2b Direct та TrucksNearMe для відстеження стану замовлень вантажу перевізниками в режимі реального часу, формування рахунків.

Українська онлайн-платформа A2B Direct працює на ринку Східної Європи, логістична компанія оголосила про переведення своєї платформи онлайн-управління поставками на технологію блокчейн. Платформа A2B Direct була запущена в кінці 2016 року і швидко отримала неофіційну назву «Uber вантажоперевезень». Вона дає змогу швидко з’єднувати вантажоперевізника з вантажовласником, підтримувати цілодобовий зв’язок з водієм, вирішує проблеми з документальним оформленням і виключає експедиторські націнки.

Платформа забезпечує пряму взаємодію між вантажоперевізниками та вантажовласниками на всіх етапах перевезення вантажу:

- прямий зв’язок і прямі угоди без залучення посередників, розширений пошук оптимального транспортного підрядника;
- пряма логістика та документообіг;

– онлайн-трекінг транспорту й вантажів;
– юридичний супровід та страхування [1].

Інтеграція блокчейну в логістику дає змогу вдосконалити логістичні процеси, зокрема: усуває непотрібних посередників, забезпечує простий та швидкий доступ до інформації за рахунок шифрування даних, захищає операторів логістичних послуг шляхом зменшення кількості помилок, знижує частку контрафактної продукції, автоматично захищає компанію від підробок, адже ці підробки неможливо буде зареєструвати у розподілену базу даних. Додатковою перевагою застосування технології блокчейн є економія витрат для галузі.

**Список використаних джерел**


1. Керничний Б. Зарубіжний та вітчизняний досвід застосування технології блокчейн в транспортно-логістичному обслуговуванні. Електронне наукове фахове видання "Соціально-економічні проблеми і держава". 2020. № 2(23). С. 48–52. DOI: https://doi.org/10.33108/sepd2020.02.046 (дата звернення: 10.03.2023).
2. Кудирко О. В. Інновації в логістиці: перспективи використання технології блокчейн у ланцюгах поставок. Науковий вісник Ужгородського національного університету. 2017. С. 159–161. URL: http://www.visnyk-econom.uzhnu.uz.ua/archive/15_1_2017ua/36.pdf (дата звернення: 10.03.2023)
3. Мазуренко О. К. Технології blockchain в інформаційному забезпеченні логістичних послуг. Бізнесінформ. 2019. С. 256–259. DOI: https://doi.org/10.32983/2222-4459-2019-12-261-267 (дата звернення: 12.03.2023).
4. Блокчейн. ВікіпедіЯ. URL: https://uk.wikipedia.org/wiki/Блокчейн (дата звернення: 12.03.2023).

# 6G — ШОСТЕ ПОКОЛІННЯ МОБІЛЬНОГО ЗВ'ЯЗКУ

*Драч І. М.*
*ivandrach12345@gmail.com*
*Черкаський державний бізнес-коледж*
*Науковий керівник: Холупняк К. О.*
*м. Черкаси, Україна*

У листопаді 2019 року була створена офіційна китайська дослідницька група з питань 6G. Розвинені країни, такі як США, Японія, Південна Корея та деякі європейські країни, почали розробляти плани досліджень і розробок для 6G, оскільки телекомунікаційний сектор завжди був місцем конкуренції. Технологія 5G спрямована на створення комплексної сенсорної системи, в якій можна легко отримати доступ до інформації та інструментів. З іншого боку, 6G допоможе побудувати перцептивну нервову систему, яка інтегрує штучний інтелект (ШІ) і бездротове пізнання, що може давати інтелектуальні відповіді. Порівняно з технологією 5G, 6G матиме меншу затримку, вищу швидкість і більшу пропускну здатність. І ця передова технологія допоможе з'єднати реальний світ з віртуальним цифровим світом. З точки зору економічного розвитку, 3G сприяло розвитку електронної комерції, а 4G – електронної комерції та мобільних платежів.

Будівництво та застосування інфраструктури 5G поклало початок інтелектуальному виробництву китайських підприємств і послужило основою для стрімкого розвитку сектора. Аналогічно, бездротова когнітивна технологія, пов'язана з технологією 6G, коли вона дозріє, ще більше сприятиме розвитку цифрової економіки. Недавня історія показує, що ті, хто очолює телекомунікаційний сектор, встановлюють стандарти для телекомунікаційних продуктів і послуг і відіграють більшу роль у майбутньому розвитку галузі.

У цифровій економіці інтелект великих даних стане справжнім поштовхом для інновацій, а мережі 6G не тільки стануть магістраллю для передачі даних, але й набагато легше інтегруватимуть периферійні та основні обчислення в рамках об'єднаної комунікаційної та обчислювальної інфраструктури. До того ж цифрова економіка, заснована на 6G, стане визначальним фактором

конкурентоспроможності країни. А технологія 6G, головною особливістю якої є бездротовий зв'язок, стане основною технологією і головним рушієм цифрової економіки. Це забезпечить багато потенційних переваг, оскільки технологія 6G почне працювати, включаючи доступ до можливостей штучного інтелекту. Очікується, що 6G підтримуватиме швидкість до терабайтів на секунду, безпрецедентну пропускну здатність і затримку, що підвищить продуктивність додатків 5G, а також розширить сферу підтримки нових та інноваційних додатків у галузі бездротового пізнання, озвучування та візуалізації. Що стосується досліджень і розробок у галузі технології 5G, Китай має дві переваги:

- по-перше, він є світовим лідером у телекомунікаційному секторі та має потужний пул талантів.
- по-друге, він має відносно повну промислову мережу, що охоплює НДДКР, проектування, виробництво і застосування, і є домом для провідного виробника обладнання 5G компанії Huawei.

Але, розвиваючи технологію 4G одночасно з розвиненою економікою, Китай став головним гравцем у цій галузі і зробив свій внесок у процес нормотворчості. Той факт, що 4G в Китаї є найсучаснішим і найпоширенішим у світі, також сприяв швидкому розвитку мобільних платежів у країні.

Починаючи з 5G, китайська телекомунікаційна галузь, завдяки своїм широким дослідженням, зайняла лідируючі позиції в стандартизації та виробництві телекомунікаційного обладнання 5G. І оскільки 6G стає рушієм нового витка економічного розвитку, китайський уряд, бізнес і дослідницькі організації повинні посилити співпрацю, щоб досягти успіху в конкурентній боротьбі з 6G.

Україна поступово скорочує відставання від західних країн у процесі запуску нових поколінь зв'язку. Таким чином, якщо 3G в нашій країні з'явився в 2015 році, відстаючи від розвиненого світу більш ніж на десятиліття, то розрив між активним розвитком нашого 4G (2018) і європейського 4G – 5-8 років.

Мережі п’ятого покоління, які масово з’явилися у світі на початку 2020-х років, швидше за все, до нас дійдуть вже після закінчення повномасштабного вторгнення росії в Україну. Хоча планувалось впровадження у 2022 році.

Тому впровадження 6G, якщо воно з’явиться у світі до 2030 року, має вплинути на наш ринок в сфері цифрової економіки.

**Список використаних джерел**


1. Матеріали XIII Всеукраїнської студентської науково-практичної конференції студентів, аспірантів та молодих вчених за тематикою «Тенденції розвитку ІТ-технологій в Україні»: збірка наукових праць. Черкаси, 2021, 204 с.
2. Василь Ткаченко. Мережі та Бізнес. С. 83-87. URL: http://sib.com.ua/sib-06-115- 2020/6g.html
3. Журнал HI-TECH [Електронний ресурс]. - Режим доступу: https://hitech.ua/catalog/
4. Інформаційний ресурс [Електронний ресурс]. - Режим доступу: https://www.pcweek.ua


## АНАЛІЗ МЕДИЧНИХ ДАНИХ ЗА ДОПОМОГОЮ МАШИННОГО НАВЧАННЯ


*Короп М. А.*
*makskorop99@gmail.com*
*Черкаський державний бізнес-коледж*
*Науковий керівник: Куцевський С. М.*
*м. Черкаси, Україна*


Машинне навчання – підгалузь штучного інтелекту в галузі інформатики, яка застосовує статистичні прийоми для надання комп’ютерам здатності «навчатися» з даних.

Для чого можна використовувати машинне навчання в медичному аналізі:

1) Для класифікації зображень: машинне навчання можна використовувати для класифікації зображень отриманих з різних медичних приладів

(рентгенівського апарату, МРТ та КТ).

