МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ
ТЕХНІЧНИЙ УНІВЕРСИТЕТ

УДК 004.4

Тези доповідей

IV Міжнародної науково-практичної конференції

"Інформаційна безпека та комп'ютерні технології"

15–16 квітня 2021 р.

Кропивницький 2021

УДК 004.4

Матеріали IV Міжнародної науково-практичної конференції “Інформаційна безпека та комп’ютерні технології”: тези доповідей, 15–16 квітня 2021 р. – Кропивницький: ЦНТУ, 2021. – 81 с.

Наведені тези пленарних та секційних доповідей за теоретичними та практичними результатами наукових досліджень і розробок. Представлені результати теоретичних досліджень в галузях проектування інформаційних систем, технологій захисту інформації, використання сучасних інформаційних технологій в управлінні системами за різними галузями народного господарства.

Матеріали публікуються в авторській редакції.

За достовірність викладених фактів, цитат та інших відомостей відповідальність несуть автори.

СЕКЦІЯ 1. ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ, СУСПІЛЬСТВА ТА ОСОБИСТОСТІ

УДК 004.056.5

О.К Конопліцька-Слободенюк, В.О. Смутко,
Ksuha80@gmail.com, vitaliismutko@gmai.com
Центральноукраїнський національний технічний університет, Кропивницький

ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У роботі розглянуті питання впровадження системи забезпечення інформаційної безпеки(СЗІБ) і координація інформаційною безпекою організації. Розглядаються заходи для встановлення та підтримання режиму інформаційної безпеки. Враховані основні положення концепції інформаційної безпеки(ІБ) організації.

Системи забезпечення інформаційної безпеки організації складаються з ряду заходів на організаційному та програмному рівні і спрямовані на захист інформаційних ресурсів. Заходи для захисту організаційного рівня реалізуються шляхом прийняття необхідних рішень, передбачених документально та оформлено згідно політиці ІБ. Заходи для захисту програмного та апаратного рівня реалізуються за допомогою необхідних програмно-апаратних засобів та методів захисту інформації.

Ефект від впровадження СЗІБ повинен проявлятися у зменшенні можливих матеріальних, репутаційних та інших видів збитків організації через заходи для встановлення та підтримання стану ІБ. і призначені для забезпечення:

- доступності інформації (можливість отримати потрібну інформаційну послугу в розумні терміни);
- цілісності інформації (відповідність та послідовність інформації, захист від несанкціонованого внесення змін);
- конфіденційності інформації;
- беззаперечності (неможливість відхилення вчинених дій);
- автентичності (підтвердження автентичності та справжності електронних документів).

Концепція ІБ організації визначає склад критичних ІР та основні принципи її захисту. Принципи підтримки режиму ІБ вимагають використання певних методів та технологій захисту. Визначення способів реалізації цих принципів за допомогою використання програмно-апаратного забезпечення ІБ та системи організаційних заходів є предметом конкретних проектів і керівних принципів ІБ та були розроблені на основі концепції, що визначає:

1) основні принципи для складання переліку критично важливих ресурсів, які слід захистити, котрий визначається після проведення аудиту безпеки та аналізу ризиків. Цей перелік повинен включати опис фізичних, програмних та ІР, визначаючи вартість ресурсу та ступінь критичності для бізнесу;

2) основні принципи захисту, що визначають стратегію забезпечення ІБ та перелік правил, яких слід дотримуватися при створенні СЗІБ організації;

3) модель порушення безпеки, яка визначається на основі огляду системних ресурсів та їх використання;

4) модель загроз безпеці та оцінка ризиків, пов'язаних з їх реалізацією, заснована на переліку найважливіших ресурсів та моделі порушення. Сюди входить визначення ймовірності загроз та шляхів їх реалізації, а також оцінка можливих збитків;

5) вимоги безпеки, визначені результатами аналізу ризику;

6) програмні, технічні й організаційні заходи безпеки для реалізації цих вимог;

7) відповідальність працівників організації за відповідність зазначеним вимогам ІБ під час роботи інформаційної системи організації.

Концепцію слід переглянути, коли будуть визначені нові методи та технології для атак на ІР. Такий огляд також слід проводити в міру розвитку інформаційної системи організації. Рекомендований термін для перегляду концепції – три роки (за умови відсутності кардинальних змін у структурі системи, в технологіях управління та передачі інформації).

Відповідальність за дотримання вимог ІБ, котрі визначаються концепцією та іншими організаційно-розпорядчими документами організації, покладається на користувачів та адміністраторів корпоративної мережі даних організації та їх менеджерів.

УДК 621.391.1

И.В. Дидур[1], О.В. Березюк[2]
digor5035@gmail.com
[1]студент
[2]научный руководитель
доцент кафедры безопасности жизнедеятельности и педагогики безопасности, к.т.н., доцент
Винницкий национальный технический университет, Винница

СОВРЕМЕННЫЕ УСЛОВИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЧЕЛОВЕКА

Одна из главных задач современного государства – обеспечение информационной безопасности личности, которая характеризуется защищенностью психики и сознания от опасных информационных воздействий: манипулирование, дезинформирование [1]. Сейчас наше общество испытывает влияния от СМИ (в частности их информационно-пропагандистской направленности), компьютерных сетей, программных средств распространения, рекламы и т. п [2, 3]. К сожалению, ни одна из приведенных сфер влияния на человека не возможна без вреда его психологическому здоровью. Информационно-психологическая безопасность личности (в узком понимании) – это состояние защищенности психики человека от негативного воздействия, который осуществляется путем внедрения деструктивной информации в сознание и (или) в подсознание человека, что приводит к неадекватному восприятию им действительности [4].

Средства массовой информации наиболее эффективны для осуществления информационно-психологического воздействия на большие массы людей, что позволяет рассматривать их как составную часть стратегических сил информационной войны. Самой опасной чертой средств массовой информации, как считают многие специалисты, является способность подавать информацию таким образом, чтобы за видимой объективностью у большой массы людей формировалась виртуальная картина реальности. Однако, как только человек начинает сомневаться в виртуальной картине мира, эффективность информационно-психологического воздействия резко падает. Эти сомнения могут быть поддержаны технологиями контрпропаганды, также реализованы с помощью средств массовой информации.

Социальные сети стали самой популярной составляющей современного интернета [5-12], которым в мире пользуются сейчас более 2 млрд. человек. Более 60% из них являются активными пользователями интерактивных сервисов Web 2.0. Из 100 самых посещаемых сайтов в мире 20 – это классические социальные сети и еще 60 – в той или иной является социализированным. Сегменты социальных сетей Facebook, Twitter и других на сегодня является наименее застрахованными от негативных внешних информационных воздействий, и это особенно опасно в условиях информационно-психологической войны, в которые вовлечено сегодня наше государство. Опасность связана с рядом факторов.

Среди которых:

- не адаптированность современного человека к растущим массивам Навои информации, различной по качеству, достоверности и социальной значимости;

− неподготовленность подавляющего большинства участников информационных обменов в сетях в технологическом плане [13], отсутствие навыков поиска качественной информации;

− чрезмерная идеализация общения в социальных сетях (при низком доверии к отечественным СМИ, политиков);

- отсутствие знаний об угрозах, которые несет с собой информационная война, об убытках, которые она может нанести государству и конкретному человеку [14].

В связи с этим, участники обменов могут легко попадать под действием специальных манипулятивных технологий, боевых технологий информационной войны. Особенно много в социальных сетях организовано групп на население Украины. Подобные сетевые сообщества являются одним из основных средств организации массовых политических акций, уличных беспорядков. Еще один манипулятивный прием в социальных сетях связан с вливанием части информации, которая заставляет индивида додумать определенное событие, ситуацию нужную для манипулятора русле.

В социальных сетях, как в самом двуручном канале общения, особую опасность представляют суггестивные влияния. Еще совсем недавно суггестия (внушение) рассматривалась в двух измерениях. Во-первых, как психическое воздействие одного человека на другого, вследствие которого у человека-объекта внушения вопреки ее воли и сознания возникают определенные представления, суждения, поступки. И, во-вторых, под этим понятием понимается психическое воздействие на человека, находящегося в состоянии гипноза [15].

Однако на сегодня, с развитием информационных технологий, приведенное формирование нельзя считать исчерпывающим. Третьим компонентом этого определения, очевидно, надо считать влияние современных, прежде всего электронных, информационных технологий на сознание человека.

Таким образом, влияние бессознательной информации на человека сейчас является очень актуальной проблемой общества. Чтобы избежать информационной войны, необходимо увеличить уровень информационной безопасности, подготавливать людей с раннего возраста. В частности, научиться: адаптироваться к растущим объемам информации; искать правдивую информацию; оказывать предпочтение живому общению, а не через социальные сети; критически относиться к информации, что получила от сомнительных источников.

Список литературы

1. А. А. Булейко, Н. Б. Мітіна, та А. В. Кудрявцев, "Життєдіяльність та інформаційна безпека людини у сучасних умовах", на IX Міжнар. наук.-техн. конф. студентів, аспірантів та молодих вчених Хімія та сучасні технології, Дніпро, 2019, Т. III, с. 40-41.

2. О. В. Березюк, та М. С. Лемешев, Безпека життєдіяльності: навчальний посібник. Вінниця: ВНТУ, 2011.

3. О. В. Березюк, М. С. Лемешев, І. В. Заюков, та С. В. Королевська, Безпека життєдіяльності: практикум. Вінниця: ВНТУ, 2017.

4. Д. М. Палагнюк, Д. С. Тищук, та О. В. Березюк, "Принципи забезпечення інформаційної безпеки", на Наук.-практ. конф. Якість і безпека. Сучасні реалії. Матеріали, Вінниця, 2018, с. 19-22.

5. О. В. Березюк, "Застосування комп'ютерних технологій під час вивчення студентами дисциплін циклу безпеки життєдіяльності", Педагогіка безпеки: міжнародний науковий журнал, № 1 (1), с. 6-10, 2016.

6. А. Б. Веліховська, С. Б. Літвінчук, та В. М. Курепін, "Мережеві технології формування професійних якостей майбутніх фахівців готельно-ресторанної справи", на VI Всеукр. наук.-практ. конф. Актуальні проблеми в системі освіти: заклад загальної середньої освіти – доуніверситетська підготовка – заклад вищої освіти, Київ, 2020, с. 47-54.

7. О. В. Березюк, "Міжпредметні зв'язки у процесі вивчення дисциплін циклу безпеки життєдіяльності майбутніми фахівцями радіотехнічного профілю", Педагогіка безпеки: міжнародний науковий журнал, № 2, с. 21-26, 2017.

8. Л. Л. Березюк, та О. В. Березюк, "Тестова комп'ютерна перевірка знань студентів із дисципліни «Медична підготовка»", на IV Всеукр. наук.-метод. конф. Науково-методичні орієнтири професійного розвитку особистості, Вінниця, 2016, с. 96-98.

9. О. В. Березюк, М. С. Лемешев, та М. А. Томчук, "Перспективи тестової комп'ютерної перевірки знань студентів із дисципліни «Безпека життєдіяльності»", на дев'ятій міжнар. наук.-метод. конф. Безпека життя і діяльності людини – освіта, наука, практика, Львів, 2010, с. 217-218.

10. О. В. Березюк, М. С. Лемешев, та І. В. Віштак, "Комп'ютерна програма для тестової перевірки рівня знань студентів", на наук.-техн. конф. студентів, магістрів та аспірантів Інформатика, управління та штучний інтелект, Харків, 2014, с. 7.

11. O. V. Bereziuk, M. S. Lemeshev, V. V. Bohachuk, and M. Duk, "Means for measuring relative humidity of municipal solid wastes based on the microcontroller Arduino UNO R3", Proceedings of SPIE, Photonics Applications in Astronomy, Communications, Industry, and High Energy Physics Experiments 2018, Vol. 10808, No. 108083G, 2018, http://dx.doi.org/10.1117/12.2501557

12. O. Bereziuk, M. Lemeshev, V. Bogachuk, W. Wójcik, K. Nurseitova, and A. Bugubayeva, "Ultrasonic microcontroller device for distance measuring between dustcart and container of municipal solid wastes", Przeglad Elektrotechniczny, No. 4, Pp. 146-150, 2019, http://dx.doi.org/10.15199/48.2019.04.26

13. В. М. Курепін, та К. М. Горбунова, "Виховання культури безпеки життєдіяльності майбутніх фахівців у закладах вищої освіти", Педагогічні науки: збірник наукових праць, 2018, с. 127-135.

14. В. М. Курепін, "Підвищення рівня підготовки здобувачів вищої освіти освітнього ступеню «Магістр» з дисципліни «Цивільний захист»", на II Всеукр. наук. конф. Актуальні питання техногенної та цивільної безпеки України, Миколаїв, 2020, с. 172-175.

15. В. М. Курепін, та В. С. Іваненко, "Психолого-педагогічні методи формування креативного мислення в майбутніх інженерів-педагогів", на XXIII міжнар. наук.-практ. інтернет-конф. Осінні наукові читання, Тернопіль, 2019, с. 48-51.

УДК: 007.51

В.Ю. Шельпяков
shelly1990@ukr.net
Глухівський агротехнічний інститут імені С.А. Ковпака Сумського НАУ, м. Глухів

ФІЗІОЛОГІЧНІ БІОМЕТРИЧНІ СИСТЕМИ ВЕРИФІКАЦІЇ ТА ІДЕНТИФІКАЦІЇ ОСОБИСТОСТІ

Біометричне розпізнавання – метод ідентифікації особи на основі фізіологічних або поведінкових рис. Зі збільшенням ролі комп'ютерів і Інтернету в повсякденному житті виникла необхідність захищати особисті дані. Використання біометрії замість традиційних методів забезпечить надійніший захист від несанкціонованого доступу до інформаційних систем і мереж [1].

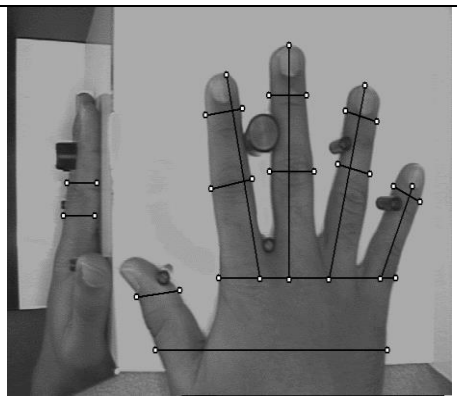
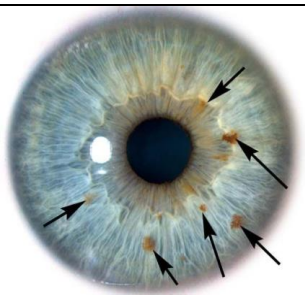
Біометрія має декілька переваг перед традиційними методами, що включають ідентифікаційні картки (маркери) або PIN-коди (паролі), а саме:

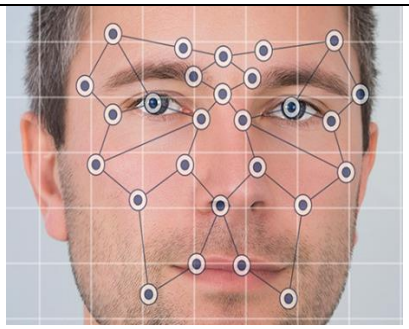
- особа, яка підлягає ідентифікації, повинна бути фізично присутньою в точці ідентифікації;
- ідентифікація на основі біометричних методів усуває необхідність запам'ятовувати пароль або носити маркер.

Біометричні ознаки зазвичай ділять на фізіологічні та поведінкові. До фізіологічних ознак відносять відбитки пальців, геометрію рук, райдужну оболонку ока, форму обличчя тощо (табл. 1). До поведінкових – динаміку натискання клавіш, ходу, почерк тощо [2].

Таблиця 1

Фізіологічні біометричні ознаки особистості

Фізіологічна ознака	Короткий коментар
	**ВІДБИТОК ПАЛЬЦЯ** **Особливість:** використання індивідуального папілярного візерунка. Забезпечується більш ніж 99% точність розпізнавання, тому метод найбільш надійний і поширений.
	**ГЕОМЕТРІЯ РУК** **Особливість:** рука кожної людини має різну форму, яка не змінюється з віком. Метод включає оцінку довжини, ширини, товщини і площі поверхні руки. За способом отримання зображення руки є контактний і безконтактний способи.
	**РАЙДУЖНА ОБОЛОНКА ОКА** **Особливість:** використання сітківки базується на тому, що структура її кровоносних судин унікальна для кожної людини. Те ж справедливо і для райдужної оболонки – кольорової області, візерунків, борозн, смуг, кілець.

	**ФОРМА ОБЛИЧЧЯ** **Особливість:** при розпізнаванні обличчя використовуються додатки, які ідентифікують або верифікують особу автоматично з цифрового зображення або відеокадру з відео джерела. Робота цих додатків спирається на порівняння певних особливостей обличь: розташування очей, носа і рота, а також відстані між ними.

При розробці біометричної системи необхідно розглянути кілька важливих питань. Всі біометричні системи працюють практично за однаковою схемою. Певна біометрична ознака користувача повинна бути зареєстрована у системі. Система запам'ятовує зразок біометричної характеристики, це називається процесом запису. Під час запису деякі біометричні системи можуть попросити зробити декілька зразків для того, щоб скласти найбільш точне описання біометричної характеристики. Потім отримана інформація обробляється і перетворюється в математичний код. Система також може попросити зробити ще деякі дії для того, щоб «приписати» біометричний зразок до певної людини. Наприклад, персональний ідентифікаційний номер (PIN) присвоюється до біометричного зразку, або смарт-карта, що містить зразок, вставляється в пристрій зчитування. В такому випадку знову робиться зразок біометричної характеристики і порівнюється з представленим [3].

Біометрична система може використовувати одну (унімодальна система) або декілька (мультимодальна) ознак. Використання кількох ознак забезпечує досягнення більш високого рівня безпеки та подолання обмежень унімодальних біометричних систем [4].

Всього в роботі біометричної системи можна виділити чотири етапи:

- запис – біометричний зразок запам'ятовується системою;
- виділення – за отриманими даними складається біометричний зразок;
- порівняння – збережений зразок порівнюється з представленим;
- збіг / розбіжність – перевірка біометричного збігу з винесенням висновку.

Залежно від ситуації, біометрична система може працювати в режимі верифікації або в режимі ідентифікації.

Верифікація порівнює скановані біометричні характеристики з раніше отриманими даними від цієї ж особи, щоб верифікувати її (чи особа та, за кого себе видає). Так як відбувається тільки одне порівняння, біометричні верифікаційні системи в цілому набагато швидше ідентифікаційних.

При ідентифікації захоплений зразок порівнюється зі всіма записами, занесеними в базу даних, на предмет збігів. Так як це вимагає порівняння з кожним існуючим записом в базі даних, то операція займає досить велику кількість часу. Ідентифікація особистості проходить успішно, якщо біометричний зразок вже є в базі даних. Біометричні ідентифікатори можна зустріти в додатках для охорони порядку або в службах правоохоронних органів (наприклад, порівняння відбитків пальців, знайдених на місці злочину, з уже наявною базою даних) [5].

Список літератури

1. «An Overview of Biometric Recognition»: https://web.archive.org/web/20120107071003/ .
2. «What are physiological biometrics?»: https://www.justaskgemalto.com/en/what-are-physiological-biometrics/.
3. «Discriminant Correlation Analysis: Real-Time Feature Level Fusion for Multimodal Biometric Recognition». Електронний ресурс: https://ieeexplore.ieee.org/document/7470527.
4. «Discriminant Correlation Analysis: Real-Time Feature Level Fusion for Multimodal Biometric Recognition»: https://ieeexplore.ieee.org/document/7470527.
5. А. Гейдарзадеган, М. Мораді, А. Турані, “Biometric recognition systems ”, 2013.

УДК 04.056.5:343.326(045)

С.В. Кавун[1], Н.С. Кавун[2]
kavun.sergii@maup.com.ua, SKavun@karazin.ua, kavun2020ks14@student.karazin.ua
[1]Харківський національний університет імені В.Н. Каразіна, Харків
[2]Міжрегіональна Академія управління персоналом (МАУП), Київ

КІБЕРТЕРОРИЗМ ТА КІБЕРБЕЗПЕКА: ОСНОВНІ АСПЕКТИ

У нинішній час найчастіше зустрічаються такі поняття, як "віртуальна реальність", "віртуальний світ", що позначає візуалізацію за допомогою програм і самого комп'ютерного інформаційного простору, всередині якого існують свого роду графічні об'єкти і символьні інформаційні місця, всередині яких працюють програми і різні інформаційні зв'язки. Тероризм – процес, з метою якого застосовується різні фізичні дії для залякування супротивника в будь-яких сферах, вони можуть бути: політичні, економічні, соціальні та ін. Також ці поняття можуть об'єднуватися. Сам термін є злиттям двох слів: "кібер" і "тероризм". Кібертероризм – це перешкода розвитку інформаційного суспільства. Основною метою є атаки на інформаційні, комп'ютерні системи, застосування насильства до цивільних осіб (рис. 1). Основні цілі кібертероризма:

- зашкодження роботоспособності електронних мереж, наведення перешкод, застосування окремих програм які перешкоджують роботі електронних мереж;
- пограбування або знищення важливої інфомарції, яка частіше являє собою статегічні або військові данні. Основними шляхами подалання системи безпеки - віруси, трояни;
- вплив на програмне забезпечення яке є джерелом багатьох многофункціональних систем. Які частіше відповідають за роботу життєво важливих систем .
- захоплення каналів телекомунікаційного мовлення що дає змогу вільно запроваджувати свої вимоги, дизаінформувати народ або вищі органи влади;
- перегруження ліній зв’язку основною метою цих дій зі сторони кібертерористів є погасення комунікації жертв на які здійснюються атаки. Повна відсутність зв’язку дає можливість спокійно виконувати всі інші дії, які були сказані вище.

Спираючись на цілі кібертерористів, виділяють 3 рівня кібертероризму:

1. **Простий** – неструктурований: використання шкідливих програм, метою яких є інформаційні системи. Найчастіше ці програми не пишуться самими кібертерористами. Пошкодження від таких атак непомітні або не значні.
2. **Розширений** – структурований: ці атаки дають можливість вести справу з багатьма системами або мережами. Часто організації володіють певною базою працівників, тому можуть визивати певний інтерес.
3. **Комплексний** – координований: у процесі атаки бере участь велика кількість осіб. Чітка координація дій призводить до масових порушень вже у глобальних об'єктах: містах, країнах і т.д. Групи осіб, що приймають участь у таких масштабних атаках, мають чіткі плани і певну структуру своїх дій.

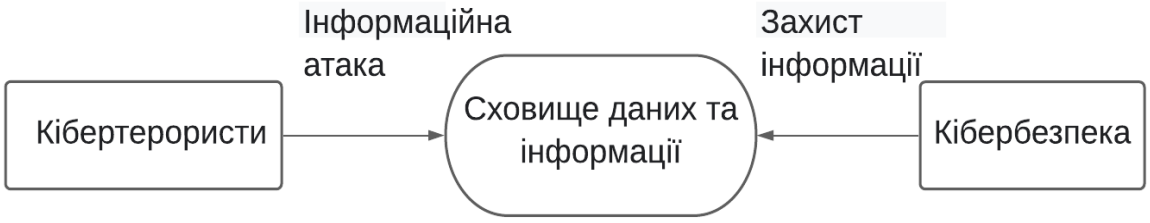


Рис. 1. Елементарна модель взаємодії Кібертероризм та Кібербезпеки

Кібербезпека – це те, що захищає нас і нашу особисту інформацію в інформаційному суспільстві, тобто в Інтернеті. Саме поняття дуже широке, являє собою захист не тільки наших особистих даних, а й захист серверів, комп'ютерів, електронних систем, мереж від шкідливих утиліт. Основною метою захисту є забезпечення цілісності даних і закриття несанкціонованого доступу. Серед множини видів захисту, виділяють основні категорії безпеки: мережева, інформаційна, операційна, безпека додатків. Це, то що допомагає нам захистити нашу інформацію і створити бар'єр для зловмисників, який не дозволить їм потрапити в нашу особисту сферу.

Інформаційна хмарна безпека. Цей тип захисту забезпечує захист даних за допомогою хмарних ресурсів і додатків, які підтримують вид захисту. **Мережева безпека.** Контролює мережевий трафік, тим самим відстежує вхідні і вихідні з'єднання. Основною метою цього захисту є перешкода поширенню і проникненню

різних загроз в мережу. **Антивіруси.** Всіма відомі програми, завданням яких є сканування комп'ютерних систем на наявність шкідливих програм. Сучасні антивіруси здатні знаходити і запобігати роботі невідомих загроз, спираючись на їх роботу і поведінку у роботі комп'ютерної системи. **Шифрування.** Процес кодування даних на наших пристроях. Даний вид захисту по-справжньому унікальний, адже під час створення шифру вся інформація стає нерозбірливою. Цей процес часто використовується для передачі секретних даних, для запобігання крадіжки інформації при її передачі.

У наш час все це є основою щодо забезпечення безпеки людини в інформаційному суспільстві, кібербезпека має сталий розвиток майже кожний день. Основними способами протидії з данною загрозою – швидке зростання розвитку науково-технічного прогрессу, тобто поннятя кібертероризм та кібербезпека є урівноваженими з усіх точок зору. Основними "ключовими" критеріями за якими розвивається кібербезпека виділяють такі:

Захищеність:

- Створення наузручнішої та найзахищеної ефективної системи управління та користування кібербезпекою.
- Оцінка кіберзагроз в момент прийннятя рішень щодо використання новітніх технологій та запровадження розпоширенню загрози , на більш маштабні етапи..
- Захист даних від взлому та керективу кібертерористів, бо у наш час данні – це найважливіше для кожної держави або людини.
- Розуміння серйозності загроз які будуть впливати на рівень безпеки. Детальна підготовка та аналіз можливих загроз.
- Розробка та застусування новітніх технологій які в подальшому будуть розробляти міцність бар'єру від нападів злоумислиників
- Тестування на проникнення та руйнування системи. Створення міцних каналів передової системи захисту.

Стійкість

- Планування відновлення систем захисту у випадку реалізації кібератак. Створення обратних шляхів щодо востоновлення даних.
- Перевірка здатності забезпечення повного захисту та відновлення пошкоджених або "слабких" місць кожної системи безпеки
- Розробка планів "швидкого реагування" при можливих атаках на різні сектори забезпечення інформаційного спокою.

Таким чином, загроза під назвою "кібертероризм " в данний час є дуже важливою і серйозною проблемою. Звичайно, в цьому страшному списку залишилося не мало країн, подібних США, але Росія і Україна в ньому займають цілком почесне третє місце. Якщо не взяти на себе ніякої відповідальності, то ці країни можуть підпалити себе будинок, привести до знищення людей і спровокувати війну. Ми докладемо всіх зусиль, щоб руйнувати провокації і робити світ більш безпечним. Актуальність цього питання буде швидко зростати, а його практичне застосування буде сильніше набирати темпи. Все це дозволяє вільно говорити проте, що вирішення проблем кібертероризма у наш час дуже важливе, та потребує швидких мір що до забеспечення інформаційної безпеки. Кожна з тих країн, які вперше зіткнуться з загрозами інформаційній безпеці, які проникли на їх територію, повинні перебувати в стані постійної готовності щодо забезпечення інформаційної безпеки, і їм слід забезпечити створення в подальшому механізмів моніторингу.

Список літератури

1. Довгань О.Д. Кібертероризм як загроза інформаційному суверенітету держави / О.Д. Довгань, В.Г. Хлань // Інформаційна безпека людини, суспільства, держави. - No3(7), 2011. - С.49-53.

2. Дубов Д.В. Кібербезпека: світові тенденції та виклики для України / Д.В. Дубов, М.А. Ожеван. - К.: НІСД, 2011. - 30 с.

3. Корченко О.Г. Кібернетична безпека держави: характерні ознаки та проблемні аспекти // О.Г. Корченко, В.Л.Бурячок, С.О.Гнатюк / Безпека інформації. - Том19, No1. - 2013. - С.40-45.

4. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект. [Підручник]. / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. – Львів: «Магнолія 2006», 2018. – 320 с.

УДК 004.81

О.К. Конопліцька-Слободенюк , Б.Є. Золотухін, О.А. Ладигіна
Ksuha80@gmail.com, b.zolotuxin@gmail.com, ladyginaoa@ukr.net
Центральноукраїнський національний технічний університет, Кропивницький

ВИДИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ОСОБИСТОСТІ

Як відомо, проблема захисту особистої інформації на сьогодні досить актуальна. Тому постає питання, як же власне захистити свої особисті дані та не бути обманутим шахраями. Я вважаю, що розв'язком цього питання слугує Біометрична ідентифікація.

Біометрична ідентифікація – це процес перевірки достовірності представленого персоною його неповторної біометричної характеристики та порівняння її з цілою базою даних. Перевірка відбувається за допомогою біометричних зчитувачів, що застосовуються для отримання людських даних. Такі системи контролю доступу досить зручні для тих, хто ними користується, оскільки інформація яку треба надати завжди з ними і не може бути втрачена чи викрадена. Такий біометричний контроль доступу визнається значно надійнішим, оскільки передача, копіювання або викрадення ідентифікаторів третіми особами унеможливлюється.

Існують статичні та динамічні біометричні способи ідентифікації особистості.

Статичні методи, що базуються на фізіологічних особливостях людини, які присутні з нею усе життя:

- ідентифікація відбитків пальців;
- ідентифікація обличчя;
- ідентифікація за райдужкою ока;
- ідентифікація геометрії рук;
- ідентифікація термограми обличчя;
- ідентифікація по ДНК;
- ідентифікація на основі акустичних характеристик вуха;
- ідентифікація за малюнком вен;

Динамічні методи базуються на поведінкових особливостях людей, а саме несвідомі рухи протягом повторення якихось дії: хода, почерк, голос:

- голосова ідентифікація;
- ідентифікація по рукописному почерку;
- ідентифікація за допомогою почерку на клавіатурі.

Також є і комбіновані заходи ідентифікації, які використовують безліч біометричних параметрів, щоб забезпечувати суворі вимоги щодо вірності та безпечності програм контролю доступу.

Проте також не треба виключати ймовірність фальсифікувати навіть біометричні дані. Підробка біометричних даних потребує певної спецпідготовки та технічної підтримки. Проте коли є можливість фальсифікувати відбиток пальця за домашніх умов, то ще не відомо про вдалу фальсифікацію райдужки ока. Адже для біометричних систем автентифікації сітківки взагалі нереально відтворити оригінал. Тому за певних обставин, можливий варіант збільшити рівень захисту системи. Збільшення рівня захисту біометричної системи контролю доступу зазвичай вдається програмними та апаратними способами. Як от технологія «живого пальця» для відбитку або аналізування природного тремтіння очей людини. Для підвищення рівня безпеки біометричний метод може бути одним із компонентів багатофакторної системи автентифікації. Включення додаткових засобів захисту до програмно-апаратного комплексу, як правило, значно збільшує його вартість. Однак для деяких методів можлива вдала автентифікація на основі стандартних компонентів: використання декількох шаблонів для ідентифікації користувачів (наприклад, множинні відбитки пальців).

Якщо ріст систем, заснованих на розпізнаванні райдужної оболонки ока, обмежений високою вартістю та низькою доступністю для споживача, то потенціал методу біометричної автентифікації, заснованої на схемі вен, очевидний. Звичайно, вибір методу біометричної ідентифікації для системи контролю доступу в першу чергу залежить від вимог до неї. Проте порівняння біометричних методів за сукупністю факторів наочно демонструє їх переваги в цілому.

УДК 621.391.1

Д.М. Палагнюк[1], О.В. Березюк[2]
brazers.d29@gmail.com
[1]студент
[2]научный руководитель
доцент кафедры безопасности жизнедеятельности и педагогики безопасности, к.т.н., доцент
Винницкий национальный технический университет, Винница

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ОСНОВНЫЕ ПРИНЦИПЫ ЕЕ ОБЕСПЕЧЕНИЯ

В новейшем обществе основной производственной силой, важнейшим стратегическим ресурсом, который обеспечивает дальнейшее его развитие, является информация. Именно поэтому информация, как и любые другие ресурсы, нуждается также в особой защите. Рядом с термином "защита информации" широко применяется термин "информационная безопасность". Защита информации характеризует процесс создания обстоятельств, которые обеспечивают нужную защищенность информации, а достигнутое состояние такого уровня защищенности отражает информационная безопасность [1, 2].

Вопрос информационной безопасности приобрел особую значимость в новейших условиях широкого использования информационных автоматизированных систем, основанных на применении компьютерных и телекоммуникационных средств [3-8]. Первые известия о несанкционированном доступе к информации связаны были, как правило, с хакерами ("электронными разбойниками"). В последнее десятилетие нарушение защиты информации растет вместе с применением программных средств, а также с помощью сети Интернет. Очень распространенной угрозой информационной безопасности также является заражение компьютерных систем с помощью компьютерных вирусов.

