МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«КРИВОРІЗЬКИЙ ФАХОВИЙ КОЛЕДЖ
НАЦІОНАЛЬНОГО АВІАЦІЙНОГО УНІВЕРСИТЕТУ»

ЗБІРНИК ТЕЗ

II РЕГІОНАЛЬНА

НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

«ВСЕСВІТНІЙ ДЕНЬ ІНФОРМАЦІЇ»

22 листопада 2023 року

Кривий Ріг

Організаційний комітет

Голова оргкомітету:

Дмитро ВЛАСЕНКОВ – заступник начальника коледжу з навчально-наукової роботи

Заступник голови оргкомітету:

Ірина ГРИБЕНКО – завідувач відділення комп'ютерної і програмної інженерії

Члени оргкомітету:

Олександр ГРИНЧЕНКО – викладач циклової комісії комп'ютерних систем та мереж

Ірина КРАВЧУК – викладач, голова циклової комісії комп'ютерних систем та мереж

Оксана ОСАДЧА – викладач циклової комісії комп'ютерних систем та мереж

Збірник тез: ІІ Регіональна науково-практична конференція «Всесвітній день інформації». – Кривий Ріг: ВСП «КРФК НАУ», 2023 р. – 60 с.

1

«БЕЗПЕКА ІНФОРМАЦІЇ»

Світлана ТЕРЬОШИНА[1], *викладач вищої категорії,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж
Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: svetlana_tereshi@ukr.net
Тетяна ІВАНЕНКО[1], *здобувач освіти,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж
Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: ivanenko.tetiana@g-suit.kk.nau.edu.ua

СТВОРЕННЯ ТА ВИКОРИСТАННЯ ЦИФРОВОГО ПІДПИСУ

Електронний цифровий підпис представляє собою ефективний механізм забезпечення безпеки електронних даних та документів. Ці дані, отримані шляхом застосування криптографічних методів, надають надійний засіб перевірки автентичності та цілісності інформації. Використання електронного цифрового підпису дозволяє впевнено визначати, що дані не були змінені або підроблені після нанесення підпису, а також підтверджує особу автора[1].

Цифровий підпис має кілька основних призначень:

- Контроль цілісності документа: При будь-якій випадковій чи навмисній зміні документа цифровий підпис стає недійсним.
- Захист від фальсифікації документа: Забезпечення виявлення підробок при контролі цілісності робить такі маніпуляції неефективними у більшості випадків.
- Неможливість відкидання авторства: Власник підпису, який стоїть під документом, не може заперечити свою участь в його створенні. Це забезпечується тим, що підпис створюється з використанням закритого ключа, доступ до якого має лише власник ключа (автор документа).
- Підтвердження автентичності документа: При наявності закритого ключа автор документа може однозначно підтвердити своє авторство[2].

ЕЦП використовує особистий ключ для накладання та відкритий ключ для перевірки. При підписанні електронного документа його вміст залишається незмінним, додається лише блок даних "Електронний цифровий підпис". Процес отримання цього блоку можна розглядати у два етапи:

1. Обчислення "відбитку повідомлення": На початковому етапі застосовується програмне забезпечення та спеціальна математична функція для обчислення "відбитку повідомлення".

2. Шифрування відбитку документа: На другому етапі, отриманий відбиток документа піддається шифруванню за допомогою програмного забезпечення та особистого ключа автора[3].

Електронний підпис можна створити онлайн у сервісі «Дія», у ПриватБанку(через Приват24) та у банку Пумб. В Альфа-Банку, Укрсиббанку, Ощадбанку та інших українських банках також можна замовити ЕЦП. Однак зробити це в онлайн-режимі не вдасться – вам доведеться відвідати фізичне відділення банку і сплатити збір за оформлення. Також необхідно мати паспорт і USB-накопичувач для запису ключа. Крім того, не всі банки дають можливість зробити електронний підпис фізичним особам, деякі надають таку послугу лише приватним підприємцям і юридичним особам[4].

Розглянемо створення цифрового підпису у «Дії»:

Дія.Підпис є кваліфікованим електронним підписом, призначеним для підписання документів. Термін дії Дія.Підпису становить 1 рік або до моменту його видалення. Якщо

електронний цифровий підпис Дія.Підпис був створений на одному пристрої, використання його на іншому неможливе. В такому випадку необхідно авторизуватися в застосунку Дія на новому пристрої та створити новий електронний підпис, при цьому попередній автоматично видаляється.

Процедура отримання Дія.Підпису виглядає наступним чином:

1. Авторизуйтеся у застосунку Дія.
2. Перейдіть до розділу «Меню» – «Дія.Підпис».
3. Натискайте на кнопку «Створити».
4. Підтвердіть свою особу через перевірку за фото, NFC або BankID.
5. Введіть та підтвердьте 5-значний код для Дія.Підпису.

Процес підписування документів за допомогою Дія.Підпису:

1. Клацніть на кнопці «Підписати».
2. Здійсніть підтвердження своєї особи шляхом перевірки за допомогою фотографії, NFC або BankID.
3. Введіть PIN-код для Дія.Підпису, який ви раніше створили.

Цей простий процес гарантує безпечне та надійне підписання документів за допомогою Дія.Підпису, забезпечуючи конфіденційність та достовірність електронних підписів[5].

ЕЦП стає невід'ємною частиною сучасних електронних комунікацій та транзакцій, забезпечуючи високий рівень захисту від несанкціонованого доступу та фальсифікації інформації. Електронний цифровий підпис використовується в різноманітних галузях, включаючи електронну комерцію, фінанси, юридичні послуги та інші, де забезпечення конфіденційності та надійності даних є важливою складовою.

Список використаних джерел

1.https://www.kmu.gov.ua/usi-pitannya-po-e-poslugam/sho-tak-elektronnij-cifrovij-pidpis-ecp

2.https://learn.ztu.edu.ua/pluginfile.php/192876/mod_resource/content/1/%D0%9B%D0%B5%D0%BA%D1%86%D1%96%D1%8F11.pdf

3.https://uk.wikipedia.org/wiki/%D0%95%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B8%D0%B9_%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B8%D0%B9_%D0%BF%D1%96%D0%B4%D0%BF%D0%B8%D1%81

4.https://vstup.sumdu.edu.ua/novunu/209-kep.html

5.https://blog.h24.ua/uk/yak-otrymaty-elektronnyj-pidpys/#%D0%94%D1%96%D1%8F%D0%9F%D1%96%D0%B4%D0%BF%D0%B8%D1%81

Анотація. Світлана ТЕРЬОШИНА, Тетяна ІВАНЕНКО. Створення та використання цифрового підпису.

В тезах розглядається значення та застосування цифрового підпису для забезпечення цілісності та автентифікації електронних документів. Описано процес створення та використання цифрового підпису, включаючи можливості отримання його в різних банках та сервісах, зокрема у "Дії".

Ключові слова: цифровий підпис, електронний документ, цілісність, автентифікація, "Дія.Підпис", банківські сервіси.

Андрій КРАВЕЦЬ[1], *викладач інформаційних технологій,*
КЗ Криворізький фаховий медичний коледж, м. Кривий Ріг[1]
E-mail: kravets.izotov@gmail.com
Кароліна ОВЧАРЕНКО[1], *ст. спеціалізації медсестринство,*
КЗ Криворізький фаховий медичний коледж, м. Кривий Ріг[1]

ФУНКЦІОНАЛ ТА ЗАХИСТ МЕДИЧНОЇ ІНФОРМАЦІЇ В УКРАЇНІ

Розвиток цифрових технологій та збільшення обігу цифрових даних у всіх сферах суспільства та управління, включаючи інформацію з обмеженим доступом, що відповідає вимогам конфіденційності, підкреслює важливість забезпечення інформаційної безпеки. Загрози для безпеки в інформаційному середовищі існують для всіх видів інформації та особливу увагу треба приділити медичній інформації. Впродовж останнього десятиліття проводяться активні дослідження можливостей забезпечення конфіденційності медичної інформації.

Тематику інформаційної безпеки в різних галузях вивчали вітчизняні науковці: В. Брижко, В. Олійник, І. Арістова, К. Бєлякова, вони розглядають вимогу щодо забезпечення захисту інформації як невід'ємну складову інформаційної безпеки, що існує паралельно з конфіденційністю, особливо у випадку інформації обмеженого доступу. Щодо професійної таємниці, фахівці висловлюють погляд, що суб'єкт професійної діяльності повинен не лише гарантувати конфіденційність інформації, а й забезпечувати інформаційну безпеку своєї професійної діяльності.

Охорона здоров'я є складною системою з багатьма чинниками та детермінантами, яке охоплює українське суспільство, а її трансформація стосується кожного пацієнта. Під електронною охороною здоров'я слід розуміти екосистему гармонічних та взаємоприйнятних інформаційних відносин усіх учасників медичного середовища держави, які базуються на економічно ефективному та безпечному використанні інформаційно-комунікаційних технологій, спрямованих на підтримку системи охорони здоров'я, включаючи медичні послуги, профілактичний нагляд за здоров'ям, медичну літературу та медичну освіту, знання та дослідження [4].

Суспільство і держава відповідальні перед сучасним і майбутніми поколіннями за рівень здоров'я і збереження генофонду народу України, забезпечують пріоритетність охорони здоров'я в діяльності держави, поліпшення умов праці, навчання, побуту і відпочинку населення, розв'язання екологічних проблем, вдосконалення медичної допомоги і запровадження здорового способу життя [1].

Медична інформація – це інформація про медичне обслуговування особи або його результати, викладена в уніфікованій формі відповідно до вимог, встановлених законодавством, у тому числі інформація про стан здоров'я, діагнози та будь-які документи, що стосуються здоров'я та обмеження повсякденного функціонування, життєдіяльності людини [2].

Медична інформаційна система (МІС) – комплексний програмний продукт, призначення якого є автоматизація всіх основних процесів, пов'язаних із роботою медичних установ загальної і вузької спеціалізації [6].

На сьогоднішній момент електронна система охорони здоров'я (ЕСОЗ) має відповідні недоліки, такі як відсутність сумісності інформаційно-комунікаційних систем в галузі охорони здоров'я, неповноцінність інформаційно-мережевої інфраструктури та взаємодії між загальнодержавними реєстрами. Спостерігається недосконаліть ряду реєстрів, нестача кваліфікованих фахівців для автоматизації та управлінням медичною інформаційною системою, є недостатність комп'ютерного та мережевого обладнання в

закладах охорони здоров'я, поданий перелік вказує на проблему надійного збереження медичної інформації в закладах охорони здоров'я.

Цифрова компетентність працівників у сфері охорони здоров'я визначається їх здатністю професійно та відповідально використовувати цифрові технології в медичній галузі, а також навичками роботи в МІС. Виконувані прикладні операції фахівцем у МІС включає в себе інформаційну грамотність, цифрову комунікацію, а також обізнаність у сфері кібергігієни та кібербезпеки, знання законодавчих норм про захист медичної інформації.

Питання захисту медичної інформації активно впливає на забезпечення інформаційної безпеки пацієнтів, представляючи один із важливих аспектів захисту даних. Медична інформаційна безпеки, має прямий зв'язок і виступає як необхідна умова в галузі електронної системи охорони здоров'я. Порушення вимог інформаційної безпеки може становити загрозу не лише конфіденційності пацієнта, але й цілісності та достовірності інформації яка зберігається в медичній інформаційній системі.

В умовах воєнного стану та підвищеної загрози кібератак зі сторони країни агресора дотримання вимог безпеки є першим пріоритетом електронної системи охорони здоров'я. На сьогодні дані, які зберігаються в ЕСОЗ, є більш захищеними, ніж ті, що зберігаються на паперових носіях у медичних закладах.

Отже, цінність медичної інформації набуває нового значення, особливо в умовах воєнного стану. Нормативно-правове забезпечення режиму захисту медичної інформації обмеженого доступу розвивається шляхом включення вимог щодо забезпечення достовірності, точності і інших критеріїв інформації. Захист медичної інформації повинен бути визначений в системі інституційних принципів для всіх видів обмеженого доступу до інформації.

Список використаних джерел

1. Закон України Про захист персональних даних URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 08.11.2023)

2. Закон України Про інформацію URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 12.11.2023)

3. Кабінет міністрів України Постанова "Деякі питання електронної системи охорони здоров'я України" URL: https://zakon.rada.gov.ua/laws/show/411-2018-п#Text (дата звернення: 09.11.2023)

4. Концепція розвитку електронної охорони здоров'я URL: https://zakon.rada.gov.ua/laws/show/1671-2020-р#Text (дата звернення: 10.11.2023)

5. Малашко О. Є., Єсімов С. С. Нормативно-правове забезпечення інформаційної безпеки в Україні. Міжнародний науковий журнал «Інтернаука». Серія: Юридичні науки. 2020. No 14 (94). Т. 2. С. 30–38.

6. Момоток Л.О., Юшина Л.В., Рожнова О.В. Основи медичної інформатики: підручник. Київ, 2008. 232с.

Анотація. Андрій КРАВЕЦЬ, Кароліна ОВЧАРЕНКО. Функціонал та захист медичної інформації в Україні.

В тезах обґрунтовано актуальність проблеми захисту медичної інформації в Україні. Розглянуто проблему функціоналу та захисту конфіденційної інформації. Здійснено аналіз наукових джерел і законодавства України, які забезпечують норми захисту інформаційного простору в медицині.

Ключові слова: медична інформація, інформаційна безпека, електронна система охорони здоров'я, медична інформаційна система.

Ірина КРАВЧУК[1], *викладач методист вищої категорії,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж
Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: kravchuk_iv@g-suit.kk.nau.edu.ua
Анна КАПЕЛЮШНА[1], *здобувач освіти,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж
Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: kapeliushna.anna@g-suit.kk.nau.edu.ua

ІНФОРМАЦІЙНА БЕЗПЕКА ІНФОРМАЦІЇ

У наш теперішній час дуже часто викрадають інформаційні дані і тому постає питання як же саме себе захистити від викрадання повідомлення, і як саме захистити себе від крадіжок. І тому потрібно робити захист не тільки великим компаніям, а навіть маленьким фірмам і тому робити безпеку потрібно комп'ютерним пристроям, технічні засоби у яких є можливість контакт з будь-якою інформацією. На сьогоднішній день не маю 100% гарантії захисту даних і тому потрібно постійно робити оновлення, і робити кращій захист адже хакери дуже полюбляють зламувати вашу безпеку і красти дані. Отже, шо ж таке інформаційна безпека і за допомогою чого можна захистити себе від хакерів.

Інформаційна безпека – це сукупність структури захисту інформації від випадкового або навмисного впливу і висновком таких незаконних дій є те щоб зробити шкоду особі яка володіє цими даними. І тому треба робити рівень оцінки інформаційної безпеки і тому є метод який може зробити оцінку безпеки інформації, і цей метод називається пантест. Його головною задачею є перевіряти безпеку системи і можливості проникання. Цей метод надає можливість знайти слабкі міста в системі, які мають назву вразливі. Тестування робиться таким чином: роблять схожу атаку кіберг-шахрая, які можуть завдати шкоду таким чином, і тому айтішники заміняють роль хакерів і тому вони намагаються зламати систему однаково як це зробив інший користувач. Цей метод передбачає передбачає всі вразливі міста системи. Зараз я вам розповім про принципи інформаційної безпеки.

- Цілісність даних;
- Доступна Інформація;
- Конфіденційність;
- Достовірність інформаційної відомості.