2) Для аналізу медичних записів: можна використовувати для аналізу різних медичних записів, таких як: історії хвороб, результати тестів.
3) Для передбачення ефективності терапії: машинне навчання може використовуватися для передбачення ефективності певної терапії та вибору оптимальної для пацієнта. Також може використовуватися для передбачення реакції організму пацієнта на певні лікарські засоби, та їх дозування

Етапи створення, налаштовування та тестування моделі машинного навчання:

1) Визначення мети аналізу медичних даних.
2) Для того щоб алгоритми машинного навчання були ефективними, та якомога точнішими, необхідна велика кількість інформації. Тому потрібно визначитись яку інформацію використовувати, як її зібрати та як її обробляти.
3) Також важливим фактором, який впливає на точність даних, є метод машинного навчання. Для аналізу медичних даних можуть бути використані різні методи машинного навчання. Наприклад нейронні мережі, дерева прийняття рішень, метод опорних векторів та інші.
4) Процес розробки та налаштування моделі для певних задач аналізу медичних даних.
5) Тестування та оцінка моделі машинного навчання. Після створення моделі потрібно провести її тестування, та оцінити її ефективність.
6) Інтеграція моделі машинного навчання у медичну практику.

Коли є достатньо даних, штучний інтелект може виконувати набагато точнішу роботу з діагностики, ніж лікарі-люди. Також він може враховувати дані кожного, щоб відповідно персоналізувати лікування або йти в ногу з величезною кількістю нових ліків, методів лікування та досліджень.[2]

Для того, щоб машинне навчання в медицині було максимально ефективним, нейронним мережам потрібна велика кількість структурованих

даних. Часто важко отримати реальні дані через відсутність згоди пацієнтів на їх використання. Проблему можна обійти за рахунок застосування генеративно-змагальних мереж, або GAN. Це алгоритм машинного навчання, який будується на комбінації двох нейронних мереж. Одна з них служить для генерації зразків, в медицині це результати досліджень. Інша мережа працює як фільтр, що відокремлює «справжні» результати від «несправжніх».[1]

Для аналізу зображень з медичних приладів зазвичай використовують згорткові нейронні мережі, оскільки вони найбільше підходять для роботи з візуальною інформацією. Також добре працює механізм уваги нейронних мереж, який застосовується для пошуку взаємозв'язків між різними частинами вхідних і вихідних даних. Згорткові мережі взяли за основу біологічний процес, а саме схему з'єднання нейронів зорової кори тварин.[3] Нейронні мережі можна використовувати для аналізу термограм під час відкритої операції на серці, діагностики хвороби Паркінсона.

Під час проведення відкритої операції на серці , його потрібно спочатку охолодити, а потім нагріти, і цей процес має бути максимально рівномірним, аби не пошкодити серце, накопичується великий масив візуальної інформації щодо змін температури, який людина не здатна обробити. Вхідні дані для мережі будуть надходити у вигляді відео, але для навчання необхідно використовувати формат зображень, саме тому відеопотік буде спочатку кадровано, а отримані зображення розділено на 2 класи – «патологія» та «норма». За ліміт градієнту температури зазвичай беруть 3ºС, оскільки при більшому градієнті тканина серця може отримати ураження.[4]

Точного методу діагностики для встановлення діагнозу хвороби Паркінсона досі немає, але є методи для виявлення симптомів. Серед таких методів є малювання спіралі Архімеда. Маючи малу кількість даних для тренування мережі, можна збільшити вибірку шляхом перетворення зображень. У якості згорткової мережі в дослідженні брали VGG, адже вона може досягати точності 92.7% під час тестування на задачах розпізнавання об'єктів на зображенні. В результаті проведених досліджень було створено модель, яка має

точність 93.7%. Тому така модель дозволить автоматизувати процес діагностики хвороби на ранніх стадіях.[5]

Охорона здоров'я на основі штучного інтелекту надає перспективу людському суспільству мати здоровіше і довше життя. Штучний інтелект започатковує нову епоху сучасної медицини. Хоч зараз є багато проблем з впровадженням ШІ в галузь охорони здоров'я, та ці проблеми не є короткочасними і потребуватимуть рішення у досить довгій перспективі. Проте аналіз наукових досліджень і практики дають оптимістичні оцінки вирішення цих проблем і невпинності розвитку ШІ в сфері охорони здоров'я.

**Список використаних джерел**


1. Машинне навчання у медицині. URL: https://avada-media.ua/ua/services/mashinnoe-obychenie-v-medicine/ (дата звернення: 12.03.2023).
2. Бродкевич В., Людвіченко В. Штучний інтелект і машинне навчання в галузі охорони здоров'я: виклики і перспективи. Інформаційні технології та суспільство. 2022. № 2 (4). С. 20–28. DOI: https://doi.org/10.32689/maup.it.2022.2.3 (дата звернення: 12.03.2023).
3. Згорткова нейронна мережа. URL: https://uk.wikipedia.org/wiki/%D0%97%D0%B3%D0%BE%D1%80%D1%82%D0%BA%D0%BE%D0%B2%D0%B0_%D0%BD%D0%B5%D0%B9%D1%80%D0%BE%D0%BD%D0%BD%D0%B0_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B0#%D2%90%D0%BE (дата звернення 12.03.2023)
4. Шапошник О., Шликов В. Нейронна мережа для аналізу термограм під час відкритої операції на серці. Біомедична інженерія і технологія. 2020. № 4. С. 61–68. DOI: https://doi.org/10.20535/2617-8974.2020.4.221874 (дата звернення: 12.03.2023).
5. Харченко Н., Сердаковський В. Нейронна мережа для діагностики хвороби Паркінсона за зображенням спіралі Архімеда. Computer-integrated technologies: education, science, production. 2021. № 45. С. 54–58. DOI:

https://doi.org/10.36910/6775-2524-0560-2021-45-08 (дата звернення: 12.03.2023).

# ЗАЛУЧЕННЯ ІТ-ТЕХНОЛОГІЙ ДЛЯ ПОКРАЩЕННЯ ТРАНСПОРТНОЇ СИСТЕМИ В М. ЧЕРКАСИ

*Михальченко І. В.*
*mihalchenkomail@gmail.com*
*Черкаський державний бізнес-коледж*
*Науковий керівник: Куцевський С. М.*
*м. Черкаси, Україна*

Транспортна система в будь-якому місті є невід'ємною його складовою. Нею щодня користується значна кількість черкащан, тому, під час модернізації суспільства, покращуються і технології, напряму пов'язані і з нею. Валідатори, відслідковувачі громадського транспорту — нині знайомі черкащанам речі, що нещодавно з'явились у нашому житті.

Автоматизована система обліку оплати проїзду в громадському транспорті — одна з ступеней розвитку країни в рамках діджиталізації (цифровізації): переведення інформації в цифрову форму у всіх можливих галузях. За безготівкову оплату проїзду відповідає система SmartTicket.City, що можна почути особисто, подорожуючи будь-яким громадським транспортом зі встановленними валідаторами. Для оплати потрібно прикласти будь-яку банківську картку, мобільний телефон або годинник, що підтримує NFC до валідатора та дочекатись звукового та візуального сигналу підтвердження. Система Smart Ticket Technology обладнана бортовим комп'ютером, LED-панеллю, що сповіщує про зупинку, стаціонарними валідаторами, GPS датчиками та камерами відеоспостереження. Наступним їх кроком стане впровадження автоматизованої системи управління інформаційними екранами з корисною інформацією, сповіщеннями населення, соціальною рекламою тощо.

GPS-моніторингом, зокрема, займається компанія DozoR. Їх інформаційні табла вже встановлені на деяких черкаських зупинках. На них зображено (по

порядку): маршрут, напрямок руху та час прибуття міського транспорту. Зручна технологія відкидає інформаційні таблички у минуле, зробивши місцеву транспортну інфраструктуру більш зручною. У компанії є власний інтернет-портал з картою міста та актуальною інформацією стосовно майбутніх зупинок будь-якого міського маршруту. Якщо казати про більш зручну форму — можна скористатися мобільним додатком BusWay. Він виконує усі вищевказані функції, будучи встановленим на Ваш смартфон.

Підсумовуючи, можна сказати, що Черкаси, як і вся Україна — розвиваються, маючи за мету збільшення комфорту життя, зокрема зручності пересування по місту. Технології ще мають пройти довгий шлях покращень та доробок, але і на сьогодні можна з впевненістю заявити про перші успіхи в рамках діджиталізації в сфері громадського транспорту в Черкасах.

**Список використаних джерел**


1. Як користуватися системою SmartTicket.City? URL: https://smartticket.city/#howitworks (дата звернення: 12.03.2023).
2. Про DozoR URL: https://dozor.tech/pro-nas (дата звернення: 12.03.2023).


## ВПЛИВ ІТ НА ТРАНСФОРМАЦІЮ УКРАЇНСЬКОЇ ПРОМИСЛОВОСТІ


*Бровко Д. Д.*
*browko.denis@gmail.com*
*Черкаський державний бізнес-коледж*
*Науковий керівник: Фальченко Н. Г.*
*м. Черкаси, Україна*


ІТ-технології в оборонному секторі України є важливим напрямком розвитку та забезпечення національної безпеки країни. Українські ІТ-компанії активно займаються розробкою та впровадженням програмного забезпечення, систем управління, комунікаційних та інших технологій, які застосовуються в оборонних галузях.