Следовательно, в связи с всевозрастающей значимостью информационных ресурсов в жизни новейшего общества, а также из-за вероятности многочисленных угроз с точки зрения их защищенности вопрос информационной безопасности требует большего и постоянного внимания. Системный характер влияния большой совокупности разнообразных обстоятельств на информационную безопасность, которые имеют, кроме того, разную физическую природу, вызывают различные последствия и преследуют разные цели, приводят к необходимости в системном подходе при решении данного вопроса.

Актуальность исследования заключается в увеличении и улучшении информационной безопасности и программного обеспечения.

Информационная безопасность (ИБ) представляет собой состояние уровня защищенности информационной среды, а защита информации – это деятельность, направленная на предотвращение утечки защищаемой информации, непреднамеренных и несанкционированных воздействий на защищаемую информацию, то есть процесс, направленный на достижение этого состояния [9]. Главной целью реализации ИБ любого объекта является реализация системы обеспечения информационной безопасности этого объекта.

Понимая информационную безопасность как "состояние уровня защищенности информационной среды общества, обеспечивающее ее формирование, развитие и использование в интересах организаций и граждан", правомерно установить угрозы безопасности информации, их источники, способы их реализации и цели, прочие обстоятельства и действия, нарушающие безопасность. Естественно, что при этом нужно рассматривать и меры защиты информации от преступных действий, влекущие нанесение ущерба.

Под угрозами информационной безопасности понимают возможные события или действия, которые могут вести к нарушениям ИБ. Разновидности угроз информационной безопасности достаточно разнообразны и имеют множество классификаций. По разновидности объекта влияния угрозы делятся на угрозы: собственно информации, деятельности по обеспечению информационной безопасности объекта и персонала объекта. После более детального рассмотрения угроз информации, их можно классифицировать на угрозы: носителям конфиденциальной информации, местам их расположения (размещения), системам информационного обмена (каналам передачи), а также информации, хранящейся в электронном (документированном виде на различных носителях информации.

Итак, действие угроз ИБ объекта нацелено на создание вероятных каналов утечки информации, которая подлежит защите, причин ее утечки и непосредственно на утечку этой информации.

Во время разработки необходимых средств, мер и методов, обеспечивающих защиту информации, нужно учитывать большое численность различных факторов.

Информация, как объект защиты, в принципе, может быть представлена на разнообразных технических носителях. Этими носителями также могут быть даже люди из числа обслуживающего персонала и пользователей. Информация может подлежать обработке с помощью компьютерных систем, передаваться с помощью каналов связи и отображаться различными устройствами. Она может различаться по своей значимости. Объектами, которые подлежат защите и в которых может содержаться информация, являются не только компьютеры и каналы связи, но и здания, помещения и прилегающая территория. Существенно может

разниться квалификация злоумышленников, а также используемые каналы и способы несанкционированного доступа к информации.

Примером применения защиты информации может служить защита криптоустойчивыми алгоритмами файлов с тестовыми вопросами и вариантами ответов, необходимых для проведения проверки знаний студентов путем компьютерного тестирования [10-12].

Итак, главными принципами обеспечения информационной безопасности являются следующие [13]: комплексности, открытости алгоритмов и механизмов защиты, системности, простоты применения защитных мер и средств, разумной достаточности, непрерывности защиты, гибкости управления и применения.

Все меры обеспечения безопасности компьютерных систем по способам осуществления разделяют на: морально-этические, законодательные (правовые), аппаратно-программные, физические, организационно-административные.

Итак, в новейших реалиях безопасность информационных ресурсов может быть обеспечена лишь с помощью комплексной системы защиты информации, которая должна быть: плановой, непрерывной, конкретной, целенаправленной, надежной, активной. Система защиты информации должна опираться на комплекс видов персонального обеспечения, способного осуществлять ее функционирование, как в повседневных обстоятельствах, так и в критических ситуациях.

Список литературы

1. О. В. Черевко, "Теоретичні засади поняття інформаційної безпеки та класифікація загроз системі інформаційного захисту", Ефективна економіка [Електронне наукове фахове видання], № 5, 2014. Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=3304.
2. Д. М. Палагнюк, Д. С. Тищук, та О. В. Березюк, "Принципи забезпечення інформаційної безпеки", на Наук.-практ. конф. Якість і безпека. Сучасні реалії. Матеріали, Вінниця, 2018, с. 19-22.
3. О. В. Березюк, та М. С. Лемешев, Безпека життєдіяльності: навчальний посібник. Вінниця: ВНТУ, 2011.
4. О. В. Березюк, М. С. Лемешев, І. В. Заюков, та С. В. Королевська, Безпека життєдіяльності: практикум. Вінниця: ВНТУ, 2017.
5. О. В. Поліщук, М. С. Лемешев, та О. В. Березюк, Методичні вказівки до самостійної та індивідуальної роботи з дисципліни «Цивільний захист та охорона праці в галузі архітектури та будівництва. Частина 1. Цивільний захист» для спеціальності 192 «Будівництво та цивільна інженерія». Вінниця: ВНТУ, 2017.
6. О. В. Березюк, "Проблеми при викладанні безпеки життєдіяльності в процесі підготовки фахівців радіотехнічного профілю", Педагогіка безпеки, № 2, с. 104-111, 2019.
7. О. В. Березюк, "Міжпредметні зв’язки у процесі вивчення дисциплін циклу безпеки життєдіяльності майбутніми фахівцями радіотехнічного профілю", Педагогіка безпеки: міжнародний науковий журнал, № 2, с. 21-26, 2017.
8. О. В. Березюк, "Застосування комп’ютерних технологій під час вивчення студентами дисциплін циклу безпеки життєдіяльності", Педагогіка безпеки: міжнародний науковий журнал, № 1 (1), с. 6-10, 2016.
9. С. В. Кавун, В. В. Носов, та О. В. Мажай, Інформаційна безпека: навчальний посібник, Ч.1. Харків: Вид. ХНЕУ, 2008.
10. О. В. Березюк, М. С. Лемешев, та М. А. Томчук, "Перспективи тестової комп’ютерної перевірки знань студентів із дисципліни «Безпека життєдіяльності»", на дев'ятій міжнар. наук.-метод. конф. Безпека життя і діяльності людини – освіта, наука, практика, Львів, 2010, с. 217-218.
11. О. В. Березюк, М. С. Лемешев, та І. В. Віштак, "Комп’ютерна програма для тестової перевірки рівня знань студентів", на наук.-техн. конф. студентів, магістрів та аспірантів Інформатика, управління та штучний інтелект, Харків, 2014, с. 7.
12. Л. Л. Березюк, та О. В. Березюк, "Тестова комп’ютерна перевірка знань студентів із дисципліни «Медична підготовка»", на IV Всеукр. наук.-метод. конф. Науково-методичні орієнтири професійного розвитку особистості, Вінниця, 2016, с. 96-98.
13. И. В. Аникин, В. И. Глова, Л. И. Нейман, та А. Н. Нигматуллина, Теория информационной безопасности и методология защиты информации: учебное пособие. Казань: Изд-во Казан. гос. техн. ун-та, 2008.

УДК 351:502.313

В.М. Анісімов
anisimov103@gmail.com
молодший науковий співробітник відділуприродно-техногенної та екологічної безпеки,
Державна установа «Інститут економіки природокористування
та сталого розвитку Національної академії наук України», Київ

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ТЕХНОГЕННІ Й ЕКОЛОГІЧНІ ЗАГРОЗИ В КОНТЕКСТІ СЬОГОДЕННЯ ТА ПЕРСПЕКТИВ МАЙБУТНЬОГО

Нинішня постіндустріальна інформаційна епоха своєю основною характеристикою має набуття інформацією значення основного стратегічного ресурсу суспільного розвитку, що зумовило цілий ряд істотних соціально-економічних наслідків. Одним з них є питання інформаційної безпеки, що загалом розуміється як недопущення в будь-який спосіб (включно з тим, що призводить до знищення) здійснення впливу на інформацію належну суб'єктам суспільного життя – будь-то державні чи громадські інституції, або ж окремі громадяни – без їх відома чи без дозволу.

Вказана проблема закономірно постала внаслідок розвитку електронно-цифрових технологій, які втілились у всесвітню мережу Інтернет, що являє собою систему взаємно сполучених мереж електронних програмно-керованих пристроїв для обробки інформації. Серед цих пристроїв найбільшого поширення набувають ті, які мають технічні характеристики кишенькового комп'ютера – смартфона.

Відтак виникла та нині реалізується в Україні концепція «держави в смартфоні», що передбачає переведення до всесвітньої електронної мережі процесів взаємодії органів державної влади між собою та, що є ключовим в названій концепції – з фізичними та юридичними особами. У зв'язку із цим широке коло документів, як повсякденного, так і тривалого чи навіть довічного користування, наразі все більше переводиться виключно у цифровий формат.

Загалом це виглядає надзвичайно привабливо, адже передбачає зникнення бюрократичної тяганини при отриманні адміністративних послуг окремим громадянином. Водночас об'єктивні закономірності суспільно-історичного розвитку не дають підстави вбачати при цьому виключно альтруїстичні мотивації державних інституцій по відношенню до пересічних громадян. Особливо контраверсійним видається припущення про виняткову безкорисливість дій з боку суб'єктів державної влади при впровадженні загальної діджиталізації в умовах сучасної України, державні інституції якої, як відомо, зараз є надзвичайно корумпованими. Натомість можливо вбачати у прискореній діджиталізації розширення можливостей для пов'язаного з українською владою великого бізнесу щодо входження до глобальної фінансової системи, яка нині активно формується [1].

Проте цей процес не спрямований на задоволення нагальних інтересів звичайних громадян і як будь-яка соціальна трансформація, що стосується глибинних основ життєвого устрою людей, під час свого здійснення об'єктивно стикається з так званою «проблемою QWERTY-ефекту». Безпосередньо ця проблема полягає в тому, що одного разу обране сполучення для клавіатури друкарської машинки, а зараз і комп'ютера (її перші зліва шість літер латиницею верхнього ряду клавіатури дали назву вказаному ефекту) не піддається зміні з-за консервативній позиції споживачів, незважаючи на те, що вже розроблені більш ефективніші розкладки клавіатур. А в загальному плані вона ілюструє думку про потужну силу суспільної традиції, закріпленої в моделях життєвої поведінки не одного покоління [2].

Поряд із тим у відсутності з боку громадськості безперечної підтримки здійснюваних акцій в рамках процесів діджиталізації наявний суб'єктивний чинник, що має підґрунтям саме питання інформаційної безпеки. Особливе незадоволення викликає відміна паперових офіційних особистих документів громадянина й особливо тих, які фіксують історію його працевлаштування, що є необхідним для майбутнього призначення пенсії. Адже інформацію яка міститься в цифровому вигляді можливо доволі легко змінити, або видалити на користь недоброчесного роботодавця.

Вказані моменти несприйняття тенденцій інформаційного часу також можливо розглядати як прояви певної відсталості, зашкарублості суспільної думки, що зокрема обумовлюється й значним рівнем комп'ютерної неграмотності в представників тих вікових груп, які народилися і виросли ще в докомп'ютерну епоху та допоки складають більшу частину населення нашої держави.

Разом із тим, має сенс поглянути на зазначену проблематику саме з точки зору загальних проблем інформаційної безпеки. Так, можливості функціонування електронно-цифрових пристроїв забезпечуються виключно можливостями їх безперебійного підключення до електромережі, або ж регулярної підзарядки від неї у випадку, коли ці пристрої є переносними. Стосовно цього в сучасних українських реаліях, коли електричної енергії, яка виробляється в нашій державі перестало вистачати для внутрішніх потреб, цілком реальною загрозою постає перспектива віялових відключень електроенергії побутовим споживачам.

Проте зазначена ситуація не є критичною для реалізації ідей концепції держави в смартфоні, хоча очевидно породить й певні проблеми. Але більш серйозним у вказаному контексті є те, що задля ліквідації нестачі електричної енергії в Україні, сьогодні урядовим рішенням здійснюється закупівля її значної частини за кордоном, причому в недружніх країнах, які потенційно здатні використовувати означену ситуацію на шкоду

нашій державі, створюючи протягом тривалого періоду дефіцит на українському ринку електроенергії. Відповідно, це загрожує техногенними аваріями внаслідок яких належне енергопостачання деякий час може бути відсутнє, що є несприятливим для гарантування інформаційної безпеки.

Однак відмічені потенційні техногенні загрози мають локальний характер, обмежуючись територією нашої держави й можуть бути нейтралізовані шляхом зміни державного менеджменту на більш ефективний, що надав би можливість задіяти потужності вітчизняної електроенергетики, яких цілком достатньо для забезпечення внутрішньо-українського попиту на електричну енергію.

Більш істотними є небезпеки пов'язані з глобальними екологічними змінами, які створюють численні загрози соціально-економічному розвиткові, у тому числі й щодо інформаційної безпеки, практично для кожної країни світу. Адже сьогодні антропогенний вплив на природу набув безпрецедентних у попередні історичні епохи масштабів, однак людина так і не стала її справжнім господарем, а навпаки отримала від природи нові виклики на які практично не здатна надати адекватної відповіді.

Передусім сучасні виклики природних загроз охоплюють посилення парникового ефекту під дією антропогенних викидів техногенного діоксиду вуглецю, що спричиняє відносно швидкі кліматичні зміни і передусім глобальне потепління. До багатьох наслідків цього процесу, зокрема, належать новий характер опадів і зсув меж екосистем, що порушить усталені умови аграрного виробництва та призведе до поширення інфекційних хвороб, характерних для теплого клімату. Але найбільш суттєвою загрозою є затоплення узбережжя та відтак зменшення площі суходолу внаслідок танення існуючих на планеті льодовиків з наступним підвищенням рівня Світового океану. Надалі зміни в родючості рослин, втрата нерухомості на узбережжях, де проживає значна частина людства, з наступною появою значних мас кліматичних мігрантів з постраждалих регіонів, а також зростання безробіття та дезорганізація економічного життя в цілому – це ключові економічні наслідки наявних на сьогодні екологічних загроз. Розвиткові вказаних негативних подій може запобігти єдино лише безпрецедентна міжнародна співпраця, на яку людство нині видається нездатним [3].

Отже, потенційно цілком вірогідна ситуація коли масштабні природно-кліматичні зміни загрожують на тривалий період перервати безперебійну подачу електричної енергії до всіх локацій, що відповідно не дозволятиме забезпечити належний рівень інформаційної безпеки. У цьому зв'язку видається непродуманим соціальний експеримент, що поспішно здійснюється в нашій державі, провідною рисою якого є форсований перехід на виключно безпаперовий цифровий документообіг.

Зазначений підхід у цілому видається таким, що фактично суперечить основним формам та тенденціям цивілізаційного процесу. Адже, як свідчить багатовіковий досвід техніко-технологічного розвитку людства, ніколи не існувало ситуації повної заміни всіх форм бувшого раніше технологічного способу виробництва. Особливо яскраво це виявляється в енергетиці. Так, незважаючи на те, що в нинішню епоху, коли відбувається перехід від домінуючих на сьогодні вуглеводневих видів енергетичного палива на альтернативні, чи так звані «зелені», джерела електроенергії, в енергетичному балансі суспільства у той же час зберігається велика роль кам'яного вугілля, бувшого перед тим основним серед інших енергоносіїв. Також не зникає з ужитку притаманне більш архаїчним епохам біопаливо в його різноманітних видах, яке нині навіть набуває нових якостей як альтернативне паливо.

Таким чином, можливо констатувати, що вірогідні з огляду на розвиток нинішньої ситуації у світі загрози техногенних катастроф та природних трансформацій навколишнього середовища, загрожують перебоями в забезпеченні доступу до інформаційної бази, що стосується як рівня державного управління, так і рівня кожної особистості. З огляду на це видається доцільним формулювання в якості стратегічного напряму державного управління завдання щодо створення резервних копій наявної життєво важливої та засадничої інформації на матеріально-речових носіях.

Список літератури

1. Білорус О.Г. Структурна трансформація глобального капіталу та гіперфінансіалізація відтворювальних процесів / О.Г. Білорус // Фінанси України. – 2016. – №1. – С. 7-19.

2. Бренделева Е.А. QWERTY-эффекты, институциональные ловушки с точки зрения теории трансакционных издержек / Е.А. Бренделева // Материалы Интернет-конференции «20 лет изучения QWERTY-эффектов и зависимости от предшествующего развития» (с 15.04.2005 по 5.06.2005) [Електронний ресурс]. – Режим доступу: https://iq.hse.ru/more/economics/qwerty-effecti

3. Сміл В. Енергія та історія цивілізації / Вацлав Сміл; пер. з англ. – Харків: Книжковий клуб «Клуб сімейного дозвілля», 2020. – 400 с.

УДК 004.92

Т.О Жирова, Н.О. Котенко, М.І. Чудік
zhyrova@knute.edu.ua, kotenkonj@knute.edu.ua, 121-6-16-chudik@knute.edu.ua
Київський національний торговельно-економічний університет, м. Київ

ЗАСТОСУВАННЯ ФРАКТАЛІВ У GAME DEV

Нові технології, як правило, є геніальними відкриттями, зробленими вченими у різних галузях науки. В прагненні людини до пізнання, вона намагається користуватись логікою в різних міркуваннях. Під час аналізу процесів, які є навколо, людина намагається вирахувати якийсь взаємозв'язок, намагається знайти закономірність там, де її немає і в принципі взагалі не повинно бути. Проте, навіть в хаосі все-таки є певний зв'язок між подіями, які, на перший погляд, є непов'язаними між собою. Саме цим зв'язком і виступає фрактал.

Відкриття фракталів стало відкриттям нової естетики мистецтва, науки і математики, а також революцією в людському сприйнятті світу. Вивчення фракталів і хаосу відкриває чудові можливості, як в дослідженні нескінченного числа застосунків, так і в області чистої математики. Саме тому фрактали і набули свого поширення у багатьох галузях. З'явився такий напрямок комп'ютерної графіки як фрактальний. Програмісти і фахівці в області комп'ютерної техніки захоплюються фракталами, так як фрактали нескінченної складності і краси можуть бути згенеровані простими формулами на комп'ютерах з невибагливою комплектацією.

Фрактали є важливим та нескінченним колодязем можливостей для розважальних сфер, а саме для сфери GameDev. Адже зазвичай величезна кількість часу витрачається на створення унікальних візуальних ефектів, котрі були би максимально наближенні до реальних. Фрактали же дозволяють це зробити максимально швидко. Тому у наш час багато провідних гігантів, або невеликих інді-розробників використовують фрактали у своїх проєктах. Тому розробка програми візуалізації фракталів для GameDev є актуальною темою, а метою дослідження є застосування фракталів та їх вплив на сферу GameDev.

Сьогодні у багатьох іграх, де є різні види природних ландшафтів, використовуються фрактальні алгоритми. Цей метод виявився досить ефективним. Справа в тому, що реальні природні об'єкти в основному мають фрактальну структуру. Взявши це за основу, програмісти намагалися створити комп'ютерні пейзажі на основі фрактальних алгоритмів. Досліджуючи сьогоднішнє різноманіття ігор, де можна спостерігати прекрасні природні ландшафти, можна однозначно сказати, що вони досягли успіху. Напевно, найкращим прикладом може виступити відео гра Minecraft.

Один із способів створення такого ландшафту – використання алгоритму переміщення випадкових середніх точок, в якому квадрат поділяється на чотири менших квадрати, а центральна точка вертикально зміщується на деяку випадкову величину. Даний процес повторюється на чотирьох нових квадратах поки не буде досягнуто бажаного рівня деталізації. Існує багато фрактальних процедур. Наприклад, поєднання декількох октав шуму Simplex, здатних створювати дані про місцевість, проте термін «фрактальний пейзаж» став більш загальним.

Також варто відзначити, що фрактали у сфері GameDev застосовуються і для створення об'ємних текстур. Також, ще одним із способів використання є встановлення фрактального зображення у вигляді заднього фону, або як додатковий ефект в меню. Проте, це застосовується досить не часто.

Одне із нововведень, яке принесли фрактали в сферу GameDev і зараз просувається ентузіастами програмістами є створення ігрового двигуна фрактальної фізики, який дозволяє швидко обчислювати колізії з фракталами та іншими процедурно створеними об'єктами.

GameDev − процес розробки відеоігор. Світовий ринок відеоігор 2019 року, за даними спеціалізованої аналітичної компанії Newzoo, оцінюється в 148,1 млрд доларів.

Перші відеоігри, розроблені в 1960-х роках, були некомерційними і не були доступні широкій публіці. Комерційний розвиток відеоігор почався в 70-х роках минулого століття з появою першого покоління ігрових консолей і ранніх домашніх комп'ютерів, таких як Apple I. У той час, завдяки низьким витратам і малим можливостям комп'ютерів, один програміст міг розробити повноцінну і повну гру. Однак в кінці 80-х і 90-х, постійно зростаюча потужність комп'ютерної обробки та посилення очікувань від геймерів ускладнювали створення відеоігор.

Ігрова індустрія, як і будь-які інформаційні технології, вимагає інновацій, оскільки видавці не можуть отримати прибуток від постійного випуску повторюваних сіквелів та наслідувань. Щороку з'являються нові незалежні компанії і деякі з них примудряються створювати хіти. Середній бюджет необхідний для створення крос платформної гри становить від 18 до 28 млн. Дол. США , а деякі надто гучні ігри часто перевищують 40 млн. дол.

Щоб приступити до написання програми з реалізації фракталів, необхідно створити консольний проект у Visual Studio 2019. Наступним кроком, після того як шаблон проекту було створено, необхідно підключити графічну бібліотеку SDL2.0.

Для створення вікна, у якому надалі буде відображатись фрактал необхідно використати наступні команди:

- SDL_Init(SDL_INIT_EVERYTING) — для ініціалізації всіх підсистем бібліотеки SDL;

– SDL_CreateWindow() — створює вікно із заданою назвою, розмірами, та розташуванням екрані;

– SDL_GetWindowSurface() — створює масив пікселів розміром x*y, який потім буде використовуватись для передачі зображення.

Для створення множини Мандельброта потрібно вибрати складну площину (C). Комплексне число, відповідне їй, має вигляд C=a+b*i . Після обчислення значення попереднього виразу: Z_1=Z_0^2+C. Використовуючи нуль, як значення, отримуємо C як результат. Наступний крок складається з присвоєння результату та повторення обчислення: тепер результат − це комплексне число. Тоді слід присвоїти значення і повторити процес знову і знову.

Цей процес можна представити як «міграцію» початкової точки C по площині. Що відбувається з моментом, коли повторно повторюється функція. Чи залишиться він поблизу від походження, чи відійде від нього, збільшуючи віддалення від походження без обмежень? У першому випадку говоримо, що C належить до множини Мандельброта, в іншому випадку говоримо, що це йде до нескінченності і присвоюємо колір C залежно від швидкості, з якою точка «втече» від початку.

Можна поглянути на алгоритм з іншої точки зору. Уявімо, що всі точки на площині притягуються обома: нескінченністю та множиною Мандельброта. Це дозволяє зрозуміти, чому:

– точки, далекі від набору Мандельброта, швидко рухаються до нескінченності,

– точки, близькі до набору Мандельброта, повільно виходять у нескінченність,

– точки всередині набору Мандельброта ніколи не виходять у нескінченність.

Програмним чином за допомогою коду даний фрактал реалізується наступним чином. Для кожного пікселя вікна виконується наступний код:

```
void    mandelbrot(t_f* f)
{
    f->draw.cre = f->x * 1.0 / f->draw.zoom + f->draw.movex - 0.5;
    f->draw.cim = f->y * 1.0 / f->draw.zoom + f->draw.movey;
    f->draw.newim = 0;
    f->draw.newre = 0;
    f->draw.oldre = 0;
    f->draw.oldim = 0;
    f->i = -1;
    while (++f->i < f->draw.maxiterations)
    {
        f->draw.oldre = f->draw.newre;
        f->draw.oldim = f->draw.newim;
        f->draw.newre = f->draw.oldre * f->draw.oldre - f->draw.oldim *
            f->draw.oldim + f->draw.cre;
        f->draw.newim = 2 * f->draw.oldre * f->draw.oldim + f->draw.cim;
        if ((f->draw.newre * f->draw.newre + f->draw.newim * f->draw.newim) > 4)
            break;
    }
    (f->i == f->draw.maxiterations) ? put_pixel_in_img(f, f->i * f->i * f->i * f->color) : put_pixel_in_img(f, f->i * f->i * f->i * f->color);
}
```

Рис. 1. Код для множини Мандельброта

Функція put_pixel_in_img() використовується для розміщення пекселя певного кольору за координатами x та y.

Щоб побачити результат виконання програми необхідно запустити цикл, який буде залишати вікно програми видимим. У цьому циклі, для оновлення інформації у вікні необхідно використовувати SDL_UpdateWindowSurfase(), опісля для відстеження різних подій, таких як рух мишки або натискання клавіші використовується SDL_PollEvent(). Якщо користувач робить якусь дію у програмі необхідно очистити інформацію на вікні за допомогою SDL_FillRect() та розпочати обробку дії користувача.

У зв’язку з тим, що папороть Барнслі належить до іншого типу фракталів ніж Мандельброт, її побудова відрізняється. У теорії папороть Барнслі може бути побудована вручну за допомогою ручки та паперу з графіком, але так як кількість необхідних ітерацій переходить у десятки тисяч, використання комп’ютера є практично обов’язковим. Багато сучасних комп’ютерних моделей папороті Барнслі популярні у сучасних математиків. Поки математика буде запрограмована правильно, використовуючи матрицю констант Барнслі, вийде така ж форма як і у папороті.

Отже, фрактали вносять чи не найбільший вклад саме у розвиток комп’ютерної графіки, завдяки чому вони змогли набули широкого застосування у сфері GameDev, де їх, зазвичай, використовують для створення текстур, фонових зображень, анімації, моделей природнього оточення (дерева, природні ландшафти, хмари) і т.д. Також є спроби створити ігровий двигун на основі фракталів, що може в майбутньому теоретично зменшити розмір ігрових програм та створювати відкритий світ із неодноманітним оточенням.

УДК 004.087

О.К. Конопліцька-Слободенюк, Т.В. Селіванов, В.В. Буза
Ksuha80@gmail.com, seluv.taras@gmail.com, vitalyhernandez14@gmail.com
Центральноукраїнський національний технічний університет, Кропивницький

КІБЕРТЕРОРИЗМ ТА ЙОГО НАСЛІДКИ У ВІРТУАЛЬНОМУ ПРОСТОРІ

Технологічний прогрес, свідками якого ми є, часто називають новою інформаційною революцією. Інформатизація всіх сфер життя суспільства дає колосальні можливості для розвитку економіки, фінансової сфери, поліпшення соціального забезпечення, освіти, медицини, проведення фундаментальних і прикладних наукових досліджень на всіх напрямках. В результаті багато сфер життя суспільства «переміщуються» в інформаційне середовище. Результати розвитку технічного прогресу дуже часто використовують для скоєння злочинів. Впровадження в інформаційну сферу відповідних програм й їх використання злочинними елементами породило явище, що називають кібертероризмом. Існує навіть думка, що при переході через критичні точки прогресу у сфері кіберзлочинів, злочинці почнуть працювати вже на знищення людства.

Термін «кібертероризм» утворюється злиттям двох понять: «Cyber» - злочинність та «Terrorism» - небезпечна діяльність. Виходячи з поняття про тероризм та його наслідки і його поєднання з незаконними діями у віртуальному просторі, можна створити такого роду визначення: кібертероризм – комплекс незаконних дій в кіберпросторі, які створюють загрозу державній безпеці, особистості людини та приносять шкоду суспільству. Основний момент тактики такого виду тероризму полягає в тому, щоб злочин мав доволі небезпечні, а інколи й критичні наслідки та став відомий населенню, і створював атмосферу загрози повторення акту без сповіщення про конкретний об'єкт.

Сучасні терористи активно використовують можливості Інтернету: легкий доступ в мережу, практично повна відсутність цензури, великий масштаб аудиторії, анонімність і т.п. У наші дні вони розглядають глобальну мережу головним чином як засіб пропаганди та передачі інформації. Так, наприклад, одна з найвідоміших терористичних організацій «Аль-Каїда» у 2011 році запустила онлайн-журнал для пропаганди своєї діяльності англійською мовою.

До основних завдань тероризму в кіберпросторі слід віднести спроби перешкоджання або руйнування процесу функціонування комп'ютерних систем або мереж інформаційної інфраструктури держави або органів управління. Подібні злочинні дії щодо критично важливих об'єктів інформаційної інфраструктури є значною загрозою, яка може мати найсерйозніші наслідки для всього суспільства. Серед основних видів кіберзлочинів в Україні найчастіше відбувається такі види злочину:

Фішинг — це вивідування інформації у довірливих громадян для доступу до банківських рахунків. Поширений в державах, де популярні послуги інтернет-банкінгу. Фішинг є методом мережевого шахрайства. С його допомогою зловмисники намагаються виманити у людини конфіденційні дані або змусити його на будь-які небажані дії. З цією метою шахраї використовують миттєві повідомлення та електронні листи, спеціально створені підроблені веб-сайти. Головне завдання фішерів - отримати паролі та логіни для фінансових сервісів (онлайн банків, систем електронних грошей) або обманом змусити жертву заплатити їм гроші. Зайшовши на підроблений сайт, користувач вводить у відповідні рядки свій логін і пароль, а далі аферисти отримують доступ в кращому випадку до його поштової скриньки, в гіршому — до електронного рахунку. Але не всі Фішери самі переводять у готівку рахунки жертв. Справа в тому, що переведення в готівку рахунків складно здійснити практично, до того ж людину, яка займається переведенням в готівку, легше засікти і залучити шахраїв до відповідальності. Тому, добувши персональні дані, деякі Фішери продають їх іншим шахраям, у яких, у свою чергу, є відпрацьовані схеми зняття грошей з рахунків.

DDos-атака – атака, яка використовується для виведення з роботи і злому обчислювальної техніки і створення технічних і економічних труднощів. Здійснюється за допомогою створення великої кількості запитів і серйозного навантаження на техніку, найчастіше на великі сервера. Популярність DDos -атак обумовлена тим, що визначити виконавця вкрай складно – він створює велике навантаження через безліч комп'ютерів в мережі. Найчастіше такі атаки використовуються тоді, коли зламати систему або сервер не виходить. Навіть якщо за допомогою DoS-атаки не вдається отримати доступ, техніка виходить з ладу або втрачає продуктивність. Жертвами таких атак найчастіше стають урядові сайти, великі портали, онлайн-ЗМІ, сервери онлайн-ігор, інтернет-магазини, корпоративні сайти фінансового сектора. Мотивація атакуючого також залежить від сфери. Найчастіше атака відбувається з причин політичних протестів, недобросовісної конкуренції, вимагань і шантажу, особистої неприязні, а також з метою розваги.

Підводячи підсумок розгляду кібертероризму, слід зазначити, що вчинення високотехнологічних терористичних акцій в XXI ст. здатне викликати глобальну інформаційну кризу і поставити під загрозу існування окремих регіонів світу. Ситуація ускладнюється тим, що кримінально-правова протидія кібертероризму в Україні поки не в належній мірі відповідає серйозності такої загрози. У зв'язку з цим вдосконалення кримінально-правової політики у сфері протидії вчиненню кібератак терористами повинно стати одним з пріоритетних її напрямків.

УДК 004.415.532.3

Б.С. Федоров, В.А. Резніченко
fedorov.bot@911@gmail.com
Центральноукраїнський національний технічний університет, Кропивницький

ЗАГАЛЬНІ ОСОБЛИВОСТІ ВИКОРИСТАННЯ МЕТОДОЛОГІЇ ТЕСТУВАННЯ «БІЛИЙ ЯЩИК» ДЛЯ АУДИТУ ІТ ІНФРАСТРУКТУРИ

На сьогоднішній день кількість кіберзагроз в мережі постійно зростає. Це обумовлене тим, що в сфері інформаційної безпеки постійно йде так звана "гонка озброєнь" в якій хакери та спеціалісти з інформаційної безпеки використовують нові вразливості та засоби їх усунення. Для виявлення загроз існує 7 типів тестування безпеки згідно з керівництвом по методології Open Source Security Testing: сканування вразливостей, сканування безпеки, тест на проникнення, оцінка ризиків, аудит безпеки, етичний злом. Для тестування вразливостей можуть використовуватися декілька різних методологій, таких як: «Білий ящик», «Чорний ящик» та «Сірий ящик». Всі вони мають свої недоліки та переваги виходячи зі своїх особливостей. При тестуванні за допомогою методології «Чорний ящик» ми не знаємо нічого про цільову ІТ інфраструктуру. А при тестуванні за допомогою методології «Білий ящик» ми навпаки знаємо внутрішню будову цільової ІТ інфраструктури. Методологія «Сірий ящик» використовує водночас і методи білого і методи чорного ящика.