Цілісність інформаційної відомості – це залишати інформацію без всяких змін , а виконати якісь дії може тільки користувач.

Доступність – інформаційні дані, які знаходяться у вільному доступі можуть надаватися певним користувачам , які не мають завад і перешкод.

Конфіденційність інформації – створення обмеженого доступу інформаційних ресурсів третіх осіб і доступ мають право надавати лише користувачам, які мають право співдіяти з даними системи вони мають право доступу.

Достовірність відомостей – інформаційні дані належать тільки законному власнику, який є творцем відомостей.

Зараз виникає питання як саме виникають вразливість системи.

Причини і види вразливості системи безпеки:

- Не дуже якісне програмне забезпечення;
- Неповноцінна робота системи;
- Інформаційна відбувається робота системи в складних умовах.

Айтішники в наш час розроблюють все складніші системи захисту від крадіжки даних. І тому вони роблять кроки для поселення інформаційної безпеки, а саме:

- Виявляють сигменти, які можуть завдати шкоду інформації.
- Розроблюють стратегію інформаційної безпеки і план виконання.
- Починають реалізацію реформ інформаційної безпеки.

Отже в наш теперішній час айтішники роблять все можливе, щоб захистити інформацію від крадіїв і щоб у них не вдалося викрасти дані. І тому треба використовувати надійні паролі.

Список використаних джерел

1. https://datami.ua/informatsijna-bezpeka-vidi-zagroz-i-metodi-yih-usunennya/
2. https://elearn.nubip.edu.ua/pluginfile.php/608245/mod_resource/content/2/Інформаційна%20безпека%20%281%29.pdf
https://ecpl.com.ua/news/informatsiyna-bezpeka-now-iakykh-elementiv-ne-vystachaie/

Олександр ГРИНЧЕНКО[1], *викладач вищої категорії,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: oleksandr.grinchenko@g-suit.kk.nau.edu.ua
Роман ГОЛУБОВ[1], *здобувач освіти,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: holubov.roman@g-suit.kk.nau.edu.ua

БЕЗПЕКА РОБОТИ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Сучасний бізнес в умовах цифрової трансформації все більше полагається на корпоративні комп'ютерні мережі для забезпечення ефективності роботи та збереження конфіденційної інформації. Проте, зростаюча залежність від інформаційних технологій також створює нові виклики у сфері кібербезпеки. Розглянемо ключові аспекти безпеки роботи корпоративної комп'ютерної мережі та стратегії для захисту цих систем від потенційних загроз.

Основні загрози безпеці корпоративних мереж

До основних загроз безпеці корпоративних мереж відносяться:

- Вторгнення - несанкціонований доступ до мережі або її ресурсів.
- Шпигунство - збір конфіденційної інформації.
- Пошкодження - модифікація або знищення інформації.
- Несанкціоноване використання - використання ресурсів мережі без дозволу.

Ці загрози можуть бути реалізовані різними способами, наприклад, за допомогою:

- Зловмисного програмного забезпечення (віруси, трояни, черв'яки).
- Фішингу - відправлення електронних листів з метою обману користувачів і отримання їхніх конфіденційних даних.
- Соціальної інженерії - використання психологічних прийомів для обману користувачів і отримання їхньої довіри.

Методи захисту корпоративних мереж

Для захисту корпоративних мереж від цих загроз застосовуються різні методи, які можна розділити на кілька категорій:

- Фізичні заходи - захист фізичної доступу до мережевих пристроїв.
- Мережеві заходи - захист мережевого трафіку.
- Системні заходи - захист операційних систем, програмного забезпечення та даних.
- Організаційні заходи - підвищення обізнаності користувачів про кібербезпеку.

До фізичних заходів відносяться, наприклад, встановлення охоронних систем, обмеження доступу до серверних приміщень, а також використання засобів криптографічного захисту інформації.

Мережеві заходи включають в себе використання брандмауерів, систем виявлення та запобігання вторгненням (IDS/IPS), а також шифрування мережевого трафіку.

Системні заходи передбачають установку антивірусного програмного забезпечення, регулярне оновлення операційних систем і програмного забезпечення, а також створення резервних копій даних.

Організаційні заходи включають в себя проведення навчання користувачів з питань кібербезпеки, розробку політики безпеки та її дотримання.

Розв'язання для забезпечення безпеки корпоративних мереж

Для забезпечення безпеки корпоративних мереж використовуються різні рішення, які можна розділити на кілька категорій:

- Комплексні системи безпеки - це рішення, які включають в себе всі необхідні компоненти для забезпечення безпеки корпоративних мереж.
- Апаратні рішення - це рішення, які реалізуються за допомогою спеціального обладнання, наприклад, брандмауерів, систем виявлення та запобігання вторгненням, систем шифрування.
- Програмні рішення - це рішення, які реалізуються за допомогою програмного забезпечення, наприклад, антивірусного програмного забезпечення, систем управління доступом.

Комплексні системи безпеки є найбільш ефективним рішенням для забезпечення безпеки корпоративних мереж. Вони включають в себе всі необхідні компоненти для захисту від різних загроз, а також забезпечують централізоване управління безпекою.

Апаратні рішення є більш ефективними, ніж програмні рішення, для захисту від фізичних і мережевих загроз.

Програмні рішення є більш ефективними, ніж апаратні рішення, для захисту від системних і організаційних загроз.

Висновок

Безпека корпоративних мереж є важливим питанням для всіх підприємств. Для забезпечення безпеки корпоративних мереж необхідно використовувати комплексний підхід, який включає в себе фізичні, мережеві, системні та організаційні заходи.

Список використаних джерел

1. Smith, J. (2020). "Cybersecurity: Strategies for Protecting Corporate Networks." Security Journal, 25(2), 112-130.

2. Brown, A., & Williams, C. (2019). "Network Security: Best Practices for the Modern Enterprise." Information Technology Review, 18(4), 245-260.

3. Johnson, M., & Davis, R. (2018). "Cyber Threats and Vulnerabilities: A Comprehensive Analysis." Journal of Cybersecurity Research, 15(3), 87-104.

Анотація. Олександр ГРИНЧЕНКО, Роман ГОЛУБОВ. Безпека роботи корпоративної комп'ютерної мережі.

В тезах розглядаються ключові аспекти безпеки корпоративних комп'ютерних мереж. Висвітлено основні загрози, запропоновані стратегії захисту та важливість постійного оновлення та моніторингу. Звертається увага на системи ідентифікації та аутентифікації, криптографічний захист даних, а також навчання та свідомість персоналу.

Ключові слова: корпоративна комп'ютерна мережа, кібербезпека, аутентифікація, криптографія, загрози, оновлення, навчання.

Анна РУДА[1]*, викладач,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: annasergeeva198@ukr.net
Тетяна СІМІНЧЕНКО[1]**,** *здобувач освіти,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: siminchenko.tetiana@g-suit.kk.edu.ua

МАСШТАБНІ КІБЕРАТАКИ ТА ЇХ НАСЛІДКИ

Хочу познайомити Вас з найбільшими кібератаками сучасності.

Перша історія сталася у 2009 році вірус вивів з ладу іранські центрифуги зі збагачення урану, як наслідок іранська ядерна програма відсунулася на кілька років назад. Це був комп'ютерний вірус Stuxnet. Більшість експертів сходиться на думці, що Stuxnet - спільне творіння Ізраїлю і США. Черв'як використовував цілу низку вразливостей нульового дня і ретельно ховався від будь-яких антивірусів. Вірус поширювався через зйомні носії (наприклад: флешка). На комп'ютерах, не пов'язаних з керуванням центрифуги, Stuxnet не проявляв себе, лише клонувався. Але, як тільки вірус запускався на SCADA-системі компанії Siemens, то він прописував свій компонент в програму, перехоплюючи комунікації між комп'ютером і керованими їм системами. Вірус мав певну вибірковість. Stuxnet починав шкодити – періодично підвищував частоту обертання до 2000 об/хв. Від цього мотори не витримували і виходили з ладу.

Stuxnet виявився найскладнішим вірусом, з яким фахівці з кібербезпеки стикалися. У світі кіберзагроз - це було справжнім витвором мистецтва – дуже небезпечний, але майже геніальний. Саме, після появи Stuxnet люди всерйоз заговорили про таке явище, як кіберзброя.

Що кіберзброя існує – це вже доведений факт, який підтвердило хакерське угрупування ShadowBrokers, що вкрало інструменти іншого угрупування, Equation. Спочатку хакери намагалися продати вкрадене, але не вийшло, тоді вони виклали всі експлойти у відкритий доступ. Так з'явився WannaCry – вірус, що складається з досить поганенького коду шифрувальника і потужного експлойта EternalBlue, що використовував для поширення уразливість нульового дня в різних версіях Windows.

Епідемію зупинив Маркус Хатчинс. Він виявив, що перед тим як зашифрувати накопичувач, вірус відправляє звернення до неіснуючому домену в Інтернеті. «Що буде, якщо я зареєструю цей домен?» – міркував він. Зареєстрував і з'ясував, що після цього вірус не припиняє поширюватися, але диски не шифрує. Так Маркус, зупинив епідемію і ненадовго став героєм. WannaCry модифікуали, тож черв'як ще тероризує планету, але Microsoft випустила патч і велика частина комп'ютерів вже невразлива.

Третя історія, найдорожча атака: епідемія NotPetya/ExPetr. Невідомий шифрувальник поширювався за допомогою експлойтів EternalBlue і EternalRomance, знову шифруючи все на своєму шляху і розносячись з шаленою швидкістю. Спочатку дослідники вирішили, що це модифікація шифрувальника Petya. Але потім зрозуміли, що це все-таки не він, звідси ім'я NotPetya. NotPetya за допомогою утиліту Mimikatz ліз в пам'ять непропатченних комп'ютерів, добував звідти паролі та заражав інші машини. NotPetya – це цільова атака. Є припущення, що вона спочатку була націлена на Україну – хтось заразив пакет оновлень для програми M.E.Doc, яку велика частина українських компаній використовує для документообігу і податкової звітності. Після глобального поширення світом, найбільше постраждала компанія морських перевізників Maersk.

Айтішники спостерігати чорну хвилю, один за іншим монітори комп'ютерів ставали чорними, і на них виводилося типове повідомлення з вимогою: «заплатите $300 в біткойн-еквіваленті, і ми розшифруємо ваші дані». NotPetya шифрував дані безповоротно, тобто в класифікації антивірусних експертів це - вайпер. Збитки постраждалих компаній склали понад $10 млрд.

Ми розглянули 3 масштабних кібератаки, дізналися про кіберзброю і побачили до яких наслідків це приводить. Тепер давайте розглянемо історію про те як користувачі необачно надають доступ до своїх даних. Проаналізуємо на застосунку GetContact.

Як саме GetContact отримує доступ до інформації? Під час першого запуску застосунок просить у вас доступ до контактів. Натомість можна побачити, як твій номер підписано в інших користувачів і будь-який інший. GetContact пропонує блокування від спаму та ідентифікацію дзвінків від абонентів з телефонної книги. Ви подумаєте: ну той що, в цьому немає нічого дивного чи підозрілого. Та це не так. Приймаючи уогоди користувача, ви надаєте згоду компанії збирати дані і ділитися ними з третіми сторонами. Неповний список інформації, яку отримує GetContact: інформація з телефонних книг (контакти та інше), поштова адреса, історія дзвінків, фотографії, IP-адреси тощо. Ваш номер може опинитися в розпорядженні розробників і без аккаунту; лише треба, щоб він опинився в адресній книжці одного з користуваців. Через порушення законів про оброблення персональних даних в Азейбарджані та Казахстані утиліту заборонили. Проте в Україні на цей застосунок ще не звернули уваги.

Які можуть бути наслідки? Найменш шкідливий варіант: інформацію збирають у базу даних, потім продають великим компаніям для здійснення спаму. Найбільш шкідливий варіант: дані використовують для атак на користувачів із застосуванням соціальної інженерії, наприклад, для дзвінків на зразок "Ваша дитина потрапила в біду, перекажіть 3 тисячі". Звичайно модна видалити акаунт, його обіцяють прибрати впродовж 24 годин. Отож, перед тим як натискати згоду, почитайте її.

Для підвищення безпеки дотримуйтеся наступних рекомендацій:

- будьте обережні з небажаними електронними листами, дзвінками і текстовими повідомленнями, особливо якщо йдеться про «надзвичайну ситуацію»
- захистіть свою домашню мережу: змініть стандартний пароль для мережі Wi-Fi на надійний, незавадило б обмежте кількість пристроїв, підключених до неї;
- зміцніть свої паролі: не забувайте використовувати довгі та складні паролі, які містять цифри, літери та спеціальні символи;
- захистіть своє обладнання: переконайтеся, що ви оновили всі свої системи та програми, встановлюйте і оновлюйте антивірусне програмне забезпечення;

Не забувайте, що зараз в Україні йде війна та кількість кібератак, що спрямовані на нашу державу великі. Російські хакери продовжують полювати на персональні дані українців. Фішинг залишається основною тактикою російських хакерів. Тож, дотримуйтесь правил користуванні інтернетом і остерігайтесь різноманітних фішингових повідомлень.

Список використаних джерел

1. https://armyinform.com.ua/2022/08/17/yak-zahystytysya-vid-kiberzlochynnosti-porady-yevroparlamentu/
2. https://itta.info/10-najbilsh-vrazhayuchix-kiberatak-v-istorii/
3. https://www.epravda.com.ua/publications/2018/03/1/634594/
4. https://ain.ua/2023/04/25/chto-takoe-getcontact-vyrusnaya-utylyta-kotoraya-sobyraet-personaln%D1%8Be-dann%D1%8Be/

Ключові слова: кібератака, фішинг, вірус, пароль, захист даних, хакер, кібербезпека.

Ірина ГЛАДИШ[1], *викладач вищої категорії,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: Irina.Gladishkr@gmail.com
Віктор Юзбеков[1], *здобувач освіти,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: vityayuzbekov602@gmail.com

ШИФРУВАННЯ ТЕКСТОВОЇ ІНФОРМАЦІЇ В ЗОБРАЖЕННЯ

Шифрування текстової інформації є важливою практикою забезпечення конфіденційності, цілісності та доступності даних.

Шифрування дозволяє захистити дані від несанкціонованого доступу. Тільки особи, які мають відповідний ключ або пароль, можуть розшифрувати і зрозуміти зміст зашифрованого тексту. У світі, де кіберзлочинці та хакери активно шукають можливості доступу до конфіденційної інформації, шифрування допомагає ускладнити їхню задачу і зменшити ризик витоку даних. Під час передачі даних через мережу, такої як Інтернет, існує ризик перехоплення інформації.

Кіберзлочинці часто спрямовуються на компанії та фізичних осіб, щоб отримати конфіденційну інформацію. Захист інформації за допомогою різних заходів, таких як шифрування та вдосконалення кібербезпеки, допомагає уникнути цих загроз.

Збереження конфіденційної інформації є важливою задачею як для компаній, так і для фізичних осіб. Захист конфіденційної інформації має кілька ключових аспектів, і виконання цього завдання може мати значущий вплив на успіх бізнесу або особисту безпеку.

Втрата конфіденційної інформації може призвести до серйозних фінансових втрат. Це може включати втрату бізнесу, порушення договорів або навіть правові санкції. Для фізичних осіб захист особистої інформації, такої як фінансові дані, медичні записи чи особисті ідентифікатори, є важливим для запобігання шахрайству, крадіжкам особистості та іншим формам злочинності.