У 2019 році було створено Державне агентство з розробки та реалізації проектів оборонної галузі, метою якого є забезпечення комплексного розвитку

національної оборонної галузі та сприяння упровадженню інноваційних рішень, в тому числі технологій ІТ.

Одним з прикладів застосування ІТ-технологій в оборонному секторі є впровадження "розумних" систем безпеки, що мають захистити об’єкти військового значення від кібератак. Також в Україні розробляють та випробовують дрони для розвідки та ударів, системи контролю за кордонами та автоматизовані системи управління військовими транспортними засобами.

Однак, використання ІТ-технологій в оборонному секторі також пов’язане з питаннями кібербезпеки, тому українські ІТ-компанії та державні органи активно співпрацюють для забезпечення захисту від кібератак. Для забезпечення кібербезпеки Україна створила Національний центр кібербезпеки та запустила державну програму з підвищення кібербезпеки національних інформаційних ресурсів.

Українська промисловість почала активно трансформуватися після 2014 р. з появою руху Industry 4.0, який передбачає повністю автоматизоване виробництво та керування всіма процесами в режимі реального часу.

Industry 4.0 ґрунтується на революційних технологіях:

- Artificial Intelligence (AI). Штучний інтелект відіграє ключову роль у створенні рішень автоматизації в промисловості. Завдяки ШІ можна підвищувати гнучкість і точність виробничих процесів, адаптувати управлінські процеси тощо.
- Internet of Things (IoT). IoT – комп’ютерні мережі, до яких підключають фізичні об’єкти зі встановленими датчиками, сенсорами та ПЗ. Це допомагає обробляти інформацію, дистанційно керувати процесами та автоматизувати виробництво.
- Big Data. Технологічні рішення Big Data дозволяють у режимі реального часу збирати, аналізувати та прогнозувати дані щодо обсягів виробництва та витрат, логістики, роботи з клієнтами та інших виробничих процесів.

Повномасштабна війна стала потужним поштовхом до розвитку military-tech в Україні. Такі компанії охоплюють усе, що потрібно українським

захисникам – від дронів до засобів тактичної медицини.

Military-tech в Україні розвивається досить стрімко: зростання ринку з 2014 р. становить від 3 до 7 разів, залежно від напрямку.

Це дозволяє суттєво скоротити час, необхідний на реалізацію проєкту: якщо у 2014 переважно потрібно було 1,5-2 роки, то розвиток цієї сфери скоротив цей показник до 2-3 місяців.

Український military-tech активно розвивається в таких напрямах:

- Робототехніка. В Україні найбільш успішним у цій сфері є виробництво та використання дронів. Серед них є як дрони для аеророзвідки та передавачі інформації, так і дрони-камікадзе для ураження ворога.
- ПЗ для військових. Українські військові забезпечені власним ПЗ, серед якого «Кропива», «Дельта», «Грізельда», «Броня», «Мілчат» тощо. Ці розробки націлені на автоматизацію збору інформації, аналіз та обробку в реальному часі тощо.
- AR/VR. Технології доповненої реальності є основою симуляторів різних видів зброї та техніки, що дозволяє із меншими витратами та втратами проводити навчання військових та вдосконалювати їхні вміння.

На даний момент збільшилась потреба в хмарних сервісах, для надання яких необхідні дата-центри з потужним сучасним обладнанням.

Продовжується автоматизація різних виробничих процесів, розробка мобільних додатків, ігор, гаджетів.

Розширення сфери послуг, упровадження інноваційних технологій у виробничу сферу вимагає збільшення числа айтішників. Однак змінились вимоги до кадрів: роботодавці все частіше віддають перевагу багатопрофільним фахівцям, а вузькоспеціалізовані працівники ризикують залишитися без роботи. Продовжується і тенденція до заміщення людської праці штучним інтелектом – витрати автоматизації багатьох процесів.

Сфера інформаційних технологій залишається одним з найбільш динамічних сегментів економіки України.

**Список використаних джерел**

1. Тенденції розвитку IT-технологій в Україні. URL: https://careerfornewlife.com/blog/find/tendentsiyi-rozvitku-it-rinku-v-ukrayini/
2. Перспективи та розвиток IT-технологій в Україні. URL: https://blog.liga.net/user/vomelchenko/article/35913
3. Перспективи розвитку інформаційних технологій. URL: http://apeps.kpi.ua/perspektivi-rozvitku-informatsiinykh-technologii
4. IT-перспективи: прогноз погоди на ринку українських інновацій у 2022 році. URL: https://speka.media/it-biznes/it-perspektivi-prognoz-pogodi-na-rinku-ukrayinskix-innovacii-v-2022-roci-9q4kyp
5. IT у фінансах. URL: https://finance.ua/ua/goodtoknow/jak-it-industrija-rozvyvae-inshi-galuzi-ekonomiky#headline_4

# РОЛЬ ТА ПРАКТИЧНЕ ВИКОРИСТАННЯ СУЧАСНИХ ТЕХНОЛОГІЙ IT СЕКТОРУ В МЕДИЦИНІ УКРАЇНИ

*Андріуца М. М.*
*wipietrampit813@gmail.com*
*Черкаський державний бізнес-коледж*
*Науковий керівник: Захарова М. В.*
*м. Черкаси, Україна*

Сучасні технології IT сектору в медицині України є важливим елементом розвитку медичної галузі. Використання таких технологій якісно змінює спосіб функціонування медичної сфери і сприяє її розвитку.

**ЕМД.** Одним з основних напрямів розвитку сучасних технологій в медицині є впровадження систем електронної медичної документації (ЕМД). Ці системи дозволяють лікарям легко зберігати та організовувати медичну інформацію про пацієнтів, що покращує якість надання медичної допомоги і забезпечує збереження медичної інформації в електронному вигляді.

**Мобільні додатки.** Зручні мобільні додатки, які дозволяють пацієнтам вести електронний щоденник свого здоров’я, отримувати рекомендації щодо правильного харчування та фізичної активності, а також отримувати

інформацію про свої аналізи та результати обстежень. Такі додатки можуть бути корисні для контролю за станом здоров'я, зокрема при хронічних захворюваннях, таких як діабет, серцево-судинні захворювання, алергії та інші.

Додатки з психологічного здоров'я також допомагають користувачам контролювати своє психічне здоров'я, надаючи можливість вести електронний щоденник своїх емоцій та відчуттів, здійснювати медитацію та релаксацію, а також отримувати психологічну підтримку від лікарів та спеціалістів.

Однак, використання мобільних додатків у медицині також має свої ризики та виклики. Зокрема, необхідно забезпечити захист персональних даних пацієнтів, оскільки ці додатки містять конфіденційну медичну інформацію. Також важливо забезпечити якість та достовірність інформації, яку надають додатки, оскільки неправильна інформація може призвести до небезпеки для здоров'я пацієнта.

**Телемедицина.** Це здійснення медичної допомоги за допомогою технологій зв'язку, таких як відеозв'язок, телефонні дзвінки, текстові повідомлення тощо. Вона дозволяє медичним працівникам консультувати пацієнтів на віддаленій відстані, робити дистанційний моніторинг здоров'я пацієнтів, проводити електронні консультації та дистанційні діагностики.

Також, телемедицина дозволяє зменшити витрати на медичну допомогу та збільшити доступність до неї, особливо в регіонах, де немає достатньої кількості медичних працівників та обладнання. Крім того, вона може допомогти зменшити час очікування на медичну допомогу, збільшити точність діагностики та покращити якість медичного обслуговування. Це особливо актуально в умовах карантину та обмежень на пересування, коли пацієнти можуть отримати консультації лікарів не виходячи з дому.

Україна також розвиває телемедицину, зокрема уряд планує впровадити електронну медичну картку та телемедичний портал для медичних консультацій та діагностики.

**Аналіз медичних даних.** Є одним з найважливіших застосувань сучасних технологій IT в медицині. Він дозволяє ефективніше обробляти та

інтерпретувати великі обсяги медичної інформації, що збирається з різних джерел, включаючи електронні медичні картки, лабораторні дані, зображення, результати діагностичних тестів, генетичні дані та інші дані.

Аналіз медичних даних може бути використаний для розробки і підтримки протоколів діагностики та лікування, виявлення та відстеження показників здоров'я пацієнтів, прогнозування розвитку захворювань та інші цілі. Ці дані також можуть бути використані для розробки і підтримки наукових досліджень, які досліджують зв'язки між різними факторами та захворюваннями, розробляють нові методи діагностики та лікування.

Один з прикладів використання аналізу медичних даних є системи моніторингу захворювань, які використовуються для відстеження поширення захворювань та їхніх симптомів у реальному часі. Ці системи дозволяють швидко виявляти та реагувати на спалахи захворювань та забезпечувати ефективне управління пандеміями.