Метою даної роботи є дослідження загальних особливостей використання методології «Білий ящик», доцільності та сфери її використання.

Методологія «Білий ящик» використовується при проведенні внутрішнього тестування безпеки. Тестувальник отримує від замовника потрібну інформацію про систему, наприклад, права адміністратора мережі і доступ до файлів конфігурації. Методологія «Білий ящик» дозволяє ретельніше дослідити інформаційний захист об'єкта тесту.

Загальна схема процесу тестування методологією «Білий ящик» виглядає наступним чином:

1. Виконання аналізу ризиків, щоб спрямувати весь процес тестування.
2. Розробка стратегії тестування, яка визначає, які дії з тестування необхідні для досягнення цілей тестування.
3. Розробка детального плану тестування, який організовує подальший процес тестування.
4. Підготовка тестового середовища для виконання тесту.
5. Виконання тестових прикладів і повідомлення результатів.
6. Підготовка звіту.

Для тестування «Білий ящик» необхідно знати, що робить програмне забезпечення безпечним або небезпечним, як думати як зловмисник і як використовувати різні інструменти і методи тестування. Першим кроком в тестуванні методом білого ящика є розуміння і аналіз доступної проектної документації, вихідного коду та інших відповідних артефактів розробки, тому знання того, що робить програмне забезпечення безпечним, є фундаментальним вимогою. По-друге, щоб створити тести, які використовують програмне забезпечення, тестувальник повинен мислити як зловмисник. По-третє, для ефективного проведення тестування тестувальникам необхідно знати різні інструменти і методи, доступні для тестування методом білого ящика. Ці три вимоги працюють не ізольовано, а разом.

Використання даної методології в сфері інформаційної безпеки є досить суперечливим рішенням. З одного боку вона дає змогу отримати більш розгорнуті та точні результати тестування. Але це досягається за рахунок перевірки взаємодій та поведінки всіх внутрішніх компоненті, що є досить затратним по ресурсам, часу та кваліфікації тестувальника. Також вона мало походить на реальну хакерську атаку. Тобто при всіх відомих даних не розглядаються усі відомі засоби їх отримання, а також не розробляються нові. А це означає що ігнорується досить значна область інформаційної безпеки: захист доступу до даних(програмний або за допомогою соціальної інженерії).

У типовому випадку для пошуку вразливих областей використовується аналіз методології «Білий ящик», а потім використовується тестування методології «Чорний ящик» для розробки робочих атак на ці області. Використання методології «Сірий ящик» ефективно поєднує в собі методи тестування «Білий ящик» і «Чорний ящик».

Висновки. Тестування безпеки методологією «Білий ящик» корисне та ефективне. Така методологія повинна слідувати підходу, заснованому на оцінці ризику, щоб збалансувати зусилля по тестуванню з наслідками збою програмного забезпечення. Аналіз ризиків на рівні архітектури та дизайну забезпечує правильний контекст для планування і проведення за допомогою методології «Білий ящик». Тестування методологією «Білий ящик» можна використовувати з тестуванням методологією «Чорний ящик» для підвищення загальної ефективності тестування. Такий підхід виявляє помилки проектування, програмування і реалізації.

УДК 004.056

В.В. Сергатий, О.К. Конопліцька-Слободенюк
sergatyijvlad1999@gmail.com, ksuha80@gmail.com
Центральноукраїнський національний технічний університет, Кропивницький

СТРАТЕГІЇ, ПОВ'ЯЗАНІ ІЗ ЗАБЕЗПЕЧЕННЯМ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОЇ БЕЗПЕКИ

В сучасному суспільстві інформація є справжньою зброєю. Поняття безпеки в світі гібридних війн стає вкрай важливим. Безпека – це стан в якому особа відчуває себе в захищеності від зовнішніх та внутрішніх факторів. Забезпечення безпеки своїх громадян - є пряма функція держави, та керівників суспільства в цілому. Аналізуючи зміст терміна “безпека”, дослідники доходять висновку, що у суспільній свідомості це поняття ототожнюється не стільки з “відсутністю загроз”, як зі станом, почуттями та переживаннями людей.

Сучасні дослідження показали, що в сучасному світі все більшу увагу привертає зв'язок між почуттям добробуту та почуттям безпеки. Проте слід зазначити, що існує тенденція інтерпретувати поняття безпеки обмежено як захист від шкоди та задоволення основних потреб. Іншими словами, ідея про те, що психологічне благополуччя та безпека є взаємодоповнюючими та взаємообумовленими поняттями, досі не розглядалася.

На сьогоднішній день у нашій країні актуальна необхідність у розробці концепції інформаційно-психологічного захисту, яка висвітлює гармонійну інтеграцію інтересів особистості та соціальних і державних інтересів. Інформаційна безпека полягає у захисті інформації та інформаційних систем від несанкціонованого доступу, використання, розкриття, порушення, модифікації або знищення з метою забезпечення конфіденційності, цілісності та доступності.

Стратегії, пов'язані із забезпеченням безпеки, спрямовані на виявлення та запобігання загрозам. Призначення безпеки можна трактувати по-різному:

- Захист людського життя.
- Захист людей від існуючих загроз.
- Забезпечення життєво важливих прав і свобод для всіх людей.

Вищезазначені підходи демонструють, що безпека людини швидше за все буде результатом ефективного політичного, економічного, соціального, культурного та природного середовища, ніж виконання ряду міністерських директив. Але це лише одна сторона "медалі". З іншого боку, безпека суспільства є побічним продуктом відчуття захищеності його членів.

Ідею безпеки можна легше застосувати до речей, ніж до людей. Оскільки матеріальні цінності часто можна замінити, їх безпеку можна підвищити за допомогою страхування збитків. Те, що включає безпеку людей, неможливо визначити так легко. Фактори, що впливають на їх безпеку - життя, здоров'я, статус, багатство, свобода - є більш складними, і багато з них не можуть бути замінені у разі їх втрати. Ось чому запорукою добробуту людей є зміцнення їх психологічної безпеки.

Варто згадати, що психологічна безпека значною мірою відноситься до гіпотетичних конструкцій, які важко виміряти. Ми не можемо побачити "невпевненість", крім випадків, коли люди самі про це говорять. Крім того, слід зазначити, що створення психологічної безпеки - це складний і трудомісткий процес, і тоді він може бути знищений одним неправильним кроком. Психологічна безпека охоплює когнітивні та емоційні конструкції, що дозволяють трактувати безпеку як психологічне явище зі стандартною структурою. Отже, безпеку можна описати як стан внутрішнього спокою, впевненості, позитивного ставлення, довіри, суб’єктивного благополуччя, відкритості та розслабленості.

Безпека та психологічне благополуччя - це поняття, що включають безліч факторів, і першим із них є суб'єктивність. Ці поняття належать до тих конструкцій, які, як і інші переконання та почуття, закладені в свідомості людини. Це означає, що окремі люди або члени групи (наприклад, етнічні групи та національні представники) сприймають безпеку та добробут через приціл свого особистого досвіду або з точки зору своєї групи та її систем. Отже, безпека та добробут - це психологічний досвід, який, у більшості випадків, можна виміряти, ставлячи під сумнів, чи почуваються люди в безпеці / невпевненості, збалансованості / неврівноваженості тощо. Тут ми можемо мати справу лише з суб’єктивними оцінками тих, кого оцінюють.

"Суб'єктивне" - це те, що люди відчувають. Суб'єктивний фактор включає як когнітивний, так і емоційний аспекти. Взаємозв'язки між когнітивною та емоційною складовими безпеки свідчать про те, що на рівні пізнання задоволення супроводжується почуттям внутрішньої безтурботності.

Отже, для визначення інформаційно-психологічної безпеки використовуються два підходи. Перший - це і стан захищеного інформаційного середовища, і стан захищених соціальних об’єктів, що відображає різні сторони цього витонченого політичного уявлення. У широкому розумінні реалізація інформаційно-психологічної безпеки соціальних суб'єктів визначається параметрами функціонування інформаційного середовища. Суспільні суб'єкти беруть участь у регулюванні та складанні інформаційного середовища.

УДК 004.056

Є.О. Кузьменко, В.А. Резніченко
deathbreath33@gmail.com
Центральноукраїнський національний технічний університет, Кропивницький

ЗАГАЛЬНІ ОСОБЛИВОСТІ СТВОРЕННЯ DMZ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ REVERSE ACCESS

На сьогоднішній день кількість кіберзагроз в мережі постійно зростає. Також майже в будь якій локальній мережі настає необхідність взаємодії з інтернетом. Особливо у випадку робочих мереж чи серверів на яких піднято певні сервіси з якими мають віддалено працювати клієнти. Існує декілька різних способів організації безпечної взаємодії локальної мережі та інтернету. Одним з таких способів є створення так званої DMZ.

Метою даної роботи є дослідження загальних особливостей використання DMZ та технології Reverse Access, а також реалізації DMZ за допомогою даної технології .

DMZ (англ. Demilitarized Zone) це сегмент мережі, що містить загальнодоступні сервіси та відокремлює їх від приватних. Його метою є обмеження доступу до внутрішніх даних мережі в разі зараження або несанкціонованого доступу. Це досягається за допомогою розділення мережі на сегменти та контролю трафіку між ними за допомогою одного або декількох міжмережевих екранів.

Існує безліч різних варіантів архітектури мережі з DMZ. Два основних — з одним міжмережевим екраном і з двома міжмережевими екранами. На базі цих методів можна створювати як спрощені, так і дуже складні конфігурації, відповідні до можливостей використовуваного обладнання та вимог до безпеки в конкретній мережі.

Правила фільтрації міжмережевих екранів виглядають наступним чином:

1. З внутрішньої мережі можна ініціювати з'єднання в DMZ і в WAN (Wide Area Network).
2. З DMZ можна ініціювати з'єднання в WAN.
3. З WAN можна ініціювати з'єднання в DMZ.

Ініціація з'єднань з WAN і DMZ до внутрішньої мережі заборонена.

Для створення мережі з DMZ може бути використаний один міжмережевий екран, який має мінімум три мережеві інтерфейси: один — для з'єднання з провайдером (WAN), другий — із внутрішньою мережею (LAN), третій — з DMZ. Така схема проста в реалізації, однак має підвищені вимоги до обладнання й адміністрування: міжмережевий екран повинен обробляти весь трафік, що йде як у DMZ, так і у внутрішню мережу. При цьому він стає «єдиною точкою відмови», а у випадку його зламу (чи помилки в налаштуваннях) внутрішня мережа виявиться вразливою безпосередньо з зовнішньої.

Безпечнішим є підхід, коли для створення DMZ використовуються два міжмережеві екрани: один із них контролює з'єднання із зовнішньої мережі в DMZ, інший — із DMZ у внутрішню мережу. У такому разі для успішної атаки на внутрішні ресурси повинні бути скомпрометовані два пристрої. Крім того, на зовнішньому екрані можна налаштувати повільніші правила фільтрації на прикладному рівні, забезпечивши посилений захист локальної мережі без негативного впливу на продуктивність внутрішнього сегмента.

Одним із підходів в організації DMZ є використання технології Reverse Access. Мережа комп’ютера може мати багато рівнів захисту(маршрутизатор NAT або брандмауери чи фаерволи) які блокують можливість створення вхідного з’єднання до комп’ютера. Міжмережевий екран зазвичай блокує відкриття портів, проте не чіпає вихідний мережевий трафік. В звичайному з'єднанні а клієнт з'єднується з сервером крізь відчинений порт сервера, але у випадку зворотнього з'єднання, клієнт відкриває порт, із яким з'єднується сервер. Зворотне з'єднання використовується головним чином для обходу обмежень фаєрволів і маршрутизаторів. Сервер прослуховує мережевий порт на локальному комп'ютері. Якщо він виявляє запит до цього порту то він ретранслює цей запит на з'єднання назад собі за встановленим з'єднанням. Це забезпечує нове з'єднання від локального комп'ютера до серверу.

Ця взаємодія дозволяє нам створити з’єднання з сервером через порт чи інший проміжний сервер, що в купі з використанням міжмережевого екрану й дозволяє нам створити DMZ за допомогою технології Reverse Access.

Висновки. Використання DMZ дозволяє підняти рівень безпеки мережі та запобігти несанкціонованому доступу до системи. А технологія Reverse Access дозволяє створити безпечне з’єднання від серверу до клієнта навіть за умови високого рівня захисту серверу що не дозволяє або ускладнює створення вхідного з’єднання.

УДК 004.6

В.А. Резніченко, Ю.С. Шовкопляс
yshovkopluas@gmail.com
Центральноукраїнський національний технічний університет, Кропивницький, Україна

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

Законом України від 6 липня 2010 року Україна ратифікувала Конвенцію Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних та. Додатковий протокол до неї. Цим самим Україна взяла на себе зобов'язання забезпечити дотримання прав і свобод людини, зокрема, права на недоторканність приватного життя, передбаченого статтею 8 Конвенції про захист прав людини і основоположних свобод та гарантованого статтею 32 Конституції України.

Цей Закон регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних.

Цей Закон поширюється на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів, а також на обробку персональних даних, що містяться у картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів.

персональні дані - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована;

розпорядник персональних даних - фізична чи юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця;

Для запровадження реальних механізмів реалізації взятого на себе зобов'язання Верховною Радою України ухвалено Закон України «Про захист персональних даних», який набув чинності 1 січня 2011 року і став основоположним актом національного законодавства у сфері захисту персональних даних.

Враховуючи досвід функціонування системи захисту персональних даних в Україні, 3 липня 2013 року Верховна Рада України прийняла Закон України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних», який набув чинності 1 січня 2014 року.

Цим Законом з метою забезпечення незалежності уповноваженого органу з питань захисту персональних даних, як того вимагає Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних, повноваження щодо контролю за додержанням законодавства про захист персональних даних покладено на Уповноваженого Верховної Ради України з прав людини (далі – Уповноважений).

Згідно із статтею 23 Закону України «Про захист персональних даних» у сфері захисту персональних даних Уповноважений має такі повноваження:

Уповноважений Верховної Ради України з прав людини також має включати до своєї щорічної доповіді про стан додержання та захисту прав і свобод людини і громадянина в Україні звіт про стан додержання законодавства у сфері захисту персональних даних.

Список літератури

1. Захист персональних даних [Електронний ресурс] – Режим доступу до ресурсу: https://www.ombudsman.gov.ua/ru/page/zpd/.

2. ЗАКОН УКРАЇНИ Про захист персональних даних [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

УДК 004.71, 004.77

О.М. Дрєєв, О.О. Майданик
drey_sanya@ukr.net, sanyamaidanyk@gmail.com
Центральноукраїнський національний технічний університет, Кропивницький

ФОРМУВАННЯ ВИМОГ ДО АПАРАТНОЇ БАЗИ З ВРАХУВАННЯМ ВИМОГ БЕЗПЕКИ ДЛЯ СИСТЕМ IOT

На етапі проектування системи пристроїв IoT (Internet of Things – Інтернет речей) встановлюються вимоги що до універсальності, безпеки та надійності роботи та зв'язку з метою забезпечення якісного викладання у вищих начальних закладах, бо для пов'язання виконання низки лабораторних робіт в пріоритеті є використання загальної апаратної бази з можливістю використати єдину мову програмування. Відповідно до пунктів, варіант класифікації вимог показано в наступній таблиці:

Таблиця

Вимоги до функціональності модульної одиниці системи розумного дому та методи їх досягнення

№ п/п	Характеристики системи	Вимога	Методи їх реалізації
1	Захищений канал бездротового зв'язку з протоколом організації мережі	Достатня швидкодія	Обрати мікроконтролер у якого обчислювальна потужність для підтримки мережевого протоколу з шифруванням
2		Можливість автоматичного підключення	Використання WPS, або більш захищені альтернативи
3	Протокол обміну інформацією між пристроями із захистом від несанкціонованого доступу	Достатня швидкодія	Обрати мікроконтролер у якого обчислювальна потужність для шифрування/дешифрування інформації, або є апаратна підтримка криптографії
4		Можливість автоматичного підключення	Використання протоколів які здатні забезпечити автоматичну реєстрацію приладу в системі за командою оператора
5	Захист від реверс-інжинірингу	Захищеність системи від зчитування встановленого програмного забезпечення	Використана апаратна база повинна блокувати зчитування коду апаратними засобами, можливе використання обфускації
6		Захищеність використаних протоколів від криптоаналізу	Протоколи обміну інформацією повинні забезпечувати можливість використання захищених каналів по типу SSH
7	Відкритість протоколів та технологій для розробки та впровадження нових пристроїв	Сумісність з підключенням до Internet	Пристрій повинен мати апаратний модуль бездротового зв'язку WiFi.
8		Підтримка універсальних протоколів керування	Використані протоколи повинні мати відкриту документацію.
9		Забезпечення вимог захищеності разом з відкритістю	В процесі формування мережі IoT повинні потрібно передбачити захищену процедуру реєстрації нового пристрою

В результаті аналізу вимог, за критеріями, які вказані в таблиці, обрано базові пристрої на основі програмованих модулів ESP32. Зокрема ESP32-WROOM. Можливості обраного пристрою показано в [1], звідки є очевидним відповідність розглянутого пристрою поставленим вимогам.

В результаті дослідження отримано обґрунтування вибору апаратної бази для створення мережевої системи Інтеренет-речей, з врахуванням вимог цифрової безпеки що до обміну інформацією пристроями, які входять до системи розумного будинку. Обраний пристрій є придатним до виконання зв'язки розроблених лабораторних робіт з використанням еволюційного розвитку пристрою, який розробляється, від початку курсу до його завершення.

Список літератури

1. ESP32 Series Datasheet // URL: https://www.espressif.com/sites/default/files/documentation/esp32_datasheet_en.pdf

2. Stephen Cobb (2016-10-24). 10 things to know about the October 21 IoT DDoS attacks // URL: https://www.welivesecurity.com/2016/10/24/10-things-know-october-21-iot-ddos-attacks/

3. Захист Інтернету речей // URL: https://www.avast.ua/technology/iot-security

УДК 338.242(477)

Х.О. Мандзіновська
k.mandzinovska@gmail.com
Українська академія друкарства, Львів

РОЛЬ ТА ЗНАЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ПАНДЕМІЇ

Світову економіку та парадигму соціально-економічного розвитку кожної країни різко змінили масштаби та вплив пандемії COVID-19. Вірусна небезпека виступила своєрідним краш-тестом на надійність та ефективність не лише системи охорони здоров'я більшості країн світу, а й перевірила здатність органів державної влади, місцевого самоврядування, економіки та бізнесу протистояти таким вагомим викликам та загрозам.

Слід зазначити, що пандемія COVID-19 активізувала процеси цифровізації, зокрема глобальна ізоляція населення за місцем проживання зумовила більш глибоке занурення у віртуальний кіберпростір, в якому люди більше зазнають впливу інформаційного цунамі.

Згідно з дослідженнями експертів міжнародних компаній WeAreSocial і Hootsuitена поочаток 2021 року 4,66 мільярда людей у всьому світі користуються інтернетом, що на 316 мільйонів (7,3 %) більше, ніж у минулому році. В Україні кількість інтернет-користувачів збільшується з року в рік, на початок 2021 року їх кількість зросла на 2,0 мільйона (+ 7,3%) відносно попереднього року [1].

З огляду на вищезазначене, справедливо сказати, що дослідження впливу пандемії COVID-19 не може бути обмеженим лише у галузі медицини. Занурення суспільства у період вірусної небезпеки в кіберпростір ставить виклики системі національної безпеки та потребує радикальних змін у стратегічних векторах. У цьому аспекті пріоритетом є забезпечення високого рівня інформаційної безпеки держави. Отже, необхідність вивчення сутності, ролі та значення інформаційної безпеки в умовах пандемії незаперечна.

В умовах сьогодення для кожного окремого громадянина, суспільства та держави в цілому набуває стратегічного значення забезпечення інформаційної безпеки.

Про важливість захисту інформаційної безпеки наголошується в Конституції України: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу» (ст. 17) [2]

У контексті нашого наукового дослідження необхідно звернути увагу на законодавче визначення інформаційної безпеки, яке зафіксоване в Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 рр.» та трактується як – стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається нанесення шкоди через: неповноту, невчасність і невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» (п. 13 Закону) [3].

Інформаційній безпеці сьогодні приділяється значна увага як науковців, так і держави. Аналіз теоретичних напрацювань фахівців убезпековій сфері дають можливість систематизувати основні концептуальні наукові підходи до визначення сутності інформаційної безпеки:

1)інформаційна безпека як складова національної безпеки;

2)інформаційна безпека як стан захищеності інформаційного середовища та національних інтересів від можливих загроз;

3)інформаційна безпека як стан системи, який здатний забезпечити цільові параметри безпеки.

Необхідно наголосити, що рользабезпечення інформаційної безпеки держави зумовлюється, по-перше, потребою забезпечення національної безпеки України в цілому, по-друге, існуванням таких загроз інформаційній сфері країни, які можуть завдавати значної шкоди загальним національним інтересам, по-третє, врахуванням того, що за допомогою інформації можна впливати на зміну свідомості і поведінку людей. Щодо завдання інформаційної безпеки то воно полягає у створенні системи протидії інформаційним загрозам та захисту власного інформаційного простору, інформаційної інфраструктури, інформаційних ресурсів держави.

Отже, характер подальшого наукового дослідження інформаційної безпеки буде зосереджений на викликах та загрозах, що виникли в результаті вірусної небезпеки.

Поняття загрози інформаційній безпеці слід трактувати, як наявні та потенційно можливі явища і чинники, які створюють небезпеку життєво важливим інтересам людини і громадянина, суспільства і держави в інформаційній сфері.

Ключовими загрозами інформаційній безпеці в період пандемії є дезінформація та кіберзлочинність.

Дезінформація завдяки сучасним інформаційним технологіям поширюється надзвичайно швидко і в умовах пандемії має суттєвий руйнівний характер і характеризується негативними ланцюговими та синергетичними ефектами.

До таких загроз можна віднести поширення неправдивої інформації щодо самої хвороби (фейкова інформація про кількість загиблих/хворих, симптоматику, кількість ускладнень після хвороби, тощо), лікування (фейкова інформація щодо ефективності певних ліків чи методик лікування, ефективності та небезпечності

певних видів щеплень тощо), джерела хвороби (вже відомі фейкові повідомлення про розповсюдження COVID-19 завдяки використанню веж 5G, непідтверджені витоки щодо штучного поширення вірусу певними державами чи іншими суб'єктами, релігійний контекст розповсюдження вірусу тощо) та інших факторів, пов'язаних з протидією пандемії (фейкові новини стосовно умов лікування у лікарнях, умов у місцях примусової обсервації, наявність ПЛР-тестівта цілої низки різних факторів)[5].

Окремим кіберінформаційним аспектом пандемії було посилення кіберзлочинності. У 2020 році Служба безпеки України [4] знешкодила 600 кібератак та кіберінцидентів.

Кібератаки на системи охорони здоров'я почастішали. Частина з них безпосередньо пов'язана з медичними установами та їх інформаційними системами, в яких злочинці шукають інформацію про ліки, тести або вакцини. В Інтернеті збільшилася і кількість пропозицій контрафактних лікарських препаратів, а також фальшивих «ліків» від коронавірусу.

Крім того, почастішали деструктивні кібердії, спрямовані на порушення функціонуваннят медичних установ, крадіжку конфіденційних даних, шифрування великих обсягів критично важливої інформації з метою отримання викупу за її відновлення. Все більше лікарень і дослідницьких центрів, у яких триває пошук засобів боротьби з пандемією, стають об'єктами нападів організованих кіберзлочинців, які шукають інформацію про новітні розробки [6].

Під час пандемії збільшилася і кількість кіберзлочинів, що стосуються електронного банкінгу та онлайн-торгівлі. Зростання у зв'язку зкарантином обсягів дистанційних онлайн-розрахунків з використанням різних електронних банківських сервісів підвищило число крадіжок коштів з рахунків клієнтів банків [7]. Як повідомили в Службі безпеки України, зловмисники розсилають електронною поштоюшкідливе програмне забезпечення, за допомогою якого отримують несанкціонований доступ до системи клієнт–банк. Збільшення обсягів онлайн-платежів із використанням різних електронних банківських послуг збільшило кількість крадіжок з рахунків клієнтів банку [7].

В умовах зростаючої активізації глобальних процесів у сучасному світі, що поряд із позитивними аспектами своїх впливів на світову спільноту створили також небезпеки інформаційної агресії, кіберзлочинності, саме загальнонаціональна система інформаційної безпеки, скоординована в своїй діяльності державою, може стати запорукою нейтралізації інформаційних загроз і використання позитивних факторів розвитку інформатизації.

Як висновок необхідно зазначити для зменшення руйнівного впливу загроз на інформаційну безпеку в контексті пандемії COVID-19, необхідно посилити захист національного сегменту кіберпростору, забезпечити розвиток вітчизняних кібер- та інформаційних технологій а також нових високотехнологічних електронних та програмних продуктів тощо. Таким чином, пандемія COVID-19 наголосила на необхідності посилення національної безпеки України та вдосконалення державної політики у сфері інформаційної безпеки.

Список літератури

1.Digital 2021. GlobalOverviewReport. Access mode:https://datareportal.com/reports/digital-2021-global-overview-report.

2. КонституціяУкраїнивід 28 червня 1996 р. URL: http://zakon5.rada.gov.ua/laws/show/254к/96-вр3.

3.Про Основні засади розвиткуінформаційногосуспільства в Україні на 2007–2015 рр. : Закон Українивід 09 січня 2007 р.

4.Офіційний сайт Служби безпеки України [Електронний ресурс]. – Режим доступу: https://ssu.gov.ua/

5. Швець Д.В. Загрозинаціональнійінформаційнійбезпеці в період ПАНДЕМІЇ COVID-19. Актуальні питання діяльності суб'єктів господарювання в умовах пандемії COVID-19.2021. С. 32-34.

6.Горбулін В.П., Даник Ю.Г. Національна безпека України: фокус пріоритетів в умовах пандемії. Вісник Національної академії наук України. 2020. № 5, С. 3-18.

7. СБУ припинила діяльність хакерського угрупування, яке завдало збитків клієнтам банківських систем на 20 мільйонів гривень. Сайт Служби безпеки України. 26.03.2020. https://ssu.gov.ua/ua/news/1/category/21/view/7352#.LHsj4OM3.dpbs

УДК 004.67

О.О. Шевченко, Є.В. Мелешко
shev4enos@gmail.com
Центральноукраїнський національний технічний університет, Кропивницький

ДОСЛІДЖЕННЯ ПІДХОДІВ ДО АНАЛІЗУ СОЦІАЛЬНИХ МЕРЕЖ

На сьогоднішній день досить важко знайти людину, яка не користується соціальною мережею. З розвитком технологій людина може вести соціальне життя в досить зручних умовах за допомогою соціальних мереж. Аналіз соціальних мереж може мати застосування в багатьох сферах людської діяльності та грає важливу роль в сучасній соціології.

Метою даної роботи є дослідження загальних підходів до аналізу соціальних мереж, його використання та перспективи.

В аналізі соціальних мереж можна виділити такі основні підходи: *структурний*, *ресурсний*, *нормативний* та *динамічний*. Кожний з них має різне призначення та різний набір методів і засобів для проведення аналізу соціальних взаємодій.

У структурному підході всі учасники мережі розглядаються як вершини графу, які впливають на конфігурацію ребер і інших учасників мережі. Основна увага приділяється структурі зв'язків соціальної мережі та інтенсивності взаємодій між її учасниками, тому досліджуються такі характеристики, як взаємне розташування вершин, центральність вершин, транзитивність взаємодій. При структурному аналізі та дослідженні поведінки зв'язків учасників мережі використовуються методи статистичного аналізу, методи виділення кластерів та методи класифікації. Вивчається від чого залежить структура мережі, напр., як вона змінюється в процесі росту мережі або як змінюються поведінка і розподіл зв'язних компонентів графу. Структурний аналіз соціальних мереж ділить мережу на ряд окремих елементів, напр., користувач або група користувачів та досліджує їх окремі властивості та робить на основі них певні висновки або прогнози. Аналіз соціальних мереж має певні стандартні метрики, які використовуються для аналізу взаємодії між своїми елементами. В структурному аналізі соціальних мереж використовують такі стандартні метрики: 1) *зв'язки* (гомогенність, множинність, взаємність, закритість мережі, сусідство), 2) *розподіл* (міст, центральність, густина, відстань, структурні пробіли, сила зв'язку), 3) *сегментація* (коефіцієнт кластеризації, згуртованість). Метрика «зв'язки» загалом досліджує взаємодію елементів мережі та її якісні характеристики. Метрика «розподіл» досліджує зв'язки та їх взаємодії в контексті самої мережі. Метрика «сегментація» досліджує розподіл користувачів мережі на певні групи та вплив їх перебування у цих групах на їх функціонування.

Ресурсний підхід розглядає можливості учасників по залученню індивідуальних і мережевих ресурсів для досягнення певних цілей і диференціює учасників, які перебувають в ідентичних структурних позиціях соціальної мережі, по їх ресурсам. В якості індивідуальних ресурсів можуть виступати знання, престиж, багатство, раса, стать. Під мережевими ресурсами розуміються вплив, статус, обсяг і характер інформації. Основним показником, який визначає відмінності в ресурсах учасників мережі, є сила структурної позиції учасника. Важливе завдання даного підходу – аналіз змісту соціальних мереж. Мережевий контент служить джерелом для широкого спектру додатків, орієнтованих на вилучення та аналіз даних. Використання змісту мережі допомагає значно поліпшити якість висновків при аналізі соціальних мереж, напр., в задачах кластеризації та класифікації. Можна виділити чотири види аналізу контенту мережі: 1) аналіз загальної інформації з довільними типами даних, 2) сенсорний і потоковий аналіз, 3) аналіз мультимедіа, 4) аналіз текстової інформації.

Нормативний підхід вивчає рівень довіри між учасниками, а також норми, правила і санкції, що впливають на поведінку учасників в соціальній мережі і процеси їх взаємодій. В цьому випадку аналізуються соціальні ролі, які пов'язані з деяким ребром мережі, напр., відносини керівника і підлеглого, дружні або родинні зв'язки. Так як в основі соціальних мереж лежить взаємодія між різними учасниками, природно припустити, що ця взаємодія впливає на учасників в термінах їх поведінки. Нормативний підхід дозволяє дослідити рівень впливовості учасників мережі та поширення впливів.

У динамічному підході об'єктами досліджень є зміни в мережевий структурі з часом: з'являються нові учасники, деякі учасники припиняють взаємодію, виникають нові зв'язки. Одним з найважливіших завдань динамічного аналізу є прогноз формування зв'язків у соціальних мережах. В процес прогнозування може бути залучена не тільки структура мережі, а й характеристики різних вершин. Для полегшення роботи з динамічним аналізом та покращення сприйняття даних використовується візуалізація мережі.

Отже, аналіз соціальних мереж дозволяє дослідити інформацію про учасників мережі та зв'язки між ними, а також їх зміни у часі. Ця інформація може бути використаною у маркетингових, соціологічних, політичних та інших дослідженнях, а також мати значення для забезпечення інформаційної безпеки.

УДК 004.056

А.Ю. Казаков
kazakov.anton97@gmail.com
Національний технічний університет «Харківський політехнічний інститут», м. Харків

ДОСЛІДЖЕННЯ МЕТОДІВ ЦИФРОВОГО ПІДПИСУ ДАНИХ

Розвиток комп'ютерних систем та мереж призвів до появи нової області взаємовідносин, предметом яких є електронний обмін даними. Виникла нова проблема – захист електронних документів, що мають юридичну силу, від модифікації і підробки. Основним способом такого захисту став Електронний цифровий підпис (ЕЦП), аналог звичайного підпису людини, що має схожу мету, але зовсім іншу реалізацію.

На практиці застосування ЕЦП дозволяє виявити або запобігти таким діям порушника: підробка документу, модифікація електронного документу та відмова одного з учасників від авторства документу.

При підписанні електронного документу його початковий зміст не змінюється, а додається блок даних, що й є безпосередньо ЕЦП.

Існують симетричні та асиметричні схеми ЕЦП. Найчастіше на практиці використовуються асиметричні схеми, як більш надійні та зручні.