Шифрування допомагає визначити будь-які спроби модифікації даних. Якщо дані були змінені безповоротно, розшифрування стане неможливим або призведе до отримання невірного змісту.

Шифрування текстової інформації в зображення допомагає зберегти конфіденційні дані. Інформація, яка знаходиться в текстовій формі, може бути зашифрована і вбудована в зображення, що робить її менш доступною для несанкціонованого доступу.

При передачі або зберіганні зображень із вбудованою зашифрованою текстовою інформацією може бути складніше перехопити чи розпізнати цю інформацію, порівняно із звичайним текстом чи файлами.

Стеганографія, тобто вміщення інформації в невидимий для звичайного спостерігача спосіб, може бути використана для заховування текстової інформації в зображеннях. Шифрування цієї текстової інформації може підвищити рівень безпеки такого захисту. На рис.1 зображена загальна модель стеганосистеми.

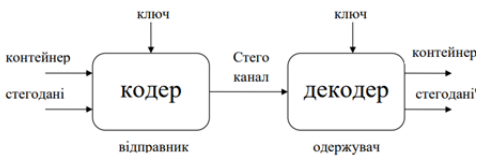

Рисунок 1 - Загальна модель стеганосистеми

Складається з контейнерів, ключа, стегоданих, стегоканала.

Контейнери - це об'єкти, які приховують секретну інформацію. Ключ - це важливий елемент для захисту та розшифрування прихованої інформації.

Стегодані - це прихована інформація або дані, які були вбудовані у існуючі дані за допомогою методів стеганографії. Це може бути текст, файл, аудіо- або відеодані, які були змінені для того, щоб приховати додаткову інформацію. Стегодані можуть бути вбудовані в зображення, звукові файли, текстові документи та інші типи мультимедіа.

Стегоканал - це комунікаційний канал або середовище, яке використовується для передачі стегоданих.

Існують методи приховування інформації в зображеннях: метод заміни найменш значущого біта (LSB), метод псевдовипадкового інтервалу, метод псевдовипадкової перестановки, Метод блочного приховування, метод заміни палітри, метод квантування зображення, метод Куттера-Джордана-Боссена, метод DDQM (Darmstaeder-Delaigle-Quisquater-Macq), метод Коха і Жао, метод Бенгама-Мемона-Ео-Юнг, метод Ху і Ву, метод Фрідріх, метод розширення спектру.

Ці методи стеганографії можуть бути використані для різних цілей, включаючи конфіденційні комунікації, захист від кіберзлочинців або вивчення навколишнього середовища для цілей безпеки.

Їх мета - приховати факт наявності інформації в іншому виді даних так, щоб звичайний спостерігач не міг легко виявити чи розпізнати цю інформацію.

Також існує велика кількість програм і утиліт для шифрування тексту у зображення: Anubis, DeepSound, Hallucinate, JHide, DeEgger Embedder, OpenPuff, OpenStego.

Програми для шифрування тексту у зображення дозволяють приховати текстову інформацію в такий спосіб, що вона стає важкою до виявлення без відповідного ключа чи пароля.

Їх мета - захистити конфіденційну інформацію та забезпечити безпеку обміну даними, використовуючи методи стеганографії та шифрування.

Шифрування текстової інформації в зображення може бути важливим елементом забезпечення безпеки в різних сценаріях, де важливо заховати або зашифрувати конфіденційну інформацію.

Список використаних джерел

1. Steganography in Digital Media: Principles, Algorithms, and Applications, Jessica Fridrich, 2010, Pages: 592

2 Digital Watermarking and Steganography: Fundamentals and Techniques, Frank Y. Shih, 2015, Pages: 436

Анотація. Ірина ГЛАДИШ, Віктор Юзбеков. Шифрування текстової інформації в зображення.

Розглядаються методи та програми шифрування текстового контенту в прихований вигляд всередині графічних файлів. Застосування різних шифрувальних алгоритмів та технік дозволяє забезпечити конфіденційність текстової інформації, а також вбудувати її в інші формати з метою захисту від несанкціонованого доступу.

Ключові слова: ключ, контейнер, інформація, стегоканал, стегодані.

Ірина КРАВЧУК[1], *викладач методист вищої категорії,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж
Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: kravchuk_iv@g-suit.kk.nau.edu.ua
Віктор БОЙКО[1], *здобувач освіти,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж
Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: burucshka@gmail.com

КІБЕРГІГІЄНА ТА ЯК ЇЇ ДОТРИМУВАТИСЬ НА КОЖНОМУ ЩАБЛІ КОМПАНІЇ

Збереження приватності особистих даних є важливим для забезпечення безпеки та захисту особистості. Захист особистих даних є важливим для запобігання несанкціонованому використанню та зловживанню.

Види загроз для даних — крадіжка даних, фішинг, втрата пристроїв, внутрішня загроза, недостатня культура безпеки.

Безпека даних – це процес захисту конфіденційності, цілісності та доступності даних від несанкціонованого доступу, втрати, пошкодження або розкриття. 5 засобів, які у комплексі дають найкращі результати:

- шифрування даних
- проведення аудиту безпеки даних
- встановлення багаторівневої системи доступу до даних
- резервне копіювання
- встановлення антивірусного програмного забезпечення

Рекомендації для роботи з корпоративною інформацією:

- Використовуйте безпечні засоби зв’язку
- Зберігайте документи в захищеному сховищі
- Використовуйте складні паролі
- Використовуйте багатофакторну аутентифікацію для додаткового рівня безпеки.
- Антивірусне програмне забезпечення:
- Не діліться доступом
- Захищений пристрій
- Фізична безпека
- Освіта і навчання
- Відповідальність

Рекомендації для «людського фаєрволу»

- Складні паролі
- 2-етапна перевірка
- Оновлення ПЗ
- Уважність у мережі
- Розсудливе використання соцмереж
- Резервне копіювання
- Уважність до фішінгу даних

Головне завдання плану реагування на інциденти – забезпечення безперервності бізнесу.

План передбачає:

1. Документування конфігурацій
2. Створення альтернативних каналів зв’язку
3. Забезпечення живлення
4. Ідентифікація усіх залежностей для додатків і процесів
5. Розуміння того, як виконувати вручну автоматичні завдання

Етапи реагування на інформаціині інциденти:

1. Підготовка.
2. Виявлення та аналіз
3. Стимулювання, ліквідація наслідків і відновлення
4. Подальша діяльність після кібератаки

Список використаних джерел

1. https://skillsforall.com/
2. https://www.netacad.com/
3. https://www.google.com/

Анотація. Ірина КРАВЧУК, Віктор БОЙКО. Кібергігієна та як її дотримуватись на кожному щаблі компанії.

В презентації надаються відомості щодо безпеки особистих даних, видах загроз, та рекомендації щодо запобігання витоку конфедиційної інформації та реагування на інформаційні інциденти.

Ключові слова: безпека даних, фішинг, антивірус, ідентифікація, кібератака.

Олександр ГРИНЧЕНКО[1], *викладач вищої категорії,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: oleksandr.grinchenko@g-suit.kk.nau.edu.ua
Владислав ДАВИДОВИЧ[1], *здобувач освіти,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: davydovych.vladyslav@g-suit.kk.nau.edu.ua

ОПТИМІЗАЦІЯ БЕЗПЕКИ МЕРЕЖЕВОГО СЕРЕДОВИЩА З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ SDN

Сучасні мережі стають все більш складними і уразливими для атак. Зловмисники використовують широкий спектр технологій для отримання несанкціонованого доступу до мережі, крадіжки конфіденційної інформації та порушення нормального функціонування мережі.

Традиційні підходи до управління мережею не завжди можуть ефективно протистояти сучасним загрозам безпеки. Ці підходи зазвичай є децентралізованими, що ускладнює виявлення і усунення загроз.

Технологія SDN пропонує новий підхід до управління мережею, який може бути використаний для підвищення безпеки мережевого середовища. SDN забезпечує централізоване управління мережею, що дозволяє більш ефективно протистояти сучасним загрозам безпеки.

Основні можливості SDN для підвищення безпеки

SDN забезпечує наступні можливості для підвищення безпеки мережевого середовища:

- Централізоване управління мережею. SDN дозволяє централізовано управляти всіма мережевими пристроями, що спрощує виявлення і усунення загроз.
- Динамічне управління потоками даних. SDN дозволяє динамічно управляти потоками даних, що дозволяє обмежити доступ зловмисників до мережі.
- Аналіз мережевого трафіку. SDN дозволяє збирати і аналізувати дані мережевого трафіку, що дозволяє виявляти загрози на ранніх стадіях.

Рішення для підвищення безпеки з використанням SDN

За допомогою SDN можна реалізувати наступні рішення для підвищення безпеки мережевого середовища:

- Використання брандмауерів SDN. Брандмауери SDN дозволяють централізовано управляти правилами брандмауера, що спрощує їхнє конфігурування і обслуговування.
- Використання систем виявлення і запобігання вторгненням SDN. Системи виявлення і запобігання вторгненням SDN дозволяють динамічно реагувати на загрози, що підвищує ефективність захисту мережі.
- Використання систем шифрування SDN. Системи шифрування SDN дозволяють шифрувати мережевий трафік, що підвищує безпеку передачі даних.

Переваги і недоліки використання SDN для підвищення безпеки

Використовуючи технологію SDN, можна отримати наступні переваги для підвищення безпеки мережевого середовища:

- Покращена видимість мережі. SDN забезпечує централізований контроль мережі, що дозволяє отримати більшу видимість мережі і виявити загрози на ранніх стадіях.

- Покращена ефективність захисту. SDN дозволяє динамічно реагувати на загрози, що підвищує ефективність захисту мережі.
- Зменшення витрат на адміністрування. SDN дозволяє автоматизувати завдання адміністрування мережі, що може призвести до зниження витрат на адміністрування.

Однак, використання технології SDN також має деякі недоліки:

- Вартість. Впровадження SDN може бути дорогим.
- Складність. Впровадження і адміністрування SDN може бути складним.
- Безпека. SDN може бути вразливою для атак.

Висновок

Технологія SDN пропонує новий підхід до управління мережею, який може бути використаний для підвищення безпеки мережевого середовища. SDN забезпечує централізоване управління мережею, що дозволяє більш ефективно протистояти сучасним загрозам безпеки.

Однак, використання технології SDN також має деякі недоліки, такі як вартість, складність і безпека. При впровадженні SDN необхідно враховувати ці недоліки, щоб забезпечити ефективну і безпечну роботу мережі.

Список використаних джерел

1. Casado, M., McKeown, N., Shenker, S., & Tootoonchian, A. (2012). "Fabric: A Retrospective on Evolving SDN." ACM SIGCOMM Computer Communication Review, 42(4), 87-98.

2. Kreutz, D., Ramos, F. M. V., Esteves Verissimo, P., Esteve Rothenberg, C., Azodolmolky, S., & Uhlig, S. (2015). "Software-Defined Networking: A Comprehensive Survey." Proceedings of the IEEE, 103(1), 14-76.

3. Porras, P., Shin, S., Yegneswaran, V., Fong, M., & Tyson, M. (2015). "A Security Enforcement Kernel for OpenFlow Networks." ACM SIGCOMM Computer Communication Review, 45(4), 303-316.

Анотація. Олександр ГРИНЧЕНКО, Владислав ДАВИДОВИЧ. Оптимізація безпеки мережевого середовища з використанням технології SDN.

Технологія програмно-визначених мереж (SDN) пропонує новий підхід до управління мережею, який може бути використаний для підвищення безпеки мережевого середовища. SDN забезпечує централізоване управління мережею, що дозволяє більш ефективно протистояти сучасним загрозам безпеки.

У тезах розглядаються можливості використання технології SDN для підвищення безпеки мережевого середовища. Представлені основні рішення, які можуть бути реалізовані за допомогою SDN, а також їхні переваги і недоліки.

Ключові слова: SDN, безпека мережі, централізоване управління, мережеві загрози.

2

«ЛЮДИНА І ІНФОРМАЦІЯ»

Олександр ГРИНЧЕНКО[1], *викладач вищої категорії,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж
Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: oleksandr.grinchenko@g-suit.kk.nau.edu.ua
Тетяна ГРИНЧЕНКО[1], *викладач вищої категорії,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж
Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: tigervillis@gmail.com

ВПЛИВ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ НА ПСИХІЧНЕ ЗДОРОВ'Я ЛЮДИНИ

ІТ мають широкий спектр позитивних наслідків для нашого життя. Вони можуть допомогти нам бути більш продуктивними, креативними, а також краще спілкуватися з іншими людьми. Однак, ІТ також можуть мати негативний вплив на наше психічне здоров'я.

Основні негативні наслідки впливу ІТ на психічне здоров'я

До основних негативних наслідків впливу ІТ на психічне здоров'я людини відносяться:

- Залежність від ІТ. ІТ можуть викликати залежність, яка може призвести до погіршення якості життя людини.
- Депресія. ІТ можуть сприяти розвитку депресії, особливо у людей, які мають фактори ризику, такі як спадковість, особистісні риси або травмуючий досвід.
- Тривога. ІТ можуть сприяти розвитку тривоги, особливо у людей, які мають фактори ризику, такі як спадковість, особистісні риси або стресові ситуації.
- Інші психічні розлади. ІТ можуть сприяти розвитку інших психічних розладів, таких як фобії, розлади харчової поведінки, інтернет-залежність тощо.

Чому ІТ можуть негативно впливати на психічне здоров'я людини?

Існує кілька причин, чому ІТ можуть негативно впливати на психічне здоров'я людини. До них відносяться:

- Постійний доступ до інформації та розваг. ІТ дозволяють нам бути постійно підключеними до інформації та розваг. Це може призвести до перевантаження інформації, інформаційного шуму, а також до зниження емоційної чутливості.
- Відрив від реального світу. ІТ можуть призвести до відриву від реального світу. Це може призвести до відчуття самотності, соціальної ізоляції, а також до погіршення міжособистісних відносин.
- Відсутність контролю. ІТ можуть викликати почуття неконтрольованості. Це може призвести до тривоги, агресії, а також до зниження рівня самооцінки.

Як мінімізувати негативний вплив ІТ на психічне здоров'я людини?

Щоб мінімізувати негативний вплив ІТ на психічне здоров'я людини, необхідно дотримуватися наступних рекомендацій:

- Встановіть обмеження на використання ІТ. Визначте, скільки часу ви можете проводити за комп'ютером або смартфоном за день.
- Фізична активність. Регулярні фізичні вправи допомагають зменшити стрес і поліпшити загальний стан здоров'я, включаючи психічне здоров'я.
- Спілкування з близькими людьми. Спілкування з близькими людьми допомагає відчувати себе більш пов'язаною з іншими людьми і зменшує відчуття

самотності.

- Допомога фахівця. Якщо ви відчуваєте, що ІТ негативно впливають на ваше психічне здоров'я, зверніться за допомогою до фахівця.

Висновок

ІТ є потужним інструментом, який може бути використаний як для позитивних, так і для негативних цілей. Щоб ІТ не негативно впливали на наше психічне здоров'я, важливо дотримуватися рекомендацій, наведених у цих тезах.

Список використаних джерел

1. Rosen, L. D., Lim, A. F., Carrier, L. M., & Cheever, N. A. (2011). "An Empirical Examination of the Educational Impact of Text Message-Induced Task Switching in the Classroom: Educational Implications and Strategies to Enhance Learning." Psicologia Educativa, 17(2), 163-177.

2. Twenge, J. M., Campbell, W. K., & Campbell, S. M. (2018). "Decreases in Psychological Well-Being Among American Adolescents After 2012 and Links to Screen Time During the Rise of Smartphone Technology." Emotion, 18(6), 765–780.