Хоча сучасні технології ІТ сектору мають багато переваг, вони також мають свої недоліки, особливо в медичній галузі. Ось кілька з них:

1) Безпека даних: використання електронних засобів збереження та передачі медичних даних може призвести до можливого порушення конфіденційності та безпеки пацієнтів, якщо не забезпечено належний захист даних.
2) Відсутність стандартів: в медицинському секторі ще не існує єдиних стандартів, що регулюють використання технологій. Це може призвести до труднощів зі сумісністю систем та програмного забезпечення, а також до неповного використання можливостей новітніх технологій.
3) Обмеження доступу: не всі пацієнти мають можливість використовувати сучасні технології через обмеженість доступу до Інтернету або відсутність належних навичок.
4) Неадекватність діагностики: хоча аналітичні програми можуть здійснювати аналіз медичних даних, вони не замінять кваліфікованого лікаря, який може використовувати додаткову інформацію, яку не може

забезпечити програмне забезпечення.

5) Вартість: сучасні технології можуть бути досить дорогими для використання в медичній галузі, що може стати перешкодою для їх широкого впровадження та використання.

У цілому, використання сучасних технологій ІТ сектору у медицині України має значний потенціал для поліпшення якості та ефективності надання медичних послуг, але водночас потребує вирішення ряду проблем, пов'язаних з захистом даних та якістю інформації.

**Список використаних джерел**


1. Наукове Мислення [Електронний ресурс]. Режим доступу: https://naukam.triada.in.ua/index.php/konferentsiji/42-dvanadtsyata-vseukrajinska-praktichno-piznavalna-internet-konferentsiya/462-it-tekhnologiji-v-meditsini (дата звернення: 01.03.2023р.).
2. Ingenius [Електронний ресурс]. Режим доступу: https://ingeniusua.org/articles/5-tekhnologiy-yaki-modernizuyut-ta-pokraschuyut-medicinu (дата звернення: 01.03.2023р.).
3. MEDSTAR [Електронний ресурс]. Режим доступу: https://medstar.ua/novi-tehnologii-v-medicini-zagalnij/ (дата звернення: 01.03.2023р.).


## СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В НАВЧАННІ


*Пустовіт М. В.*
*pustovitmax405@gmail.com*
*Черкаський державний бізнес-коледж*
*Науковий керівник: Люта М. В.*
*м. Черкаси, Україна*


Під інформаційною технологією навчання розуміють таку модель навчально-виховного процесу, у якій мета досягається насамперед за рахунок найповнішого використання можливостей комп'ютерів та програмного забезпечення.

Основною метою нових інформаційних технологій є підготовка учнів до

комфортного самопочуття в умовах інформаційного суспільства. Нові інформаційні технології передбачають:

- Інтенсифікацію навчання;
- Формування інформаційної культури учнів;
- Підготовку фахівців у галузі інформатики.

ІТН відкривають учням доступ до нетрадиційних джерел інформації, підвищують ефективність самостійної роботи.

Використання комп'ютера на інших уроках передбачає знання учителем принципів роботи комп'ютера, його можливостей, а також доцільності застосування комп'ютера при вивченні тих чи інших тем. Важливою умовою успішного використання комп'ютера на уроках є співпраця вчителя інформатики і вчителя предметника. Вчитель інформатики забезпечує технічний бік процесу навчання, консультує вчителя-предметника з питань програмного забезпечення.

Інформаційно-комунікаційні технології (ІКТ) – інформаційні технології на базі персональних комп'ютерів, комп'ютерних мереж і засобів зв'язку, для яких характерна наявність доброзичливого середовища роботи користувача.

**По-перше**, впровадження ІКТ у сучасну освіту суттєво прискорює передавання знань і накопиченого технологічного та соціального досвіду людства не тільки від покоління до покоління, а й від однієї людини до іншої.

**По-друге**, сучасні ІКТ, підвищуючи якість навчання й освіти, дають змогу людині успішніше й швидше адаптуватися до навколишнього середовища, до соціальних змін. Це дає кожній людині можливість одержувати необхідні знання як сьогодні, так і в постіндустріальному суспільстві.

**По-третє**, активне й ефективне впровадження цих технологій в освіту є важливим чинником створення нової системи освіти, що відповідає вимогам ІС і процесу модернізації традиційної системи освіти.

Важливість і необхідність впровадження ІКТ у навчання обґрунтовується міжнародними експертами і вченими. ІКТ торкаються всіх сфер діяльності людини, але, мабуть, найбільш сильний позитивний вплив вони мають на

освіту, оскільки відкривають можливості впровадження абсолютно нових методів викладання і навчання.

Розвиток суспільства, науки і техніки ставить систему освіти перед необхідністю використовувати нові засоби навчання. До таких засобів навчання відносяться комп'ютери і комп'ютерні інформаційні технології, які в останні 10-15 років активно входять в наше життя. Комп'ютер сьогодні - це що найпотужніший інструмент отримання і обробки інформації, можливості комп'ютерних і мережних технологій, їх швидкодія приголомшують уяву. Тому абсолютно природно упровадження цих засобів в сучасний учбово-виховний процес. Використання комп'ютера в учбовому процесі перетворює навчання в захоплюючий процес, з елементами гри, сприяє розвитку дослідницьких навиків учнів.

Проте труднощів на цьому шляху більш ніж достатньо, основна з яких - недостатнє або нульове фінансування їх розвитку в школах. Ці технології є дорогими: придбання комп'ютерів, їх поточна модернізація, а розвиток технологічної бази і рівня безпеки вимагають оновлення комп'ютерного парку не рідше, ніж кожні 2-3 роки, обслуговування комп'ютерів і сітей, покупка програмного забезпечення, підключення до Internet. Крім цього потрібна висока кваліфікація викладачів, їх безперервна перепідготовка і професійне зростання.

Здавалося б, нескладно заперечити, що немає нічого простіше відмовитися від подібних технологій на користь яких-небудь більш дешевих, таких як діа- епі- і інші проектори, книги, дошка і крейда, нарешті, і навчати так само як вчилися самі. Безумовно, чому-небудь і як-небудь ми так навчимо, і, можливо, виховаємо. Але чого зможе досягти такий вихованець в сучасному технократичному суспільстві? В кращому разі стане торговцем на ринку. Персонал сучасних торгових центрів вимагає вже принципово іншого рівня, а про виховання і "вирощування" лідерів і керівників за такими технологіями доведеться забути. Таким чином, комп'ютерні технології в освіті є реальною частиною культури, і упроваджувати ці технології в сучасній школі необхідно.

Технологія проведення уроків з використанням комп'ютера тренує і

активізує пам’ять, спостережливість, кмітливість, концентрує увагу учнів, примушує їх по-іншому оцінити пропоновану інформацію. Комп’ютер на уроці значно розширює можливості представлення учбової інформації. Застосування кольору, графіки, звуку, сучасних засобів відеотехніки дозволяє моделювати різні ситуації і середовища. Це дозволяє усилити мотивацію учнів до навчання.

Крім того, застосування комп’ютера на уроках дозволяє усунути одну з найважливіших причин негативного відношення до навчання – неуспіх. Працюючи на комп’ютері, учень дістає можливість довести рішення задачі до кінця, спираючись на необхідну допомогу.

Використання ІТ має ряд переваг:

- використання у навчанні здобутків новітніх інформаційних технологій;
- забезпечує збільшення об’єму і оптимізацію пошуку потрібної інформації;
- підвищує пізнавальну активність студентів за рахунок різноманітної відео- та аудіоінформації;
- здійснює контроль завдяки тестуванню і системи запитань для самоконтролю;
- забезпечує спілкування студентів між собою та з викладачами в режимі онлайн поза межами навчальної аудиторії та ін.

**Список використаних джерел**


1. Інформаційні технології навчання. [Електронний ресурс]. URL: https://sites.google.com/site/informacijninavcanna/
2. Сучасні інформаційні технології у школі. [Електронний ресурс]. URL: https://osvita.ua/school/method/34855/
3. Впровадження інформаційних технологій у навчальний процес. [Електронний ресурс]. URL: https://itcentres.lnu.edu.ua/e-learning/introduction-it-in-education/

# ШТУЧНИЙ ІНТЕЛЕКТ У ВІЙСЬКОВІЙ СПРАВІ

*Шпак М. О.*
*maksimshpak20047@gmail.com*
*Черкаський державний бізнес-коледж*
*Науковий керівник: Люта М. В.*
*м. Черкаси, Україна*

Лише уявіть, вороже військо рятується втечею, а їх переслідують десятки маленьких дронів, які з далеку зовсім не відрізняються від аматорських. Але дрони не зовсім аматорські, а обладнані спеціальними камерами та процесором для сканування місцевості та автономного прийняття рішень та обрання цілі. Також обладнанні датчиками та вибухівкою, щоб знищувати ворожу техніку та солдат вибухаючи при контакті з цілю.

І це не наукова фантастика, а реальність, що наступила на весні 2020 року. Саме тоді солдати, які були вірні Халіфі Хафтару, відступали втечею від сил лівійського уряду, яких переслідували дрони, здатні працювати без участі людини, та стежили за втікачами. Тоді ООН зафіксували перший випадок, коли безпілотник без наказу оператора вбив людину. І це лише один приклад застосування штучного інтелекту на полі бою, але є безліч прикладів його застосування для різних завдань.