Симетричні схеми. Для електронного документу підраховується хеш-функція. До визначеної хеш-функції також додаються деякі дані, зокрема, про автора документу та час його створення, це і буде електронним підписом. Отриманий ЕЦП шифрується блочним симетричним алгоритмом шифрування. Для перевірки підпису треба обчислити хеш-функцію отриманого документу та розшифрувати його ЕЦП і перевірити чи збігається отримана та розшифрована хеш-функція. У випадку достовірності документу – вони збігаються. При симетричній схемі безпека підпису заснована на ключі симетричного шифрування. Постає питання як його зберігати, щоб тримати у секреті, та хто повинен мати до нього доступ для перевірки достовірності документу. В такому випадку тільки центр генерації ключів матиме можливість створювати те перевіряти ЕЦП, а для кожного нового підписання треба буде генерувати новий ключ. Це значно звужує можливості використання такого ЕЦП.

Асиметричні схеми. Використовують асиметричні алгоритми шифрування. Загальновизнана схема цифрового підпису, охоплює три процеси:

1. *Генерація пари ключів*, закритого для встановлення підпису та відкритого для перевірки підпису.
2. *Формування підпису*. Для заданого електронного документу за допомогою закритого ключа обчислюється хеш-функція.
3. *Перевірка підпису*. Для заданого документу та ЕЦП за допомогою відкритого ключа визначається дійсність підпису. Тобто порівнюється одержана та розшифрована хеш-функція до даного документу.

Для того, щоб використання цифрового підпису мало сенс, необхідно виконання двох умов:

– Верифікація підпису повинна проводитися відкритим ключем, відповідним саме тому закритому ключу, який використовувався під час підписання.

– Без володіння закритим ключем має бути обчислювально складно створити легітимий цифровий підпис.

Види асиметричних алгоритмів ЕЦП. Щоб ЕЦП виконував свої функції, необхідно, забезпечити таку складність створення легітимного підпису, при якій без знання закритого ключа було б обчислювально складно і практично неможливо при наявному часі та ресурсах його підробити. Забезпечення цього у всіх асиметричних алгоритмах цифрового підпису спирається на наступні обчислювальні завдання:

– Завдання дискретного логарифмування (напр., алгоритм EGSA).

– Завдання факторизації, тобто розкладання числа на прості множники (напр., алгоритм RSA).

Алгоритми ЕЦП підрозділяються на звичайні цифрові підписи і на цифрові підписи з відновленням документу. При верифікації цифрових підписів з відновленням документа тіло документа відновлюється автоматично, його не потрібно прикріплювати до підпису. Звичайні цифрові підписи вимагають приєднання документа до підпису. Ясно, що всі алгоритми, що підписують хеш документу, відносяться до звичайних ЕЦП. До ЕЦП з відновленням документа відноситься, зокрема, RSA.

Схеми електронного підпису можуть бути одноразовими і багаторазовими. В одноразових схемах після перевірки справжності підпису необхідно провести заміну ключів.

До відомих на сьогоднішній день алгоритмів асиметричного ЕЦП можна віднести RSA, схему Ель Гамаля, DSA, ECDSA тощо.

В Україні використовується ЕЦП, що заснована на еліптичних кривих, її алгоритм описує стандарт ДСТУ 4145-2002. Послуги з надання ЕЦП в Україні впроваджуються акредитованими центрами сертифікації ключів. Актуальний перелік акредитованих центрів сертифікації ключів публікується на сайті Центрального засвідчувального органу.

УДК 327.8

А.О. Лукіянчук
Annaluki0207@gmail.com
корпоративні курси іноземних мов, викладач-методист
м. Київ

СУЧАСНИЙ СТАН СФЕРИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

На сьогоднішній день до важливих питань безпеки кожної держави відносять поточний стан її інформаційної безпеки, а також наявність потенційних та реальних загроз у зазначеній сфері. Так як Україна є державою, в якій сфера інформаційних технологій стрімко розвивається, цей процес супроводжується появою принципово нових загроз інтересам особистості, суспільства та держави. Інформаційна безпека є важливою складовою національної безпеки держави. Під станом її захищеності розуміється стан при якому операції зовнішньої інформаційної агресії, інформаційний тероризм, незаконне зняття інформації за допомогою спеціальних технічних засобів, комп'ютерні злочини та інший деструктивний інформаційний вплив не завдають суттєвої шкоди національним інтересам України [5]. Також інформаційна безпека розглядається як глобальна система захисту інформації, інформаційного простору, інформаційної інфраструктури країни.

Забезпечення інформаційної безпеки держави включає інформаційно-аналітичне забезпечення діяльності державних органів, інформаційне забезпечення роботи органів внутрішньої і зовнішньої політики, систему захисту інформації з обмеженим доступом, протидію правопорушенням в інформаційній сфері та комп'ютерним злочинам [5]. Забезпечення інформаційної безпеки держави через послідовну реалізацію сформованої національної інформаційної стратегії сприяє забезпеченню досягнення успіху при вирішенні задач у політичній, військово-політичній, військовій, соціальній, економічній та інших сферах державної діяльності. Впровадження якісної інформаційної політики може безпосередньо впливати на розв'язання внутрьошньополітичних, зовнішньополітичних та військових конфліктів.

В Україні сфера захисту інформації включає систему правових, організаційних, технічних та інших заходів, спрямованих на забезпечення збереження не тільки інформації з обмеженим доступом, а й відкритої інформації, необхідність захисту якої визначається законодавством. Ці заходи поширюються також на інформаційні ресурси, системи, технології та засоби їх забезпечення. Важливим чинником процесу створення даної системи безпеки інформації в Україні є розробка та вдосконалення правового підґрунтя діяльності у сфері інформації та інформаційної безпеки, зокрема, нормативної бази, яка повинна, враховуючи вимоги часу, регламентувати суспільні відносини у сфері захисту інформації та забезпечення її безпеки під час інформаційного обміну [1]. Процеси формування та вдосконалення нормативно-правової бази системи захисту інформації повинні відповідати вимогам українського та міжнародного законодавства, а також вони мають створювати для України можливість бути рівноправним учасником міжнародного інформаційного обміну за умови збереження інформаційного суверенітету держави.

Ефективна діяльність держави у сфері забезпечення інформаційної безпеки має відображати успішну роботу структур, на які покладено реалізацію державної політики щодо захисту інформаційних ресурсів, захисту інформації, забезпечення безпеки інформаційного обміну. Це дозволить реалізувати державну політику у сфері інформаційної безпеки та забезпечити інформаційну безпеку особи, суспільства і держави. Під єдиною державною політикою інформаційної безпеки розуміється колегіальне обговорення й документальне закріплення основних напрямів адміністративної діяльності, пов'язаної з процесами інформатизації, захистом конфіденційної інформації, а також профілактикою і боротьбою з правопорушеннями з використанням інформаційних технологій [3].

Інформаційна безпека держави характеризується ступенем її захищеності, та, як наслідок, стійкістю головних сфер життєдіяльності у відношенні до небезпечних інформаційних впливів, тобто наявних чи потенційних загроз. Інформаційна безпека визначається здатністю нейтралізувати такі загрози. За своєю загальною спрямованістю загрози інформаційній безпеці України можна поділити на: загрози інформаційному забезпеченню державної політики України; загрози розвиткові вітчизняної індустрії інформації, включаючи індустрію засобів інформатизації, телекомунікацій і зв'язку; загрози безпеці інформаційно-телекомунікаційних систем на території України; загрози конституційним правам і свободам людини і громадянина у сфері духовного життя й інформаційної діяльності, індивідуальній, груповій і суспільній свідомості, духовному відродженню України [2].

Відповідно до Стратегії національної безпеки України прийнятої у 2020 році, серед викликів для стану інформаційної безпеки України сьогодні критичними є агресія Російської Федерації, що продовжує гібридну війну, системно застосовує політичні, економічні, інформаційно-психологічні, кібер- і воєнні засоби [6]. Доктрина інформаційної безпеки України, будучи логічним продовженням Стратегії національної безпеки, визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері. Метою доктрини є уточнення засад формування та реалізації

державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни.

Серед актуальних загроз національним інтересам та національній безпеці України в інформаційній сфері з боку держави-агресора є проведення РФ спеціальних інформаційних операцій в інших державах, що має на меті створення негативного іміджу України у світі. Також це здійснення спеціальних інформаційних операцій, що спрямовані на підрив обороноздатності, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні [4]. Інформаційна експансія держави-агресора також здійснюється шляхом розширення власної інформаційної інфраструктури на території України та в інших державах, де важливу роль відіграє інформаційне домінування РФ на тимчасово окупованих територіях, а також поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні. В свою чергу недостатня розвиненість національної інформаційної інфраструктури обмежує можливості України ефективно протистояти інформаційній агресії та активно діяти в інформаційній сфері для реалізації національних інтересів. Цьому сприяють неефективність державної інформаційної політики, недосконаліть законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіа-культури суспільства.

Інформаційна безпека держави є станом інститутів держави і суспільства, за якого забезпечується надійний захист національних інтересів країни і її громадян в інформаційній сфері. Актуальними практичними завданнями у сфері забезпечення інформаційної безпеки України є такі, що відповідають актуальним викликам, що створюються державою-агресором Російською Федерацією. З метою протидії визначеним загрозам були розроблені та впроваджені такі основоположні документи як Доктрина інформаційної безпеки, Стратегія національної безпеки, Стратегія кібербезпеки та інші. Для досягнення єдиного підходу до визначення оптимальних моделей і шляхів забезпечення інформаційної безпеки держави необхідно і надалі послідовно втілювати сучасні стратегії національної безпеки у сферу інформаційної політики держави.

Список літератури

Боднар І. Р. Інформаційна безпека як основа національної безпеки / І. Р. Боднар // Mechanism of Economic Regulation. - 2014. - № 1. - С. 68-75. - Режим доступу: http://nbuv.gov.ua/UJRN/Mre_2014_1_8.

Вавринчук М.П. Інформаційна безпека держави / М. П. Вавринчук, О. В. Когут // Правові засади організації та здійснення публічної влади : зб. тез II Всеукр. наук.-практ. інтернет-конф. (м. Хмельницький, 2-8 трав. 2019 р.). - Хмельницький : ХУУП, 2019. - С. 37-40.

Гаврильців М.Т. Інформаційна безпека держави в системі національної безпеки. Львівський державний університет внутрішніх справ. Юридичний науковий електронний журнал, 2020, № 2. – С. 200-203. DOI https://doi.org/10.32782/2524-0374/2020-2/52

Доктрина інформаційної безпеки України. Указ Президента України від 25 лютого 2017 р. № 47/2017.

Мужанова Т.М.. Інформаційна безпека держави. Навчальний посібник. Київ: Державний університет телекомунікацій, 2019. 131 с.

Стратегія національної безпеки України. Безпека людини – безпека країни. Указ Президента України від 14 вересня 2020 р. № 392/2020.

СЕКЦІЯ 2. ПРОГРАМУВАННЯ ТА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004.853

О.К. Конопліцька-Слободенюк, В.О. Ковальов
Ksuha80@gmail.com, vladkov228@gmail.com
Центральноукраїнський національний технічний університет, Кропивницький

РОЗГЛЯД ПРИНЦИПІВ ТА МОЖЛИВОСТЕЙ ШТУЧНОГО ІНТЕЛЕКТУ

Штучний інтелект(ШІ) - це технологія, а точніше напрямок сучасної науки, що вивчає способи, які навчають комп'ютер, роботизовану техніку, аналітичну систему розумно мислити як людина. Власне мрія про інтелектуальні роботи-помічники виникла задовго до винаходу перших комп'ютерів.

Людей ще в минулому столітті сильно вразили можливості обчислювальних машин, особливо здатності ЕОМ(електронна обчислювальна машина), безпомилково виконувати безліч завдань одночасно. У головах вчених і письменників відразу виникли фантастичні ідеї про мислячі машини. Саме в цей період починають зароджуватися перші технології штучного інтелекту.

Дослідження в сфері ШІ ведуться шляхом вивчення розумових здібностей людини і перекладання отриманих результатів в поле діяльності комп'ютерів. Таким чином, штучний інтелект отримує інформацію з різних джерел і дисциплін. Це і інформатика, і математика, і лінгвістика, і психологія, і біологія, і машинобудування. На основі масиву даних за допомогою технології машинного навчання комп'ютери намагаються імітувати інтелект людини.

Головні цілі ШІ досить прозорі:

Створення аналітичних систем, які володіють розумною поведінкою, можуть самостійно або під наглядом людини навчатися, робити прогнози і будувати гіпотези на основі масиву даних.

Реалізація інтелекту людини в машині - створення роботів-помічників, які можуть вести себе як люди: думати, вчитися, розуміти і виконувати поставлені завдання.

Слід зазначити, що штучний інтелект має свої принципи.

Перш ніж описуватися технологічні принципи, без яких неможливий розвиток штучного інтелекту, варто познайомитися з етичними законами робототехніки. Їх в 1942 році вивів Айзек Азімов у своєму романі «Хоровод»:

- Робот або система з штучним інтелектом не може нашкодити людині своєю дією або ж своєю бездіяльністю допустити, щоб людині була заподіяна шкода.
- Робот повинен виконувати накази, які отримує від людини, крім тих, які суперечать Першому закону.
- Робот повинен піклуватися про себе та свою безпеку, якщо це не суперечить Першому і Другому Законам.

Хочеться відмітити, що штучний інтелект, незважаючи на свою цінність має і проблеми. Як ви розумієте можливості штучного інтелекту на даній стадії розвитку не безмежні.. Отже основні проблеми, як на мене, що має ШІ:

- Навчання машин можливо тільки на основі масиву даних. Це означає, що будь-які неточності в інформації сильно позначаються на кінцевому результаті.
- Інтелектуальні системи обмежені конкретним видом діяльності. Тобто розумна система, налаштована на виявлення шахрайства в сфері оподаткування, не зможе виявляти махінації в банківській сфері. Ми маємо справу з вузькоспеціалізованими програмами, яким ще далеко до багатозадачності людини.
- Інтелектуальні машини не є автономними. Для забезпечення їх «життєдіяльності» необхідна ціла команда фахівців, а також великі ресурси.

Отже, завдання штучного інтелекту полягає в імітації поведінки об'єктів реального світу. І це зовсім не складно, якщо почати розгляд штучного інтелекту з базових компонентів - від низькорівневих правил і алгоритмів пошуку шляхів до більш високого рівня, на якому працює тактичний і стратегічний ШІ. При цьому, слід домогтися високої ефективності роботи системи ШІ, оптимізувати її для використання на комп'ютерах з великою кількістю обчислювальних ядер. Можливості ШІ в системі повинні обмежуватися тільки фактично наявними ресурсами обладнання, а не нездатністю використовувати ці ресурси.

УДК 004

Т.В. Смірнова, О.М. Дрєєв, О.А. Смірнов
sm.tetyana@gmail.com, drey.sanya@gmail.com, dr.SmirnovOA@gmail.com
Центральноукраїнський національний технічний університет, Кропивницький

ХМАРНА ІНФОРМАЦІЙНА СИСТЕМА ОЦІНЮВАННЯ ШОРСТКОСТІ З ВИКОРИСТАННЯМ ДИСКРЕТНОГО ЧАСТОТНОГО АНАЛІЗУ МАКРОФОТОГРАФІЙ

Технологічні процеси відновлення та зміцнення металевих поверхонь часто вимагають попередньої підготовки поверхонь. До підготовчих технологічних операцій відноситься дробовоструменева обробка, в результаті якої збільшується шорсткість, а внаслідок і площа, обробленої поверхні. Завдяки цьому сила зчеплення покриття до основи є значно кращою. В дрібносерійному виробництві обробка проводиться вручну кваліфікованим спеціалістом, який в більшості випадків за виглядом обробленої поверхні визначає досягнення заданих характеристик результатів обробки.

Однак, автоматична обробка, або обробка спеціалістами низької кваліфікації, потребує об'єктивний контроль за показниками шорсткості поверхні. Об'єктивний контроль, який реалізовано засобами комп'ютерного зору, дозволить підвищити продуктивність, завдяки усуненню зайвих замірів або занадто довгої обробки поверхні, а також підвищить якість результату обробки за рахунок вчасного виявлення недостатнього ступеню обробки металевих поверхонь. Таким чином, відстеження обробки за допомогою камери та автоматичне вимірювання параметрів поверхні є актуальною задачею.

В процесі визначення характеристик поверхні металу постала задача безконтактного визначення середнього розміру зерна за допомогою відеокамери, яка приєднана до комп'ютеризованої системи через USB, й дані з якої передаються у відповідну хмарну інформаційну систему як сервіс. В результаті до програмного модуля поступає потік кадрів з відомим масштабуванням. Завдяки цьому задача зводиться до визначення середнього розміру зерна у пікселях, після чого для запису результату в метричній системі достатньо використати виміряний коефіцієнт пропорційності. Для мікрофотографій відношення пікселя до метричної системи вимірювання довжини задано в технічній документації до приладу або проводиться експериментально за допомогою фотографування еталону розміру.

Основна ідея розробленого алгоритму полягає у визначенні домінуючої частоти зміни яскравості пікселів на зображенні. Для цього можна використати методи основані на перетворенні Фур'є, вейвлет аналізуванні, автокореляційні методи та методи, які використовують регресії гармонік.

Однак, як показав експеримент, перелічені методи мають недоліки і не можуть бути використані на практиці самостійно. В результаті стає актуальною задача розробки нового методу, який мав би можливість усереднювати частотні властивості на всьому зображенні, але при цьому використовував локальність фазових спотворень сигналу.

Розробка методу алгоритму визначення середнього розміру елементів на зображенні вимагає наявності бази даних зображень для визначення якості роботи алгоритму. Однак створення такої бази вимагає вкладення трудових ресурсів та матеріальних витрат. Тому на етапі формування математичних методів та їх властивостей потрібно мати джерело зображень для аналізу з регульованими параметрами. Відповідно до зазначеної потреби поставлено задачу створення генератора синтетичних зображень для тестового аналізування.

Нехай зображення представлене у вигляді дискретних даних, які врівноважено, тобто коливання відбуваються відносно нуля.

З метою наближення синтезованого зображення до реального, на утворені коливання яскравості було накладено рівномірний шум з амплітудою в 25% від амплітуди генерованого коливання. Потрібно зауважити, що доля шумів на реальній фотографії залежить від якості не лише самої камери, але й від якості освітлення в момент зйомки.

Завдяки використаному нормуванню, коливання відбуваються навколо нульового значення, але амплітуда не є обов'язково рівною одиниці, з причини сканування лінії між локальними максимумами. Теоретично можна отримати зріз, який не міститиме коливань взагалі, тому в алгоритмі обробки зображення потрібно врахувати таку особливість.

В результаті використання дискретного частотного аналізу макрофотографій обробленої поверхні металу з відомим масштабуванням, було розроблено метод оцінювання середнього розміру утворених нерівностей. На основі розробленого методу отримано обчислювальний алгоритм, якість якого підвищено додаванням до алгоритму ітераційних уточнень.

УДК 303.444

В.І. Слюсар[1], В.В. Сотник[2], А.В. Купчин[3]
swadim@ukr.net, otvladislav@gmail.com, kupchyn.artem@ukr.net
[1]головний науковий співробітник, д.т.н., проф.,
[2]заступник начальника інституту з наукової роботи, к.т.н., с.н.с.,;
[3] ад'юнкт 3 року навчання,
Центральний науково-дослідний інститут озброєння та військової техніки Збройних Сил України,Київ

ПЕРЕВІРКА ДОСТОВІРНОСТІ МОДЕЛІ ТЕХНОЛОГІЧНОГО ПРОГНОЗУВАННЯ НА ОСНОВІ САМОНАВЧЕНОЇ НЕЙРОННОЇ МЕРЕЖІ

Авторами роботи опрацьована модель прийняття рішення щодо визначення критичності технологій, математичною основою якої є апарат нечіткої логіки [1]. Результатом впровадження моделі є рейтинговий перелік критичних технологій. Однак, відкритим залишається питання щодо перевірки моделі на адекватність та визначення достовірності отриманих даних.

Адекватність моделі зазвичай перевіряється оцінюванням відхилень передбачених значень від експериментально знайдених, усереднених за числом повторень та ін. У випадку стохастичних математичних моделей, вони можуть бути піддані перевірці на адекватність, зокрема за критерієм Фішера.

Однак, у випадку моделей прогнозування, ми не можемо оперувати для перевірки адекватності набором випадкових величин, у зв'язку з їх відсутністю. Подія технологічного прогнозування не повторювана, тому вихідні дані не носять стохастичного характеру. Крім того, еталонна вибірка з ідеальним переліком технологій відсутня в реальному часі і з'явиться лише після досягнення кінцевого строку прогнозування. Тобто, у випадку прогнозування на період 20 років, реальну перевірку як адекватності моделі, так і достовірності результатів прогнозу можна провести лише через 20 років, коли буде встановлено факт критичності або некритичності досліджуваних технологій [2].

З цієї ситуації пропонується вийти наступним чином. Відомі дані про систему прийняття рішення щодо визначення критичності технологій дають нам можливість встановити логічні правила. Наприклад, «Якщо технологія має за всіма показниками найвищі оцінки, то вона вважається критичною, якщо найнижчі – ні»; або «Якщо за більшістю показників оцінки не менші за 90 відсотків, а за рештою – більше 50, то технологія критична».

На основі вагомості показників також можна створити певну сукупність правил. Наприклад, «Якщо технологія має відмінні оцінки за найвагомішими показниками, а за рештою – низькі, то технологія – критична».

Таким чином, є можливість створити ідеальну вибірку з вхідними оцінками та відповідними висновками щодо критичності технологій.

Фактично технологічне прогнозування є завданням класифікації (кластеризації), тобто віднесення певної технології до класу (кластеру) критичних, проривних чи некритичних. Такий тип задач останнім часом досить ефективно вирішується за допомого нейронних мереж. Широкий спектр вже сформованих та навчених нейронних мереж у вільному доступі, що здійснюють кластеризацію, дозволяє на основі розробленої ідеальної вибірки провести процес донавчання нейромережі.

Розроблена авторами модель технологічного форсайту має дванадцять вхідних показників. При цьому експертним оцінюванням вже встановлені вагові коефіцієнти для кожного показника.

Після того, коли раніше навчена для схожих завдань кластеризації нейронна мережа пройде процес незначного перенавчання, слід ввести реальні вхідні дані за реальними технологіями для отримання результату у вигляді переліку критичних технологій. Цей перелік можна вважати еталонним.

Таким чином, з'явилась можливість порівнювати результати визначення критичності технологій за моделлю на основі нечіткої логіки та еталонної вибірки, що отримана від нейромережі.

Варто додати, що попередньо розроблений авторами метод формування функції належності на основі еквідистантних точок може бути застосований і для визначення функцій активації нейронів у різних шарах нейромережі.

Запропонований підхід є новим та не достатньо дослідженим. Проте, зважаючи на відсутність адекватної перевірки результатів прогнозування, такий варіант вирішення поставленої задачі заслуговує на увагу.

Список літератури

1. В.І. Слюсар, В.В. Сотник, А.В. Купчин, "Проривні технології в оборонній сфері України", Озброєння та військова техніка, №4, с. 13-23, 2020. DOI: 1034169/2414-0651.2020.4(28).13-23

2. В.І. Слюсар, В.В. Сотник, А.В. Купчин, "Модель визначення переліку критичних і проривних технологій в оборонній сфері України", VIII Міжнар. наук.-пр. конф. «Проблеми координації воєнно-технічної та оборонно-промислової політики в Україні», м. Київ, 2020, С. 420.

УДК 621.39

Р.С. Одарченко [1], Д.К. Григоренко [2]
pc_boy@i.ua
[1]д.т.н., доцент,
[2]науковий співробітник
Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації, м. Київ

ЕВОЛЮЦІЯ СТІЛЬНИКОВИХ МЕРЕЖ ЗВ'ЯЗКУ: ШЛЯХ ДО 5G

Сучасні телекомунікаційні мережі характеризуються великими можливостями. Стратегічна мета розвитку національної телекомунікаційної інформаційної інфраструктури - забезпечити країну якісними засобами та послугами зв'язку в необхідному обсязі з оптимальною вартістю. Створення високоякісних мереж зв'язку, мереж передачі даних, високошвидкісних факсимільних систем, високошвидкісних систем пошуку в базах даних, систем обробки повідомлень і бездротового зв'язку, які забезпечують обмін голосовими та файловими даними різного розміру. Проблему розгортання мереж в деяких районах країни в основному визначаються низькою щільністю населення (великий розкид цього показника по регіонах), а також високим рівнем питомих витрат. Це вимагає використання таких технічних засобів і рішень, як концентратори, парні пристрої, системи радіозв'язку з багаторазовим використанням обраного частотного діапазону, а також використання систем передачі. Всі ці системи повинні бути адаптовані до організації мобільного зв'язку. 5G дає нові можливості для розвитку, п'яте покоління мобільних мереж називають стандартами телекомунікацій які замінять 4G. Телекомунікаційні мережі 5G повинні вирішувати проблеми, що виникають в мережах 4G. Можливості мобільних технологій вже давно вийшли за рамки голосових послуг і створюють нові способи обміну даними. Відповідно зросла потреба до збільшення трафіку в мережах по всьому світу. Технології будуть продовжувати розвиватися до більшої кількості можливостей. З кожним новим поколінням з'являються нові технології, які дозволяють задовільнити нові потреби користувачів[1].Інтеграція існуючих і нових технологій буде сприяти підвищенню якості призначених для користувача послуг та розширення їх спектру. Покоління систем мобільного зв'язку перераховані в таблиці 1.

Таблиця 1
Покоління систем мобільного зв'язку

Покоління	Назва стандарту
0G	**PTT, MTS,IMTS, AMTS, Mobitex, Autotel/PALM, ARP**
1G	**NMT, AMPS, Hicap**
2G	**GSM, iDEN, D-AMPS, IS-95, PDC, CSD, GPRS, HSCSD, WiDEN**
2.75G	**EDGE/EGPRS, CDMA2000 (1xRTT)**
3G	**UMTS (W-CDM A, FOMA), CDMA2 00 0, TD- SCDMA, WiMAX**
3.5G	**UMTS (HSPA, HSDPA, HSUPA), CDMA2000 (EV-DO Rev.A)**
3.75G	**UMTS (HSPA+), CDMA2000 (EV-DO Rev.B/3xRTT)**
4G	**WiMAX, LTE**
5G	**WiMAX, LTE, CDMA**

З моменту появи мереж мобільного зв'язку до сьогодні досить стрімко пройшли свій шлях розвитку. Системи другого покоління засновані на методі TDMA (множинного доступу з тимчасовим поділом). Уже в 1992-1993 роках. в США був розроблений стандарт для системи стільникового зв'язку на основі методу CDMA (множинного доступу з кодовим поділом) - стандарт IS-95 (смуга 800 МГц) використовувався з 1995 по 1996 рік. Був найбільш поширений в Гонконзі, Сполучених Штатах, Південній Кореї. В США використовувався варіант 1900 МГц цього стандарту. 3.5G - HSDPA (високошвидкісна передача пакетних даних від базової станції до мобільного телефону) - це стандарт мобільного зв'язку, який експерти вважають одним з проміжкових етапів переходу до технологій мобільного зв'язку четвертого покоління (4G). Максимальна швидкість передачі теоретичних даних за стандартом становить 14,4 Мбіт/с. Практично можна досягти в існуючих мережах - приблизно 8 Мбіт/с. 4G - технологія четвертого покоління для мобільних широкосмугових мереж, яка замінила 3G. Перша в світі мережа LTE в Стокгольмі та Осло була запущена альянсом TeliaSonera/Ericsson - розрахункове значення максимальної швидкості передачі даних на одного абонента становить 382 Мбіт/с та 86 Мбіт/с від абонента. 4G використовує високошвидкісну систему завантаження/вивантаження пакетів як метод передачі даних. Мережі 4G дозволяють користувачам отримувати доступ до широкосмугових швидкостей на ходу. У всіх відношеннях 4G насправді є високотехнологічною і сучасної радіосистемою, яка дає можливості для подальшого вдосконалення та розширення можливостей.

5G - це покоління мобільного зв'язку, яке працює відповідно до стандартів телекомунікацій, які йдуть за існуючою технологією LTE. Збільшення швидкості буде пов'язано з переходом на більш високу смугу частот, яку раніше не використовували. Наприклад, частота домашнього WiFi становить 2,4 або 5 ГГц, а частота

існуючих мобільних мереж - до 2,6 ГГц. Однак коли ми говоримо про 5G, то відразу говоримо про десятки гігагерц, відповідно швидкість передачі даних збільшується в багато разів, а мережа в цілому розвантажується. Частота збільшилася в десятки разів, тому в 5G використовуються міліметрові хвилі. Вони погано проходять через перешкоди, в зв'язку з цим змінюється архітектура мережі. Раніше зв'язок забезпечували великі вишки на великі відстані, але тепер потрібно повсюдно встановлювати багато компактних і малопотужних вишок. На відміну від LTE, 5G працює в трьох різних діапазонах спектру. Низькочастотний спектр також може бути описаний як спектр нижче 1 ГГц. Низькочастотний спектр забезпечує велику зону покриття і проникнення, хоча є великий недолік: пікова швидкість передачі даних не перевищує 100 Мбіт/с. Спектр середнього діапазону забезпечує більш швидке покриття і меншу затримку, ніж низькочастотний діапазон. Однак він не проникає в будівлі так як низькочастотний діапазон. Очікуються пікові швидкості до 1 Гбіт/с. Оператори використовують Massive MIMO для поліпшення проникнення і покриття. Масивні MIMO об'єднують кілька антен в одному корпусі та створюють кілька променів одночасно для різних користувачів в одній вишці стільникового зв'язку. 5G також буде використовувати формування променя для поліпшення обслуговування. Формування променя відправляє один сфокусований сигнал кожному користувачеві в осередку та системі, які його використовують, відстежують кожного користувача, щоб переконатися, що він має узгоджений сигнал. Високочастотний спектр - це те, про що більшість людей думають, коли чує про 5G, хоча високочастотний спектр може пропонувати пікові швидкості до 10 Гбіт/с з дуже низькою затримкою. Основним недоліком високочастотного діапазону є те, що він має низьку зону покриття і погане проникнення в будівлях. Бездротові мережі 5G стануть альтернативою провідного інтернету в наших квартирах. Якщо раніше кабель заводили в квартиру, то в майбутньому - сигнал буде передаватися від вежі 5G до роутера, який буде роздавати його, як звичайний домашній WiFi. Типовий маршрутизатор 5G забезпечує швидкість завантаження 2-3 Гбіт/с. Так оператори зможуть вирішити проблему «останньої милі» та знизять вартість прокладки кабелів[2].

Одним з основних недоліків використання стільникового зв'язку попередніх поколінь є проблематичне використання мережі в місцях, де багато людей, мережа стає перевантаженою, адже з'явилися нові типи пристроїв - смартфони, планшети, пристрої доповненої реальності, дрони і.т.д. Але 5G може допомогти вирішити цю проблему, тому ця технологія важлива для таких сценаріїв. Згідно з дослідженнями, проведені компанією Ericsson, більше 70 відсотків глобального трафіку мобільного широкосмугового зв'язку (MBB) відбувається всередині приміщень. Тому автоматизація промислового виробництва зробила заміну дротових з'єднань бездротовими технологіями пріоритетом. У зв'язку з цим створення цифрової мобільної мережі всередині приміщень стає все більш важливою з приходом 5G. При побудові 5G мережі з'являється проблема з проникнення зовнішніх макро-радіосигналів всередину будівлі, тому концепція побудови 5G мережі на основі розподілених антенних систем (DAS), тобто отримання маленьких сот всередині будівлі. По мірі розвитку мереж 5G невеликі осередки будуть відігравати велику роль в задоволенні попиту на передачу голосу та даних всередині приміщень. Технологія DAS не нова, вона була успішно застосована в 4G, але з прогресом та збільшенням трафіку дана мережа вже не справляється з забезпеченням потрібної ємності швидкості[3].

Висновки

Новий стандарт бездротового зв'язку має велику кількість переваг, перед іншими телекомунікаційними стандартами минулих поколінь. Нова технологія відкриває нові напрямки розвитку бізнесу. Так само вона допоможе вирішити проблеми, з якими на сьогоднішній день не справляються попередні стандарти. З впровадженням 5G якість зв'язку зросте в рази. Очікується збільшення попиту на відеострімінг та відео високої роздільної здатності.

Список літератури

1. Huaweilampsite, DigitalIndoorSolution/ Huaweiproducts, 2020 – електрона версія статі на сайті https://e.huawei.com/se/products/wireless/lampsite.