3. Lattie, E. G., Nicholas, J., Knapp, A. A., Skerl, J. J., Kaiser, S. M., & Mohr, D. C. (2019). "Opportunities for and Barriers to the Use of Technology-Enabled Mental Health Services in a College Student Population: A Qualitative Evaluation." Psychiatric Services, 70(7), 615-618.

Анотація. Олександр ГРИНЧЕНКО, Тетяна ГРИНЧЕНКО. Вплив інформаційних технологій на психічне здоров'я людини.

Інформаційні технології (ІТ) стали невід'ємною частиною нашого життя. Ми користуємося ними на роботі, вдома, для спілкування з друзями та рідними, для навчання, розваг та інших цілей. Однак, ІТ також можуть негативно впливати на наше психічне здоров'я. У статті розглядаються основні негативні наслідки впливу ІТ на психічне здоров'я людини, а також способи їх мінімізації.

Ключові слова: інформаційні технології, психічне здоров'я, негативний вплив, залежності, депресія, тривога.

3

«ЗАСОБИ ПЕРЕДАЧІ ІНФОРМАЦІЇ»

Наталя АНДРУСЕВИЧ[1], *викладач, спеціаліст вищої категорії,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж
Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: andrusevich.nv@gmail.com
Рената АРТАМОНОВА[1], *здобувач освіти,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж
Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: artamonova.renata@g-suit.kk.nau.edu.ua

ЕВОЛЮЦІЯ ЗАСОБІВ ПЕРЕДАЧІ ІНФОРМАЦІЇ

У процесі розвитку суспільства нагромаджується інформація, необхідна для життєдіяльності суспільства, а також змінюється середовище та спосіб життя людини. Це супроводжується появою нових способів спілкування, що виражається в появі нових форм і засобів інформаційних зв'язків[1].

Першими засобами передачі інформації були мова жестів, наскальні малюнки та людська мова.

Завдяки постійному розвитку засобів передачі інформації, людство змогло зробити революційні відкриття, пов’язанні із передачею даних. Наприклад, першим революційним винаходом була писемність. Завдяки неї суспільні відносини набули значних змін в області опрацювання інформації. Передання знань, освіти, фактів, основних понять та іншої інформації стало набагато доступніше.

Розвиток писемності дало початок першому такому засобу комунікації, як пошта. Хоча до цього люди використовували гонців та посланників, як шлях для передачі усної інформації, на разі після першої революції він набув значення доставки цінних паперів за допомогою особи або ж голубиної пошти. Люди почали використовувати цей метод у різних епохах та різних частинах світу, адже він мав значні переваги в надійності та ефективності.

Серед способів відтворення написання для мас розрізняють ручне написання та друкарство.

Друга революція зумовлена винаходом електромагнітних технологій, а саме появленню телеграфа, телефона, радіо та інше. Одразу було помітно великі зміни у швидкості передачі та збереження інформації, адже тепер інформація передавалася за допомогою електромагнітних сигналів, що змінюватлися на зорово-звукові сигнали. Винаходи в області електромагнітної техніки були одним з етапів у розвитку технологій і є основою для багатьох сучасних систем комунікацій.

У середині XIX століття Семюель Морзе та його співробітники створили телеграф, який використовував електромагнітні сигнали для передачі кодованих повідомлень на відстань.

Розвиток оптики, включаючи електромагнітні хвилі світла, також став можливим завдяки дослідженню електромагнітних хвиль, що призвело до розробки таких інструментів, як волоконно-оптичні системи зв’язку.

Жорсткі диски, магнітні картки та інші пристрої для обробки та зберігання даних почали використовувати електричні та магнітні поля, що теж являє собою великим проривом.

Третім проривом в еволюції розвитку засобів передачі інформаційних технологій є винахід сучасних технологій.

Зараз активно розвиваються засоби передачі інформації в фінансовій сфері. Наприклад, використовується технологія блокчейн, яка дає змогу людям здійснювати безпечні та надійні транзакції в цифровому середовищі. Інформація записується в

пов’язаних між собою блоках (ланцюжок), кожен з якого містить інформацію про попередній блок. Такий незмінний ланцюжок блоків називається блокчейн. Процес додавання нового блоку у ланцюжок називається “майнінгом”. Для його виконання потрібно розв’язати математичну задачу, яка потребує достатньо великих обчислювальних потужностей. Та виконується багатьма комп’ютерами по всьому світу. Коли новий блок додано в ланцюжок, інформація в ньому стає доступною для всіх учасників мережі, після чого перевірити транзакцію і переконатися в її законності може будь хто[3].

Можливості, які надає сучасна техніка, виходить за усі межі можливого. У наш час людство має змогу не тільки виконувати складні операції за допомогою різних роботів і комп’ютерних машин, а й керувати ними дистанційно.

За допомогою штучного інтелекту людина може отримувати, переробляти та передавати інформацію. Штучний інтелект – це «складова частина інформатики, в якій створюються наукові й технічні передумови для розв’язання за допомогою систем обробки інформації задач, які до цього були пов’язані головним чином з людськими здібностями»[4].

Наприклад, програма AlphaGo, розроблена компанією Google DeepMind, у 2015 році виграла матч у професійного гравця у гру го на стандартній дошці. У 1997 році комп’ютер Deep Blue обіграв Гаррі Каспарова у шахи, але виграти в людини в ґо значно складніше, бо японські шашки передбачають більше варіантів ходів[5].

У 2015 році був розроблений ChatGPT, спектр можливостей якого дуже широкий: від відповідей на запитання до генерації тексту, від аналізу тексту до автоматичної підтримки клієнтів, від перекладу до створення діалогів, від надання інформації про першу медичну допомогу до надання інтерактивної допомоги у навчанні, від написання сценаріїв, поезії до створення музики, мистецтва. З 2023 року ChatGPT став доступний в Україні і вже змінив наш спосіб взаємодії з технологіями[6].

Список використаних джерел

1. Арляпова Є.В. Інформаційні процеси в суспільстві. URL: https://studfile.net/preview/9141508/page:10
2. Історія засобів передачі інформації. URL: https://www.timetoast.com/timelines/b7dfda52-298a-4a35-93f6-ab7a55fb999d
3. ZetaChain. Еволюція передачі інформації. URL: http://surl.li/ndydp
4. Порохова О.Є. Сутність і проблематика штучного інтелекту. URL: http://surl.li/edfrg
5. Топ-10 наукових відкриттів десятиліття за версією New Scientist. URL:https://hmarochos.kiev.ua/2020/01/03/top-10-naukovyh-vidkryttiv-desyatylittya-za-versiyeyu-new-scientist/
6. Що таке ChatGPT? Історія створення і можливості. URL: https://gptchat.in.ua/chat-gpt/

Анотація. Наталя АНДРУСЕВИЧ, Рената АРТАМОНОВА. Еволюція засобів передачі інформації.

Розглядаються основні етапи розвитку засобів передачі інформації від давніх часів до сучасності, поява та розвиток писемності, друкарства та сучасних технологічних інновацій, які являються способом передачі інформації впродовж багатьох поколінь.

Ключові слова: *Еволюція, інформація, передача, засоби.*

Ірина ГРИБЕНКО[1], *викладач вищої категорії,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: gribenkoirina@g-suit.kk.nau.edu.ua
Валерій САМОРОДНИЙ[1]**,** *здобувач освіти,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: valery.native@g-suit.kk.nau.edu.ua

МАГНІТОМЕТРИ– НОВІ МОЖЛИВОСТІ В РОЗМІНУВАННІ

З початку російського вторгнення в нашій країні постало питання з розмінування, наразі, Україна входить у першу трійку країн за забрудненням території мінами. [1]

Міни залишаються загрозою десятиліттями після закінчення війн, створюючи перешкоди для розвитку і загрожуючи безпеці місцевого населення. Відповідно до цього, розмінування є важливим елементом відновлення. [2]

Нас зацікавили питання: «Які існують методи виявлення мін, що візуально не помітні?», «Які з методів виявлення мають переваги?», «Які перспективні засоби розмінування?», «Чи можна зменшити вартість і підвищити безпеку процесів розмінування?»

Вивчаючи магнітне поле, ми торкнулися питань виявлення мін і вибухонебезпечних предметів шляхом аналізу змін магнітного поля Землі. Ми почали своє дослідження з аналізу методів виявлення мін і їх знешкодження. [1] Встановили, що заради дотримання безпекових норм для саперів та підвищення продуктивності роботи у світі використовують методи дистанційного пошуку небезпечних об’єктів (UXO — unexplodedordnance). [3]

Наразі російська армія використовує 97 типів різних мін – як застарілих, так і сучасних розробок [1], відповідно і методів виявлення теж існує велика кількість: використання детекторів металу, тренованих собак або щурів, дронів, роботів і спеціалізованих машин. Вибір методики залежить від типу і кількості мін, географії замінованої території, доступних ресурсів і технологій. [2] Ми ознайомилися з більшістю з них, але детально досліджували використання магнітометрів.

Відомо, що для пошуку та розвідки деяких корисних копалин з вмістом феромагнітних мінералів використовують магніторозвідку. Метод заснований на фіксації аномальних (відхилення від норми) зон магнітного поля Землі за допомогою магнітометру з подальшим аналізом та комбінацією геологічної та геофізичної інформації для виявлення родовищ. Цей же метод можна використовувати під час пошуку вибухонебезпечних об’єктів. Основна вимога – наявність заліза в об’єкті, який ми шукаємо. [3] Для виявлення діелектричних (з пластмаси, дерева тощо) і діамагнітних об'єктів (з дюралюмінію, золота, срібла, бронзи тощо) цей метод непридатний. [4, с.33] Доречним буде даний метод для дослідження об'єктів, що знаходяться під водою (у болотах) і з часом покриваються донними відкладеннями, що ускладнює їх візуальне виявлення оптичними методами. [4, с.44]

Система магнітометра є важливим компонентом навігаційної системи будь-якого дрона, адже дозволяє йому точно визначати своє положення та напрямок і виявляти об’єкти на своєму шляху.

Для дистанційного виявлення мін під коптером, який літає над мінним полем за точно завданою траєкторією, підвішується додатковий магнітометр на спеціальну конструкцію - виніс, яка кріпиться до дрона. У процесі польоту магнітометр безперервно фіксує параметри магнітного поля Землі із точною прив'язкою до координат.

Магнітометри мають високу чутливість і дозволяють знаходити металеві об’єкти вагою від 200 г як на поверхні землі, так і на глибині до 2 м, здатні працювати вдень і вночі, незалежні від метеоумов. Після виконання польових робіт, результати сканування завантажуються з магнітометра на комп’ютер і обробляються в спеціальних програмах для побудови карт магнітних аномалій з зазначенням координат небезпечних об’єктів (див. ДОДАТОК 2). Отримані результати можна завантажити на телефон, що дозволить саперу виходити на місце обстеження в необхідній локації. [3]

Польський благодійний фонд «Поступ» наводить розрахунки роботи саперів в команді з операторами дронів зі спеціальною конструкцією кріплення магнітометра, що мають економію витрат часу на розмінування у 32 %. Така технічна підтримка допоможе прискорити процес звільнення наших земель від наслідків війни та зменшить кількість втрат людського ресурсу, дозволить повернути українські землі до нормального процесу їх використання, обслуговування та обробки.[3]

Сьогоднішня війна змінює старі правила: військові використовують сучасні технології на полі бою – знімки з супутників, дрони в повітрі, на воді та інше. В Україні, наразі, з'явилася інтерактивна мапа замінованих територій, що розміщена на сайті Державної служби з надзвичайних ситуацій.

Міна – не тільки грізна зброя, а й сильний психологічний чинник, який впливає на військових, які потрапляють на мінне поле. Тож якщо існує обладнання, яке допоможе зберегти стресостійкість, а головне, життя хоча б одного українця – воно вже того варте. На завершення нагадуємо: справа розмінування не любить дилетантів і самоучок. Це справа професіоналів, які мають необхідний рівень знань та навиків.[1] Наше дослідження дало нам відповіді на низку запитань, але і виникли нові, які ми плануємо далі досліджувати. Відомий вислів Вінстона Черчилля «Хто володіє інформацією, той володіє світом!» інтерпретуємо до нашого дослідження: застосовувати інноваційні технології в виявлення мін і їх знешкодженні - означає пришвидшити перемогу України над ворогом і максимально швидко повернутися до безпечного та звичного життя.

Список використаних джерел

1. Обережно: міни!: https://armyinform.com.ua/2019/07/27/oberezhno-miny/(дата звернення: 15.10.2023). – Заголовок з екрана. – Мова укр. – Останнє оновлення: 27.07.19.

2. Методики розмінування: різноманітність підходів до мінної загрози: https://mil.in.ua/uk/blogs/metodyky-rozminuvannya-riznomanitnist-pidhodiv-do-minnoyi-zagrozy/ (дата звернення: 20.09.2023). – Заголовок з екрана. – Мова укр. – Останнє оновлення: 03.06.23.

3. Один день бойових дій - місяць розмінування: одеський геолог — про те, як убезпечити та прискорити роботу саперів: https://dumskaya.net/news/odin-den-boyovih-diy-misyatc-rozminuvannya-odesk-170654/ (дата звернення: 21.09.2023). – Заголовок з екрана. – Мова укр. – Останнє оновлення: 21.11.22.

4. Лікаренко Володимир Янович /Дипломний проєкт на здобуття ступеня бакалавра за освітньо-професійною програмою «Інформаційні вимірювальні технології та системи» спеціальності 152 «Метрологія та інформаційно-вимірювальна техніка» на тему: «Система локалізації магнітних аномалій» НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО» Приладобудівний факультет Кафедра інформаційно-вимірювальних технологій: https://ela.kpi.ua/bitstream/123456789/42014/1/Likarenko_bakalavr.pdf (дата звернення: 15.09.2023). – Заголовок з екрана. – Мова укр. – Останнє оновлення: 2021.

4

«НЕЙРОМЕРЕЖІ ТА ОБРОБКА ІНФОРМАЦІЇ»

Ярослава ГРИНЧУК[1]*, викладач,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: slavagrinchuk@i.ua
Кирило ІВАНОВ[1]**,** *здобувач освіти,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: cyril.ivanov@g-suit.kk.nau.edu.ua

НЕЙРОМЕРЕЖА - ЩО ЦЕ ТАКЕ, ЯК ПРАЦЮЄ ТА НА ЩО ЗДАТНА

Нейромережа — це математична модель, яка імітує структуру та функціонування біологічних нейронних мереж з метою вирішення різноманітних задач, таких як класифікація, регресія, прогнозування та генерація. [1]

Штучні нейрони - основа нейромереж. Вони об'єднуються в графові структури і передають сигнали один одному через ваги зв'язків. Це є однією з причин чому нейромережі здатні до виявлення закономірностей та залежностей у вхідних даних, та чому їх почати активно використовувати та застосовувати в багатьох галузях (сферах). В наш час, час діджиталізації та інформаційного буму, нейромережі відіграють важливу роль у вирішенні безлічі проблем, які виникають у людства в різних сферах та видах діяльності тому, що саме вони – нейромережі, можуть вирішувати складні завдання, які людству іноді не під силу (наразі це стосується медицини, т.як це - саме найголовніше в наш час, час, коли за життя наших Героїв лікарі борються кожну секунду). Тому, на мою думку, головною метою застосування нейромереж є те, щоб знайти шаблони для даних, які нам відомі та застосовувати їх для передбачення або класифікації нових даних, які нам стануть відомими.