Тому давайте розберемося де саме використовується штучний інтелект у військовій справі. Отже, ШІ використовують:

- Міністерства оборони використовують ШІ для вербування солдатів, прийняття стратегічних рішень, розпізнавання загроз тощо.
- ЗСУ застосовують технології біометричної ідентифікації, роботів-саперів, інструменти пошуку підозрілих осіб та інструменти аналізу супутникових знімків.
- Армія Ізраїлю використовує турелі, дрони та системи ліквідації цілей керовані за допомогою ШІ.
- США тестують AR – окуляри та гвинтокрили які керуються дистанційно.
- Нідерланди використовують БТР, які є автономними
- Китай використовує ШІ для передбачення можливого курсу польоту

ракети.

Історія використання ШІ у військовій справі почалася ще з 1950-х років коли почалася програма протиракетної оборони, та 1960-х – застосування обчислювальних систем для командування та управління, які були підтримуванні Пентагоном. Однак уявлення про системи командування наближені до сучасних почали формуватися лише в останні десятиліття холодної війни. Планувалося створити систему допомоги для прийняття рішень, що виходить за межі існуючих в той час. Основним варіантом на той час була «Всесвітня система військового командування та управління». Вона була побудована на точних та своєчасних рішеннях з використанням інтелектуальних обчислювальних машинах, які могли допомогти в плануванні та формулюванні рішень та управлінні невизначеністю в бойовій обстановці, яка швидко змінюється.

З того часу було використано безліч інновацій, і тепер ШІ та алгоритм машинного навчання відіграють ключову роль у військовій справі. Велику роль ШІ відіграю при вербуванні та пошуку кваліфікованих кандидатів, що готові для служби в армії. Це відбувається за рахунок швидкої обробки великої кількості даних, та оптимізації безлічі аспектів процесу найму. ШІ здатний допомогти в навчанні солдатів багатьом навичкам. Наприклад, у лютому компанія «Northrop Grumman» уклала контракт із «DARPA» на розроблення асистента для тренувань пілотів на гвинтокрилах «Black Hawk».

Очікується, що система, яка вбудовується в AR-гарнітуру за допомогою мовлення і графічних підказок, зможе допомгти льотчикам вивчити як виконувати нові завдання, скоротити кількість помилок і прискорити виконання місій.

Армія США також використовує програмне забезпечення для моделювання бойових тренувань. ПЗ дозволяє солдатам виконувати завдання у VR та отримувати навички, які потім можна застосувати у реальному житті.

За останні кілька років усе більше країн розробляє різні бойові пристрої та ШІ-системи. І деякі рішення з використанням Штучного інтелекту успішно

тестуються ЗСУ.

24 лютого 2022 року російські війська вторглися на територію України, розпочавши повномасштабну війну. Незважаючи на чисельну та вогневу перевагу Росії, українські війська успішно витісняють супротивника, і технології грають в цьому не останню роль.

25 лютого ШІ-стартап Reface оголосив про створення алгоритму розпізнання російських військ за супутниковими знімками. У березні Міністерство оборони почало використовувати систему розпізнавання облич від ClearViev AI. У квітні розробник на основі відкритих даних YouControl спільно з ШІ-компанією Artellence за підтримки СБУ запустили додаток «ТиХто», який дозволяє виявити підозрілих осіб. У червні Армія США погодилася передати Україні робо-пса «Spot» від Boston Dynamics для допомоги в знешкодженні мінометних снарядів та касетних боєприпасів в деокупованих регіонах. У серпні «Нова Пошта» та ДСНС повідомили про створення роботів-саперів.

## Список використаних джерел


1. Війна та нефромережі: як штучний інтелект використовується на полі бою [Електронний ресурс]. Режим доступу до ресурсу: https://forklog.com.ua/exclusive/vijna-ta-nejromerezhi-yak-shtuchnyj-intelekt-vykorystovuyut-na-poli-boyu.
2. Штучний інтелект та нейромережі: про що мріють сучасні командири [Електронний ресурс]. Режим доступу до ресурсу: https://focus.ua/uk/voennye-novosti/523613-iskusstvenny-intellekt-na-vojne-o-chem-mechtayut-sovremennye-komandiry.
3. Як штучний інтелект допомагає ЗСУ громити ворога [Електронний ресурс]. Режим доступу до ресурсу: https://minfin.com.ua/ua/2022/12/07/96818537/
4. Штучний інтелект для армії, чи готова Україна до високотехнологічно переоснащення [Електронний ресурс]. Режим доступу до ресурсу:

https://lb.ua/economics/2021/10/15/496227_shtuchniy_intelekt_armii_chi_gotova.html

# Секція 4.

# РОБОТОТЕХНІКА ТА АДМІНІСТРУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ

# СТВОРЕННЯ МІКРОПРОЦЕСОРНОЇ ОХОРОННОЇ СИСТЕМИ

*Ільченко Є. І.*
*lizailch17@gmail.com*
*Черкаський державний бізнес-коледж*
*Науковий керівник: Михайлюта С. Л.*
*м. Черкаси, Україна*

**Актуальність теми** роботи. Завдання збереження майна та цінностей зберігає свою актуальність попри плин часу. Особливе місце серед цінностей займають музейні експонати. Вирішенню завдання створення охоронної системи музейних експонатів присвячена тема даної роботи.

**Метою роботи** є створення діючої моделі охоронної системи музейних експонатів, виконаної з використанням лазерних випромінювачів.

Для досягнення поставленої мети у ході роботи вирішені такі завдання:

1) Проведено аналіз джерел та відомих технічних рішень.
2) Розроблено комплект схем на основі мікропроцесорного модуля Arduino.
3) Виконано імітаційне моделювання системи у програмному середовищі Tinkercad.

**Об’єктом дослідження** є охоронні системи та системи контролю і обмеження доступу.

**Предметом дослідження** є мікропроцесорна охоронна система на основі лазерних випромінювачів.

Аналіз джерел та відомих технічних рішень дозволив класифікувати відомі рішення та виділити серед них такі: система відеоспостереження, системи контролю доступу до периметра, системи на основі датчиків руху – інфрачервоних та радіохвильових, волоконно-оптичні системи виявлення, наземні радіолокаційні системи, мікрохвильові бар’єри, електрифіковані огорожі, тощо. Серед розглянутих систем оптимальними за критеріями максимуму ефективності та мінімуму затрат на створення виявилися системи на основі лазерних випромінювачів.

На основі аналізу відомих схемотехнічних рішень розроблена електрична

структурна схема мікропроцесорної охоронної системи (рис.1).

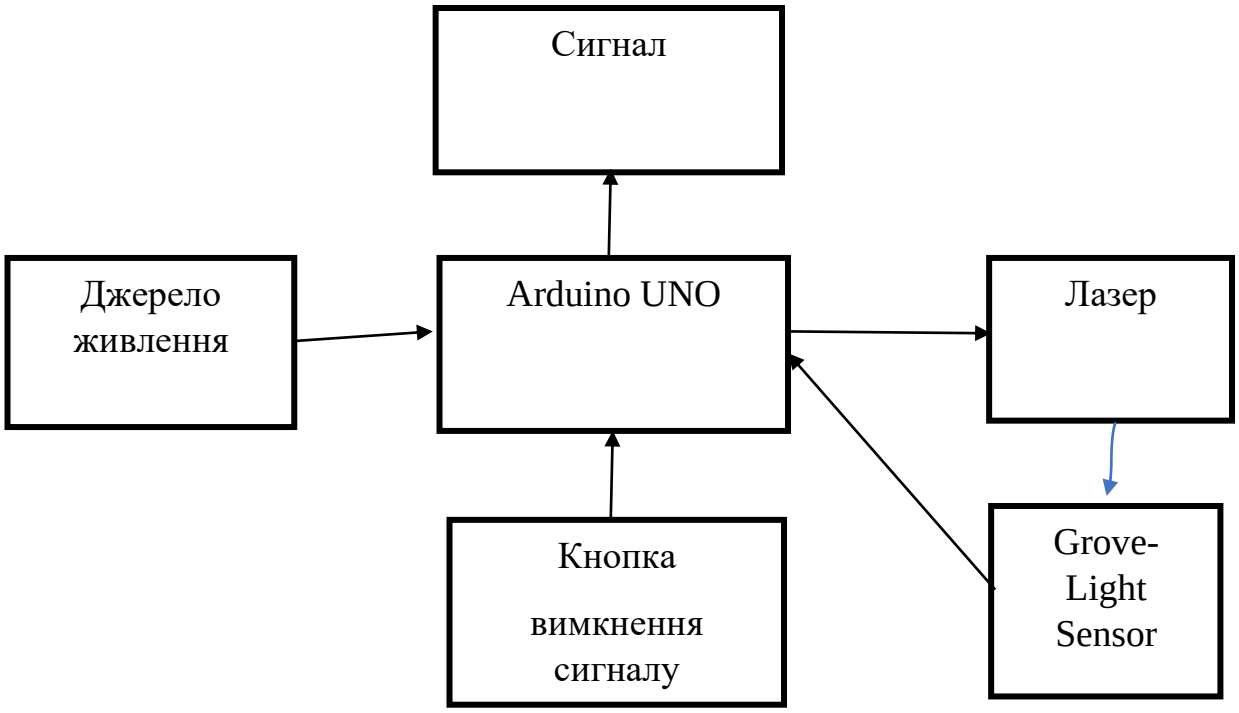



Рисунок 1 – Схема електрична структурна мікропроцесорної охоронної системи.