2. Ericssonradiodotsystem/ Ericssonproducts, 2020 – електрона версія статі на сайті https://www.ericsson.com/en/portfolio/networks/ericsson-radiosystem/radio/indoor/radio-dot-system

3. Mahesh K Choudhary. BuildingFullyConnectedIntelligent LATAM with 5G. 2019

УДК 621.397

В.І. Солодка
valyaonas@gmail.com
Державний університет інтелектуальних технологій та зв'язку, Одеса

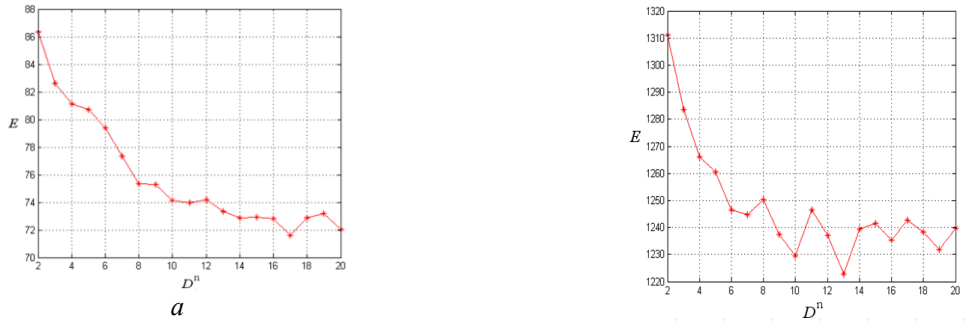
РОЗВИТОК СИГНАЛІВ ВЕЙВЛЕТ – ПЕРЕТВОРЕННЯ В ЗАДАЧІ СТИСНЕННЯ ЦИФРОВОГО ПОТОКУ

Для формування сигналів вейвлет – перетворення з урахуванням порогових функцій в задачі стиснення цифрового потоку необхідно розглянуто стандартний підхід до вирішення завдання очищення сигналу від перешкод і випадкових спотворень, що застосовує вейвлети Добеши і коригування коефіцієнтів розкладання сигналу по базису вейвлет-функцій із застосуванням м'якого і жорсткого варіантів завдання порогового значення. З огляду на значний інтерес до даної проблеми і численні дослідження, пошук шляхів оптимізації придушення перешкод, присутніх в сигналах і зображеннях, продовжує залишатися актуальною і важливою.

При реалізація сигналів вейвлет – перетворення з урахуванням порогових функцій в задачі стиснення цифрового потоку необхідно реалізація алгоритмів швидкого розкладання сигналу в вейвлет-базисі довжина вибірки вибирається рівною мірою двійки $N = 2^j$, так як перехід від одного рівня декомпозиції до іншого (більш детальному) еквівалентно зменшенню вдвічі довжини вибірки. $y_{\text{нч}}(k) = (x * g)(k) = \sum_{i=-\infty}^{\infty} x(i)g(k-i).\cdot$ Для цифрової обробки сигналів, синтезу фільтрів, розпізнаванні об'єктів і стисненні зображень в якості основних функцій для реалізації ДВП застосовують вейвлети Хаара, Добеши. Що стосується аналізу зображень процедура розкладання по вейвлет передбачає перехід до двовимірної реалізації дискретного вейвлет-перетворення двовимірного ДВП. Такий підхід, зокрема, використовується в комп'ютерній графіці в рамках формату JPEG2000. При практичної реалізації даного формату розглядається розширення одновимірного ДВП, при якому окремо аналізуються рядки і стовпці двовимірного зображення. У цьому випадку проводиться аналіз зображення по горизонталях, вертикалях і діагоналях з однаковим дозволом, і відповідні фільтри формуються на основі творів характеристик НЧ і ВЧ-фільтрів [6] для одновимірного випадку.

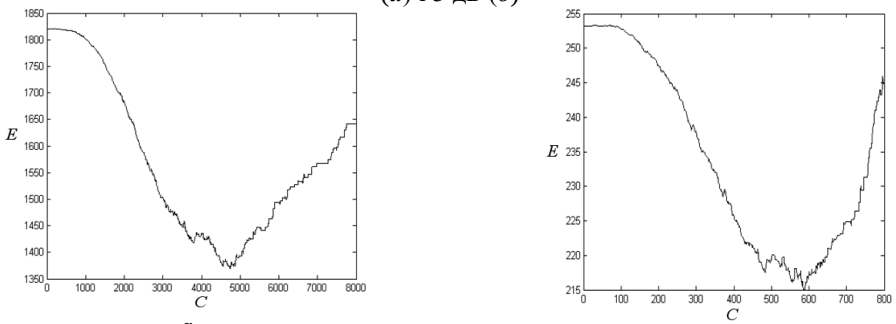
При аналізі сигналів або зображень дослідник має справу з сильно структурованими об'єктами, зокрема, порядок проходження відліків відображає важливі інформаційні характеристики. Внесення спотворень буде впливати на якість інформаційного повідомлення, однак ці спотворення можуть не відбиватися в величині E. E не залежить від часових або просторових взаємозв'язків між вибірками вихідного сигналу. Стосовно до сигналів, зазвичай вводять в розгляд величину середньоквадратичної помилки $E = \frac{1}{N}\sum_{i=1}^{N}\left[x(i) - y(i)\right]^2$. Дана величина дозволяє порівняти два сигнали і кількісно охарактеризувати ступінь подібності (або, навпаки, ступінь відмінності) між ними. Крім середньоквадратичної помилки або квадратного кореня з величини (9) при аналізі результатів фільтрації розглядають відношення сигнал / шум: $SNR = 10\lg\left(\frac{\sum_{i=1}^{N}\left[x(i)\right]^2}{\sum_{i=1}^{N}\left[x(i) - y(i)\right]^2}\right)$. Де $x(i)$ – вихідний сигнал, що містить флуктуації, $y(i)$ – відфільтрований сигнал, тобто оцінка сигналу, «очищеного» від шуму, і, відповідно, різниця значень $|x(i) - y(i)|$ характеризує шумову складову (в разі ідеального фільтра). Розрахунки кількісних критеріїв доцільно проводити на додаток до візуальної оцінки якості фільтрації. Що стосується аналізу зображень коригуються таким чином: $E = \frac{1}{NM}\sum_{i=1}^{N}\sum_{k=1}^{M}\left[x(i,k) - y(i,k)\right]^2$,

$PSNR = 10\lg\left(\frac{255}{\sqrt{\frac{1}{NM}\sum_{i=1}^{N}\sum_{k=1}^{M}\left[x(i,k) - y(i,k)\right]^2}}\right)$. В даному випадку оцінюється так зване пікове відношення сигнал / шум «Peak Signal to Noise Ratio». На рис. 1 наведені характерні приклади залежностей середньоквадратичної помилки фільтрації від вибору базисної функції сімейства вейвлетів Добеши. Відповідно до рис. 1*а*, найменша помилка досягається при виборі базису D^{17} (Відносна помилка фільтрації 2.8%), а на рис. 1*б* - для вейвлета D^{13}. Незважаючи на те, що залежно, представлені на рис. 2, є в значній мірі «порізаними», вони також дозволяють зробити висновок про наявність мінімальної помилки, що досягається при відповідному виборі порогового значення.



а *б*

Рис. 1 – Залежно середньоквадратичної помилки фільтрації від вибору базисної функції сімейства вейвлетів Добеши при жорсткому варіанті завдання порогової функції і двох відносинах сигнал/шум: 30 дБ (*а*) і 3 дБ (*б*)



а *б*

Рис. 2 – Залежно середньоквадратичної помилки вейвлет-фільтрації з використанням вейвлетів Добеши D^{10} і жорсткого варіанта завдання порогової функції від величини порогового значення для траси сейсмограми при відносинах сигнал / шум 3 дБ (*а*) і 20 дБ (*б*)

Відповідно до рис. 2, при м'якому варіанті завдання порогової функції відбувається зниження помилки відновлення сигналу по його вейвлет-коефіцієнтами приблизно на 8% в порівнянні з жорстким варіантом. Ще один важливий момент, на який необхідно звернути увагу. Мінімум залежності помилки від величини С для м'якого варіанту досягається при менших значеннях С. Оскільки дана величина задає поріг для вейвлет-коефіцієнтів, які можуть бути обнульовані при фільтрації перешкод, зменшення С означає, що менша частина інформативних коефіцієнтів буде усуватися на етапі фільтрації. В результаті знижується ймовірність видалити коефіцієнти, які характеризують корисний сигнал, і, як наслідок, знижується ймовірність внесення випадкових спотворень. Даний висновок підтверджується додатковими розрахунками, проведеними при різних відносинах сигнал / шум. У всіх розглянутих випадках м'який варіант завдання порогової функції призводить до зниження ризику порогової фільтрації (рис. 3 *б*).

а *б*

Рис. 3 – Залежно середньоквадратичної помилки вейвлет-фільтрації при використанні вейвлетів Добеши D^{10} (*а*) і залежно оптимального порогового рівня від відносини сигнал / шум, дБ (*б*) для випадків м'якого (1) і жорсткого (2) варіантів завдання порогової функції

Таким чином, важливим завданням є вибір параметра С, який повинен проводитися з урахуванням рівня шуму в аналізованих експериментальних даних. До числа широко застосовуваних способів вибору відноситься універсальний пороговий рівень: $C = \sigma\sqrt{2\ln N}$, де σ – стандартне відхилення шуму, N – число вейвлет-коефіцієнтів ($N \geq 4$).При проведенні дискретного вейвлет-перетворення число коефіцієнтів змінюється в 2 рази при переході від одного рівня дозволу до іншого. З цієї причини можуть застосовуватися як підходи на основі глобального введення порогу, так і більш гнучкі підходи, що передбачають завдання різних порогових рівнів Сj в залежності від роздільної здатності j. Це дозволяє рекомендувати метод комплексного вейвлет-перетворення в якості ефективного інструменту очищення від перешкод сигналів і зображень різної природи.

УДК 004.056

Р.М. Минайленко, Н.М. Якименко, Т.Ю. Хільченко
aron70@ukr.net, yakimenko_n_m@ukr.net
Центральноукраїнський національний технічний університет, Кропивницький

ПЕРЕВАГИ РОЗРОБКИ ПАРАЛЕЛЬНОЇ ПРОГРАМИ З ВИКОРИСТАННЯМ MPI

В обчислювальних системах з розподіленою пам'яттю процесори функціонують незалежно один від одного. Для організації паралельних обчислень в таких умовах необхідно мати можливість розподіляти обчислювальне навантаження та організовувати інформаційну взаємодію (передачу даних) між процесорами. Рішення цих питань забезпечує інтерфейс передачі даних (message passing interface – MPI). В загальному плані, для розподілу обчислень між процесорами необхідно проаналізувати алгоритм розв'язку задачі, виділити інформаційні незалежні фрагменти обчислень, провести їх програмну реалізацію і потім розмістити отримані частини програми на різних процесорах. В рамках MPI прийнятий простіший підхід – для рішення поставленої задачі розробляється одна програма, яка запускається одночасно на виконання на всіх наявних процесорах. Для уникнення ідентичності обчислень на різних процесорах, можна підставляти різні дані для програми на різних процесорах та використовувати наявні в MPI засоби для ідентифікації процесора, на якому виконується програма (тим самим надається можливість організувати в обчисленнях в залежності від використовуваного програмою процесора). Такий спосіб організації паралельних обчислень отримав назву моделі "одна програма множина процесів" (single program multiple processes or SPMP).

Для організації інформаційної взаємодії між процесорами інформаційної взаємодії між процесорами в самому мінімальному варіанті достатньо операцій прийому і передачі даних (повинна існувати технічна можливість комунікації між процесорами - канали чи лінії зв'язку). В MPI існує ціла множина операцій передачі даних, які забезпечують різні способи пересилання даних, реалізують практично всі раніше розглянуті комунікаційні операції. Саме ці можливості є найбільш сильною стороною MPI. Намагання створення програмних засобів передачі даних між процесорами почали здійснюватись практично відразу з появою локальних комп'ютерних мереж. Проте ці засоби часто були часто незрозумілими і несумісними. Тобто одна з самих серйозних проблем в програмуванні – можливість перенесення програм при переведенні програмного забезпечення на інші комп'ютерні системи – проявлялась при розробці паралельних програм в максимальному ступені. Як результат, вже з 90 - х років XX ст. стали вживатися заходи із стандартизації засобів організації передачі повідомлень в багатопроцесорних обчислювальних системах. Початком робіт, що призвели до появи MPI, послужило проведення робочої наради із стандартів для передачі повідомлень в середовищі розподіленої пам'яті (the Workshop on Standards for Message Passing in a Distributed Memory Environment, Williamsburg, Virginia, USA, April 1992). За підсумками наради була утворена робоча група , пізніше перетворена в міжнародне товариство MPI Forum, результатом діяльності якого було створення і прийняття в 1994 р. стандарту інтерфейсу передачі повідомлень (message passing interface – MP) версії 1.0. В наступні роки стандарт MPI послідовно розвивався. В 1997 р. був прийнятий стандарт MPI версії 2.0.

Тепер можна пояснити значення поняття MPI. По – перше, MPI - це стандарт, якому повинні задовольняти засоби організації передачі повідомлень. По – друге – це програмні засоби, які забезпечують можливості передачі повідомлень і при цьому відповідають всі вимогам стандарту MPI. Так, за стандартом ці програмні засоби повинні бути організовані у вигляді бібліотек програмних функцій (бібліотека MPI) і повинні бути доступними для найбільш використовуваних алгоритмічних мов C та Fortran. Подібну "двоїстість" MPI слід враховувати при використанні термінології. Як правило, абревіатура MPI застосовується при згадуванні стандарту, а сполучення "бібліотека MPI" вказує ту чи іншу програмну реалізацію стандарту. Проте достатньо часто для скорочення позначення MPI використовується для бібліотек MPI, і, тим самим, для правильної інтерпретації терміну слід враховувати контекст.

Розробка паралельної програми з використанням MPI надає наступні переваги:

– дає змогу в значній мірі знизити гостроту проблеми перенесення паралельних програм між різними компонентами системи - паралельна програма, розроблена на алгоритмічній мові C чи Fortran з використанням бібліотеки MPI, як правило, працюватиме на різних обчислювальних платформах;

– сприяє підвищенню ефективності паралельних обчислень, оскільки нині практично для кожного типу обчислювальних систем існують реалізації бібліотек MPI, які враховують можливості комп'ютерного обладнання;

– зменшує складність розробки паралельних програм, оскільки більша частина основних операцій передачі даних передбачається стандартом MPI, з іншого боку, на даний час існує велика кількість бібліотек паралельних методів, створених з використанням MPI.

УДК 004.031 42

SH.F. Mansurova
sahane.mansurova@gmail.com
Institute of Information Technology of ANAS, Baku, Azerbaijan

SOME ISSUES OF APPLICATIONS ARTIFICIAL INTELLIGENCE IN THE FRAMEWORK OF SCIENCE 4.0

With the application of Industry 4.0, the development trends in the technological sphere continue with increasing dynamics.The article explores new technological solutions and the problems they bring. Thus, the rapid growth of heterogenous data makes it difficult to store and process it in the traditional way. Delays in traditional data processing create serious difficulties in real-time decision-making. For this reason, machine learning methods were discussed to make the most of the data obtained through the application of technologies used in the context of Industry 4.0.

As a result of rapid development in accordance with the requirements of modern era, the application of information and communication technologies (ICT) in many areas of scientific activity has led to fundamental changes. These changes bring new opportunities along with them and the large-scale application of these opportunities lays the foundation for the concept of the “Industry 4.0” revolution.This revolution is unlike any previous experience in terms of complexity, scope and scale. It leads to the emergence and development of large-scale technological breakthroughs, including nanotechnology, biotechnology and many other fields [1]. New technological concepts have created development perspectives that will be important for various fields of science. The revolutions that take place within this concept, in turn, are accompanied by technological innovations, and the acquisition of knowledge is related to the manifestations and opportunities they create. The occurrence of Industry 4.0 revolution is related to the development of Internet of Things (IoT), cyber-physical systems (CPS), artificial intelligence (AI), cloud and Big data) technologies.

The application of Industry 4.0 technologies in the scientific environment stimulates the emergence of new development trends [2].Thus, the new opportunities created by Industry 4.0 in science have led to the emergence and development of the term “Science 4.0”. The application of IoT, CPS, AI etc. technologies within Science 4.0leads to rapid data growth.Rapid digitalization and evolving intelligent analysis technologies have caused the emergence of the “Big Data” phenomenon.This phenomenon has common characteristics, regardless of the areas in which it is applied. These characteristics reflect the main problems. Big data creates new opportunities through a new approach to research of the potential value of data, storage and data analysis.Data analysis in the Big Data environment is understood as making more optimal decisions from the original data in different formats, aimed at solving a specific problem, minimizing costs, saving time and offering new types of services etc. The technologies used within Science 4.0make Big Data even more complicated.Machine learning (ML) is considered one of the most relevant computing paradigms to make use of the scientific data obtained from these technologies. MLalgorithms has emerged as a result of the development of AI. ML helps machines and smart devices extract useful information from device- or human-generated data. In addition, a large amount of data obtained can also be used for forecasting and assessment. ML algorithmsandmethods are widely used in various areas of application such as fraud detection, bioinformatics, malware detection, identification and speech recognition. ML algorithms build behavioral models using mathematical techniques on large datasets.Having a multidisciplinary nature, ML has its roots in engineering and many fields of science including artificial intelligence, optimization theory, information theory and cognitive science. These algorithms can be implemented in the following four directions [3, 4]:

- Supervised Learning;
- Unsupervised Learning;
- Semi-supervised Learning;
- Reinforcement Learning.

Supervised learningis performed when specific targets are setwith certain input data. For this type of learning, firstly the data is labeled, then the labeled data is trained. That is, the data labeled here refers to the input and the desired output data. This type of learning automatically sets rules from the data set and defines different classes. In the end predicts which class the given element belongs to. This isalgorithms are the most commonly used algorithms.These algorithms include KNN, Naive Bayes, Regression, Random forest, Decision algorithms [5].

KNN, in addition to being a simple algorithm,is used to solve classification and regression problems.This algorithm searches for the nearest neighbors in the given data every time and classifies according to it.

The algorithm calculates the probability of the newly entered data for each situation and classifies it according to the highest probability.

Decision trees (DT) is a supervised learning algorithm used mainly to solve classification problems.It applies to both categorical and constant dependent variables. The Decision tree algorithm divides the overall data into two or more groups based on the most important or independent variables. Decision tree is easy to understand, and strong in interpretability. Decision tree can handle unrelated features and make feasible and good results for large data sources in a relatively short time. Overfitting is prone to occur. Moreover, Decision tree is easy to ignore the correlation between data.

Regression:Regression analysis method is performed to determine correlation between two or more variables having cause effect relations &to make prediction for the topic by using relations. Regression methods fall within the category of supervised ML The regression using single independent variable is called univariate regression analysis while the analysis using more than two independentvariableis called multivariate Regression analysis. Linear Regression methodsconsists of first Loading the Data& then Exploring the Data. Next that we have to do Slicing the Data then Train and Split Data to Generate the Model. Finally evaluate the accuracy.There are several types of regression and these types includeSimple Linear Regression, Multiple Linear Regression, Polynomial Regression, Support Vector Regression, Decision Tree Regression, Random Forest Regression. The easiest method is linear regression, where linear mathematical equation ($y = m * x + b$) is used to model the data set[6].

The following is an example of the application of AI and ML technologies to scientific fields.

Biomonitoring: Various state drives to trace probable outbreaks of diseases by using ML algorithms. The summary gathers data on admissions to hospital emergency rooms. The ML program is designed using agreed patient profiles to identify aberrant symptoms, their trends, and the number of areal. Research is ongoing to incorporate some additional data into the system, such as purchasing history of record medicines to provide more training data. only machine learning techniques can manage the complexity of this kind of complex and dynamic data sets effectively [7].

Astronomy:The application of AI and ML technologies in astronomy - the discovery of extrasolar planetsand gravitationally-lensed systems; discovery and classification of transient object; forecasting solar activity; assignment of photometric redshifts within large-scale galaxy surveys; and the classification of gravitational wave signals and instrumental noise [8].

It is noted that the widespread application of the technologies that make up the concept of Industry 4.0 in the scientific environment has led to the emergence of “Science 4.0” and the exponential growth of scientific data. The importance of applying more optimal methods and techniques with the actualization of the issue of acquiring new scientific knowledge is emphasized. The main advantage of the methods used in these analysis technologies is that they are faster than traditional methods.

References

1. A.G. Frank, L.S. Dalenogare, N.F. Ayala. Industry 4.0 technologies: Implementation patterns in manufacturing companies, International Journal of Production Economic,Vol.210, № 1, pp.15–26, 2019.

2. T.X. Fataliyev, S.A. Mehdiyev. Integration of Cyber-Physical Systems in EScience Environment: State-of-the-Art, Problems and Effective Solutions, I.J. Modern Education and Computer Science, №9,pp. 35-43,2019.

3.I.Lee, Y.J.Shin. Machine learning for enterprises: Applications, algorithm selection, and challenges. Business Horizons, Vol.63, Issue 2,pp. 157-170, 2020.

4.F.Hussain, R.Hussain, S.A.Hassan, and E.Hossain. Machine Learning in IoT Security: Current Solutions and Future Challenges, IEEE Communications Surveys & Tutorials, Vol.22, Issue 3, pp. 1-23, 2019.

5. Rongchen Zhu, Xiaofeng Hu, Jiaqi Hou, Xin Li, Application of machine learning techniques for predicting the consequences of construction accidents in China, Process Safety and Environmental Protection, Vol. 145 , pp.293–302, 2021.

6. Vidya S. Kadam, Shweta Kanhere, Shrikant Mahindrakar, Regression Techniques in Machine Learning &Applications: A Review. International Journal for Research in Applied Science & Engineering Technology (IJRASET), № 10, pp. 826-830, 2020.

7. Bilal Abdualgalil, Sajimon Abraham, Applications of Machine Learning Algorithms and Performance Comparison: A Review, International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE),pp. 1-6, 2020.

8. Christopher J. Fluke, Colin Jacobs, Surveying the reach and maturity of machine learning and artificial intelligence in astronomy, pp.1-4, 2019.

УДК 004.2:004.9

О.П. Доренський, О.С. Дробко
ms.alenas@gmail.com
Центральноукраїнський національний технічний університет, Кропивницький

СТРУКТУРНА МОДЕЛЬ МУНІЦИПАЛЬНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ МЕДИЧНИХ ПОСЛУГ

Розвиток сучасних технологій, популяризація проекту “Країна в смартфоні”, намагання органів місцевого самоврядування покращити співпрацю з населенням стали передумовою ініціативи зі створення інформаційних систем, які підвищують ефективність надання громадянам муніципальних послуг. У праці [1] запропоновано структуру й методологічні засади реалізації мобільного застосунку муніципальної інформаційної системи (ІС) медичних послуг. Метою цієї роботи є синтез структурної моделі означеної ІС.

Одним із основоположних артефактів розроблення будь-якої ІС є структурна модель. Синтез структурної моделі для муніципальної інформаційної системи медичних послуг потребує чіткого визначення основних структурних елементів відповідно до архітектури й методологічних засад створення системи [1]. Основними елементами даної ІС виступають програмне забезпечення клієнта та комплекс інформаційних сервісів, що зберігаються в мережі інтернет. Проте такий рівень деталізації є недостатнім для побудови структурної схеми, тому необхідно визначити складові цих елементів. Отже, пропонується програмне забезпечення клієнта реалізувати з таких структурних елементів: 1) UI, 2) бізнес-логіка, 3) навігація, 4) нетворк, 5) аналітика, 6) робота з мапою. Разом з тим, елементами комплексу інформаційних сервісів слід визначити: 1) сервер (для зв’язку з БД), 2) Firebase, 3) Google Maps (рис. 1).

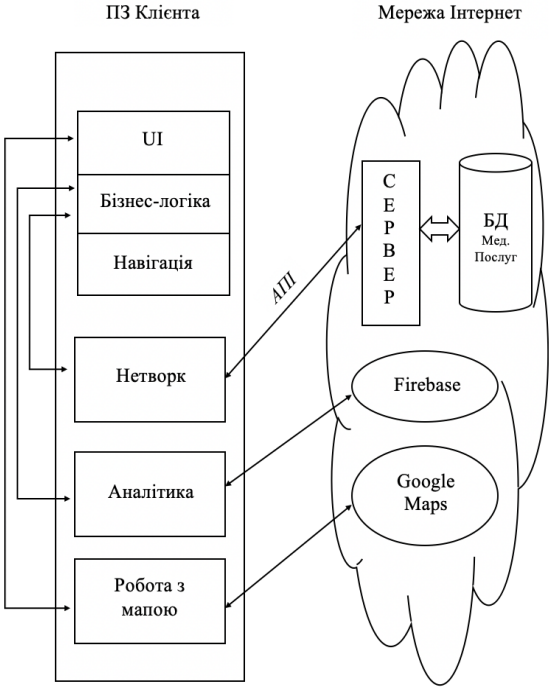


Рис. 1. Структурна модель мобільного застосунку муніципальної ІС медичних послуг

Окрім означеного вище, слід визначити типи зв’язку між елементами. Комунікація з Google Maps та Firebase забезпечуються бібліотеками цих сервісів, що інтегруються в клієнтське ПЗ. А зв’язок з сервером забезпечується за допомогою АПІ (сукупність засобів та правил, що уможливлюють взаємодію між окремими складниками програмного забезпечення [2]).

Перспективою подальших розвідок є реалізація функціональної моделі на основі запропонованої структурної моделі застосунку муніципальної інформаційної системи медичних послуг.

Список літератури

1. Дробко О. С. “Структура і методологічні засади реалізації мобільного застосунку муніципальної інформаційної системи медичних послуг”, *Комп’ютерна інженерія і кібербезпека: досягнення та інновації*: матеріали ІІ Всеукр. наук.-практ. конф. здобувачів вищої освіти й молодих учених, м. Кропивницький, 25–27 листоп. 2020 р., с. 23-24. URL: http://dspace.kntu.kr.ua/jspui/handle/123456789/10346.

УДК 004.89

В.И. Слюсар
swadim@ukr.net
главный научный сотрудник, д.т.н., проф.
Центральный научно-исследовательский институт вооружения и военной техники Вооружённых Сил Украины, Киев

АНАЛИЗ ПРЕДПОЧТЕНИЙ НА ОСНОВЕ ТОРЦЕВОГО ПРОИЗВЕДЕНИЯ МАТРИЦ

Обработка больших данных является одним из важных направлений применения технологий искусственного интеллекта. В ряде приложений существенная роль при этом отводится поиску статистических закономерностей, например, в интересах предсказания действий на основе анализа предпочтений. В этой связи актуальной задачей является автоматизация процедуры вычисления предпочтительных шаблонов по всему набору предпочтений в интересах раннего распознавания намерений. Целью работы является описание метода решения задач статистического анализа предпочтений на основе предложенного автором в 1996 г. торцевого произведения матриц [1 - 3].

Предположим, что имеется 3 человека, указывающих свой предпочтительный объект в исходном множестве из четырёх объектов. При этом потребуем, чтобы в процессе выбора отдавать предпочтение какому-либо из объектов можно было лишь один раз. Для простоты рассмотрим три последовательных процедуры отдания предпочтений, пример которых представлен в табл. 1.

Таблица 1

Порядковый номер анкетируемого	1-е предпочтение	2-е предпочтение	3-е предпочтение
Человек 1	Объект 3	Объект 1	Объект 4
Человек 2	Объект 2	Объект 3	Объект 1
Человек 3	Объект 2	Объект 4	Объект 1

Чтобы сохранить преемственность по отношению к решению задач анализа текста в качестве объектов выбора рассмотрим четыре слова, образующих текстовый фрагмент из трех предложений, рассмотренных в [4]: 1) I like math; 2) You like math; 3) I like you.

Составим для каждого из последовательных предпочтений так называемую матрицу инцидентности [4]. Ее строки будут соответствовать конкретному человеку, а столбцы - выбранному слову. При этом единичные элементы в каждой строке соответствуют слову, которому было отдано предпочтение, тогда как для всех остальных слов будут стоять нули. Количество столбцов должно соответствовать максимальному количеству слов в рассматриваемом текстовом множестве. В указанном выше фрагменте наибольшее количество слов – четыре. Прежде чем непосредственно перейти к матрицам инцидентности, составим с учетом сказанного для наглядности таблицу, соответствующую результатам последовательных предпочтений (табл. 2).

Таблица 2

Порядковый номер анкетируемого	X_1=I	X_2=like	X_3=math	X_4=you
Первое предпочтение				
1	0	1	0	0
2	1	0	0	0
3	1	0	0	0
Второе предпочтение				
1	1	0	0	0
2	0	1	0	0
3	0	0	0	1
Третье предпочтение				
1	0	0	1	0
2	0	0	0	1
3	0	1	0	0

Отсюда, получим матрицы инцидентности вида:

$$X=\begin{bmatrix}0&1&0&0\\1&0&0&0\\1&0&0&0\end{bmatrix};\ Y=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\end{bmatrix};\ Z=\begin{bmatrix}0&0&1&0\\0&0&0&1\\0&1&0&0\end{bmatrix}$$

Перейдем к задаче анализа сочетаний объектов в последовательности предпочтений. Как указано в [4], для этого необходимо воспользоваться торцевым произведением матриц. В частности, согласно [4], матрица совместной встречаемости для анализа тройных сочетаний может быть сформирована на основе исходной матрицы инцидентности и ее версии в виде торцевого произведения (символ □):

$$C = X^T (Y \square Z) = \left[\begin{array}{cccc} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{array}\right]^T \left[\begin{array}{cccc|cccc|cccc|cccc} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{array}\right] =$$

$$= \left[\begin{array}{ccc} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{array}\right] \left[\begin{array}{cccc|cccc|cccc|cccc} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{array}\right] = \left[\begin{array}{cccc|cccc|cccc|cccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

Полученная в результате матрица имеет размерность 16×4 и может быть представлена в виде 4 блоков, каждый из которых соответствует одному из слов в парных словосочетаниях (см. табл. 3).

Таблица 3

	Y_1=I				Y_2=like				Y_3=math				Y_4=you			
	Z_1	Z_2	Z_3	Z_4	Z_1	Z_2	Z_3	Z_4	Z_1	Z_2	Z_3	Z_4	Z_1	Z_2	Z_3	Z_4
X_1	0	0	0	0	0	0	0	**1**	0	0	0	0	0	**1**	0	0
X_2	0	0	**1**	0	0	0	0	0	0	0	0	0	0	0	0	0
X_3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
X_4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Цифры в роли элементов матрицы C характеризуют частоту появления конкретных троек слов в исследуемой последовательности предпочтений с учетом их порядка в последовательности. Например, из первого блока матрицы следует, что набор предпочтений ($X_2Y_1Z_3$) встречается однажды, равно как ($X_1Y_2Z_4$) и ($X_1Y_4Z_2$). Остальные комбинации предпочтений не наблюдались. Фактически табл. 4 отражает диаграммы предпочтений, выбранных пользователями.

Альтернативное решение рассмотренной задачи позволяет получить переход к тройному торцевому произведению матриц инцидентности: I3=X □ Y □ Z. Для анализируемого фрагмента текста такое произведение приводит к 16-блочной матрице, состоящей из 4 квартетов блоков:

$$\left[\begin{array}{cccc|cccc|cccc|cccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{array}\right]$$

$$\left[\begin{array}{cccc|cccc|cccc|cccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right] \cdot$$

Первый блок полученной матрицы соответствует тройкам $X_1Y_1Z_m$, а последний - $X_4Y_4Z_m$ (m=1,…,4). Совокупная статистика по всем предпочтениям может быть получена путем суммирования строк матрицы X □ Y□ Z, что эквивалентно операции умножения её на вектор-строку единиц:

$$\mathbf{1}^T \text{I3} = \mathbf{1}^T (X \square Y \square Z).$$

Аналогичный результат может быть получен на основе квадратичной формы торцевого произведения: $\mathbf{1}^T$ (X □ Y□ Z)=diag[(X □ Y □ Z) ^{T} (X □ Y □ Z)], где diag(C) – вектор-строка из диагональных элементов матрицы C. Указанные соотношения позволяют получить все тот же набор предпочтений, в котором отсутствуют любые комбинации, содержащие X_3 и X_4, тогда как для X_1 и X_2 выбор однократно выпал на сочетания ($X_1Y_2Z_4$), ($X_1Y_4Z_2$) и ($X_2Y_1Z_3$). В общем случае наибольший результат суммирования строк матрицы X □ Y□ Z будет соответствовать комбинации объектов выбора, на которую пришлось максимальное количество предпочтений.

Представленный метод обработки результатов выбора позволяет узнать о “предпочтительных” шаблонах (паттернах) на основе первого предпочтения, например, “если кто-то выберет X в качестве первого предпочтения, то второй выбор, скорее всего, будет...”. Рассмотренная процедура вычисления шаблонов предпочтений по всей совокупности статистик позволяет автоматизировать соответствующий анализ. Это важно при большом количестве элементов выбора и соответствующих ему этапов, поскольку вручную сделать аналогичные подсчёты было бы сложно. В то же время, если предпочтения формулируются в виде коротких ответов из нескольких слов, то применению рассмотренного метода должна предшествовать предварительная токенизация словесного описания выбора.