Нейромережі виконують різноманітні типи завдань та задач, в залежності від архітектури мережі та початкових даних, які є. До найосновніших видів задач належать, а саме: класифікація, регресія, генерація тексту, обробка зображень.

Окрім різноманітних завдань та задач, які можуть вирішувати нейромережі, є більше 30 типів різних нейронних мереж, які підходять до різних типів завдань. Приведу приклад самих основних, а саме:

- згорткові нейронні мережі (CNN), які довели свою ефективність в розпізнаванні візуальних образів (відео та зображення), рекомендаційних системах і обробці мови;
- рекурентні (RNN), які застосовуються в розпізнаванні і обробці текстових даних;
- нейрона мережа Хопфілда, яка працює до досягнення рівноваги, коли наступний стан мережі дорівнює попередньому. [2]

Звичайно, що в кожної мережі - своя задача. Чимало було створено для вирішення задач з математики або фізики, також є і такі, які можуть оновити фотографію для більш якісної картинки для користувача або замовника, також є і такі, які можуть зробити цілу картину, або допомогти в праці веб - дизайнерів. Але, на мою думку, наразі велика заслуга застосування нейромереж є в галузі медицини, що відповідає сучасним викликам в умовах воєнного стану, це є і діагностування захворювань, аналіз медичних зображень, можливість передбачати чи є ефективним те чи інше лікування, яке призначено, можливість розпізнавати патологічні зміни на зображеннях, які отримані за допомогою магнітно-резона́нсної томогра́фії, комп'ютерної томографії, рентгену, а також інших різноманітних діагностичних методів, проведення аналізу даних та/або захворювань по генетиці, можливий прогноз результату лікування та розробка нових лікарських засобів, які необхідні в боротьбі з недугою або виявленими патологіями.

В час діджиталізації та використання нейромереж (штучного інтелекту) ми можемо бачити у кожної людини, бо це є використання людством гаджетів та різних застосунків, які дають корегувати поведінку, а саме: використання фітнес-браслетів та смарт-годинників, які допомагають встановлювати цілі та відстежувати виконання, нагадують про профілактичні обстеження, необхідність фізичної активності, прийом ліків, що так вкрай необхідно для людей похилого віку.

Підсумовуючи, мою доповідь можна з упевненістю сказати, що нейромережі відіграють важливу роль у розвитку сучасних технологій, серед яких є моделювання складних та надскладних процесів, вирішення задач, які раніше через різноманітні причини, часто не залежні від людства, були не під силу класичним алгоритмам.

Список використаних джерел

1. https://termin.in.ua/neyromerezha/#Bazova_struktura_ta_komponenti_nejromerezi
2. https://www.poznavayka.org/uk/nauka-i-tehnika-2/neyronni-merezhi-yih-zastosuvannya-robota/
3. https://merehead.com/ua/blog/neural-networks-healthcare-industry/
4. https://www.google.com/search?q=%D0%BD%D0%B5%D0%B9%D1%80%D0%BE%D0%BD%D0%BD%D1%96+%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D1%96++%D0%B2%D0%B8%D0%BA%D0%BE%D1%80%D0%B8%D1%81%D1%82%D0%B0%D0%BD%D0%BD%D1%8F+%D0%B2%D0%B4%D0%B8%D0%B7%D0%B0%D0%B9%D0%BD%D0%B5%D1%80%D1%96%D0%B2

Анна РУДА[1]*, викладач,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: annasergeeva198@ukr.net
Богдана КОВАЛЬ[1]**,** *здобувач освіти,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: koval.bohdana@g-suit.kk.nau.edu.ua

НЕЙРОМЕРЕЖІ В МЕДИЦИНІ

Нейронні мережі - це складні мережі алгоритмів, які намагаються імітувати роботу людського мозку. Вони складаються з великої кількості взаємопов'язаних штучних нейронів, які обробляють інформацію. Обробка інформації в нейронних мережах полягає в здатності моделі адаптуватися до вхідних даних, виявляти закономірності з цих даних і вирішувати різні завдання, такі як розпізнавання об'єктів на зображеннях, прогнозування майбутніх подій і управління процесами. [1]

Такі нейромережі використовуються в багатьох сферах, включаючи, обробку природної мови, *комп'ютерний зір,* медицину та фінанси тощо. Вони особливо ефективні, коли потрібно обробити великі обсяги даних, або створити точні правила аналізу для вирішення проблеми складно або неможливо.

Мета: дати визначення терміну нейромережі, дослідити її позитивні і негативні аспекти, а також довести, що вона може допомогти покращити діагностику, передбачити захворювання, розробити ефективні методи лікування та запропонувати більш персоналізоване лікування.

Актуальність: Нейронні мережі все більше стають невід’ємною частиною сучасного життя людини. Вони відіграють ключову роль у багатьох сферах діяльності людини, зокрема, і у покращенні діагностики, прогнозуванні захворювань, підтримці медичних рішень і покращенні систем охорони здоров’я.

Однією з ключових сфер застосування нейронних мереж у медицині є обробка медичних зображень. Нейронні мережі можуть допомогти визначити патології на таких зображеннях, як рентгенівські знімки, магнітно-резонансна томографія (МРТ), комп’ютерна томографія (КТ) тощо. Вони допомагають спеціалістам швидше і точніше виявити ознаки захворювання.

Штучний інтелект також використовується для прогнозування ризиків захворювання. Здатність аналізувати великі обсяги даних пацієнтів штучна мережа дозволяє створювати моделі для прогнозування можливого ризику захворювання або розвитку певних патологій або їх відсутності.

Однак важливо враховувати, що для ефективної роботи в медичній сфері нейронним мережам потрібні точні та надійні дані. Під час використання таких технологій також необхідно враховувати етику та конфіденційність даних пацієнтів.

Небезпеки використання нейромереж у медицині:

1. Якість даних. Результати нейромереж можуть бути лише такими точними, наскільки точні дані, на яких вони навчаються. Неправильні або несвідомі змішування даних може призвести до неточних результатів.

2. Етика та конфіденційність. Використання медичних даних для навчання нейромереж має етичні аспекти, особливо в контексті конфіденційності та захисту особистої інформації пацієнтів, збереження лікарської таємниці.

3. Експлуатаційна надійність. Нейромережі можуть давати неправильні результати через артефакти навчання або вразливості до внутрішніх або зовнішніх впливів.

4. Взаємодія з лікарською практикою. При впровадженні систем, що ґрунтуються на штучному інтелекті, важливо забезпечити взаємодію з медичними фахівцями та прийняття ними певних рішень.

5. Підвладність змінам. Медична наука постійно змінюється, тож системи на основі технологій штучного інтелекту повинні бути гнучкими й здатними адаптуватися до нових даних та досліджень.

На сьогоднішній день особливу увагу приділяють серцево-судинним захворюванням, оскільки саме вони утримують сумне лідерство в списку причин смертності. На другому місці знаходяться онкологічні захворювання. Один з головних напрямів, в якому зараз йдуть роботи по використанню нейронних мереж, — діагностика раку молочної залози. Ця недуга — причина смерті кожної дев'ятої жінки.[2]

На сьогодні вже винайшли штучний інтелект, який розробляє білки, створює ліки, про які люди навіть ще не мріяли у 2022 році. Вчені з університету Вашингтона використали алгоритм глибокого навчання, щоб не лише передбачити загальну площу функціонального складу білка, але й сформувати його структуру. Команда використовувала нове програмне забезпечення для створення ліків, які "борються з раком", і створила вакцини проти звичайних, хоча іноді й смертельних, вірусів. [2]

Можна з впевненістю стверджувати, що технології штучного інтелекту охоплять більшість та сфер та галузей життя сучасної людини. Наша задача – спрямувати розвиток штучного інтелекту у правильне русло, а не використовувати його як «зброю» проти людства.

Список використаних джерел

1. https://livingfo.com/shcho-take-nejronni-merezhi-ta-iak-vony-pratsiuiut/
2. https://uk.wikipedia.org/wiki/%D0%9D%D0%B5%D0%B9%D1%80%D0%BE%D0%BD%D0%BD%D1%96_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D1%96_%D0%B2_%D0%BC%D0%B5%D0%B4%D0%B8%D1%86%D0%B8%D0%BD%D1%96#%D0%9D%D0%B5%D0%B9%D1%80%D0%BE%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B8,_%D0%B3%D0%B5%D0%BD%D0%B5%D1%82%D0%B8%D0%BA%D0%B0_%D1%96_%D0%BC%D0%BE%D0%BB%D0%B5%D0%BA%D1%83%D0%BB%D0%B8

Ключові слова: медицина, штучний інтелект, нейронна мережа, машинне навчання, діагностика.

Ірина ГЛАДИШ[1], *викладач вищої категорії,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: Irina.Gladishkr@gmail.com
Володимир СВІДИНЕНКО[1], *здобувач освіти,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: vovasvidinenko@gmail.com

НЕЙРОМЕРЕЖІ, ОБРОБКА ІНФОРМАЦІЇ ТА НАВЧАННЯ

Нейромережа - це клас алгоритмів машинного навчання, які імітують структуру та функцію людських нейронних мереж. Вони використовуються для розв'язання складних завдань та обробки інформації завдяки навчанню на даних.

Нейромережі застосовуються в багатьох областях, в таких як розпізнавання та імітування мови та речі, фінанси, медицині, в комп'ютерних технологіях та інші.

Щоб нейромережа працювало справна треба виконати обробку інформації яка в себе включає декілька етапів:

Спочатку потрібно чітко визначити, яке завдання має вирішувати нейромережа. Це може бути класифікація зображень, розпізнавання мови, прогнозування числових значень і так далі. Для навчання нейромережі необхідно мати велику вибірку даних, яка включає у себе вхідні дані та правильні відповіді. Дані також потрібно підготувати для оптимального використання. Обираються типи шарів, кількість нейронів у кожному шарі, функції активації і інші параметри, щоб створити модель, яка найкраще підходить для вирішення конкретного завдання.

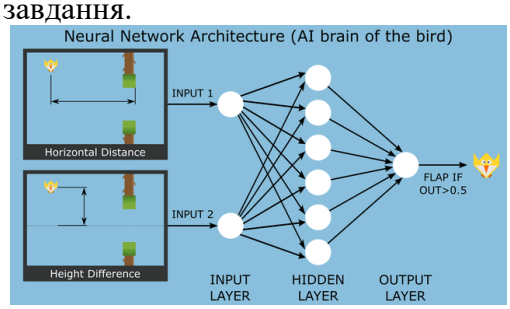

Рисунок 1 - Архітектура нейромережі на прикладі гри Flappy Bird

Мережа навчається на вхідних даних, підлаштовуючи свої внутрішні ваги для мінімізації помилки між передбачуваними та фактичними відповідями. Цей процес може вимагати багато ітерацій.

Після навчання модель тестується на даних які не залежать від ходу навчання , щоб оцінити її точність та ефективність. Після успішного навчання та тестування, модель може бути використана для обробки нових даних.

На сьогоднішній день існують три парадигми навчання нейронних мереж: навчання з вчителем, навчання без вчителя та навчання з підкріпленням.

Для навчання з вчителем правильні відповіді на вході сигналу вже відомі. Навчання мережі відбуватиметься доки значення виходів мережі не стануть максимально наближені до правильних відповідей входів мережі.

Навчання без вчителя не передбачає наявність правильних відповідей для вхідних сигналів. Нейронна мережа навчається давати найкращі вихідні сигнали лише з урахуванням вхідних сигналів

Третя парадигма, навчання з підкріпленням, передбачає наявність довкілля; у цьому випадку навчання відбувається за допомогою взаємодії мережі із зовнішнім середовищем; зовнішнє середовище посилає сигнали, на основі яких мережа навчається

Як приклад можемо розглянути один із методів навчання це «Навчання нейромереж через еволюцію поколінь». Основна ідея полягає в тому, щоб використовувати механізми природного відбору для покращення нейромережі

Основні етапи методу навчання нейромереж через еволюцію поколінь виглядають наступним чином:

- Початкова популяція - створення початкової популяції нейромереж із випадковими архітектурами та вагами.
- Оцінка пристосованості - кожна нейромережа в популяції оцінюється за допомогою функції пристосованості, яка визначає, наскільки добре модель вирішує поставлене завдання.
- Еволюція - відбувається відбір за пристосованістю, де кращі моделі мають більше шансів брати участь у формуванні нового покоління. Здійснюється рекомбінації та мутації, щоб створювати нові архітектури та ваги.
- Нове покоління - створення нової популяції на основі відібраних та модифікованих нейромереж.
- Повторення - процес еволюції повторюється протягом декількох поколінь.

В підсумку можу зазначити переваги та недоліки навчання нейромережі через еволюцію поколінь:

Переваги:

- Налаштування: система автоматично налаштовує параметри моделі, такі як архітектура та ваги, що зменшує необхідність у ручній оптимізації.
- Необов'язковість експертного втручання: навчання через еволюцію може бути ефективним, навіть якщо відсутнє експертне знання про структуру або параметри мережі.
- Застосування до різних завдань

Недоліки:

- Великі обчислювальні витрати: процес еволюції може бути витратним з точки зору обчислень, оскільки потрібно оцінювати багато різних архітектур та параметрів.
- Час: навчання може вимагати багатьох поколінь для досягнення оптимальних результатів, що збільшує час.
- Оптимізація: в алгоритмах є багато гіперпараметрів, які потрібно оптимізувати.

Список використаних джерел

1. Нейронні мережі: основи теорії / Галушкін, А.І. - К.: Альянс, 2014. - 496 с.
2. Нейронні мережі. Основи теорії та застосування / Ю.А. Зуєв, А.С. Журавльов, Д.А. Лазарєв, 2018. -304с.
3. Нейронні мережі: Навчальне посібник для вузів. /А.І. Галушкін, Я.З. Ципкін. - К.: Альянс, 2019. - 840 с.

Анотація. Ірина ГЛАДИШ, Володимир СВІДИНЕНКО. Нейромережі, обробка інформації та навчання.

Розглядаються тип завдання нейромереж, збір та обробка даних, створення архітектури, навчання моделі, тестування, використання для обробки нових даних.

Ключові слова: нейромережа, обробка інформації, парадигми.

Дмитро БАЛИК[1], *завідуючий лабораторією,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: dmytro.balyk@gmail.com

СТВОРЕННЯ СПЕЦІАЛІЗОВАНИХ ШТУЧНИХ ІНТЕЛЕКТІВ: ПРИЧИНИ, ПЛЮСИ ТА МІНУСИ, ОСНОВНІ КРОКИ СТВОРЕННЯ ШТУЧНИХ ІНТЕЛЕКТІВ

Розробка спеціалізованих штучних інтелектів сьогодні поширене явище серед корпорацій та інтернаціональних компаній, а також створення окремих підрозділів які спеціалізуються на розробці штучного інтелекту.

Компанії створюють власний штучний інтелект з різних причин, керуючись потенційними перевагами та можливостями, які надає використання технології ШІ. Основними причинами для інвестицій у розробку власного ШІ зазвичай є специфічні випадки, інноваційні методи, покращення інструментів безпеки, підвищення ефективності.

На сьогоднішній день ШІ з легкістю справляються з сортуванням текстових або візуальних даних, що до звуків все ще насправді залишаються деякі питання.

Інше застосування це створення цехів Industry 4.0.