На основі структурної схеми у середовищі Tinkercad розроблена електрична принципова схема мікропроцесорної охоронної системи (рис. 2) та схема з'єднань (рис.3).

Крім апаратної частини також розроблено програмне забезпечення.

Для впевненості у працездатності розробленої мікропроцесорної охоронної системи проведено її моделювання у середовищі Tinkercad (рис. 3). Моделювання у середовищі Tinkercad дозволило переконатися у працездатності розробленої системи, як апаратно – програмного комплексу.

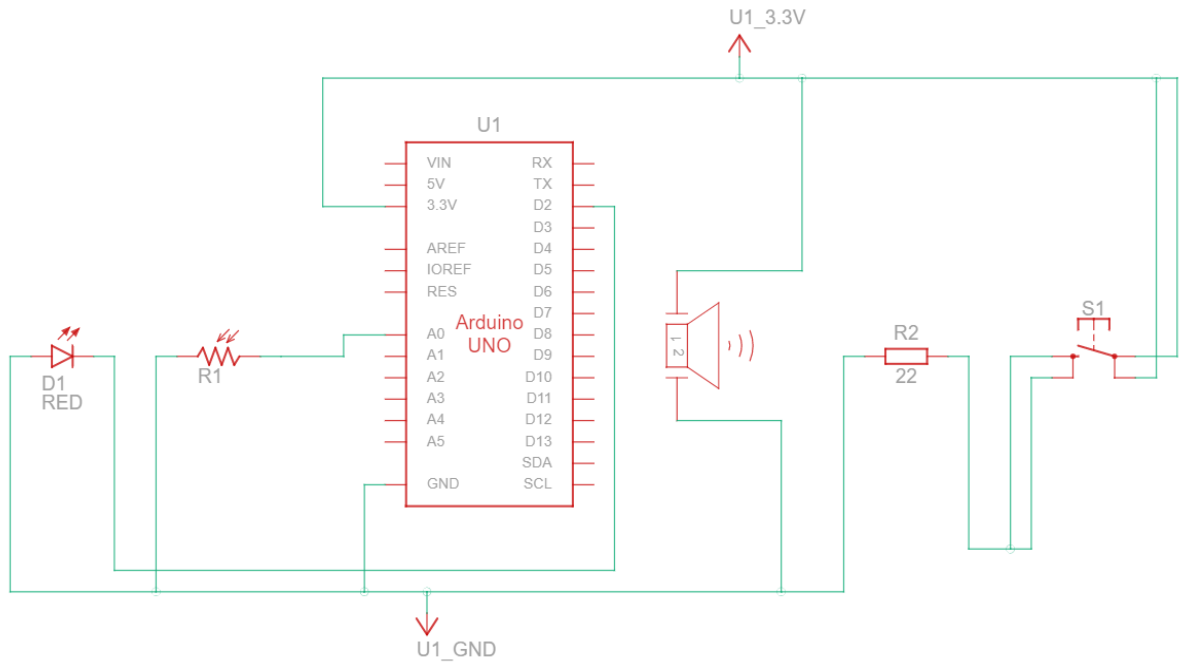



Рисунок 2 – Схема електрична принципова охоронної системи

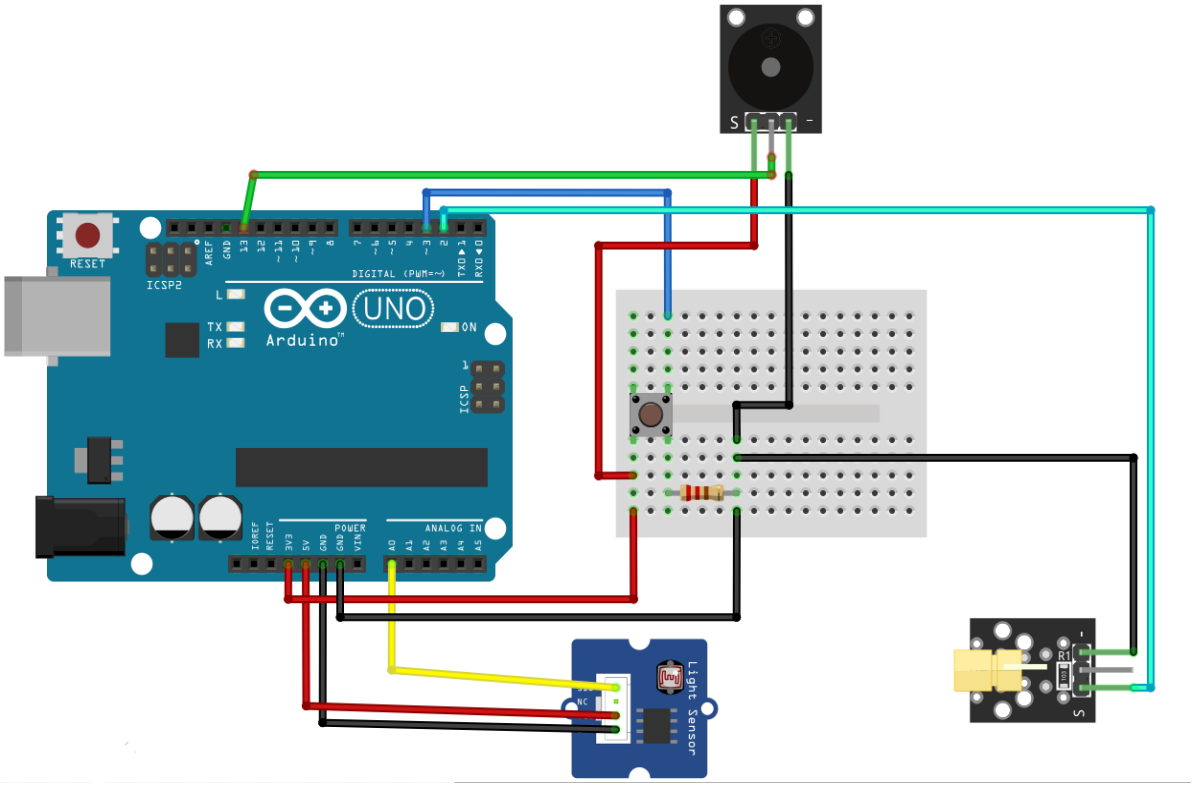



Рисунок 3– Схема з’єднання модулів розробленої системи для моделювання у середовищі Tinkercad.

### *Висновки*

На основі аналізу джерел та відомих рішень розроблені електричні схеми мікропроцесорної охоронної системи (структурна схема, принципова схема, схема з'єднань). Створено програмне забезпечення. Проведено імітаційне моделювання розроблюваної системи у середовищі Tinkercad, що дозволило переконатися у працездатності системи загалом та розробленого для неї програмного забезпечення зокрема.

### Список використаних джерел


1. David Kushner (2011-10-26). "The Making of Arduino". IEEE Spectrum. URL: https://spectrum.ieee.org/the-making-of-arduino
2. Безпека лазерних виробів – Частина 1: Класифікація обладнання та вимоги (2-е видання). Міжнародна електротехнічна комісія. 2007 рік.


## СВІТЛОМУЗИЧНИЙ ПРИСТРІЙ


*Петренко А. В.*
*arsfix2004@gmail.com*
*Черкаський державний бізнес-коледж*
*Науковий керівник: Михайлюта С. Л.*
*м. Черкаси, Україна*


**Актуальність теми.** Світломузичний пристрій – це спеціальний вид освітлювача, який створює візуальні ефекти, синхронізовані з музикою. Він є невід'ємною частиною сучасної розважальної індустрії, створює незабутню атмосферу та допомагає глибше зануритися у музику на концертах, вечірках, у нічних клубах. Основним принципом роботи світломузичного пристрою є перетворення електричних сигналів, які перетворюються у звукові коливання, у світлові ефекти.

**Метою** даної роботи є створення світломузичного пристрою з безпечною напругою живлення (до 36В) та практично закріпити теоретичні знання, отримані при вивченні навчального курсу – комп'ютерна електроніка.

Для досягнення поставленої мети у роботі вирішені такі завдання:

1) Проведено аналіз джерел та відомих рішень, на їхній основі розроблені електричні структурна, функціональна та принципова схеми світломузичного пристрою.
2) Розроблені монтажні плати блоків: живлення, підсилювача та фільтрів.
3) Здійснено монтаж та налагодження світломузичного пристрою.
4) Виготовлена відеопрезентація-звіт виконаної роботи.