Список литературы

1. Слюсар В.И. Торцевые произведения матриц в радиолокационных приложениях// Известия высших учебных заведений. Радиоэлектроника.- 1998. - Том 41, № 3.- С. 71 - 75.

2. Слюсар В.И. Семейство торцевых произведений матриц и его свойства// Кибернетика и системный анализ. – 1999.- Том 35; № 3.- С. 379-384.- DOI: 10.1007/BF02733426

3. Основы военно-технических исследований. Теория и приложения. Том. 2. Синтез средств информационного обеспечения вооружения и военной техники. / А.И. Миночкин, В.И. Рудаков, В.И. Слюсар. – Киев:«Гранмна, 2012. – С. 7 – 98, 354 – 521.

4. Слюсар В.И. Применение торцевого произведения матриц в задачах обработки естественного языка. //Збірник наукових праць XIX Міжнародної наукової конференції «Нейромережні технології та їх застосування НМТіЗ-2020». - Краматорськ. -2020 . - С. 156 - 162. - DOI: 10.13140/RG.2.2.31568.53762.

УДК 004.738.5

Н.В. Ламекін, В.О. Кривоконєв, Л.І. Поліщук
jjpp1605@gmail.com, vladkryvokoniev@gmail.com, pli_80@ukr.net
Центральноукраїнський національний технічний університет, Кропивницький

ПЕРЕВАГИ ВИКОРИСТАННЯ ХМАРНИХ ОБЧИСЛЕНЬ

Хмарними обчисленнями називають надання різноманітних послуг через мережу Інтернет. Це відноситься до інструментів та застосунків, таких як зберігання даних, серверів, баз даних, мереж та програмного забезпечення.

Хмарне сховище дозволяє зберігати файли у віддаленій базі даних замість того, щоб зберігати їх на локальному запам'ятовуючому пристрої,. До тих пір поки користувач має доступ до Інтернету, він має доступ до програмного забезпечення та даних у хмарі. Хмарні технології – це популярне рішення для людей та бізнесу з ряду причин, включаючи економію витрат, підвищення продуктивності, швидкості та ефективності.

IaaS (Інфраструктура-як-послуга), PaaS (Платформа-як-послуга) і SaaS (Програмне-забезпечення-як-послуга) - три найпоширеніші моделі хмарних служб, і це не рідкість для організації використовувати всі три. Однак часто існує плутанина серед трьох і того, що входить до кожного.

SaaS - також відоме як хмарне програмне забезпечення або хмарні програми - це прикладне програмне забезпечення, яке розміщується в хмарі, і до якого ви отримуєте доступ та користуєтесь через веб-браузер, спеціальний настільний клієнт або API, який інтегрується з настільною або мобільною операційною системою. У більшості випадків користувачі SaaS сплачують щомісячну або річну плату за підписку; деякі можуть пропонувати ціноутворення "на виплату" залежно від вашого фактичного використання.

PaaS надає розробникам програмного забезпечення платформу на вимогу - апаратне забезпечення, повний стек програмного забезпечення, інфраструктуру та навіть засоби розробки - для запуску, розробки та управління програмами без витрат, складності та гнучкості утримання цієї платформи на місці.

IaaS надає доступ до вимог до основних обчислювальних ресурсів - фізичних та віртуальних серверів, мереж та сховищ - через Інтернет на основі оплати. IaaS дозволяє кінцевим споживачам масштабувати та скорочувати ресурси за необхідності, зменшуючи потребу у великих, попередніх капітальних витратах.

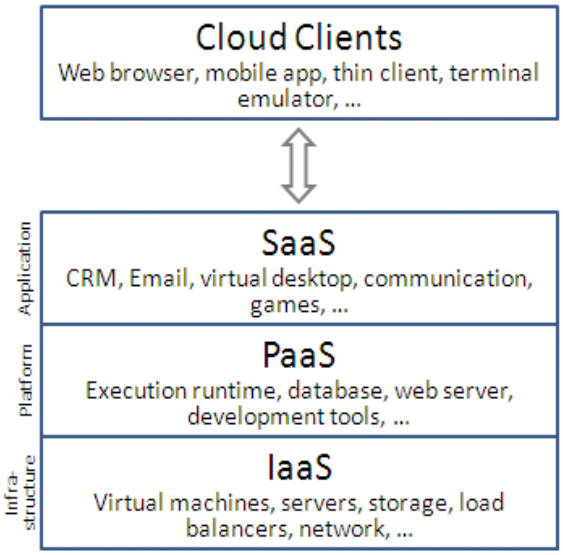


Рис. 1. Моделі хмарних обчислень, розташовані у вигляді шарів у стеку

Програмне забезпечення засноване на технологіях хмарного обчислення (рис.1), надає ряд переваг, до яких можна віднести можливість використовувати програмне забезпечення з будь-якого електронного пристрою, як з власного застосунку, так і з браузера. Як результат користувач має можливість перенести свої файли та налаштування на інші свої прилади. Завдяки сервісам хмарного обчислення користувач має можливість переглядати свою електронну скриньку з будь-якого комп’ютера, зберігати свої файли використовуючи сервіси на кшталт Google Drive або Dropbox. Хмарні технології надають компаніям величезний потенціал для збереження коштів. З появою хмарних обчислень компаніям більше не потрібно купувати та підтримувати серверні центри та IT-відділи.

УДК 004.457

В.В. Сидоренко, Р.М. Минайленко, С.В. Михайлов
vvsidorenko37@gmail.com, aron70@ukr.net, svmihailov@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький

ВИКОРИСТАННЯ ПРОГРАМНИХ МОДЕЛЕЙ ПРИСТРОЇВ В ПРОЦЕСІ ВИВЧЕННЯ ДИСЦИПЛІНИ “КОМП’ЮТЕРНА СХЕМОТЕХНІКА”

Впровадження інформаційних освітніх технологій у навчальних закладах України є одним з головних чинників у підготовці високоякісного фахівця. Найбільш характерною ознакою освіти на сучасному етапі розвитку є її інформатизація, обумовлена насамперед розповсюдженням у навчальних закладах сучасної комп’ютерної техніки та програмного забезпечення, використанням можливостей Інтернет, набуттям і накопиченням фахівцями досвіду використання інформаційних технологій (ІТ) у своїй діяльності .

Дослідження показали, що на сьогоднішній день у вітчизняній системі освіти використовуються апаратні емулятори (стенди) та програмні імітаційні моделі, призначені для вивчення обчислювальної техніки, її складових і процесів, які в ній протікають. Програмні емулятори дозволяють візуалізувати процес програмування мікросхем у спрощеному вигляді, а також процеси системи.

Так, наприклад, програма-емулятор інтервального таймера i8253 дозволяє візуалізувати процес програмування та функціонування цієї мікросхеми. Реалізація емулятора повністю відповідає внутрішній будові та принципам функціонування реальної схеми та системи (рис.1).

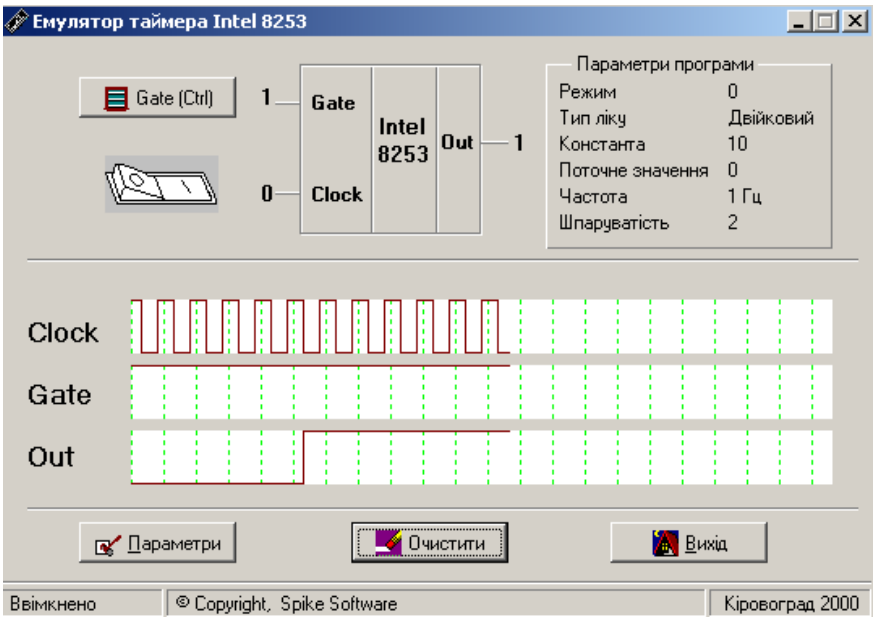


Рис.1. Емулятор таймера i8253

Програмні моделі демонструють функціональні взаємозв’язки і взаємодію вказаного пристрою, відображають результати його програмування, а також дозволяють користувачу спостерігати за всіма функціями та внутрішніми процесами.

Робота програмного забезпечення моделей дозволяє також здійснювати спостереження за процесом у необхідному масштабі часу. В моделі реалізовано покроковий режим роботи, що наочно відображує принцип функціонування пристрою та стане невід’ємним засобом для кращого розуміння і вивчення відповідної теми навчальної дисципліни.

Крім того, програми-емулятори дають можливість провести дослідження та проаналізувати відповідні системи або пристрої. Демонстраційний експеримент не вичерпує всіх можливостей активного сприйняття студентами досліджуваних явищ, не завжди забезпечує отримання ними дійових знань, оскільки його тільки спостерігають, а не проводять самі. А тому демонстрації із залученням програм-емуляторів потрібно доповнювати виконанням студентами лабораторних робіт з їх допомогою. Програмний емулятор дозволяє проводити відповідну роботу і самостійно (позааудиторно), без залучення викладача. Це дозволяє розширити область зв’язку теорії з практикою, привчити студентів до самостійної дослідницької роботи. Крім того, можливість проводити досліди віддалено від ВНЗ вказує на перспективу використання емуляторів для дистанційного навчання. Програмні моделі загалом дають можливість організувати якісний навчальний процес підготовки фахівців з обчислювальної техніки та комп’терних систем.

УДК 519.87, 519.85

О.Д. Міхнова[1], С.М. Коваленко[2], В.І. Древіна[1]
mikhnova@khntusg.info, svetkovalenko@khntusg.info, barbarast350000@gmail.com
[1] Харківський національний технічний університет сільського господарства імені Петра Василенка,
[2]Національний технічний університет «Харківський політехнічний інститут», Харків

ОПТИМІЗАЦІЙНА МОДЕЛЬ ВИБОРУ АПАРАТНИХ ЗАСОБІВ В ПРОЦЕСІ АВТОМАТИЗАЦІЇ СКЛАДНИХ ОБ'ЄКТІВ

В процесі автоматизації роботи людей на підприємстві обов'язково виникає задача пошуку найоптимальнішого плану використання матеріальних ресурсів при забезпеченні достатнього рівня якості апаратних засобів, що дозволяють зробити цю автоматизацію. Мова може йти від обрання складових персональних комп'ютерів до більш спеціалізованого обладнання, яке безпосередньо приймає участь у технологічному процесі. В будь-якому випадку, виникає потреба у мінімізації видатків, але при цьому необхідно зберігати не тільки безпеку роботи людей на підприємстві, але й поліпшувати виконання їх функцій при вивченні взаємодії та можливого впливу на інших користувачів і технічні засоби. Ці зв'язки пропонується встановити та формалізувати за допомогою лінійної моделі оптимізації.

Абстрактна математична модель пошуку таких невід'ємних значень вектора невідомих змінних $X = \left| x_j \right|_n$, які задовольняють заданій системі лінійних обмежень

$$a_{11}x_1 + a_{12}x_2 + a_{1j}x_j + ... + a_{1n}x_n \geq b_1,$$
$$. \quad .$$
$$a_{k1}x_1 + a_{k2}x_2 + a_{kj}x_j + ... + a_{kn}x_n \geq b_k,$$
$$. \quad .$$
$$a_{k+l,1}x_1 + a_{k+l,2}x_2 + a_{k+l,j}x_j + ... + a_{k+l,n}x_n \geq b_{k+l}, \text{ де}$$

$x_j \geq 0;\ j = 1, 2, ..., n;\ m = k + l$. При цьому задана функція мети (або цільова функція) набуває максимального (чи мінімального значення:

$$F(X) = c_1x_1 + c_2x_2 + c_jx_j + ... + c_nx_n \to \max(\min),$$

де $\left\| a_{ij} \right\|_{m \times n}, \left| b_i \right|_m, \left| c_j \right|_n$ – задані параметри [1].

Побудова такої моделі та ідентифікація вагомих складових системи дозволяє в подальшому виконувати аналіз даних за допомогою більш просунутих методів, в тому числі методом регресійної та кореляційної оцінки складових моделі [2]. Окрім використання статистичних методів аналізу даних та видобування знань, можна застосувати динамічне програмування, нелінійні методи оптимізації, навіть генетичні алгоритми або нейронні мережі із самонавчанням [3, 4]. Це дозволить не тільки оцінити існуючі можливості складної організації, але й отримати прогностичні рішення.

Найпростішим прикладом роботи даної моделі є відбір параметрів, наприклад, монітору, таких як: частота оновлення картинки, потужність, тип матриці та час її реакції, діагональ, роздільна здатність, фактична вага, співвідношення сторін екрану, яскравість, інтерфейс підключення, підтримка різноманітних технологій та стандартів передачі даних, виробник і навіть термін гарантії. Зрозуміло, що деякі параметри будуть високо корелювати між собою, наприклад, певний виробник дає на свою продукцію в основному однаковий гарантійний термін. Тобто такі атрибути доцільно вилучати із аналізу, аби не ускладнювати модель. Саме для цього необхідні додаткові процедури з використанням більш вузькоспеціалізованих методів. Але запропонована для використання у даному випадку модель є найбільш універсальною.

Список літератури

1. Y.E. Megel, et.al., Operations Research. Харків, Україна: Міськдрук, 2015.
2. J. Fox, Applied Regression Analysis and Generalized Linear Models. Third Edition. Hamilton, Canada: McMaster University, 2015.
3. S. Wright, J. Nocedal, Numerical Optimization. New York, USA: Springer-Verlag, 2006.
4. B. Marr, M. Ward, Artificial Intelligence in Practice: How 50 Successful Companies Used AI and Machine Learning to Solve Problems. United Kingdom, Chichester: Wiley, 2019.

УДК 004.056

О.В. Оришака, А.К. Марченко
oryhsaka@gmail.com,nazarrodead@gmail.com
Центральноукраїнський національний технічний університет, Кропивницький

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ HTML ЯК ІНСТРУМЕНТА ДЛЯ ФОРМУВАННЯ СКЛАДНИХ ТЕКСТОВИХ ДОКУМЕНТІВ

Під визначенням «складний текстовий документ» автори розуміють текст з таблицями, формулами, гіперпосиланнями, графічними та іншими мультимедійними елементами. Під визначенням «документи» в цій статті автори розуміють на увазі звіти, статті, книги, web-публікації і т.п. Під визначенням «html» автори мають на увазі не тільки саму «мову гіпертекстової розмітки» (від англ. HyperText Markup Language), а html в комплекті з CSS (від англ. Cascading Style Sheets - каскадні таблиці стилів).

У нашій країні, як і в багатьох інших країнах світу, для підготовки текстових документів зараз найчастіше використовується текстовий процесор MS Word. Такий підхід має свої переваги і недоліки. До переваг можна віднести: широке поширення цього програмного продукту і відносну легкість використання для підготовки невеликих (об'ємом в кілька сторінок) текстових документів.

Про недоліки такого підходу можна віднести пропрієнтарность і, як наслідок, закритість сирцевого коду програми, низька безпека і надійність (особливо у складних документах обсягом понад 100 сторінок), відсутність повноцінної міжплатформовості (cross-platform). Далека від ідеалу можливість формувати документи для розміщення в мп'ютерних мережах.

З іншого боку, html же була с самого спочатку створена для роботи у мережі.

Безпосереднім результатом застосування html як інструмента для формування складних текстових документів є простий текстовий файл (не бінарний), який, відповідно, не має недоліків бінарного, зокрема, низької надійності. Більш того, такий файл практично непорушний і його можна використовувати як для друку документів, так і для web-публікацій.

Мова html динамічно розвивається, а з появою CSS вийшла на новий рівень.

І html і CSS добре документовані, сирцевий код відкритий, а також є можливість враховувати не тільки вимоги до оформлення документів того чи іншого видавництва, а й особливості web-публікацій.

Прикладом такої web-публікації може служити список наукових та навчально-методичних робіт, складений за *Формою 11,* який опублікуван за адресою: http://www.vvv96.narod.ru/mat/spis.html

В розглянутому прикладі файл spis.html містить опис стилів CSS, яке розміщене у тегі <style>. За допомогою таблиці стилів CSS є можливість вказувати властивості (вигляд) одного і того ж документа в різних умовах, наприклад, вид документа на екрані комп'ютера і мобільного телефону, вид при друкуванні (розбивка на сторінки) і т. д.

Так як вищезгаданий файл документа є структурованим текстом, причому явно структурованим, то він може з успіхом застосовуватися в самих різних сферах, починаючи від автоматичного озвучення тексту за допомогою відповідного програмного забезпечення і закінчуючи конвертацією (експортом) в pdf, jpg, etc. формати.

Виходячи з усього вищесказаного, перспективи використання html як інструмента для формування складних текстових документів вбачаються самими обнадійливими.

Список літератури

1. Оришака О.В., Марченко К.М. Підготовка документів за допомогою Свободного програмного забезпечення : тези доп. Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих учених «Напрями економічного зростання та інноваційного розвитку підприємства» : – Кропивницький: ЦНТУ. – 2020. – С. 25-26.

2. Кононенко Л.В., Назарова Г.Б., Оришака О.В. Організація обліку і аудиту розрахунків за податками та платежами в умовах використання сучасного інформаційного забезпечення. Вісник Чернівецького торговельно-економічного інституту. Економічні науки – Номер I-II (77-78) – Чернівці: Вид-во ЧТЕІ КНТЕУ. –2020.–С. 194-202. URL: http://chtei-knteu.cv.ua/herald/content/download/archive/2020/v1_2/17.pdf

УДК 004.9, 004.056

Н.В. Ламекін, В.О. Кривоконєв, Л.В. Константинова
jjpp1605@gmail.com, vladkryvokoniev@gmail.com, liliyashel1976@gmail.com
Центральноукраїнський національний технічний університет, Кропивницький

ДОСЛІДЖЕННЯ ЗАСТОСУВАННЯ ДОПОВНЕНОЇ РЕАЛЬНОСТІ

Доповнена реальність або Augmented Reality(AR) - термін, що виник у сфері IT, яким спочатку позначали технологію накладання віртуальної інформації на навколишній світ в режимі реального часу. Висока швидкість поширення AR дає багато можливостей її використання в різних галузях, в тому числі й для кібербезпеки, тому дослідження доповненої реальності є актуальним на даний час.

Доповнену реальність (ДР) часто приймають за віртуальну реальність (ВР). Основна відмінність між ними полягає в тому, що, віртуальна реальність замінює все реальне середовище на штучне, а доповнена реальність застосовується в прямому огляді наявного реального середовища й додає в нього такі елементи, як звуки, відео чи графіку. Голова компанії Apple Тім Кук заявив, що саме доповнена реальність володіє достатнім потенціалом для того, щоб змінити світ [1].

Термін доповнена реальність був введений ще в 1990 році дослідником Томом Коделом, і одне з перших комерційних застосувань цієї технології було на телебаченні та у військовій галузі [2]. По мірі того, як світ рухався до того, щоб ставати все більш керованою технологією, ДР стала дедалі помітнішою у багатьох сферах, розгортаючи свою другу хвилю та наближаючи свій зв'язок до інтерактивної концепції. У міру розвитку технології з’являється кілька нових тенденцій у доповненій реальності. Коли застосовується пристрій або додаток, що увімкнений за допомогою технології ДР, апаратне забезпечення пристрою або додатку робить зображення об'єкта, передаючи його програмі комп'ютерного зору, яка потім обробляє зображення, щоб зібрати всі відповідні дані, такі як виміри об'єкта, будь-які інші об'єкти, що знаходяться на одній поверхні, одночасно обчислюючи віддаленість цих та інших об'єктів від основного об'єкта у фокусі. Застосовуючи ці уявлення, пристрій з підтримкою ДР розробляє та створює віртуальну інформацію, яка буде служити накладанням на реальний об’єкт, забезпечуючи унікальний досвід клієнтів.

За останні роки доповнена реальність сильно розвинулася. Однак світ доповненої реальності не обмежується лише цікавими фільтрами Snapchat, які можна отримати для застосування на смартфонах, або грою в Pokémon Go (рис. 1).

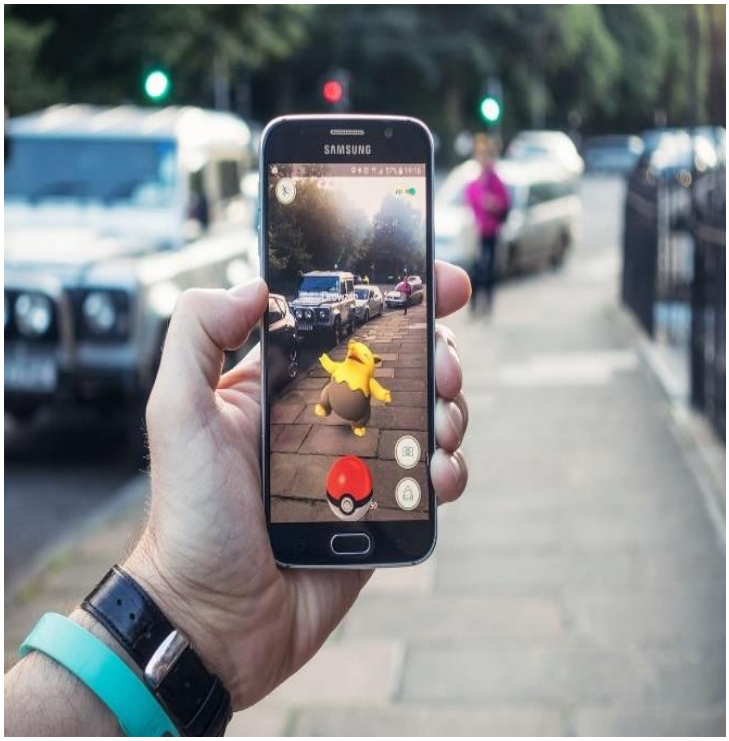


Рис. 1. Доповнена реальність у грі Pokémon Go

Найважливішим застосуванням доповненої реальності у випадку військової галузі є Heads-Up Display (HUD) [3]. У цій технології прозорий дисплей розміщується безпосередньо на виду пілота винищувача. Цей дисплей полегшує дані для пілота, що включає інформацію про лінію горизонту, швидкість повітря та висоту, а

також інші обов'язкові дані. Тут „вгору" означає, що завдяки дисплею пілоту не потрібно дивитись вниз до приладів літального апарату, щоб отримати доступ до потрібної йому інформації. Іншим додатком є головний дисплей (HMD), який приймається наземними військами. Ці важливі дані, включаючи місце знаходження ворога, можуть відображатися в межах прямої видимості солдата. Ця технологія також застосовується для розробки симуляцій для допомоги у навчанні.

Також AR технологію застосовують студенти медичних закладів, щоб допомогти їм у практиці хірургії в контрольованому середовищі. Візуалізації допомагають продемонструвати пацієнтам складні захворювання. Доповнена реальність також сприяє посиленому сенсорному сприйняттю для хірургів, тим самим допомагаючи зменшити шанс ризику в операціях. Поєднана з МРТ або рентгенівською розширеною реальністю може надати хірургу все, що є в одному огляді. Що стосується хірургічних застосувань, роль ДР у нейрохірургії залишається найбільш помітною. Потенціал технології розробки тривимірного зображення, включаючи точні координати мозку, на додаток до реальної анатомії пацієнта стає надзвичайно вигідним для хірурга.

Однією з областей, де доповнена реальність доводить свою перевагу найбільше, є випадок навігаційних програм. У сучасному світі навігація ДР стала остаточним рішенням. Ці програми дозволяють додавати реальні об'єкти, що супроводжуються безліччю підказок, які проглядаються на екрані програми під час наведення на них камери пристрою. Ці поради включають інформацію про будівлі та маршрути, куди їде автобус або де знаходиться певний магазин чи ресторан. Удосконалені системи GPS приймають доповнену реальність, щоб полегшити бездоганну навігацію від точки А до точки Б. За допомогою камери смартфона та GPS користувач може спостерігати за обраним маршрутом замість огляду в реальному часі перед автомобілем.

Нещодавні розробки в галузі технологій, а також обчислювальної потужності проклали шлях доповненої реальності до утвердження в ігровій індустрії. Завдяки пристроям, що носяться на голові, зростає доступність, а обчислювальна потужність стає все більш портативною, ДР значно покращує ігровий досвід. Однією з таких популярних ігор є Pokemon Go (рис. 1), яка з'явилась у 2016 році й стала новою тенденцією. У грі гравці знаходять і захоплюють персонажів покемонів, які з'являються в реальному світі, будь то на тротуарі, у фонтані, можливо навіть у власній ванній.

Що стосується кібербезпеки та несанкціонованого доступу через хакерські атаки та шкідливе програмне забезпечення, як і всі пов'язані технології, доповнена реальність вразлива до того самого. Як і деякі інші пов'язані технології, ці атаки можуть спричинити відмову в обслуговуванні або накласти неправильні дані, що призведе до екстремальних та жахливих результатів. Наприклад, хакер може ввести водія в оману, використовуючи контрольовану ДР-структуру маршруту, і спричинити невдачі. Реальні небезпеки ДР не можуть залишати поза увагою, не зважаючи на її популярність. Якщо їх не вирішити на початковому етапі, ці небезпеки можуть призвести до значних труднощів та загострень.

На сьогодні існують дослідження щодо впровадження засобів AR в освітній процес, проте серед них мізерно мало застосувань AR у галузі кібербезпеки [4]. Використання доповненої реальності для візуалізації даних у контексті кібербезпеки створює природний інтуїтивно зрозумілий інтерфейс, що полегшує та покращує розуміння явища чи процесу.

Отже, підсумовуючи все, у сучасному світі доповнена реальність застосовна майже до всіх секторів. Провідні технічні гіганти, такі як Google, Amazon та Facebook, широко використовують програмне забезпечення цієї технології. Вже можна спостерігати значний ступінь зростання в галузях, які застосовують ДР, оскільки вони розширюють його застосування, включаючи його у свої повсякденні операції. Прийнявши доповнену реальність, прогрес можна досягти в багатьох сферах, але необхідно звертати увагу на небезпеки застосування AR та досліджувати методи захисту від них.

Список літератури

1. Кузнєцов В. Тім Кук бачить доповнену реальність такою ж «великою ідеєю, як і смартфони» / ComputerREX / 14 лютого 2017 р. [Електронний ресурс] – Режим доступу: http://www.computerrex.com/materials/apple/id/377

2. Brian X. Chen. If You're Not Seeing Data, You're Not Seeing / 2009-08-25 [Електронний ресурс] – Режим доступу: https://web.archive.org/web/20101225055146/http://www.wired.com/gadgetlab/2009/08/ augmented-reality/ #more-22882

3. R. Azuma, A Survey of Augmented Reality Presence: Teleoperators and Virtual Environments, pp. 355—385, August 1997.

4. Козак Р. Використання засобів доповненої реальності для вдосконалення освіти в галузі кібербезпеки / Р. Козак, Ю. Скоренький, Н. Загородна // Матеріали VI науково-технічної конференції „Інформаційні моделі, системи та технології", 12-13 грудня 2018 року. — Т. : ТНТУ, 2018. — С. 31.

УДК 621.39

В.И. Слюсар
swadim@ukr.net
главный научный сотрудник, д.т.н., проф.,
Центральный научно-исследовательский институт вооружения и военной техники Вооружённых Сил Украины, Киев

ИНТЕГРАЦИЯ N-OFDM И UFMC

Одним из перспективных направлений развития систем связи является применение спектрально эффективных сигналов на основе неортогонального частотного дискретного мультиплексирования (not-orthogonal frequency division multiplexing, N-OFDM) [1 - 5]. Для минимизации ошибок оценивания квадратурных составляющих амплитуд N-OFDM сигналов при количестве поднесущих более 16 лучшим выбором является применение неэквидистантной частотной схемы [5]. Такое решение позволяет не только снизить погрешности демодуляции, но повысить частотное уплотнение сигнального пакета за счет перехода от совместной обработки всей совокупности поднесущих к параллельной демодуляции их изолированных групп. Как показано в [5], при неэквидистантном частотном плане такой подход возможен за счет рассредоточения по частоте, например, квартетов поднесущих с определенным защитным интервалом между сигнальными группами. Это позволяет применить дополнительную фильтрацию частотных квартетов для усиления их частотной развязки и создаёт предпосылки для демодуляции сигналов каждого из квартетов независимо от остальных частотных групп, в пренебрежении их присутствием. Поскольку аналогичный подход используется и в технологии универсальной фильтрации множества поднесущих (the universal filter multi-carrier, UFMC), предлагается интегрировать неэквидистантную концепцию N-OFDM с UFMC. Целью работы является рассмотрение особенностей такой интеграции в интересах повышения спектральной эффективности перспективных систем связи.

Следует отметить, что первая публикация по методу UFMC в 2013 г. [6] практически совпала по времени с выходом в свет статьи [4, 5]. При этом, в отличие от [5], процедуру фильтрации групп поднесущих при реализации UFMC предполагалось выполнять в передатчике в отношении сигналов, имеющих равномерный разнос поднесущих по частоте. По сравнению с традиционным OFDM сигналом использование в UFMC-передатчике набора смещенных по частоте FIR-фильтров позволило перед излучением в эфир подавить боковые лепестки в спектре сигналов и тем самым снизить требования к ширине защитного частотного интервала между соседними каналами передачи данных.

Такой подход может быть применен и в отношении N-OFDM сигналов, в дополнение к уже предусмотренной в [5] фильтрации отдельных групп поднесущих в приёмнике. В отличие от фильтра Чебышева, использованного в [6] и в последующих публикациях, развивающих UFMC концепцию, в приёмнике N-OFDM сигналов предлагается применить набор цифровых I/Q-демодуляторов, предложенных в [7]. Наряду с частотной селекцией групп поднесущих при этом становится возможным формировать квадратурные составляющие их напряжений. Важным условием для успешного извлечения заложенной в N-OFDM сигналы информации является компенсация паразитных фазовых набегов и искажений амплитуд сигналов, возникающих в процессе формирования откликов I/Q-демодуляторов. Аналогичная компенсация должна проводиться и для устранения искажений в сигналах, возникающих при их прохождения через FIR-фильтры передатчика.

Представленный метод обработки позволяет повысить степень развязки групп поднесущих за счет сочетания их фильтрации в передатчике и частотно-селективной I/Q-демодуляции в приёмнике.

Список литературы

1. Слюсар В.И. Патент РФ № 2054684, G01R23/16. Способ измерения амплитудно-частотных характеристик. - 1992 р. - Опубл. 20.02.96, Бюл. № 5.

2. Pat. of Ukraine № 47835 A. IPC8 H04J1/00, H04L5/00. Method of frequency-division multiplexing of narrow-band information channels// Slyusar Vadym Ivanovych, Smoliar Viktor Hryhorovych. – Appl. № 2001106761, Priority Data 03.10.2001. – Official publication data 15.07.2002, Official bulletin № 7/2002.

3. Слюсар В.И., Смоляр В. Г. Частотное уплотнение каналов связи на основе сверхрелеевского разрешения сигналов.// Известия высших учебных заведений. Радиоэлектроника.- 2003. - Том 46, № 7. - С. 30 - 39.

4. Слюсар В. И. Неортогональное частотное мультиплексирование (N-OFDM) сигналов. Часть 1. //Технологии и средства связи. – 2013. - № 5. - С. 61- 65.

5. Слюсар В. И. Неортогональное частотное мультиплексирование (N-OFDM) сигналов. Часть 2. //Технологии и средства связи. – 2013. - № 6. - С. 60 - 65.

6. Vida Vakilian, Thorsten Wild, Frank Schaich, Stephan ten Brink, Jean-Francëois Frigo. Universal Filtered Multi-Carrier Technique for Wireless Systems Beyond LTE. // 9th Int'l. Wksp. Broadband Wireless Access, IEEE GLOBECOM '13, Atlanta, GA, Dec. 2013. - DOI: 10.1109/GLOCOMW.2013.6824990.