Industry 4.0(четверта промислова революція) — злиття автоматизованого виробництва, обміну даних і виробничих технологій в єдину саморегульовану систему, з малим втручанням людини у виробничий процес. Це дає змогу економити ресурси завдяки усуненню людського фактора та цілодобовій роботі.

Звісно металеві механізми потребують обслуговування, і тут ШІ визначить потребу краще, бо весь час буде аналізувати дані роботи кожного елементу конвеєру.

У випадку виникнення небезпечної ситуації або потрапляння людини у небезпечну зону, вірогідність шкоди людині знизиться. Таким чином маємо попередження проблем, додатковий шар безпеки та виконання рутинної роботи.

І звісно ж основний мінус, це зменшення робочих місць, адже тепер замість відділу сортування буде 1 людина яка просто слідкує за якістю і звітує про всі інциденти з ШІ, що призводить до ще більших покращень у його роботі. Машинне навчання та глибоке навчання: усі ці терміни дуже переплетені між собою. Збільшення потужності обчислень і хмарні обчислення дають нам інструменти для створення ШІ.

Починати створювати власний ШІ з нуля може бути надзвичайно складно. Тому інструменти для цього створені інженерами вищого рівня. Але на ринку є сотні рішень, як комерційних, так і з відкритим кодом, призначених для полегшення створення та навчання. Маючи правильну структуру і кілька вказівок, можна створити власний ШІ.

Будь-яка мова програмування цілком здатна створювати системи ШІ, але деякі з них виділяються як найкращі мови для цього. Наприклад Python, Julia та R.

Щоб створити свою систему ШІ, потрібно зробити певні кроки:

Визначити мету. Перш ніж будь що робити треба визначити, яку проблему має вирішувати ШІ. Чим більший набір задач, тим складніше створити рішення.

Зібрати та структурувати дані. Якість моделі залежить від даних, за допомогою яких вона була навчена, тому наявність хороших даних для ШІ є надзвичайно важливо.

На щастя для компанії як вже працюють отримати дані не буде проблемою. Але для даних є такі вимоги: приналежність проблемі, даних має бути багато, дані не мають бути упередженими. Здебільшого доводиться чистити дані для ШІ.

Створити алгоритм. Нейронні мережі, глибоке навчання, випадкові ліси, k-найближчі сусіди (KNN), символічна регресія – це деякі з математичних основ штучного інтелекту, які виконують певну функцію та вирішують певний тип проблеми.

Деякі компанії, такі як Google, мають попередньо навчені моделі, які можна налаштовувати. Вони вже навчені з мільйонів записів даних і є точнішими, ніж те, що ми можемо досягти. Замість навчання з нуля варто скористатися такими моделями.

Навчити алгоритм. ШІ треба навчити виконувати завдання, етап машинного навчання. За стандартом більшість використовують 80% свого набору даних, а решта використовуються для перевірки прогнозних можливостей. Навчання означає, що ШІ визначає шаблони в даних і робить прогноз на основі них. Мета це звісно отримати низького рівня помилок під час виконання завдань.[1]

Кінцевий результат. З навченим штучним інтелектом можна деталі та розгорнути продукт. На цьому етапі треба визначити інтерфейс користувача. Як правило алгоритм ШІ після навчання фіксується та використовується без навчання, щоб не були створені непередбачувані закономірності. Але незважаючи на цю фіксацію існує практика використовувати дані які проаналізував фіксований інтелект продовжуючи навчання, щоб цей самий інтелект весь час покращився.

Одним із способів створення може стати адаптація якогось існуючого штучного інтелекту під конкретні потреби підприємства. У випадку аналізу неструктурованих даних підійде використання таких ШІ: Polymer, Tableau, Microsoft Power BI, Akkio. Вони мають API для розробників за допомогою якого і відбувається зв’язок з оригіналом.

Від автомобільної промисловості до звичайних повсякденних завдань, штучний інтелект стає основною технологією майже в кожній галузі, і з раптовим зростанням інтересу та потенціалу доходу можна очікувати, що з’явиться ще більше нових інструментів для розробників для створення інтелектуальних систем.

Список використаних джерел

1. How to Create an AI System in 5 Steps URL: https://www.bairesdev.com/blog/how-to-develop-an-ai-system-steps/
2. Preparing Your Dataset for Machine Learning: 10 Basic Techniques That Make Your Data Better URL: https://www.altexsoft.com/blog/preparing-your-dataset-for-machine-learning-8-basic-techniques-that-make-your-data-better/
3. The Best 10 AI Tools to Analyze Data in 2023 URL: https://www.polymersearch.com/blog/the-best-10-ai-tools-to-analyze-data
4. Як бізнес може використовувати штучний інтелект URL: https://www.epravda.com.ua/columns/2023/05/8/699875/

Анотація. Дмитро БАЛИК. Створення спеціалізованих штучних інтелектів: причини, плюси та мінуси, основні кроки створення штучних інтелектів.

Розробка штучних інтелектів стала поширеним явищем серед корпорацій та міжнародних компаній. Компанії створюють власні рішення з штучного інтелекту для поліпшення ефективності, забезпечення безпеки даних та зменшення витрат. Вже застосовується в обробці інформації та промисловості, включаючи автоматизовані виробництва Industry 4.0, де штучний інтелект забезпечує повну автоматизацію та безпеку робочих процесів без працівників.

Ключові слова: штучний інтелект, розробка, Industry 4.0, промисловість, безпека робочих процесів.

5

«ІНФОРМАЦІЙНА ГІГЄНА»

Оксана ОСАДЧА[1], *викладач першої категорії,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: ksenya_kr@ukr.net
Олександра КРИВУЛЯ[1], *здобувач освіти,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: aleksakr3007@gmail.com

БОТОФЕРМИ: СЕКРЕТНІ ІНСТРУМЕНТИ ПРОПАГАНДИ У СОЦІАЛЬНИХ МЕРЕЖАХ

Нейромережа - це клас алгоритмів машинного навчання, які імітують структуру та функцію людських нейронних мереж. Вони використовуються для розв'язання складних завдань та обробки інформації завдяки навчанню на даних.

Нині складно уявити особу, що не має своєї сторінки в соціальних мережах і, відповідно, яка не мала досвіду взаємодії з ботами у віртуальному середовищі. Проте, не всі мають чітке уявлення про те, що це і як саме працює. Основне ж питання полягає в тому, наскільки користувачі усвідомлюють небезпеку, яку можуть нести боти.

Термін «бот», що є скороченням від «робот», з’явився з появою та розповсюдженням в Інтернет саме соцмереж. З масовим створенням віртуальних образів для анонімного спілкування, в цьому світі комунікації, з'явились інтернет-боти – акаунти, які не пов'язані із конкретними особистостями. Відповідно з’явились і ботоферми, які керують десятками і навіть сотнями таких акаунтів.

Ботофермами називають організовані групи, що займаються створенням та управлінням мережею ботів або фейкових акаунтів у соцмережах, поштових сервісах та месенджерах [4].

Особливо небезпечною стає діяльність ботів під час війни, адже вони впливають на суспільні настрої шляхом поширення фейкових новин, пропаганди певних наративів, маніпуляційної інформації, що може призвести до сплутування, паніки та хаосу. Переважно поширюється повна дезінформація та спотворені інфоприводи: перекручені слова лідерів держави, відеонарізки з вирваними з контексту фразами, замовлені дописи у Telegram-каналах [1]. Це може підривати довіру суспільства до медіа та уряду.

Також ботоферми можуть використовуватися для масового збирання особистих даних громадян. Ці дані можуть потрапити до списків окупантів чи до рук шахраїв, ними можуть неправомірно скористатися чи передати для шантажу, махінацій та інших злочинів.

Як бачимо, діяльність ботоферм несе багато негативних наслідків для суспільства, однак переважно, вона є дуже прихованою та важкопомітною, оскільки ці боти можуть мати автентичний зовнішній вигляд та розміщувати повідомлення, які імітують поведінку реальних користувачів. Крім того, організаторами ботоферм використовуються найсучасніші розробки не тільки у сфері цифрових та управлінських технологій, а й та різноманітні психотехнології. Відповідно державні програми боротьби з цим явищем повинні також містити інтегровані рішення, зокрема пов’язані зі створенням спеціалізованого програмного забезпечення. Однак важливе місце у цій боротьбі займає суспільний контроль [2].

Для того, щоб розпізнати бота, необхідно звертати увагу на такі ознаки:

– облікові записи з великою кількістю підписників, що мають низький рівень активності;

– однотипний або повторюваний контент;

– практично миттєва швидкість реакції на повідомлення або коментарі;

– відповіді, що містять шаблонні ключові слова та фрази і не демонструють глибокого розуміння інформації.

Тому гортаючи, в черговий раз, стрічку новин, потрібно не забувати аналізувати, хто пише, хто коментує, які пабліки це поширюють та навіщо. І пам'ятати про ботів, яких використовують для поширення і коментування спеціально відібраних медіаповідомлень чи конструювання видуманої (штучної) реальності, що не відображують реального світу, а лише несуть ретельно відібрані, для досягнення певних цілей, уявлення про нього для розхитування ситуації, що несе шкоду країні [3].

Список використаних джерел

1. Виговська Ірина. Я працюю ботом і пишу сотні коментарів у соцмережах на день. *The Village Україна.* URL: https://www.village.com.ua/village/knowledge/mediahramotnist/340413-ya-pratsiuiu-botom (дата звернення 11.11.2023)

2. Курбан О.В. Специфіка створення та функціонування нелегальних локальних соціальних он-лайн мереж. *Slovak international scientific journal № 47, (2020)* URL: https://elibrary.kubg.edu.ua/id/eprint/39786/1/O_Kurban_SISJ_3_IJ.pdf (дата звернення 12.11.2023)

3. Пророк Н. В. До питання психологічного впливу на людину сучасних інформаційних продуктів. Збірник тез наукових доповідей ІІІ Всеукраїнської конференції: Психологічні виміри особистісної взаємодії суб'єктів освітнього простору в контексті гуманістичної парадигми. URL: http://surl.li/njpow (дата звернення 12.11.2023)

4. Шиншинов Аркадій. Боти і ботоферми. Як це працює і що робити, щоб не потрапити на гачок дезінформації. URL: https://varosh.com.ua/life/boty-i-botofermy-yak-cze-praczyuye-i-shho-robyty-shhob-ne-potrapyty-na-gachok-dezinformacziyi/ (дата звернення 12.11.2023)

Тетяна НОВІК[1], *викладач,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: novik_tanya@g-suit.kk.nau.edu.ua

СПЕРШУ ПЕРЕВІР – ПОТІМ ПОВІР

З самого початку воєнного конфлікту з Україною російська державна пропаганда систематично використовує фейки як активний інструмент інформаційної війни. Починаючи з 24 лютого 2022 року, коли почалося вторгнення, пропаганда посилила свою активність з новою енергією.

Одним із ключових інструментів такої пропаганди є фотографії, особливо через те, що вони викликають більше довіри, ніж звичайний текст. Фотофейки, як інструмент маніпуляції, не є обмеженими лише російською пропагандою; їх можна зустріти, наприклад, у "циклічних" фейках, які розповсюджуються в соціальних мережах [2].

Для перевірки автентичності фотографій важливо досліджувати їх та приділяти увагу деталям, порівнюючи їх із текстом, що супроводжує зображення. Наприклад, можна отримати такі деталі, як погодні умови, розташування, архітектура, назви вулиць та номери машин. Це допоможе впевнитися, що фото було зроблене саме в тому місці, як показано.

Один із методів перевірки фотографій на їхню автентичність - використання системи пошуку зображень, і найбільш популярна з них - Google. Щоб скористатися цією послугою, слід натиснути правою кнопкою миші на зображення, позначити «Пошук зображення через Google Lens» і у відкритому вікні позначити «Знайти джерело зображення». Після цього можна переглянути інформацію про те, де ще було опубліковано це зображення (див. рисунок 1).

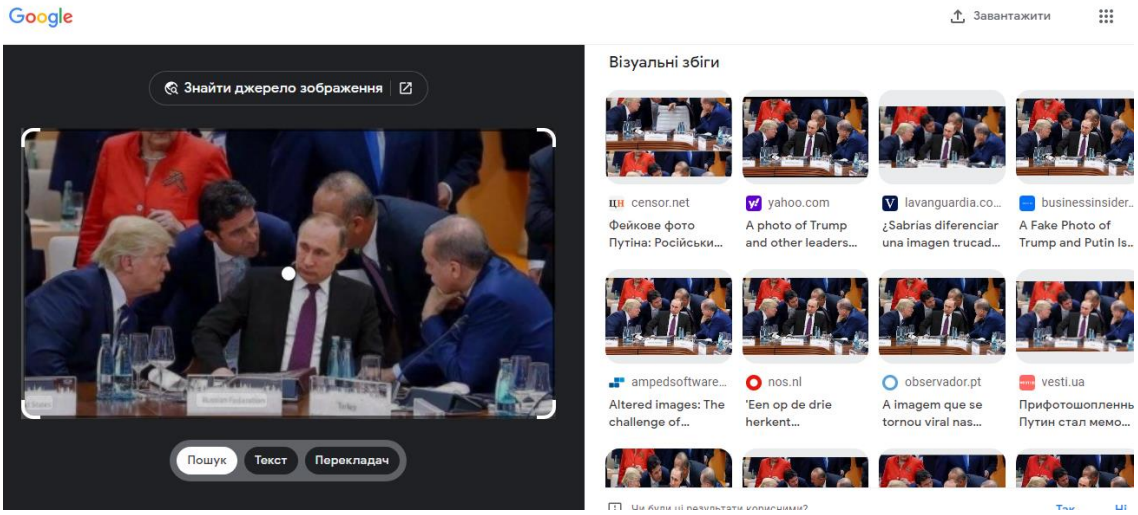

Рисунок 1 - Пошук зображення через Google Lens

Завдяки цьому методу ви перевіряєте відразу два важливих аспекти. Перше: чи є зображення оригінальним або піддавалося обробці. Другий важливий момент, який можна перевірити таким способом дата публікування зображення, а також те, що на ньому насправді зображено

Якщо перейшовши за посиланням, вихідний контент представлений іншою мовою, ми виконуємо його переклад на українську, а потім вивчаємо, порівнюємо зображення,

перевіряємо дату публікування. Якщо є розходження з першоджерелом, можна вважати, що фотографія є фейком (див. рисунок 2).

Міністр закордонних справ Чавушоглу супроводжує президента Ердогана під час його візиту до Німеччини для участі у саміті G20 у Гамбурзі, 7-8 липня 2017 р.

Міністр закордонних справ Чавушоглу супроводжував президента Ердогана під час його візиту до Гамбурга 7-8 липня 2017 року для участі у саміті G20.

7 липня президент Ердоган взяв участь у робочій сесії саміту G20 на тему «Глобальне зростання та торгівля» та знову зустрівся з президентом США Трампом під час саміту.

Під час саміту президент Ердоган також мав переговори з президентом Мексики Ньєто, генеральним секретарем ООН Гутеррішем, прем'єр-міністром Японії Абе, Солбергом з Норвегії та Джентілоні з Італії.

Того ж дня міністр Чавушоглу зустрівся з міністром закордонних справ Франції Жан-Івом Ле Дріаном. Під час зустрічі було оцінено двосторонні відносини та регіональний розвиток.

Рисунок 2 – Першоджерело, перекладено українською мовою [3]

Список використаних джерел

1. Богуш В. М. Інформаційна безпека держави. Київ: МК-Прес, 2005. 432 с.

2. Іванов В. Медіаосвіта та медіаграмотність: короткий огляд. Академія української преси. 2011. 58 с.