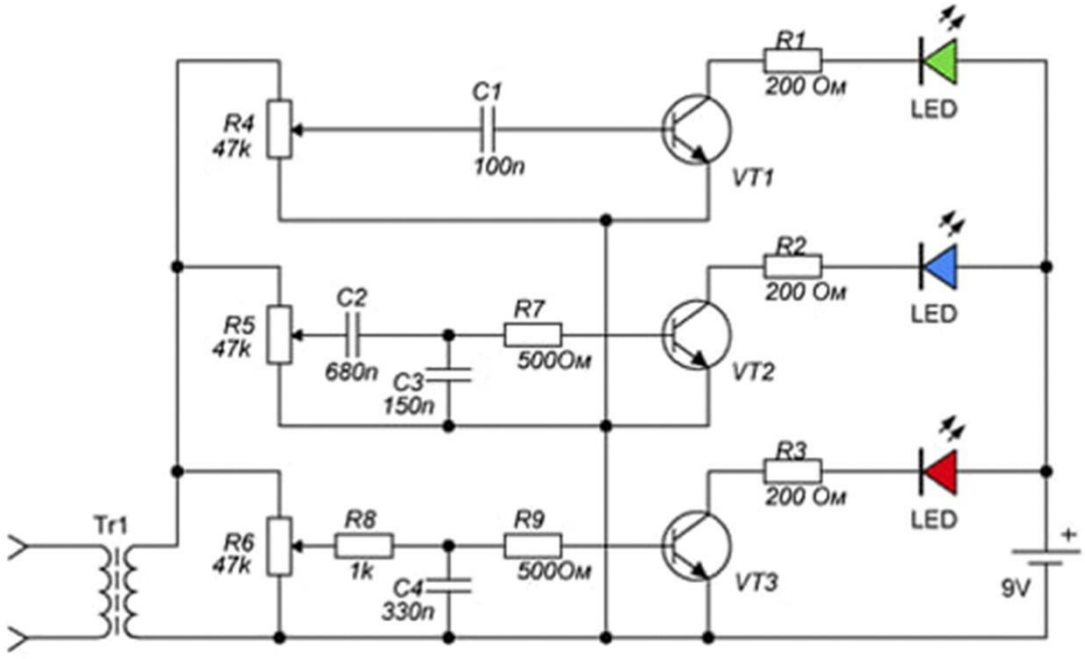
**Об'єктом роботи** є світломузичний пристрій, **предметом роботи** є технологія розробки та виготовлення світломузичного пристрою з низьковольтним живленням (12В).

**Принцип роботи** світломузичного пристрою полягає у підсиленні електричного сигналу, який надходить з джерела сигналу звукового діапазону частот, наступного розділення полоси частот на три піддіапазони та перетворення отриманих трьох електричних сигналів, за допомогою світлових стрічок, у світлові потоки.

Згідно перетворенню Фур'є, любий сигнал може бути представлений набором гармонічних сигналів визначених амплітуд та частот. Отже, по суті, опрацьовуючи електричний сигнал, який надходить від музичного пристрою, відбувається опрацювання кінцевого числа набору гармонічних сигналів. За допомогою фільтрів ці сигнали розділяються на три групи частот: низькі, середні та високі. Сигнали кожної групи частот підсилюються транзисторними підсилювачами, після чого передаються на світлодіодні стрічки, які розміщені у спеціальних балках (коробах) і генерують світло, відповідно до параметрів вхідного сигналу, що дозволяє створювати різноманітні світлові ефекти. Джерелом вхідного сигналу, зазвичай, є музичний програвач, або мікшерний пульт. Створений пристрій виконано на основі принципової схеми, зображеної на рис.1.

Сигнальний трансформатор на вході схеми використовується для гальванічної розв'язки між даним блоком і каскадом попереднього підсилення (використаний з перспективою дослідження інших схемотехнічних рішень). Резистори R4-R6 використовуються для незалежного керування рівнем сигналу

у кожному з трьох каналів. На С1 реалізований фільтр високих частот (ФВЧ), на С2-С3-R7 - реалізований фільтр середніх частот (ФСЧ), на R6-C4-R7 реалізований фільтр низьких частот (ФНЧ). Транзистори VT1-VT3 виконують функції напівперіодних випрямлячів та підсилювачів сигналів. Резистори R1-




R3 обмежують струми світлодіодних стрічок.

Рисунок 1 – Схема електрична принципова базового блоку

Застосування транзисторів VT1-VT3 та світлодіодних стрічок дозволяє використовувати низьку напругу живлення (12V). Джерело живлення містить трансформатор, який зменшує напругу з 220В до 11В, двонапівперіодний діодний випрямляч та згладжуючий фільтр на електролітичних конденсаторах ємністю 4000мкФ. Завдяки використанню транзисторів та світлодіодних стрічок, у порівнянні з тиристорними схемами, світломузичний пристрій дозволяє створювати більш складні світлові ефекти,

Для попереднього підсилення сигналу використано підсилювач, електрична принципова схема якого зображена на рис. 2.

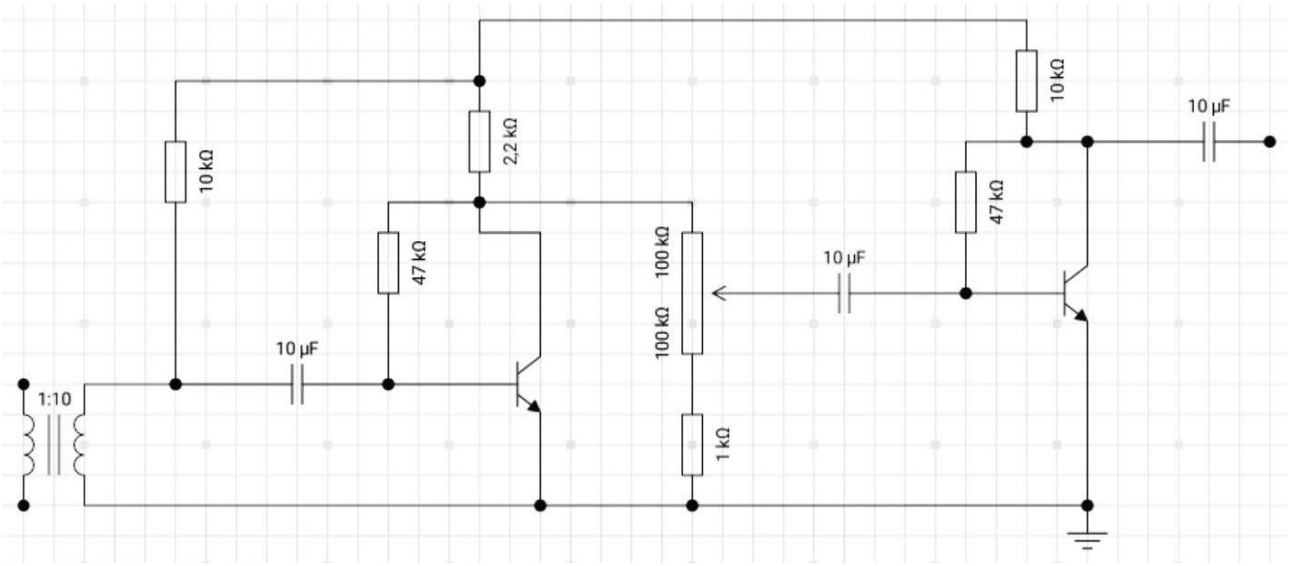



Рисунок 2 - Схема електрична принципова попереднього підсилювача сигналу

## Висновки

Технології, які можуть бути використані для виготовлення світломузичних пристроїв, розвиваються й урізноманітнюються, що дозволяє створювати пристрої, здатні відтворювати все більш складні та вражаючі світлові ефекти: застосування силових транзисторів та світлодіодних стрічок, у порівнянні з тиристорними схемами, дозволяє відтворювати складніші візуальні ефекти, отримати більш точну їхню відповідність відтворюваним звуковим коливанням, разом з тим, реалізувати пристрій з безпечною, низькою напругою живлення. У ході роботи виконані поставлені завдання та досягнена мета роботи – виготовлено світломузичний пристрій з безпечною напругою живлення. Оскільки напруга живлення становить 12 В, створений світломузичний пристрій зручний для використання у автомобілі з бортовою напругою 12 В.