7. Slyusar, V., Serdiuk, P. Synthesis Method of Procedure for Odd-Order I/Q Demodulation based on Replacing Multistage with Equivalent Single-Stage Demodulation Schemes.// Radioelectron.Commun.Syst. 63, 273–280 (2020).

УДК 004.45

Г.М. Дрєєва, О.Г. Собінов, С.А. Смірнов
gannadreeva@gmail.com, sagcob14@gmail.com, smirnov.ser.81@gmail.com
Центральноукраїнський національний технічний університет, Кропивницький

СИСТЕМНЕ ПРОГРАМУВАННЯ В СФЕРІ СУЧАСНОГО ВИКЛАДАННЯ У ВИЩИХ НАЧАЛЬНИХ ЗАКЛАДАХ

Сучасні вимоги забезпечення якісного викладання матеріалів в процесі підготовці програмістів в сфері системного програмування, в умовах обмеження обсягу годин, вимагає більш якісного виділення змістовних модулів та моніторингу вимог ринку праці ІТ-індустрії. По результату зазначених вимог є потреба у створені гнучкого курсу з системного програмування, в якому можна змінювати акценти викладання без порушення цілісності та послідовності наданих знань та навичок. Однак, розглянута сфера розробки програмного забезпечення є широкою, і має гнучкість в трактуванні прийнятих задач та рівнів. Відповідно з часом трактування поняття «системне програмування» набувало трансформацій та змін, зокрема до системного програмування з часом почали відокремлювати програмне забезпечення операційної системи та драйверів, і схожі процеси сьогодні можна спостерігати з ускладненням структури та збільшенням обчислювальної потужності вбудованих систем на базі мікроконтролерного керування. Розглянуто приклади означень терміну «системне програмування», деякі з них наведено нижче.

Системне програмування створення комп'ютерних програм, які дозволяють апаратному забезпеченню комп'ютера взаємодіяти з прикладним програмним забезпеченням, що призводить до ефективного використання апаратних ресурсів обчислювальної системи. Типові системні програми включають *операційну систему* та *мікропрограму BIOS*, та засоби програмування, такі як *компілятори, підпрограми вводу-виводу, інтерпретатори, планувальник, завантажувач*, та *лінкери* [1].

До системного програмування відносяться програми не лише програми, які контролюють базове комп'ютерне обладнання, але й програми для побудови інших програмних систем. Також до системного програмного забезпечення відносяться програми для побудови інших програм та служб. Часто до системних програм відносять операційні системи, компілятори, драйвери пристроїв, програми автоматизації роботи заводу, роботів, високопродуктивного математичного програмного забезпечення, ігор (Xbox, PlayStation, ПК), та обчислювальної техніки [2].

Узагальнення дає наступні пріоритетні напрямки, які можна розглядати умовно незалежними для області системного програмування:

1)Завантажувачі та операційні системи.

2)Драйвери операційної системи.

3)Компонувальники (лінкери та компілятори).

4)Утиліти (архіватори, дефрагментатори дисків, системні монітори).

5)Програмне забезпечення для вбудованих систем, які не мають операційної системи.

Додатково, для професій, які пов'язані з кібербезпекою, є необхідним розглядання захищеності розглянутих систем на більш високому теоретичному та практичному рівні.

Відповідно до позначених пунктів проводиться розробка курсу системного програмування, яка б враховувала сучасні тенденції та вимоги бізнесу, де вказані розділи поділено на три рівні деталізованості. В результаті теоретичний матеріал та лабораторні заняття можуть мати унікальну траєкторію, яка враховує наявний аудиторний час, можливості окремого студента, наявну апаратну та програмну базу.

В результаті, шаблон робочої начальної програми містить розгорнутий курс, який стосується системного програмного забезпечення, але може бути динамічно, навіть під час викладання, трансформований за складністю по вимогам бізнесу або можливостями окремого студента. Недоліком запропонованої системи є методика оплати праці викладача, за якою не враховується значне перевищення складності курсу по виділеним на її вивчення годин.

Список літератури

1. System Programming URL: https://www.techopedia.com/definition/9616/system-programming

2. Charles Torre, Bjarne Stroustrup, Andrei Alexandrescu, Rob Pike, Niko Matsakis / Panel: Systems Programming in 2014 and Beyond// URL: https://channel9.msdn.com/Events/Lang-NEXT/Lang-NEXT-2014/Panel-Systems-Programming-Languages-in-2014-and-Beyond

3. Wirth, Niklaus. PL360, A Programming Language for the 360 Computers.// Journal of the ACM. 15 (1): 37–74.

УДК 004.4

Д.М. Подкопаєв, Є.В. Мелешко
devonoset@gmail.com, elismeleshko@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький

ДОСЛІДЖЕННЯ ПЕРЕВАГИ ВИКОРИСТАННЯ ЧАТ-БОТІВ ПЕРЕД ДОДАТКАМИ І ВЕБ-СЕРВІСАМИ

На сьогоднішній день спостерігається активний розвиток веб-сервісів та мобільних додатків. Вони дозволяють задовольнити потреби практично всіх користувачів, маючи функціональність, яка полегшує вирішення певних завдань або пошук певної інформації. Більшість сучасних компаній, фірм та установ мають власні веб-портали, на яких розміщена певна інформація. Однак користувачі стикаються з проблемою неоднорідності й низькою якістю даних, малою швидкістю відповіді від сервісу та високою собівартістю в його виробництві.

У більшості випадків дані погано сформовані, додатки та їх веб-сервіси мають надлишковий інтерфейс, що погіршує якість використання такого сервісу, доводиться абстрагуватися, щоб знайти необхідне. Витрачається велика кількість часу на перемикання між сервісами або додатками для вирішення своїх потреб. Також через високу собівартість розробки і обслуговування цих додатків страждає функціональність, в більшості випадків відсутнє машинне навчання, використання не оптимальних алгоритмів погіршує продуктивність і якість програм.

Метою даної роботи є дослідження чат-ботів як альтернативи веб-сервісам та додаткам.

Чат-бот – це програмний додаток, який імітує письмову або усну людську мову з метою створення розмови або взаємодії з реальною людиною, розробляється на основі технологій машинного навчання і нейронних мереж.

Основні переваги чат-ботів:

1. Легко створити і запрограмувати.
2. Багатоплатформність основного місця роботи чат-бота (приклад Telegram).
3. Єдиний інтерфейс.
4. Відсутність потреби в постійному оновленні.
5. Не вимагає встановлення як окремого додатку, тому не займає багато місця в пам’яті.
6. Чат-боти людяні.

Мобільні додатки допомагають вирішити всі повсякденні проблеми і зробити життя простішим. Але вони не можуть спілкуватися «людяно». Чат-боти можуть розуміти людську мову, тому що використовують обробку природної мови (NLP). NLP може зрозуміти синтаксис, а також семантику мови людини.

Крім того, в мобільних додатках, користувачам доводиться переміщатися по розділах меню, щоб знайти один потрібний пункт. Для використання будь-якого чат-бота не потрібно робити багато дій. Достатньо його активувати, а потім чат-бот допомагає вам виконувати повсякденні завдання за лічені хвилини.

Використання чат-ботів в різних сферах дозволяє більш ефективно використовувати свої ресурси, наприклад:

– адаптувати нових співробітників в умовах високої плинності кадрів;

– полегшити перехід на віддалений варіант роботи, оскільки чат-бот замінює фізичне спілкування з підрозділами, а отже забезпечує більш комфортний перехід на віддалений формат;

– залучити нових клієнтів та покращити взаємодію з існуючими, оскільки багатьом людям легко і зручно взаємодіяти з програмним забезпеченням у форматі бесіди в чаті.

Висновки. Чат-бот як заміна мобільного додатку – це шлях розвитку для бізнесу, новий варіант взаємодії з клієнтом або співробітником та легкий в освоєні інструмент для виконання власних потреб. Повністю замінити додатки або веб-сервіси, на даний момент чат-боти не зможуть. Але це тільки початок історії, коли нам достатньо буде мати один основний месенджер з функціоналом, який змінюється з додаванням необхідних чат-ботів.

УДК 004.056

М.О. Бубела, В.О. Шевчук, Л.В. Константинова
ya.bubela@gmail.com, vlad3032002@gmail.com, liliyashel1976@gmail.com
Центральноукраїнський національний технічний університет, Кропивницький

ОГЛЯД ЗАСОБІВ ЗАХИСТУ ДАНИХ НА ТРАНСПОРТНОМУ РІВНІ

У наші часи ми бачимо неймовірний потік інформації, цей потік здебільшого існує у комп'ютерних системах, що викликає велике питання про їх захист. Дані можуть бути піддані ризику як під час транзиту, так і в стані спокою, і потребують захисту. Хоча розробка технологій забезпечення безпеки ведеться не перший рік, і на їх реалізацію витрачаються чималі кошти, віруси, хробаки, шпигунські та інші зловмисні програми залишаються основною проблемою, з якою стикаються компанії. Тому дослідження наявних засобів захисту даних та їх огляд для створення нових засобів наразі є актуальною задачею.

Аналіз мережевого трафіку 41 великої компанії показав, що, незалежно від сфери, порушення регламентів інформаційної безпеки є в 100% корпоративних мереж, підозрілий трафік — в 90%, активність шкідливого програмного забезпечення - 68%. Ця статистика доказує необхідність пошуку дієвих засобів захисту даних.

Існує безліч різних підходів до захисту даних [1]. Шифрування відіграє важливу роль у захисті даних і є популярним інструментом. Для захисту даних під час транспортування підприємства часто вирішують зашифрувати конфіденційні дані перед переміщенням або використовувати зашифровані з'єднання (HTTPS, SSL, TLS, FTPS тощо) для захисту вмісту даних, що передаються. Для захисту даних у стані спокою підприємства можуть просто зашифрувати конфіденційні файли перед їх зберіганням та/або вибрати шифрування самого накопичувача. Передача інформації здійснюється за допомогою протоколів транспортного рівня що надають транспортні послуги, а саме протокол TCP і протокол дейтаграм UDP. Потрібно розуміти, що протокол UDP не може гарантувати нам доставлення дейтаграм. Такі протоколи не перевіряють джерела інформації саме це становить велику загрозу.

Такі криптографічні протоколи як SSL (Secure Sockets Layer) та TLS **(**Transport Level Security) надають допомогу при захисті передач даних [2]. У протоколи TLS входять наступні властивості:

- Цілісність: кожне повідомлення містить код, за допомогою якого є можливість перевірити дані на їх зміну та чи не були вони втрачені у процесі передачі.
- Безпека: симетричне шифрування захищає інформацію.
- Аутентифікація: учасника підключення можна перевірити за допомогою асиметричного шифрування.

Взагалі протокол SSL був розроблений компанією Netscape. В минулому вона була американською компанією з надання комп'ютерних послуг зі штаб-квартирою в Маунтін-В'ю, Каліфорнія. У компанії була своя думка, що безпечне з'єднання між клієнтом та сервером буде успішним кроком у розвитку інструмента. Найкращим засобом захистити її була шифровка та дешифровка по різні кінці встановлюваного з'єднання. Таким чином і з'явився протокол SSL, який працює поверх TCP, а також надає TCP-подібний інтерфейс для додатків більш високого рівня. У теорії, одним з переваг SSL для розробників була можливість замінити всі традиційні TCP виклики на нові SSL виклики.

Принцип роботи SSL і TLS [2] однаковий. Поверх протоколу TCP / IP встановлюється зашифрований канал, всередині якого передаються дані по прикладному протоколу - HTTP, FTP, і так далі. Прикладний протокол «загортається» у TLS / SSL, а той у свою чергу в TCP / IP. По суті дані по прикладному протоколу передаються по TCP / IP, але вони зашифровані. Розшифрувати дані, що передаються може тільки та машина, яка встановила з'єднання. Для всіх інших, хто отримає передані пакети, ця інформація не буде мати сенсу, тому що вони не зможуть її розшифрувати.

Також можна розглянути технологію SPI [3] (Stateful Packet Inspection) – використання механізмів контролю сесій. Цей підхід реалізує контроль за з'єднанням, але не фільтрує пакети за небажаним змістом, що не дозволяє запобігати розповсюдження вірусів. Для захисту від розповсюдження вірусів та інших загроз. До того, як перевірка стану стане загальнодоступною, використовувалась подібна технологія, яка називається статичною фільтрацією пакетів.

Ця давня альтернатива перевіряє лише заголовки пакетів, щоб визначити, чи слід їх пропускати через брандмауер. В результаті хакер може просто вказати «відповідь» у заголовку, щоб витягти інформацію з мережі. Навпаки, державна інспекція має на меті провести більш досконале розслідування. Ось чому він аналізує прикладний рівень пакетів. Динамічний фільтр пакетів, такий як перевірка стану, може запропонувати кращу безпеку для мереж шляхом запису Stateful Packet Inspection інформації про сеанс, наприклад номерів портів або IP-адрес.

Сьогодні деякі брандмауери також можуть виконувати глибоку перевірку потоків пакетів. Ці правила глибоко вдаються у вміст пакету, окрім заголовків IP та TCP / UDP, і виконують сканування на рівні програми. Якщо брандмауер дозволяє доступ до порту 80, оскільки на сайті є веб-сервер, хакери швидко виявлять, що ці пакети проходять прямо через брандмауер. Ці брандмауери не тільки захищають веб-сайти, але й можуть

швидко знаходити хробаків електронної пошти та створювати правила регулярних виразів, щоб уникнути їх поширення.

Доречно буде розглянути сигнатурний аналіз є метод виявлення вірусів, що перевіряє на наявності у файлах сигнатур вірусів. Сигнатурний аналіз є найбільш відомим методом розпізнання вірусів та використовуються практично у всіх антивірусах сьогодення. Для проведення перевірки антивірусу необхідний набір вірусних сигнатур, що зберігається в антивірусній базі. Цей метод може допомогти технології SPI з її вразливими сторонами. Можна відмітити, що на наш час більшість маршрутизаторів сьогодні має SPI-брандмауери, тому на власну думку вважаю доречним було згадати про сигнатурний аналіз.

Для високорівневого захисту найбільш ефективним є комплексний захист. Системи на базі CDN ефективно вирішують проблему захисту від DoS та DDoS-атак не тільки на прикладному, а і на мережевому і транспортному рівнях. Наприклад, компанія CISCO пропонує рішення щодо захисту за допомогою технології NAC [4] (Network Admission Control). Вона починає працювати вже в момент підключення пристрою в розетку, дозволяючи або блокуючи доступ виходячи з багатьох параметрів, заданих адміністратором згідно з політикою безпеки компанії. Це можуть бути такі параметри, як час і місце підключення, mac- і ip-адреси, логін і пароль облікового запису в середовищі Windows і багато інших. Рішення NAC допомагають організаціям контролювати доступ до своїх мереж за допомогою наступних можливостей [4]:

1. Управління життєвим циклом політики: Застосовує політики для всіх сценаріїв роботи, не вимагаючи окремих продуктів або додаткових модулів.

2. Профілювання та видимість: розпізнає та профілює користувачів та їх пристрої, перш ніж шкідливий код може заподіяти шкоду.

3. Доступ до мереж для гостей: керуйте гостями за допомогою порталу самообслуговування, що налагоджується, який включає реєстрацію гостей, аутентифікацію гостей, спонсорство гостей та портал управління гостями.

4. Security posture check: оцінює відповідність політики безпеки за типом користувача, типом пристрою та операційною системою.

5. Відповідь на випадки : пом’якшує мережеві загрози, застосовуючи політику безпеки, яка блокує, ізолює та відновлює невідповідні машини без уваги адміністратора.

6. Двонапрямна інтеграція: інтегруйте з іншими безпековими та мережевими рішеннями через API open / RESTful.

Як висновок, можна затвердити, що на наш час є багато протоколів, систем та навіть комплексних захистів даних на транспортному рівні, але ні один з вище вказаних методів не дає сто відсоткову гарантію захисту, тому питання щодо захисту даних залишається відкритим та невирішеним по сьогодні.

Список літератури

1. Ромашко С. М. Конспект лекцій з дисципліни «Комп'ютерні мережі і телекомунікації» — Львів: ЛРІДУ НАДУ, 2006. — 62с.

2. Ilya Grigorik High Performance Browser Networking O'Reilly Media, Inc.September 2013 [Електронний ресурс] – Режим доступу: https://www.oreilly.com/library/view/high-performance-browser/9781449344757/

3. Dameon D. Welch-Abernathy. Essential Check Point Firewall-1 NG(TM): An Installation, Configuration, and Troubleshooting Guide. — Addison-Wesley Professional, 2004. — P. 5. — ISBN 9780321180612.

4. Контроль доступа в сеть Network Admission Control (NAC) – Обеспечение защиты сети // Cisco. [Електронний ресурс] – Режим доступу: https://www.cisco.com/web/RU/netsol/ns466/networking_ solutions_white_paper0900aecd800fdd66.html (дата звернення: 18.03.2021).

УДК 004.457

М.І. Мосольд, Є.В. Мелешко
maximmosold@gmail.com, elismeleshko@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький

ДОСЛІДЖЕННЯ ТА РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ МОДЕЛЮВАННЯ ТА ПРОГНОЗУВАННЯ НАСЛІДКІВ ЕПІДЕМІЙ

Моделювання процесів поширення та наслідків епідемій як інфекційних, так і інформаційних є важливим завданням у наш час.

Метою даної роботи було дослідити існуючі програмні засоби для моделювання та прогнозування наслідків епідемій у соціальних мережах, а також розробити власне програмне забезпечення.

Епідемічні моделі поділяють на два основні види: стохастичні та детерміновані моделі.

Стохастична модель – математична модель, в якій параметри, умови функціонування і характеристики стану об'єкта, що моделюється, представлені випадковими величинами і пов’язані нерегулярними залежностями. При побудові моделі застосовуються методи кореляційного і регресійного аналізу.

Детерміновані моделі, як правило, призначені для поглиблення в певний основний механізм або природний процес. Вони відрізняються від статистичних моделей метою – практично оцінити зв’язки між змінними. Детермінована модель розглядається як корисне наближення до реальності, яку простіше побудувати і інтерпретувати, ніж стохастичну. Проте, такі моделі можуть бути надзвичайно складними через велику кількість вхідних і вихідних даних, і часто незворотними, фіксований єдиний набір вихідних даних може бути отриманий за допомогою декількох наборів вхідних. Таким чином, використання надійних параметрів і невизначеності моделі є вирішальним, можливо, навіть більшою мірою, ніж для стандартних статистичних моделей [1].

У якості існуючого інструменту для моделювання епідемій у даній роботі було розглянуто програмне забезпечення EpiModel.

EpiModel – це набір програмних інструментів для моделювання математичних моделей, динаміки інфекційних захворювань, який може значно спростити процес моделювання та прогнозування наслідків епідемій [2]. Класи епідемічних моделей включають детерміновані компартментні моделі, стохастичні моделі індивідуального контакту та стохастичні моделі мережі. Мережеві моделі використовують надійні статистичні методи моделей випадкових графіків експоненціальних сімей (ERGM) із набору програм Statnet. Стандартні шаблони для моделювання епідемій включають такі типи захворювань: SI, SIR та SIS. EpiModel має простий API для розширення цих шаблонів для вирішення нових цілей наукових досліджень.

Для поширення інфекційних захворювань може використовується класична модель SIR. Населення в моделі ділиться на три частини в залежності від статусу: сприйнятливий до захворювання, заражений і одужавший. Ця модель створена методом системної динаміки. Щоб відображати дійсність, модель повинна ґрунтуватися на реальних властивостях конкретної хвороби і враховувати зміни системи під зовнішніми впливами. Також враховується рівень ризику хвороби в залежності від віку пацієнта і різні сценарії введення карантину [3].

При моделюванні коротких епідемій в великих містах можна знехтувати зміною демографічної структури населення за час епідемії. Зовнішній вплив на епідемію – попередня вакцинація, ймовірна госпіталізація та інше.

Зовнішнім чинником початку епідемії є поява серед жителів міста деякої кількості носіїв вірусу, які можуть заражати інших жителів при контакті з ними. Моделювання розповсюдження захворювання починається з моменту його виникнення до моменту майже повного затухання епідемії.

Основним процесом моделювання є процес розповсюдження захворювання через контакти між людьми. Одним з варіантів отримання контактів між людьми є сканування соціальної мережі, але у деяких користувачів соціальної мережі число друзів набагато перевищує число Данбара – обмеження на кількість постійних соціальних зв'язків, які людина може підтримувати. За різними оцінками, число Данбара лежить в діапазоні від 100 до 230, найчастіше умовно приймається рівним 150 [4]. Тому щоб мати в базі даних більш реалістичні дані, додаток може ігнорувати людей з надто великим та надто малим числом соціальних зв’язків.

Багато веб-додатків використовують API для підключення до різних сторонніх сервісів. Самостійне створення таких інструментів може зайняти дуже багато часу, а API дозволяють за лічені хвилини підключитися до джерела і отримати доступ до його функцій і даних. Тому використання API значно спростить сканування соціальної мережі.

Не всі профілі користувачів соціальної мережі знаходяться у відкритому стані, деякі закриті або заблоковані – з них неможливо отримати потрібну інформацію. Було б логічно не вносити їх до бази даних, але кількість запитів з одного авторизованого користувача до серверів соціальної мережі може бути обмеженою. Тому заради економії запитів база даних містить і таких користувачів. У подальшій підготовці до моделювання вони будуть проігноровані.

Для зберігання даних моделювання епідемії можна використовувати SQLite. SQLite – це компактна вбудована СУБД, яка підтримує досить повний набір команд SQL [5]. Ця СУБД зберігає всю базу даних в єдиному стандартному файлі на тому комп'ютері, на якому виповнюється програма. Вона є дуже надійною та простою у використанні а також швидкою і не вимагає спеціальної установки. Декілька процесів або потоків можуть одночасно без будь-яких проблем читати дані з однієї бази. Запис в базу можна здійснити тільки в тому випадку, якщо ніяких інших запитів в даний момент не обслуговується.

По результатам моделювання наслідків епідемій можна зробити висновки про необхідність прийняття тих чи інших соціальних обмежень: заборон публічних заходів, закриття ресторанів, обмежень пересування і т.п.

У даній роботі також було запропоновано власне програмне забезпечення для моделювання та прогнозування наслідків епідемій. Розроблена система складається з двох консольних додатків та одного додатку з графічним інтерфейсом. Один з консольних додатків виконує функцію наповнення бази даних користувачами соціальної мережі, а інший – аналізує цю базу даних, відбирає потрібну інформацію та приводить її до єдиного формату. Останній додаток, оперуючи багатьма факторами, моделює епідемію та відображає статистичний графік.

Наповнення бази даних відбувається через запити до серверів соціальної мережі vk.com. Щоб використовувати API ВКонтакті на повну потужність, необхідно мати Standalone-додаток. Він надає можливість здійснювати запити до серверу в значно більших кількостях на одну одиницю часу.

Процедуру отримання інформації про користувачів було створено в налаштуваннях Standalone-додатку, вона написана на VkScript. Ця процедура приймає рядок з 25 id, виймає по одному id, робить запит до friends.get, а потрібна інформація буде повертатися в словнику, де ключі – це id, а значення – список друзів даного id.

Наступним кроком після наповнення бази даних є її обробка та структурування. Інформація фільтрується та структурується в потрібних таблицях. Кожний користувач має зв'язки з іншими користувачами соціальної мережі, але не всі вони містяться в базі даних, тому процес налагодження зв'язків займає достатньо багато часу. В результаті виконання цих дій, вихідна база даних може значно зменшитися в обсязі.

Продуктивність масової вставки SQLite може варіюватися від 85 вставок в секунду до більш 96000 вставок в секунду. Виявляється, продуктивність SQLite може значно відрізнятися (як для масових вставок, так і для вибірок) в залежності від того, як налаштована база даних і як використовується API. При найгіршому сценарії операції занадто повільні, тому що SQL буде скомпільовано в код VDBE для кожної вставки, і кожна вставка буде відбуватися у своїй власній транзакції. За замовчуванням SQLite буде оцінювати кожен оператор INSERT / UPDATE в рамках унікальної транзакції. Якщо виконується велика кількість вставок, рекомендується укласти операцію в транзакцію.

Використання транзакції було величезним поліпшенням, але повторна компіляція оператора SQL для кожної вставки не має сенсу, якщо використовується один і той же SQL багаторазово. Скомпілювавши оператор SQL один раз, а потім зв'язавши параметри з цим оператором, використовуючи sqlite3_bind_text, можна подвоїти продуктивність.

В наш час пандемія COVID-19 показала, що загрози глобальних епідемій – не віртуальні, а цілком реальні. Для світової економіки, яка побудована на довірі та впевненості у майбутньому, виявилося, що людству доведеться ще багато чому навчитися. В межах України в недостатній мірі представлені вітчизняні розробки в області програмного моделювання епідемій. У відкритому доступі мало напрацювань на дану тему, тому тема даної роботи є досить актуальною, а вирішення поставленої задачі допоможе прогнозувати епідемії та вчасно приймати правильні рішення щодо їх попередження та усунення.

Список літератури

1. Adrian E. Raftery, "Inference for Deterministic Simulation Models: The Bayesian Melding Approach", Journal of the American Statistical Association 95, 2000, с. 1244–1255.

2. EpiModel [Електронний ресурс] – Режим доступу до ресурсу: https://www.epimodel.org/.

3. Hethcote H., "The Mathematics of Infectious Diseases", SIAM Review, 2000, с. 599–653.

4. Dunbar R.I.M., " Neocortex size as a constraint on group size in primates", Journal of Human Evolution, 1992, с. 469–493.

5. SQLite [Електронний ресурс] – Режим доступу до ресурсу: https://www.sqlite.org/.

УДК 004.75

Є.С. Прокопенко, О.С. Улічев
prokopenko19712002@gmail.com, askin79@gmail.com
Центральноукраїнський національний технічний університет м. Кропивницький

ПОРІВНЯННЯ ГЕШ-ФУНКЦІЙ ДЛЯ РЯДКОВИХ ДАНИХ В КОМБІНАЦІЇ З РІЗНИМИ МЕТОДАМИ ВИРІШЕННЯ КОЛІЗІЙ

Алгоритми гешування сьогодні дуже розповсюдженні для реалізації швидкого пошуку, створення контрольних сум файлів, захисту інформації тощо. Використовуючи адресну книгу чи енциклопедію, отримуємо доступ до функцій швидкого пошуку, в більшості випадків вони реалізується за допомогою алгоритмів гешування. Процес гешування базується на розбиті множини ключів, на підмножини, що не перетинаються і володіють певною характерною властивістю. Данна властивість описується функцією гешування, або геш-функцією, і називається геш-адресою.

Вирішення оберненої задачі покладено на геш-структури (геш-таблиці): використовуючи геш-адресу забезпечується швидкий доступ до потрібного елементу. В ідеальному випадку, для задач пошуку, геш-адреса має бути унікальною, щоб за одне звернення отримати доступ до елемента, який характеризується заданим ключем, тобто мати прямий доступ за 1 крок (ідеальна геш-функція). Однак, на практиці отримання ідеальної геш-функції ускладнене тим, що наперед невідомо кількість даних, які підлягають гешуванню та їх структурні особливості. Зазвичай в реальних умовах при побудові геш-функції виникають колізії – геш-функція повертає для двох чи більше різних вхідних наборів однакове геш-значення (ключ). Виникає задача пошуку компромісу між складністю побудови геш-функції, що наближається до ідеальної, та проблемою розв'язання колізій.

Геш-таблиці дозволяють отримати кращі показники оцінки операцій, в порівнянні з масивами та зв'язаними списками, тобто в середньому пошук, вставка, та видалення елементу з геш-таблиці відбувається за час O(1).

Таблиця 1

Порівняння швидкості операцій в геш-таблиці з операціями в інших структурах

Алгоритм	Геш-таблиці (Середній випадок)	Геш-таблиці (Найгірший випадок)	Масиви	Зв'язані списки
Пошук і-го ел.	**O(1)**	**O(n)**	**O(1)**	**O(n)**
Вставка (початок/кінець)	**O(1)**	**O(n)**	**O(n)**	**O(1)**
Видалення (початок/кінець)	**O(1)**	**O(n)**	**O(n)**	**O(1)**

Найгірший випадок для використання геш-таблиць виникає в результаті появи великої кількості колізій, в цьому випадку підхід втрачає всі свої переваги. Відповідно, актуальними стають ефективні алгоритми вирішення колізій в геш-таблицях.

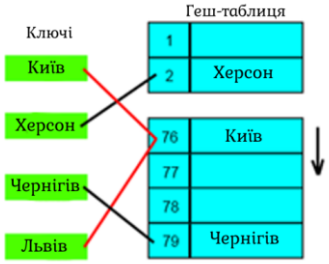


Рис. 1. Приклад колізії

Теоретично неможливо визначити геш-функцію так, щоб вона повертала випадкові різні результати з реальних невипадкових вхідних даних, кількість яких наперед не задана. Однак на практиці реально створити досить хорошу імітацію за допомогою простих арифметичних дій. Більш того, для геш-функції з мінімальним числом колізій часто можна використати особливості даних [2].

Найрозповсюдженішими методами гешування є метод ділення, ваговий метод та мультиплікативний метод (метод множення).

Метод ділення полягає , в тому що гешування буде виконуватись завдяки знаходженню остачі від ділення на певне число M (зазвичай це розмір геш-таблиці):

$$h(K) = K \bmod M, \quad (1)$$

де h(K) – результат гешування, K – об'єкт який потрібно «загешувати», M – розмір геш-таблиці.

Для мультиплікативного гешування використовується наступна формула:

$$h(K) = M * ((C * K) \bmod 1), \quad (2)$$

де h(K) – результат гешування, K – об’єкт який потрібно «загешувати», M – розмір геш-таблиці, C – довільна дійсна константа, C Є [0,1].

Якщо константа «C» обрана вірно, то можна отримати досить прийнятні результати, тобто створити геш-функцію із мінімальним числом колізій, однак, цей вибір складно зробити.

Ваговий метод є модифікованим методом ділення для текстових вхідних даних:

$$h(K) = \sum_{i=1}^{n}(K[i] * i) \bmod M, \quad (3)$$

де де h(K) – результат гешування, K – «рядок» який потрібно загешувати, M – розмір геш-таблиці, n – кількість символів у рядку, i - позиція символу у рядку, K[i] – i-й символ рядка.

Ваговий метод за рахунок побудови геш-функції, і урахування позиції символів виключає виникнення колізій для рядків, створених перестановкою символів (бар, раб)[1, 4].

Експериментальна частина дослідження передбачала порівняння базових методів гешування та обробки колізій, з метою знаходження оптимального (за швидкістю створення геш-таблиці та обробки колізій) поєднання цих методів. Варто зауважити, що для мультиплікативного методу бралось випадкове значення константи «C».

В результаті експериментального дослідження виявлено, що кількість колізій мінімально залежить від використання конкретного методу, суттєву залежність виявлено від кількості вхідних даних. Для розв’язання колізій використовуються різноманітні методи, основними з яких є методи «ланцюжків» і «відкритої адресації».

Методом ланцюжків називається метод, в якому для розв’язання колізій у всі записи вводяться покажчики, які використовуються для організації списків – «ланцюжків переповнення». У випадку виникнення колізій при заповненні таблиці в динамічний список, що відповідає певній адресі геш-таблиці додається ще один елемент. Пошук в геш-таблиці з ланцюжками переповнення включає етапи: обчислення адреси за значенням ключа; послідовний пошук в списку, що відповідає обчисленій адресі. Процедура вилучення з таблиці зводиться до пошуку елемента та його вилучення з ланцюжка переповнення (динамічного списку). Метод відкритої адресації полягає в тому, що застосовується алгоритм, який забезпечує перебір елементів таблиці, переглядаючи її в пошуках вільного місця для нового запису.

На рисунку 2 показано - як змінюється час потрібний для «гешування» даних залежно від вибраного методе обробки колізій: обробка колізій ланцюжковим методом (зліва) та відкритою адресацією (справа).