3. https://www.mfa.gov.tr/disisleri-bakani-mevlut-cavusoglu-G20-hamburg-zirvesine-katilan-sn-cumhurbaskanina-refakati_en.en.mfa

Анотація. Тетяна НОВІК. Спершу перевір — потім повір.

Маніпуляції з фотозображенням можуть відбуватися у різний спосіб: 1) на етапі зйомки, у випадку, коли автор робить постановку; 2) на етапі постобробки, коли можливими є ретуш і монтаж зображення; 3) на етапі контексту, коли світлина отримує заздалегідь хибний підпис або заголовок [1]. Іноді маніпуляції можуть відбуватися на двох або на трьох етапах одразу, посилюючи загальний ефект фейкового повідомлення.

Ключові слова: пропаганда, фотофейк, Google Lens, інформаційна війна, пошук зображення.

Ірина КРАВЧУК[1]*, викладач методист вищої категорії,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж
Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: kravchuk_iv@g-suit.kk.nau.edu.ua
Ігор КРАВЧУК[1]*, викладач вищої категорії,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж
Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: kravchuk21@g-suit.kk.nau.edu.ua
Вікторія ПШЕНИЧНА[1]**,** *здобувач освіти,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж
Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: pshenychna.viktoriia@g-suit.kk.nau.edu.ua

РИЗИКИ, ЩО НЕСЕ ІНФОРМАЦІЙНА БУЛЬБАШКА, ТА СПОСОБИ ПОДОЛАННЯ

Збереження приватності особистих даних є важливим для забезпечення безпеки та захисту особистості. Захист особистих даних є важливим для запобігання несанкціонованому використанню та зловживанню.

Інформаційна бульбашка - це стан інформаційної ізоляції або явище спричинене наслідком ефектів персоналізованого пошуку, де алгоритми веб-сайту вибірково враховують, яку інформацію користувач бажає отримати, опираючись на збір та використання інформації про користувача [2].

Інформаційна бульбашка може нести різноманітні ризики для людини, включаючи:

1. Обмежений кругозір:
2. Поляризація поглядів:
3. Підвищення вразливості до маніпуляцій:
4. Погіршення ментального здоров'я:
5. Зменшення довіри до інших:
6. Втрата об'єктивності:

Як вирватися з інформаційної бульбашки?

- Змусіть веб-сервіси забути про вас. Щоб знищити всю інформацію, яку браузер зберігає про вас, необхідно видалити всі файли cookie та історію.

- Якою б «геніальною» не була б ваша позиція варто дослухатися й до альтернативної думки. Майже завжди є факти які, можливо, не помічаємо або не хочемо помічати. Щоб вибратися з «інформаційної бульбашки», треба чути інші альтернативні точки зору та час від часу критично ставитися до власних знань і поглядів на події [1].

- Підписуйтесь і слідкуйте за якісними ЗМІ. Список таких ЗМІ періодично публікує Інститут масової інформації.

- Менше використовуйте соцмережі. Це краще для здоров’я фізичного та психічного.

- Використовуйте різні платформи перегляду інформації для отримання різних точок зору.

- Навчайтесь розпізнавати маніпуляції та фейкову інформацію.

- Розвивайте навички аналізу та критичного оцінювання інформації.

- Частіше цікавтеся тим, що виходить за межі ваших знань.

Список використаних джерел

1. Розірвати інформаційну бульбашку: 7 порад про те, як зробити соцмережі кращим місцем [Електронний ресурс]. – Режим доступу : https://bit.ua/2021/09/filter-bubble-7-porad-pro-te-yak-zrobyty-sotsmerezhi-krashhym-mistsem/

2. Більше ніж спілкування [Електронний ресурс]. – Режим доступу : http://mediadriver.online/sotsialni_media/bilshe-nizh-spilkuvannya/

6

«ВИКОРИСТАННЯ ІНФОРМАЦІЙНОГО ПРОСТОРУ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЗАГАЛЬНООСВІТНІХ ДИСЦИПЛІН»

Алла ТАРАДУДА[1], *викладач,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: allataraduda@gmail.com

ОСВІТНІЙ ПРОЦЕС ІЗ ЗАСТОСУВАННЯМ ІНТЕРНЕТ – РЕСУРСІВ

З самого початку воєнного конфлікту з Україною російська державна пропаганда систематично використовує фейки як активний інструмент інформаційної війни. Починаючи з 24 лютого 2022 року, коли почалося вторгнення, пропаганда посилила свою активність з новою енергією.

Сучасне суспільство – інформаційне. В ньому виробництво інформації та забезпечення знань є головним продуктом. Інформаційно – комунікаційні технології (ІКТ), інтернет їх розвиток створили можливості доступу до величезних обсягів інформації, що є простором для обміну інформацією. І тут значної ролі набуває робота викладача над навчально – методичним забезпеченням дисциплін і навчання взагалі.

Розвиток і використання ІКТ в навчальному процесі дає багато основних і розширює додаткові можливості.

Інтернет в цьому питанні має особливу роль, яка відкриває широкі можливості ефективного її використання в освіті. Інтернет включає можливості широкого використання:

- навчальні дистанційні курси;
- дистанційні олімпіади;
- дистанційні конкурси;
- бібліотеки;
- інтерактивні енциклопедії та словники;
- перекладачі;
- віртуальні музеї та вистави;
- курси підвищення кваліфікації;
- профорієнтаційні ролики. [1, с.151]

Організований доступ до мережі інтернет надає можливість навчання здобувачам освіти в довільному місці в будь – який час. Джерелом активної, комунікативної та інтелектуальної діяльності (знання, уміння, навички) є інтернет. А також надає можливість доступу до освітньої інформації. Важливим є те, що і здобувач освіти і викладач має змогу знайти, переробити і представити у мережу власні здобутки.

На даний час (в умовах військового стану) активно вдосконалюються і розробляються методики і форми використання Інтернет – ресурсів в освітньому середовищі.

http://www.osvita.ua – інформаційний освітній інтернет - ресурс України: новини, законодавство, тестування, вища освіта, ЗНО/ НМТ

http://www.nbuv.gov.ua/ - Національна бібліотека України імені В.Г. Вернадського, Київ. Містить інформацію про: інформаційні ресурси; інтернет-путівники; національні доповіді.

Використання Інтернет – ресурсів значно допомагає оптимізувати, наповнити цікавою сучасною інформацією освітній процес. Надає можливість створити ефективні, зручні умови для навчальної діяльності здобувачів освіти. Це надає багато перспектив у навчанні. Вони значно полегшують життя як викладачу так і здобувачу освіти. Однак потрібно враховувати і те, що викладач обов’язково має донести до здобувачів освіти,

що запропоновані сервіси використовуються, як допоміжний освітній ресурс, а не лише для розваг.

Список використаних джерел

1. Гуревич Р.С. Інформаційні технології навчання: інноваційний підхід : навчальний посібник / Р. С. Гуревич, М. Ю. Кадемія, Л. С. Шевченко ; за ред. Гуревича Р. С. – Вінниця : ТОВ фірма «Планер», 2012. – 348 с.

2. Биков В. Ю. Моделі організаційних систем відкритої освіти : монографія / В. Ю. Биков – К. : Атіка, 2009. – 684 с.

Анотація. Алла ТАРАДУДА. Освітній процес із застосуванням Інтернет – ресурсів.

Тези присвячені відображенню основних аспектів та напрямків ефективності використання і застосування в освітньому процесу Інтернет – ресурсів для вивчення дисциплін.

Ключові слова: Інтернет – ресурси, освітній процес, здобувач освіти

Марія КИСЛОВА[1], *к.пед.н., викладач-методист,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: kislova@g-suit.kk.nau.edu.ua
Дмитро ЛУЦЕНКО[1], *здобувач освіти,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: lutsenko.dmytro@g-suit.kk.nau.edu.ua

ДИНАМІЧНЕ МОДЕЛЮВАННЯ У НАВЧАЛЬНОМУ ПРОЦЕСІ

Найважливішими проблемами освіти, зокрема - математичної, є проблеми зацікавленості здобувача освіти у вивченні того або іншого матеріалу і можливості його ефективного засвоєння.

Сама проблема засвоєння навчального матеріалу пов'язана з певною методикою роботи з матеріалом, що вивчається. А саме: зрозуміти і засвоїти деякий об'єкт (чи сукупність об'єктів як об'єкт) означає добитися за допомогою моделювання можливості застосування відомих підходів до розв'язування відповідних задач. Тому процес моделювання, а саме динамічного моделювання, є основним в дослідницькій роботі при вивченні математичних дисциплін.

Під динамізацією розуміють насамперед процес дослідження математичних об'єктів та їхніх структур за допомогою зміни базисних елементів або параметрів, що їх визначають, встановлення функціональних зв'язків та інваріантів.

Методи динамізації обмежені необхідністю введення числових параметрів, а сам процес відірваний від процесу моделювання.

Таким чином, постає проблема можливого розширення об'єктів і методів динамізації, а також розширення умов, за яких динамізація розкриває всі свої можливості.

Як об'єкти динамізації можна брати різні типи моделей тих чи інших понять і не тільки суто геометричних, а й синтактичних. Так, наприклад, як об'єкти можна використовувати висловлювання і умовиводи ...

Динамізація можлива не тільки на стадії розв'язання задач, а й на стадій роботи над поняттям, над доказом тощо.

Проблема динамізації при викладанні математичних дисциплін може розглядатися в двох аспектах: по-перше, динамізація в математиці може розглядатися як мета (при цьому формулюються і розв'язуються спеціальні динамічні завдання, вводяться спеціальні терміни); по-друге, динамізація в математиці може розглядатися як засіб постановки нових проблем, формулювання нових завдань на різних етапах навчальної діяльності.

Основними перевагами динамічного моделювання у навчальному процесі є:

1. Динамічне моделювання розвиває математичну інтуїцію і саме є евристичним прийомом, що виходить за межі власне математики.

2. Належний підбір динамічних моделей з урахуванням вікових особливостей здобувачів освіти надає можливість опустити вікову планку для цілісного засвоєння пов'язаної між собою групи понять (наприклад: корінь, логарифм), надає нові можливості для випереджаючого навчання і пропедевтики.

3. Динамічне моделювання розвиває мислення здобувачів освіти, формує методологічні принципи навчальної і дослідницької роботи.

4. Динамічне моделювання надає можливість диференціювати навчання здобувачів освіти і інтегрувати різні теми.

5. Динамічне моделювання надає можливість безболісно використати в процесі вивчення математичних дисциплін теоретико-множинний і аксіоматичний підходи, ширше використати точкові і інші перетворення.

6. Розширює можливості складання дослідницьких програм, виявляє нові можливості для навчання здобувачів освіти складанню і розв'язуванню завдань, у тому числі - і нестандартних.

7. Надає можливість ввести в навчальний процес математичний експеримент, чітко виділити змістовну і логічну складові теми, що вивчається, здійснити багаторівневий підхід до навчання здобувачів освіти як змістовною, так і логічною складових і їх використанню.

8. Динамічне моделювання відкриває можливості для математичного експерименту з метою отримання відповідей на поставлені питання, і для ставлення самих питань (дослідницькі програми).

Отже, динамічне моделювання виводить навчальний процес за межі власне математики, на ширше поле діяльності: в область логіки, семантики, гносеології, методології науки, а кількість використовуваних моделей зовсім не обтяжує навчальний процес, а робить його цікавішим, насиченим і, в той же час, методологічно прозорим.

Список використаних джерел

1. Коробова М.В. Основи математичного моделювання економічних, екологічних та соціальних процесів/ М.В. Коробо- ва, І.М. Ляшенко, А.М. Столяр. – Тернопіль: "Навчальна книга – Богдан", 2006. – 304 с.

2. Кравець І.О. Імітаційне моделювання: Навч. посібник. – ЧДУ ім. Петра Могили, 2010.- 107 с.

Анотація. Марія КИСЛОВА, Дмитро ЛУЦЕНКО. Динамічне моделювання у навчальному процесі.

Аргументовано та доведено доцільність використання динамічних моделей у навчальному процесі при вивченні математичних дисциплін. Показано переваги використання динамічних моделей у навчанні.

Ключові слова. Навчання, процес навчання, динамічна модель, динамізація.

Наталя МОРОЗКІНА[1], *викладач соціальних дисциплін, спеціаліст вищої категорії,*
Інгулецький фаховий коледж «Криворізького національного університету»,
м. Кривий Ріг[1]
E-mail: morozkina@knu.edu.ua

УРІЗНОМАНІТНЕННЯ ІНФОРМАЦІЙНИХ МЕТОДІВ ВИКЛАДАННЯ ІСТОРІЇ ПІД ЧАС ДИСТАНЦІЙНОГО НАВЧАННЯ

У статті розкрито проблему урізноманітнення інформаційних методів викладання історії під час дистанційного навчання, доцільність використання роботи з онлайн-дошкою Padlet, а саме її функцію хронометраж часу, що дозволить студентам наочно споглядати основні історичні дати з обраної теми.

Актуальність проблеми. У сучасних умовах тривалого дистанційного навчання, яке було спричинене спочатку карантином з приводу пандемії COVID-19, а потім повномасштабним вторгненням і російською агресією проти України формат навчання істотно змінився. Сучасний викладач повинен був урізноманітнювати методи викладання свого предмета, шукати нові, цікаві способи подачі інформації студентам для того, щоб їх зацікавити, надати широкий вибір пошуку інформації, її обробки й систематизації.

На сучасному етапі головними труднощами, які необхідно долати управлінцям й освітянам будуть організація ефективного плідного дистанційного навчання, адаптація сучасної освіти до вимог сьогодення, забезпечення підвищення кваліфікації викладачів та опанування ними нових інформаційних методів викладання. Технології дистанційного навчання дозволяють продовжувати освітній процес під час карантину та інших надзвичайних обставин (без переведення студентів на дистанційну форму).

Разом з тим відповідно до Державного стандарту базової середньої освіти [1], Закону України про фахову передвищу освіту [3] в сучасному навчальному закладі фахової передвищої освіти відбувається системне оновлення змісту та перехід на нову структуру навчання. Новітнє суспільство висуває нові вимоги до освіти, однією із яких є підготовка людей, спроможних приймати критичні рішення, знаходити спосіб спілкування в новому оточенні, які достатньо ефективно встановлюють нові стосунки у швидко змінюваній реальності. Активність, самостійність, творчість, здатність адаптуватися до стрімких змін – ці риси особистості стають найважливішими на сучасному етапі історичного розвитку, а їх формування потребує реалізації нових підходів до процесу навчання і запровадження нових інформаційних методів навчання.

У зв’язку з цим особливого значення набуває проблема урізноманітнення інформаційних методів викладання історії під час дистанційного навчання.

Переспективність використання результатів нашого дослідження полягає в тому, що сформульовані в ньому висновки про особливості урізноманітнення методів викладання історії під час дистанційного навчання можуть бути використані викладачем у практичній діяльності на заняттях з історії в закладах фахової передвищої освіти.

Виклад основного матеріалу. З початку пандемії освітянам довелося швидко опановувати нові онлайн-сервіси, різноманітні цифрові застосунки та додатки. На сьогодні стрімкий розвиток технологій в освіті дозволяє використовувати віртуальні помічники: сервіси для створення тестів та інтерактивних завдань, онлайн-дошки і т. ін.