## Список використаних джерел

1. Світломузика – схема. [Інтернет-ресурс] – режим доступу: https://cxem.net/sound/light/light23.php

2. Світломузика: що це таке і як вона працює. [Інтернет-ресурс] – режим доступу: https://www.avm.ua/blog/av-obsuzhdeniya/svetlomuzyka-chto-eto-i-kak-ona-rabotaet/
3. Що таке світломузика. [Інтернет-ресурс] – режим доступу: https://www.svetlomuzika.com.ua/ua/news/23-shcho-take-svitlomuzika.html
4. Світломузика: робота з іншими професіями. [Інтернет-ресурс "Український портал звукорежисерів та аудіоінженерів"]. – режим доступу: https://sound.com.ua/svetlomuzika-robota-z-inshymi-profesi.html
5. Як зробити світломузику вдома. [Інтернет-ресурс] – режим доступу: https://lifehacker.ua/yak-zrobiti-svitlomuziku-vdoma/

## СИСТЕМА ДИСТАНЦІЙНОГО КЕРУВАННЯ МУЛЬТИВАРКОЮ

*Самоїд Д. С.*
*diana.samoid@gmail.com*
*Черкаський державний бізнес-коледж*
*Науковий керівник: Михайлюта С. Л.*
*м. Черкаси, Україна*

**Актуальність теми.** При сучасних технологіях завдання віддаленого керування технікою є актуальним. Особливої популярності набула концепція “розумного будинку”, при якій реалізовується віддалене керування домашньою технікою: смарт-чайник, кондиціонер з віддаленим керуванням, холодильник, роботи-пилососи, лампочки, кавоварки, пральні та сушильні машини, інше.

**За мету** даної **роботи** була поставлена розробка системи дистанційного керування мультиваркою, у ролі пульта керування якою є смартфон.

В ході виконання роботи, для досягнення її мети, вирішено такі завдання:

1) Проведено аналіз джерел та відомих схемотехнічних рішень.
2) Розроблено комплект електричних схем системи керування мультиваркою на основі плати мікроконтролера ESP8266 та смартфона.

**Об’єктом аналізу та дослідження у ході проведеної роботи** стала мультиварка.

**Предметом роботи с**тала система дистанційного керування мультиваркою

від смартфону.

Проведена робота виконана кількома етапами, розглянутими далі.

Щоб керувати мультиваркою віддалено необхідно спочатку наповнити чашу необхідними продуктами, для чого потрібна безпосередня участь людини. Якщо плани на вечір раптом змінилися, процес приготування можна перервати дистанційно. Зрозуміло, що такий режим роботи прийнятний у випадку відсутності необхідності помішувати вміст та додавати інгредієнти.

До блок-схеми, яка відображає роботу системи дистанційного керування мультиваркою, входять: силовий ключ, плата мікроконтролера з Wi-Fi 8266, електронагрівач, блок живлення 220 В (50 Гц), смартфон. Разом з тим, джерелом сигналу керування може бути любий пристрій з підтримкою передачі сигналу по Wi-Fi технології. В даній роботі у якості джерела сигналу використовуються смартфон.

В ході проведеного аналізу джерел та відомих схемотехнічних рішень, у якості контролеру був вибраний ESP8266 (рис.1).


Рисунок 1 — модуль мініатюрний WeMos D1 mini ESP8266

Характеристики модуля мініатюрного WeMos D1 mini ESP8266:

1) Напруга живлення 5 В (через USB-порт або через пін 5V) або 3,3 В (через пін 3V3)
2) Напруга логічних сигналів 3,3 В
3) Дискретних входів-виходів 11

4) Аналоговий вхід 1 (максимальна вхідна напруга 3,3 В)
5) Тактова частота процесора 80 МГц/ 160 МГц
6) USB-UART конвертер - CH340
7) LED підключений до GPIO2 (D4)
8) Флеш пам’ять 4 МБ
9) Довжина 34,2 мм
10) Ширина 25,6 мм
11) Вага 10 г

Модуль вмонтовано в плату живлення та керування мультиварки (схема електрична принципова подана на рис. 2, зовнішній вигляд плати – на рис. 3).

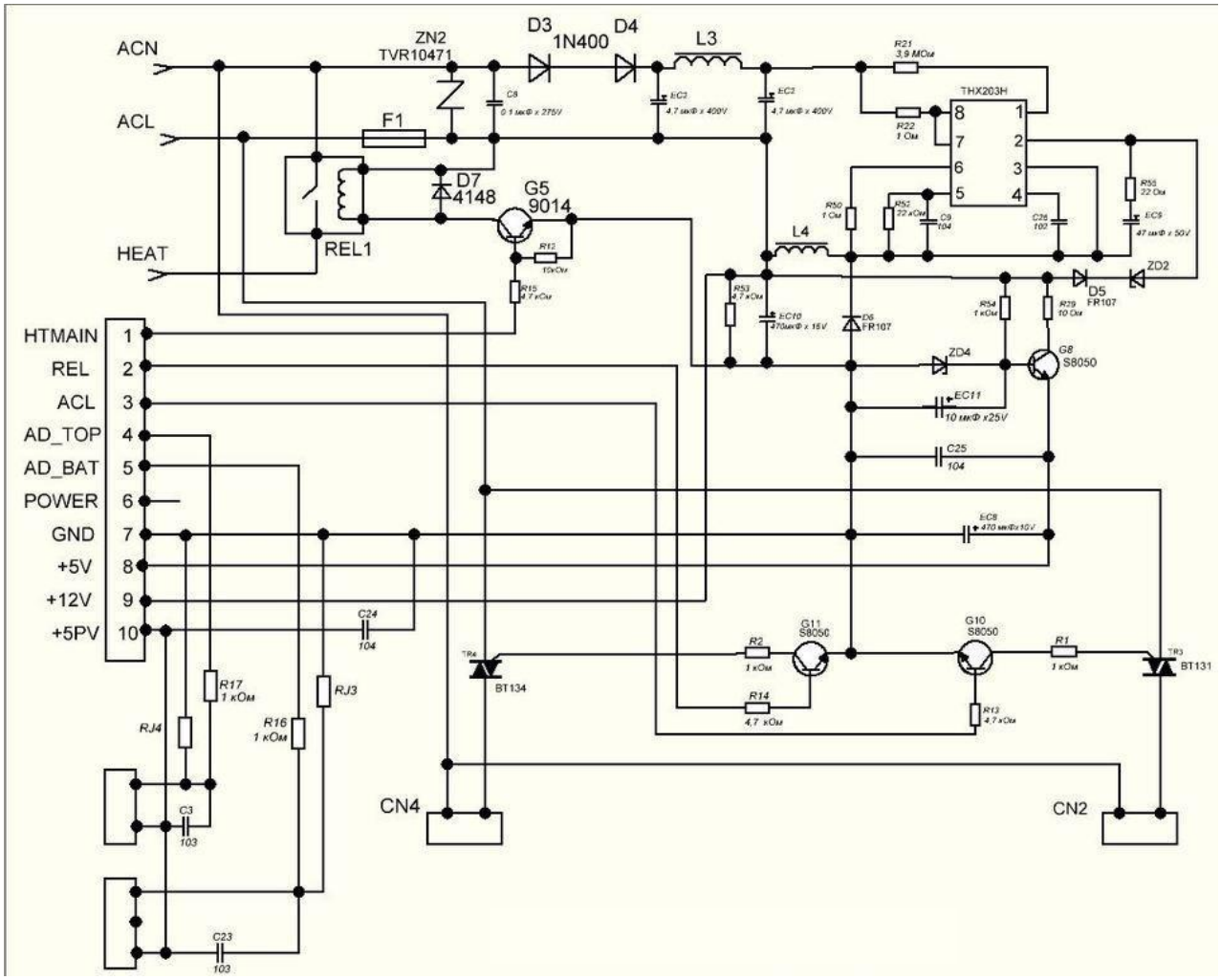



Рисунок 2 — Схема електрична принципова плати живлення та керування мультиварки


Рисунок 3 — Зовнішній вигляд плати живлення та керування мультиварки

***Висновки***

В ході виконання роботи були виконані поставлені завдання та досягнена мета роботи – розроблення системи дистанційного керування мультиварки. Закріплені теоретичні знання та вдосконалені практичні навики з дисциплін «Комп’ютерна електроніка» та «Комп’ютерна схемотехніка».

***Список використаних джерел***

1. Мініатюрний WeMos D1 mini ESP8266 — Доступно за посиланням: https://geekmatic.in.ua/ua/nodemcu_esp8266_wemos
2. Приклади мультиварок — Доступно за посиланням: https://ek.ua/ua/ek-list.php?katalog_=746&brands_=&save_podbor_=1
3. Плата живлення мультиварки Redmond RMC-4502 — Доступно за посиланням: https://izi.ua/p-28593220-plata-pitaniya-multivarki-redmond-rmc-m223s

Наукове електронне видання

# ЗБІРКА НАУКОВИХ ПРАЦЬ

**XV Студентська**
**науково-практична конференція**
**студентів, аспірантів та молодих вчених**

**за тематикою**
**«Тенденції розвитку ІТ-технологій в Україні»**

ISBN 777-777-7777-77-7

**(електронне видання)**

**Матеріали XV Студентської**
**науково-практичної конференції**
**студентів, аспірантів та молодих вчених**

Комп’ютерна верстка: *Марченко С. В.*
Відповідальний за випуск: *к.т.н., Хотунов В. І.*
Дизайн обкладинки: *Оліфіренко В. М.*