На сьогодні є багато способів застосування інтерактивних дощок під час дистанційного навчання. В основному їх використовують для узагальнення та систематизації знань, організації групової або проєктної роботи, проведення «мозкового

штурму» або ж для рефлексії. Ще такі дошки зручні для розміщення навчальної інформації в узагальненому та систематизованому вигляді.

Padlet – це адаптований до онлайн-навчання та простий у використанні веб-сервіс для зберігання, узагальнення, систематизації, організації та спільної роботи з різним навчальним контентом (документи, матеріали). Дана віртуальна дошка зручна тим, що має необмежену кількість створюваних сторінок, а також підтримує різні мовні формати. У закладах фахової передвищої освіти даний веб-сервіс буде зручним інструментом при організації колективної діяльності та викладу нового матеріалу під час дистанційного навчання та застосування цифрових технологій [2].

Навчальна інтерактивна дошка Padlet поступово набуває свого поширення у навчально-виховному процесі, а саме, її можна застосовувати для:

- виконання тестових завдань;
- узагальнення й систематизації знань студентів;
- спільного виконання домашнього завдання;
- розміщення завдань на пошук інформації;
- як площину для розміщення навчальної інформації;
- «мозкового штурму», для узагальнення та систематизації знань;

– як місце для збирання ідей для проектів та їх обговорення.

Засоби сервісу Padlet надають можливість відтворити й систематизувати навчальний матеріал аудіально й візуально, а також представити його більш привабливо та зрозуміло, що допоможе викладачу цікаво й різноманітно провести заняття, а студентам – краще й продуктивніше засвоїти новий навчальний матеріал.

Упродовж усіх етапів заняття з історії доцільно використовувати роботу з онлайн-дошкою Padlet, а саме її функцію хронометраж часу, що дозволить студентам наочно споглядати основні історичні дати з обраної теми.

Кожна дошка має свою унікальну адресу, яку можна повідомити іншим користувачам з метою спільного наповнення та редагування, що дозволить максимально продуктивно використати час. Під час роботи з віртуальними інтерактивними дошками в процесі самостійної пошукової діяльності студентів викладач має можливість стежити за виконанням запропонованих завдань і вносити нотатки чи певні зауваження до віднайденого ними матеріалу, що робить процес більш контрольованим [2].

Висновки. Отже, можна сказати, що викладачі, які використовують у навчально-виховному процесі віртуальні інтерактивні дошки, відзначають їх позитивний вплив на мотивацію навчання в цілому, стрімке підвищення інтересу студентів до навчання.

Список використаних джерел

1. Державний стандарт базової середньої освіти (2020). URL: https://mon.gov.ua/ua/osvita/zagalna-serednya-osvita/nova-ukrayinska-shkola/derzhavnij-standart-bazovoyi-serednoyi-osviti

2. Качанюк Н. В. Використання віртуальної стіни Padlet на практичному занятті у вищій школі / Освітологічний дискурс. 2014. № 3. С. 102-112. URL: http://nbuv.gov.ua/UJRN/osdys_2014_3_13

3. Про фахову передвищу освіту/ Документ 2745-VIII, чинний, поточна редакція — Редакція від 23.03.2023, підстава - 2940-IX/ URL: https://zakon.rada.gov.ua/laws/show/2745-19#Text

Анотація. Наталя МОРОЗКІНА. Урізноманітнення інформаційних методів викладання історії під час дистанційного навчання.

Ключові слова: технології дистанційного навчання, онлайн-сервіси, інтерактивна дошка, Padlet, хронометраж часу.

7

«БЛОК ПРАКТИЧНОГО НАВЧАННЯ (ТЕХНІЧНОЇ ТВОРЧОСТІ)»

Володимир САРНІЦЬКИЙ[1], *викладач вищої категорії,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: sarnickiv@gmail.com
Володимир СЕРДЮК[1], *викладач першої категорії,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: volodymyr.serdyuk@g-suit.kk.nau.edu.ua
Данило КОМАРОВ[1], *здобувач освіти,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: Komarov.danylo@g-suit.kk.nau.edu.ua

РОЗРОБКА ТА ПРОГРАМУВАННЯ НАВЧАЛЬНО-МЕТОДИЧНОГО СТЕНДУ НАВЧАННЯ ПРОГРАМУВАННЮ

Вже понад три роки освіта в Україні працює в екстремальних умовах. Весною 2020 року почалася пандемія коронавірусу, яка повністю перевела освіту на дистанційне навчання. А весною 2022 року грянула нова біда – агресія Росії проти України. Але Україна виявилася досить просунутою країною у плані інформаційних технологій. Це дозволило налагодити ефективний процес дистанційного навчання.

Застосування технічних засобів навчання у навчальному процесі сучасних закладів освіти стало чи не найнагальнішою потребою в їх освітній діяльності. Як би не був досконалий процес навчання в школі, все одно неможливо дати людині всі ті знання, які будуть необхідні їй в подальшій роботі без застосування інноваційних форм та методів технічних засобів навчання. Використання одного з таких технічних засобів, а саме навчально-методичного стенду навчання програмуванню, пропонується у нашій роботі(рис.1).

Рисунок 1 – Навчально-методичний стенд навчання програмуванню

Список використаних джерел

1. Сергій Шкарлет та інші. Освіта України в умовах воєнного стану. Інормаційно-аналітичний збірник. Київ,2022;

2. Закон України «Про освіту». URL : http://zakon2.rada.gov.ua/laws/show/2145-19. (дата звернення 16.08.2019).

Анотація. Володимир САРНІЦЬКИЙ, Володимир СЕРДЮК, Данило КОМАРОВ. Розробка та програмування навчально-методичного стенду навчання програмуванню.

Розглядаються методи навчання здобувачів освіти програмуванню за допомогою технічних засобів навчання. Демонструється розроблений навчально-методичний стенд, що дозволяє наглядно демонструвати реальну роботу розроблених здобувачами освіти комп'ютерних програм для різного роду технічних пристроїв та систем.

Ключові слова: *навчально-методичний стенд, програмування, технічні засоби навчання.*

Анна РУДА[1]*, викладач,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: annasergeeva198@ukr.net
Денис ДОРОШ[1]**,** *здобувач освіти,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: dorosh.denys@g-suit.kk.nau.edu.ua

СТВОРЮЮЧИ ІНТЕРНЕТ: ПОГЛЯД НА МОЇ РОБОТИ У ВЕБ-ПРОГРАМУВАННІ

Мета: показати важливість мов програмування, їх можливості, та практичний результат використання.

Актуальність: в наш час багато інформації ми отримуємо через Інтернет. Ми користуємося результатом роботи ІТ-фахівців, але те, що створювалося за лаштунками не видно, тобто як код перетворюється на сайт.

Я здобувач освіти групи 3-038, закладу освіти ВСП «Криворізький фаховий коледж НАУ» хочу презентувати свої практичні роботи, які приносять користь реальним користувачам та компаніям.

Під час свого навчання я вивчив широкий спектр нових навичок в галузі програмування. Оволодівши мовами гіпертексту **HTML**, стилів **CSS** та **JavaScript**, а також отримавши досвід роботи з базами даних, я став впевненим фахівцем у сфері Веб-розробки.

Під час активного вивчення нових технологій, мені вдалося впровадити в практику інноваційні підходи, такі як використання мови PUG замість **HTML**. **PUG** вражає своєю стислістю і вимагає більше уваги до деталей, зокрема, необхідно правильно форматувати вкладеності за допомогою табуляцій. Це робить код більш компактним та ефективним порівняно з традиційним **HTML**. Додатково почав використовувати інноваційний метод розташування елементів - "**Flex-Box**", який принципово відрізняється від простого "**Position**". У той час як "**Position**" оперує примітивним розташуванням "по пікселях", "**Flex-Box**" надає можливість розташовувати елементи відносно один одного відсотковим чином, що значно полегшує створення гнучких та адаптивних макетів.

За допомогою набутого досвіду, я успішно реалізував свій перший великий проект - "Розумний будинок" (рис. 1). Це був значущий крок у моєму професійному розвитку. В подальшому мені запропонували створити Веб-сайт для стоматологічної клініки "Family Dental Center" (рис. 2), який відзначився своєю якістю та функціональністю.

Мета даної доповіді полягає у презентації не лише мого професійного зросту в програмуванні, але і у висвітленні моїх найкращих практичних реалізацій реально діючих проєктів.

Рисунок 1 – Проєкт «Розумний будинок»

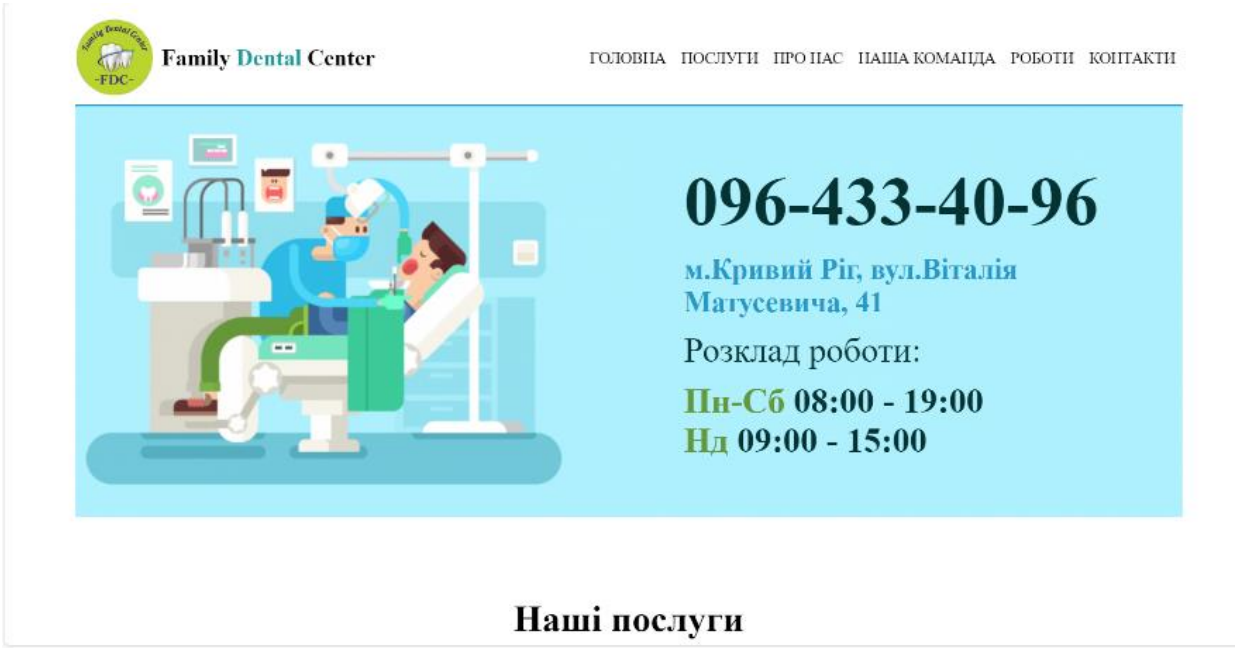

Рисунок 2 – Проєкт Веб-сайт "Family Dental Center"

Ключові слова: веб-сайт, мови програмування, html, pug, проєкт, розумний будинок.

Олександр ГРИНЧЕНКО[1], *викладач вищої категорії,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: oleksandr.grinchenko@g-suit.kk.nau.edu.ua
Артем ОРЛОВ[1], *здобувач освіти,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: artemorlov015@gmail.com
Денис ЛАГОДА[1], *здобувач освіти,*
Відокремлений структурний підрозділ «Криворізький фаховий коледж Національного авіаційного університету», м. Кривий Ріг[1]
E-mail: lagoda1den@gmail.com

РОЗРОБКА ТА РЕАЛІЗАЦІЯ МЕТЕОСТАНЦІЇ З СИСТЕМОЮ ПЕРЕДАЧІ ДАНИХ НА СМАРТФОН

Погодні умови мають значний вплив на наше повсякденне життя. Збір та моніторинг погодних даних стають все важливішими завданнями в контексті швидко змінюючогося клімату. У цих тезах розглядається розробка та реалізація метеостанції, яка не лише вимірює погодні параметри, але й передає отримані дані на смартфон, забезпечуючи користувачам доступ до актуальної інформації в режимі реального часу.

Метеостанція оснащена рядом сенсорів, які забезпечують точне вимірювання температури, вологості, тиску, вітру та інших погодних показників. Архітектура системи включає мікроконтролер для обробки та зберігання даних, а також модуль бездротового зв'язку для передачі інформації на смартфон.

Використання бездротових технологій, таких як Bluetooth або Wi-Fi, дозволяє забезпечити швидку та ефективну передачу даних між метеостанцією та смартфоном. Забезпечення безпеки комунікацій включає в себе шифрування даних та механізми аутентифікації, що гарантує конфіденційність та цілісність інформації.

Розроблений мобільний додаток надає користувачам інтуїтивний інтерфейс для візуалізації та аналізу погодних даних. Користувач може отримувати сповіщення про зміни погоди, а також переглядати статистику за певний період часу. Це надає користувачам можливість оперативно реагувати на зміни погоди та планувати свої дії.

Для забезпечення точності та надійності роботи метеостанції проводяться експерименти з порівнянням отриманих результатів з існуючими метеостанціями та стандартами. Методи тестування включають аналіз вимірювань, оцінку стійкості системи та перевірку правильності передачі даних.

Розроблена метеостанція з системою передачі даних на смартфон відкриває нові можливості для збору та моніторингу погодних даних. Ця інтегрована система спрощує доступ до інформації та дозволяє користувачам бути в курсі змін погоди в будь-який момент. Подальший розвиток та впровадження подібних технологій в області метеорології відкривають нові можливості для покращення нашого розуміння та прогнозу погоди.

Список використаних джерел

1. Smith, J. (2018). "Introduction to Weather Station Technologies." WeatherTech Journal, 15(2), 45-62.

2. Brown, A., & Johnson, C. (2020). "Wireless Communication Protocols for IoT Devices." Journal of Internet of Things Research, 8(4), 112-130.

3. Kim, S., & Lee, M. (2019). "Mobile Application Development for Environmental Monitoring." International Conference on Software Engineering, 235-245.

4. Meteorological Standards Institute. (2017). "Guidelines for Weather Data Accuracy and Precision." MSI Publications.

5. Garcia, R., & Patel, S. (2021). "Security Measures in Wireless Sensor Networks." Journal of Network Security, 14(3), 78-91.

Анотація. Олександр ГРИНЧЕНКО, Артем ОРЛОВ, Денис ЛАГОДА. Розробка та реалізація метеостанції з системою передачі даних на смартфон.

Дані з метеостанцій є важливим елементом для вивчення та передбачення погодних умов. У даній роботі розглядається розробка та реалізація метеостанції з інтегрованою системою передачі даних на смартфон. Запропонована система спрощує збір та моніторинг погодних параметрів, забезпечуючи користувачам швидкий та зручний доступ до актуальної інформації.

Ключові слова. Метеостанція, система передачі даних, смартфон, сенсори погоди, бездротові технології, мікроконтролер.

ЗМІСТ

7. Блок практичного навчання (технічної творчості)

НАУКОВЕ ВИДАННЯ

ЗБІРНИК ТЕЗ

ІІ Регіональна науково-практична конференція

«ВСЕСВІТНІЙ ДЕНЬ ІНФОРМАЦІЇ»

Матеріали опубліковані в авторській редакції

Видавництво: ВСП «Криворізький фаховий коледж НАУ».
Розмножувальна дільниця.
50000, м. Кривий Ріг, вул. Туполєва 1.
E-mail: pochta@kk.nau.edu.ua