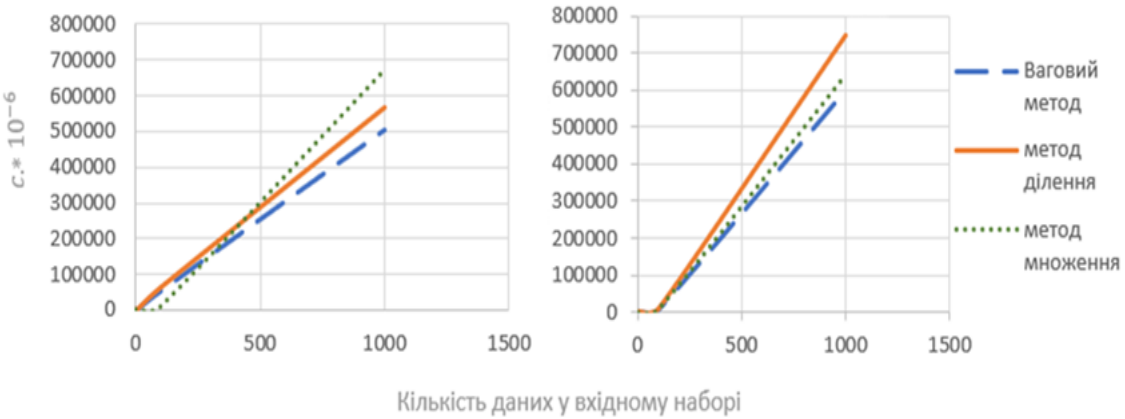


Рис. 2. Швидкість створення геш-таблиці, залежно від методу реалізації обробки колізій

Висновки

В результаті експерименту, найкращим виявилось поєднанням вагового методу та обробки колізій ланцюжковим методом, а найгірший варіант – метод ділення та вирішення колізій відкритою адресацією, відповідно. Звідси можна зробити висновок, що найбільш ефективним, з точки зору швидкості побудови геш-таблиці, є поєднання вагового способу гешування та обробки колізій ланцюжковим методом, що, у середньому, на 10% швидше за інші комбінації. Варто зауважити, що ефективність використання геш-таблиць, отриманих з використанням різних комбінацій методів, для пошуку, буде суттєво залежати від відсотка наповненості таблиці.

Список літератури

1. Бхаргава А. Грокаем алгоритмы. Илюстрованое пособие для програмистов и любопытсттвующих. – Спб: Питер,2017. – 288 с.
2. Кнут Д.Э. Искусство программирования. Том 3. Сортировка и поиск под ред. В.Т.Тертышного (гл. 5) и И.В.Красикова (гл. 6).— 2-е изд.— Москва: Вильямс, 2007.— Т.3.— 832с.
3. Чмора А., Современная прикладная криптография., М.: Гелиос АРВ, 2001.- 256с.
4. Кормен Т., Лейзерсон Ч., Ривест Р., Алгоритмы: построение и анализ, М.: МЦНМО, 2001.-960 с

УДК 004.424.7

В.В. Міхав, Є.В. Мелешко
mihaw.wolodymyr@gmail.com, elismeleshko@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький

ЗАСТОСУВАННЯ МЕТОДУ DELTA-ENCODING ДЛЯ ПРЕДСТАВЛЕННЯ ДАНИХ РЕКОМЕНДАЦІЙНОЇ СИСТЕМИ

Рекомендаційні системи значним чином впливають на те, яким користувачі сприймають інформаційний простір. Вибір методу представлення даних, якими оперує рекомендаційна система, має вагомий вплив, оскільки ефективний спосіб представлення даних, необхідних для роботи такої системи, може зменшити кількість потрібних ресурсів та збільшити кількість доступних алгоритмів для формування списків рекомендацій.

Delta-encoding – це метод, який полягає у представленні ряду чисел як ряду різниць між сусідніми числами, тобто замість ряду $n_0, n_1, n_2, \ldots, n_j, \ldots$ зберігається ряд $n_0, n_1 - n_0, n_2 - n_1, \ldots, n_j - n_{j-1}, \ldots$ [1]. Якщо перед застосуванням цього методу відсортувати числа за зростанням, то усі елементи нового ряду гарантовано будуть додатними та меншими, ніж члени початкового ряду. Це відкриває можливості для оптимізації використання пам'яті, оскільки новим числам потрібно менше бітів для представлення у пам'яті. Головний недолік цього підходу полягає у тому, що між елементами є рекурсивна залежність, і для доступу до випадкового елементу необхідно вирахувати значення усіх його попередників.

Для оптимізації методом delta-encoding було обрано структуру даних «розгорнутий зв'язний список». Це зв'язний список, кожен елемент якого містить масив логічних елементів. Блокова структура дозволяє запровадити додаткову оптимізацію: кожен елемент списку містить окрему послідовність чисел, оброблених за допомогою delta-encoding, а перше число зберігається розпакованим. Завдяки цьому можна швидко визначити блок, у якому має знаходитися шукане значення.

Для того, щоб використовувати менше пам'яті, необхідно виділяти для представлення різниці між числами менше байтів, ніж на початкові числа. У цьому випадку необхідно мати алгоритм розв'язання ситуації, коли для представлення різниці необхідно більше байтів, ніж було передбачено. Одним з варіантів вирішення цієї проблеми є VarLen Encoding [2]. Цей метод передбачає можливість виділяти для числа лише необхідну кількість байтів, використовуючи старший біт кожного байту як маркер кінця послідовності. Головний недолік цього методу полягає у складній процедурі кодування та декодування даних.

Один із запропонованих нами альтернативних методів схожий з VarLen Encoding. Значення різниці розбивається на комірки таким чином, що якщо воно більше, ніж максимальне допустиме значення комірки, то у комірку записується максимальне значення, а у наступну комірку записується зменшена різниця. Таким чином, при використанні комірок по два байти для представлення різниці у 1000000 необхідно $[1000000 / 2^{16}] = 16$ комірок, або 32 байти. Цей метод простіший у кодуванні/декодуванні, але вимагає більших витрат пам'яті.

Наступний запропонований нами метод полягає у тому, щоб виділяти достатньо байтів для розміщення числа повністю, зарезервувавши перший біт, якщо різниця перевищує максимальне значення комірки. Це дозволяє скоротити накладні витрати і полегшити відтворення чисел. Головний недолік цього підходу у тому, що для додавання числа всередину послідовності блок необхідно створити знову.

Наступний запропонований нами метод використовує особливості структури розгорнутого списку. У випадку, коли вставка відбувається у кінець блоку, а різниця перевищує максимальне значення комірки, то перевіряється можливість вставки на початок наступного блоку. Якщо це неможливо, то для числа створюється новий блок. Цей варіант усуває необхідність зберігати у блоці гетерогенні дані, проте спричиняє підвищені витрати пам'яті за рахунок часткового заповнення блоків.

Нами було запропоновано декілька варіантів застосування методу delta-encoding для представлення даних рекомендаційної системи. Кожен з них має свої переваги та недоліки, тому вибір необхідно робити на основі експерименту над типовими даними системи.

Список літератури

1. Hunt J.J., Vo K.P., Tichy W.F. Delta algorithms: An empirical analysis, ACM Transactions on Software Engineering and Methodology (TOSEM), 1998, 7(2), pp. 192-214.

2. Selavo L., "Dynamic data encoding for page-oriented memories", Doctoral dissertation, University of Pittsburgh, 2004.

УДК 004.65

Д.В. Бащенко, М.С. Якименко, Є.В. Мелешко
Lesy4152@gmail.com, m.yakymenko@gmail.com, elismeleshko@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький

ДОСЛІДЖЕННЯ МОЖЛИВОСТІ ЗАСТОСУВАННЯ ГРАФОВОЇ БАЗИ ДАНИХ NEO4J ДЛЯ ПОБУДОВИ СИСТЕМ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ

Система підтримки прийняття рішень – це комп'ютерна автоматизована система, що здійснює допомогу людям у прийнятті рішень в складних умовах. Для аналізу проблеми та створення пропозицій користувачам в системах підтримки прийняття рішень використовуються різні методи: інформаційний пошук, інтелектуальний аналіз даних, пошук знань в базах даних, висновки на основі прецедентів, імітаційне моделювання, еволюційні обчислення і генетичні алгоритми, нейронні мережі, ситуаційний аналіз, когнітивне моделювання тощо.

Важливою частиною систем підтримки прийняття рішень є бази знань, що містять правила та набори фактів, до яких слід застосовувати наявні правила. Бази знань можуть бути побудованими на основі різних моделей, наприклад, семантичної, фреймової, продукційної, гібридної тощо.

Оскільки Neo4j є графовою базою даних типу NoSQL, у ній досить зручно створювати семантичні бази знань.

В основі семантичної моделі представлення знань лежить *семантична мережа* – інформаційна модель предметної області, що має вигляд орієнтованого графу. Вершини такого графу відповідають об'єктам предметної області, а ребра відображають відносини між ними (напр., рис. 1).

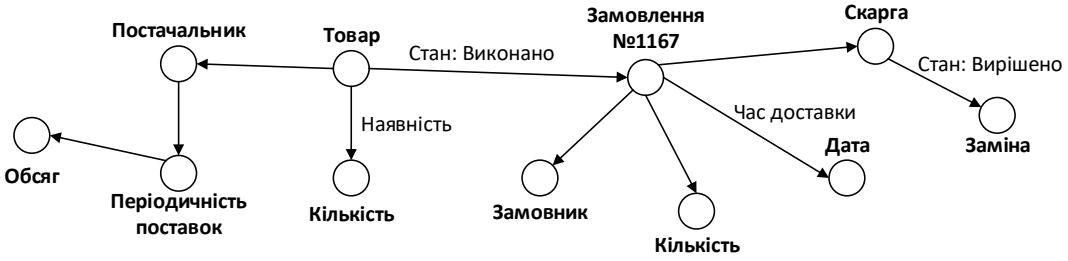


Рис. 1. Приклад частини семантичної мережі для бази знань системи підтримки прийняття рішень для роботі з клієнтами магазину

СУБД Neo4j має наступні структурні елементи, що дають змогу створити семантичну мережу:

– node – вузол графа. Кількість вузлів обмежено значенням 2^{35}, тобто ~ 34 більйони.

– node label – мітка вузла, поставивши такі мітки в подальшому їх можна використовувати для фільтрації даних.

– relation – ребро, зв'язок між двома вузлами. Кількість ребер також обмежено значенням 2^{35}.

– relation identirfier – тип зв'язку (ребра). Максимальна кількість типів зв'язків 32767.

– properties – властивості вузлів та ребер, набір даних, які можна призначити вузлу чи ребру. Наприклад, якщо вузол – це товар, то у властивостях вузла можна зберігати id товару, його назву, характеристики тощо, а якщо ребро зв'язує товар з замовленням, то воно може містити у властивостях статус замовлення, час присвоєння відповідного статусу тощо.

– node ID – унікальний ідентифікатор вузла, аналог ключового поля у реляційних базах даних.

Отже, СУБД Neo4j надає всі необхідні інструменти для створення бази знань на основі семантичної моделі представлення предметної області, що можна в подальшому застосовувати у системі підтримки прийняття рішень.

Перевагами СУБД Neo4j є гнучка модель даних, аналіз в реальному часі, можливості простого пошуку та фільтрації даних, масштабованість та надійність, наявність візуального інтерфейсу, а також існування додатоку Neo4j Aura для застосування у вигляді хмарного сервісу.

Також СУБД Neo4j може працювати з REST API для роботи з такими мовами програмування, як Java, Spring, Scala тощо, з Java Script для роботи з користувацькими інтерфейсами MVC, такими як Node JS, підтримує два види Java API: Cypher API і Native Java API для розробки додатків Java.

Все вище перераховане дозволяє використовувати СУБД Neo4j як середовище для реалізації бази знань для найрізноманітніших систем підтримки прийняття рішень.

УДК 004.65

С.В. Шимко, Є.В. Мелешко, В.А. Резніченко
shymko97@gmail.com, elismeleshko@gmail.com, upsbilly@meta.ua
Центральноукраїнський національний технічний університет, м. Кропивницький

ДОСЛІДЖЕННЯ МОЖЛИВОСТІ ЗАСТОСУВАННЯ ПРОГРАМНОЇ БІБЛІОТЕКИ TENSORFLOW В ЗАДАЧАХ АВТОМАТИЗАЦІЇ

Автоматизація є технологією, за допомогою якої процес або процедура виконуються з мінімальною людською участю [6]. Автоматизація вже давно дозволяє домогтися підвищення продуктивності праці, що часто веде до зниження собівартості одиниці продукту. Методи автоматизації, як і області їх застосування, стрімко удосконалюються і протягом останніх століть розвинулися від простих механізмів до промислових роботів [5, 6]. Автоматизація починає зачіпати не тільки фізичну працю, а й інтелектуальну, добираючись до порівняно нових областей, включаючи і машинне навчання. Автоматизація машинного навчання вже знайшла своє застосування в ряді комерційних продуктів, наприклад, Google AutoML, SAP AutoML тощо.

Машинне навчання – великий підрозділ штучного інтелекту, що вивчає методи побудови алгоритмів, здатних навчатися [5, 7, 8]. Машинні алгоритми навчання використовують обчислювальні методи, щоб «вчитися» безпосередньо на основі отриманих даних, а не покладатися на заздалегідь визначені рівняння в якості моделі. Системи з машинним навчанням є адаптивними. Ціль машинного навчання – частково або повністю автоматизувати рішення різних складних аналітичних задач.

Одним з найпопулярніших методів машинного навчання є штучні нейронні мережі [8]. Вони використовують принципи роботи біологічних нейронних мереж для вирішення задач класифікації, кластеризації, управління, прогнозування тощо. Тип архітектури нейронної мережі визначає коло задач, що вона може вирішувати. Нейронні мережі зазвичай застосовують для моделювання складних взаємозв'язків між вхідними та вихідними даними та пошуку закономірностей у них. Частковим випадком штучних нейронних мереж є глибинне навчання – нейронні мережі з великою кількістю прихованих прошарків нейронів, застосовується для аналізу великих об'ємів даних з досить складними та невідомими взаємозв'язками.

TensorFlow – програмна бібліотека для машинного навчання з відкритим серцевим кодом [3], розроблена компанією Google для вирішення задач побудови і тренування нейронних мереж з метою автоматизації процесів знаходження та класифікації образів, керування, прогнозування, ідентифікації тощо. Основний API для роботи з бібліотекою реалізовано для мови програмування Python, також існують реалізації для R, C#, C ++, Haskell, Java, Go і Swift [3].

Google Brain, розробник бібліотеки TensorFlow, також створив комплексну платформу для розгортання виробничих конвеєрів машинного навчання – TensorFlow Extended (TFX) [3]. TFX уже успішно використовується для автоматизації вирішення деяких проблем у різних галузях, зокрема, медичній галузі [3, 2], електронній коменріції [1, 3], віртуальних соціальних мережах [3, 4] тощо.

Таким чином бібліотеку TensorFlow та нейронні мережі можна використовувати для вирішення ряду задач з автоматизації, зокрема, у електронній комерції, медичній сфері, аналізі даних тощо.

Список літератури

1. Bonnin R. Using TensorFlow to predict product weight and dimensions. – 2019. – URL: https://blog.tensorflow.org/2019/09/using-tensorflow-to-predict-product.html
2. Polzin J.A. Intelligent Scanning Using Deep Learning for MRI. – 2019. – URL: https://blog.tensorflow.org/2019/03/intelligent-scanning-using-deep-learning.html
3. TensorFlow. – URL: https://www.tensorflow.org/
4. Zhuang Y., Thiagarajan A., Sweeney T. Ranking Tweets with TensorFlow. – 2019. – URL: https://blog.tensorflow.org/2019/03/ranking-tweets-with-tensorflow.html
5. Болотова Л.С. Системы искусственного интеллекта: модели и технологии, основанные на знаниях. – Москва: «Финансы и Статистика». – 2012. – 663 с.
6. Иванов А.А. Автоматизация технологических процессов и производств: Учебное пособие / А.А. Иванов. – М.: Форум, 2012. – 224 с.
7. Люгер Дж.О. Искусственный интеллект: стратегии и методы решения сложных проблем / Дж.О. Люгер. – М.: Диалектика, 2016. – 864 с.
8. Редько В.Г. Эволюция, нейронные сети, интеллект: Модели и концепции эволюционной кибернетики / В.Г. Редько. – Москва: СИНТЕГ, 2017. – 224 с.

УДК 004.65

Є.В. Мелешко, В.В. Босько, Р.М. Минайленко
elismeleshko@gmail.com, victorvv2@ukr.net, aron70@ukr.net
Центральноукраїнський національний технічний університет, м. Кропивницький

ГРАФОВА БАЗА ДАНИХ NEO4J ЯК ПРОГРАМНЕ СЕРЕДОВИЩЕ ДЛЯ НАВЧАННЯ СТУДЕНТІВ ОСНОВАМ РОБОТИ З СУБД ТИПУ NOSQL

Однією з важливих компетенцій, якою повинен володіти інженер-програміст, є вміння проектувати та реалізовувати бази даних, а також організовувати їх взаємодію з програмним забезпеченням.

В наш час все більшої популярності здобувають нереляційні бази даних типу NoSQL, зокрема графові бази даних. Часто вони бувають більш зручними, ніж традиційні бази даних, для використання у розподілених системах та хмарних сховищах. У графових базах даних інформація зберігається у вузлах графу, а взаємозв'язки між різними інформаційними об'єктами зберігаються у ребрах.

Neo4j – це графова база даних з відкритим сирцевим кодом, створена у 2003 році американською компанією Neo Technology. Для здійснення запитів до цієї бази даних можна використовувати її вбудовану мову Cypher або мову обходів та зміни графів Gremlin. Також існують бібліотеки для роботи з Neo4j для багатьох мов програмування, зокрема, для Java, Python, Clojure, Ruby та PHP.

Крім API для можливості роботи з СУБД Neo4j з використанням різних мов програмування, вона також має зручний та зрозумілий візуальний інтерфейс користувача. Для доступу до нього достатньо завантажити та встановити з офіційного сайту бази даних додаток Neo4j Desktop. У даному додатку можна безпосередньо робити запити до СУБД Neo4j та одержувати результат у вигляді таблиці, графу або тексту. Цей функціонал дозволяє швидко опанувати основи роботи з даною СУБД перед тим як створювати додаток, що буде її використовувати.

Розглянемо навчальний приклад створення запитів у додатку Neo4j Desktop для збереження та аналізу даних соціальної мережі.

Запит №1. Запишемо до бази даних граф соціальної мережі та виведемо увесь її вміст на екран.

```
CREATE (p1:Person {name: "Ганна"}), (p2:Person {name: "Максим"}),
       (p3:Person {name: "Віктор"}),(p4:Person {name: "Поліна"}),
       (p5:Person {name: "Марина"}),
       (p1)-[:friends]->(p4), (p1)-[:friends]->(p2), (p2)-[:friends]->(p3),
       (p5)-[:friends]->(p1), (p5)-[:friends]->(p2), (p5)-[:friends]->(p3)
MATCH (n) RETURN (n)
```

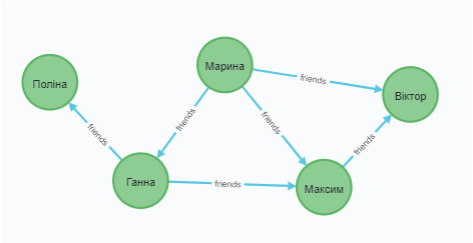


Рис. 1. Виконання запиту №1 у Neo4j Desktop

Запит №2. Отримаємо список усіх друзів деякого учасника соціальної мережі, вказавши його ім'я.

```
MATCH (p1:Person{name:"Максим"})-[r:friends]-(p2:Person) RETURN p2
```

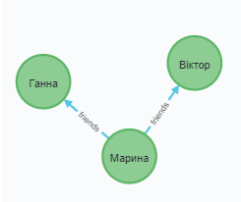


Рис. 2. Виконання запиту №2 у Neo4j Desktop

Зручний інтерфейс і наочність виконання запитів робить дане середовище зручним для навчання студентів роботі з графовими базами даних. А висока функціональність і наявність бібліотек для сумісності з багатьма мовами програмування дозволить потім їм використовувати дану СУБД у реальних проектах.

УДК 004.021

В.С. Гермак, О.В. Коваленко
germak_vs@ukr.net, dr.kovalenkoov@gmail.com
Центральноукраїнський національний технічний університет, Кропивницький

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ АПРОКСИМАЦІЇ ТА ІНТЕРПОЛЯЦІЇ ФУНКЦІЙ

При вирішенні практичних задач, пов'язаних з програмуванням реальних систем, будь то системи автоматизованого керування, складні фізичні, соціальні чи соціотехнічні системи, часто доводиться стикатись з проблемою, пов'язаною з високою складністю математичної моделі системи. Однією з основних причин такої складності часто є велика кількість параметрів системи, які треба врахувати при побудові моделі та подальшій програмній реалізації, а також високий рівень складності функціональних зв'язків між окремими параметрами. В зв'язку з цим, на практиці доводиться дещо нехтувати точністю відображення реальної системи в математичній моделі для спрощення процесу подальшої роботи з цією моделлю, зокрема програмної обробки. Також досить часто при програмуванні реальних систем, зокрема при прогнозуванні їх подальшого розвитку та визначенні необхідного керуючого впливу на систему, доводиться стикатись з тим, що результати вимірювань різноманітних параметрів реальної системи надходять в дискретному вигляді, як значення певних параметрів, виміряні в дискретні моменти часу.

Як у випадку високої функціональної складності математичної моделі, так і у випадку надходження вхідних даних у дискретному вигляді, для подальшої роботи з даними та математичною моделлю доводиться застосовувати апроксимацію та інтерполяцію функцій. Апроксимація це заміна відомої функції наближеною з виконанням умови мінімального відхилення апроксимуючої функції від заданої. Якщо стоїть задача досягти точного збігу вхідної та наближеної функцій в деяких визначених точках (наприклад в ті моменти часу, коли виконувались вимірювання параметрів), застосовують методи інтерполяції функцій, такі як інтерполяція поліномами Лагранжа або Ньютона. На перший погляд, що може бути краще в ролі наближеної функції, ніж функція, яка точно проходить через точки, що відображають результати вимірювань параметрів реальної системи. Але насправді це не зовсім так. По перше, для інтерполюючої функції важливий збіг з початковою функцією в конкретних точках, а між цими точками або за межами інтервалу вимірювань функція може вести себе як завгодно. Така поведінка наближеної функції може призвести до досить великих похибок між точками виміру або за межами інтервалу вимірювань. Зважаючи на те, що досить часто основною метою дослідження реальних систем є визначення їх поведінки в моменти часу між вимірюваннями та прогнозування поведінки систем на майбутнє, тобто за межами інтервалу вимірювань, такий механізм наближення в деяких випадках не є оптимальним. Ще одним мінусом застосування інтерполяційних методів є те, що при вимірюванні параметрів системи неможливо уникнути похибок вимірювання, як мінімум пов'язаних з класом точності вимірювальних приладів. Тому, якщо в деяких випадках для наближення таблично заданої функції застосувати інтерполяційні методи, особливість, яка на перший погляд сприймається як перевага методу (збіг наближеної функції і точної в точках виміру), перетвориться на недолік. Завдяки цьому збігові в поведінку наближеної функції будуть перенесені всі похибки вимірювань та проміжних обчислень вхідних даних. Інколи це може призвести до значних похибок. Таким чином, на практиці досить часто доцільнішим буде застосування методів апроксимації, ніж інтерполяції.

Одними з найпоширеніших методів апроксимації функцій є:

1. Наближення рядом Тейлора. Даний метод має багато недоліків, застосовується переважно для неперервних гладких функцій на локальних інтервалах. Майже не застосовний для розривних періодичних функцій або неперервних недиференційованих функцій.

2. Метод найменших квадратів. Досить простий в реалізації, але може давати суттєве відхилення від вузлових точок (тобто результатів вимірювань). Для підвищення точності наближення може знадобитись збільшення степеня полінома, а це в свою чергу приводить до необхідності здійснювати повний перерахунок полінома без можливості використання раніше отриманих результатів.

3. Наближення ортогональними поліномами Чебишева. Збільшення степеня полінома не призводить до зміни коефіцієнтів при нижчих степенях.

4. Апроксимація поліномами Бернштейна. Метод, застосовний для спрощення вигляду складної аналітично заданої функції. Недоліком є досить вузький інтервал наближення, метод працює на відрізку (0;1). Тому для розширення інтервалу наближення вимагає використання заміни змінної.

Отже, при програмному моделюванні складних систем потрібно відповідально підходити до вибору методу інтерполяції чи апроксимації функціональної залежності, покладеної в основу моделі. Це допоможе уникнути зайвих похибок та отримати точніший прогноз поведінки системи.

УДК 338.47

М.А .Дем'янчук[1], Н.Д. Маслій[2]
ma-demyanchuk@ukr.net, masliy.natalia@gmail.com
[1]д. е. н., доцент кафедри фінансів, банківської справи та страхування, Одеський національний університет імені І.І. Мечникова; старший науковий співробітник відділу ринку транспортних послуг, Інститут проблем ринку та економіко-екологічних досліджень НАН України, Одеса,:
[2]д. е. н., професор кафедри фінансів, банківської справи та страхування Одеський національний університет імені І.І. Мечникова; старший науковий співробітник відділу ринку транспортних послуг, Інститут проблем ринку та економіко-екологічних досліджень НАН України, Одеса

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ПІДПРИЄМСТВАМИ СФЕРИ ВОДНОГО ТРАНСПОРТУ

Основним трендом інноваційної трансформації та цифровізації портів світу є інтеграція всіх учасників глобального ланцюга поставок у єдину взаємопов'язану мережу на основі цифрової платформи зі створенням єдиного цифрового транспортного коридору та використанням штучного інтелекту. Останніми роками зростає обсяг використання хмарних технологій, що обумовлено необхідністю аналізу «великих даних» (табл. 1). Тому одним із трьох пріоритетних напрямків Стратегії розвитку морських портів України на період до 2038 року виступає покращення сервісу в морських портах, що передбачає впровадження сучасних інформаційних систем для спрощення процедур міжнародної торгівлі та забезпечення привабливості морських портів України для користувачів транспортних послуг. Це обумовлено низкою причин, зокрема: нереалізованим потенціалом вантажопотоку портів, низьким залученням внутрішнього водного транспорту як інтеграційної точки у мультимодальних ланцюгах вантажних перевезень, недостатній рівень екологічної та кібернетичної безпеки в морських портах тощо.

Таблиця 1.

Кількість підприємств сфери водного транспорту, які купували послуги хмарних обчислень та проводили аналіз "великих даних" протягом 2017-2019 років

Показники	одиниць			у % до загальної кількості підприємств	
	2017	2018	2019	2018	2019
1. Кількість підприємств, що проводили аналіз "великих даних", за джерелами "великих даних"					
– дані, отримані зі смарт-пристроїв або датчиків	298	283	294	7,2	7,3
– геолокаційні дані, отримані із портативних пристроїв	240	260	288	6,6	7,1
– дані, сформовані із соціальних медіа	102	87	86	2,2	2,1
– інші джерела	281	215	186	5,5	4,6
2. Кількість підприємств, які купували послуги хмарних обчислень	274	296	327	7,5	8,1
з них за видами послуг хмарних обчислень					
– електронна пошта	136	149	176	3,8	4,4
– офісне програмне забезпечення	130	129	151	3,3	3,7
– хостинг бази даних підприємства	74	83	120	2,1	3,0
– сервіс для зберігання файлів	87	105	131	2,7	3,2
– фінансові або бухгалтерські прикладні програми	149	154	193	3,9	4,8
– програми для управління взаємовідносинами з клієнтами	56	65	82	1,6	2,0
– комп'ютерна потужність для функціювання програмного забезпечення підприємства	77	87	93	2,2	2,3

Джерело: сформовано авторами на основі даних [1].

Наразі головною метою Міністерства інфраструктури України є повна цифровізація всіх процесів та створення єдиної smart-системи на транспорті, що дозволить не лише забезпечення мультимодальності транспорту та створення цифрових транспортних коридорів, а й приведе до спрощення отримання транспортних послуг. Впровадження таких цифрових рішень на транспорті дозволить Україні швидше інтегруватись у єдину транспортну мережу, що об'єднує Європу з Азією, перетворившись на міжнародний транспортний хаб, а також допоможе у розвитку Шовкового шляху та інших транспортних коридорів [2].

Підкреслимо, що такі процеси вимагають проведення великих капітальних вкладень. Проте протягом

останніх чотирьох років капітальні інвестиції є незначними та складають менше 1% від капітальних інвестицій транспортної сфери. В свою чергу це вплинуло на зміну обсягів експорту та імпорту транспортних послуг. Дослідження показали, що на відміну від обсягів експорту транспортних послуг морського транспорту, які протягом аналізованого періоду скоротились на 19,0%, обсяги імпорту транспортних послуг зросли на 42,8%. Також спостерігається зменшення імпортних транспортних послуг річкового транспорту. Тому важливим питанням на даний час для сфери водного транспорту є залучення інвесторів, спроможних на значні вкладення з метою розвитку цифрового транспортного коридору, який має передбачати не тільки впровадження інформаційних систем у діяльність транспорту, зокрема морських портів, але й використовувати електронне управління ланцюгами поставок (e-supply chain management), екологічний менеджмент, проводити технічне та технологічне оновлення, заходи з екологізації флоту та відтворення природних водних ресурсів, цифрове брендування портів, що сприятиме ефективному впровадженню концепції «смарт порту».

Також слід зазначити, що застосована на підприємствах великого масштабу різних сфер економічної діяльності, ECM-система (enterprise content management – система управління корпоративним контентом) є стратегічною інтеграцією функціональних та технологічних рішень, що забезпечує управління цифровими документами і контентом різного типу та формату, їхнє зберігання, обробку та доставку по заздалегідь заданому маршруту. Сучасні ECM-системи підтримують механізми e-docflow и e-workflow, тобто пропонують автоматизацію діловодства та автоматизацію діяльності компанії, що дозволяє ефективно організувати роботу із дорученнями згідно набору певних правил.

На даний час за даними [3] морські порти Одеса, Чорноморськ та Південний приєднані до інформаційної системи портового співтовариства (ІСПС) на базі ТОВ «ППЛ 33-35» для інтеграції всіх учасників транспортного і вантажного процесів в порту в єдиний інформаційний простір, в який включені понад 1300 організацій різних форм власності, державні контролюючі та правоохоронні органи. Зокрема це експедитори, перевізники, морські агенти, вантажовласники, портові оператори, адміністрації портів, контролюючі органи та постачальники морських послуг. За допомогою ІСПС проводиться більше 5 млн. транзакцій на місяць при електронному документообігу більш ніж 90%.

Застосування e-invoicing (системи електронного документообороту) та e-contracting сприяє поширенню виставлення електронних рахунків, що забезпечує дотримання умов угод між портом й замовником послуг та зменшує бюрократію. Слід зазначити, що відповідно до Угоди про асоціацію України з ЄС [4] має бути імплементована у вітчизняне законодавство європейська директива про електронні рахунках (eInvoicing, 2014/55/EU) до 01.01.2024. Проте слід зазначити, що для ефективного та безперебійного функціонування на міжнародному ринку для портів, як мінімум, які задіяні у міжнародних транспортних маршрутах, необхідно подолати адміністративно-правовий бар'єр з оформлення товарно-транспортних накладних, оскільки кожна країна має свої затверджені форми, що призводить до нелегітимності на даний час міжнародних електронних перевізних документів. Уніфікація таких накладних, зокрема на міжнародному рівні, потребує внесення відповідних змін у нормативні документи і надання можливості здійснювати взаємодію із застосуванням електронних цифрових підписів.

Вирішення таких проблем сприяло б розробленню та впровадженню системи міжнародного процесингового центру для здійснення та обробки платежів, що здійснюються у кожній інтеграційній точці міжнародного транспортного маршруту, оскільки наразі процедури оплати перевезень та їхньої перевірки доволі складні і потребують значного часу, що, в свою чергу, збільшує час знаходження вантажу на маршруті. Проведення цифрового брендування портів на міжнародному рівні передбачає використання прогресивних практик маркетингу, зокрема принципів B2B, поширення інформації щодо їхньої інвестиційної привабливості, інфраструктурних можливостей та позиціонування як сучасних цифрових портів, які здатні забезпечити високий рівень сервісу та захисту від кіберзагроз. Таким чином, зазначені інноваційні процеси трансформації транспортної, зокрема тотальна цифровізації вітчизняних портів, системи здатні забезпечити прискорений розвиток національної економіки, сформувавши транспортний хаб на міжнародному транспортному маршруті між Азією та Європою.

Список літератури:

1. Державна служба статистики України. Статистична інформація. Використання інформаційно-комунікаційних технологій на підприємствах. URL: http://www.ukrstat.gov.ua/operativ/operativ2018/zv/ikt/arh_ikt_u.html (дата звернення: 15.03.2021).

2. Міністерство інфраструктури України. Наша мета – повна цифровізація процесів і створення єдиної smart-системи на транспорті, - Владислав Криклій. URL: https://mtu.gov.ua/news/32228.html (дата звернення: 15.03.2021).

3. Єдине вікно – локальне рішення. URL: http://singlewindow.org/conception (дата звернення: 27.02.2021).

4. Про ратифікацію Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: Закон України від 16.09.2014 р. №1678-VII. Дата оновлення: 16.09.2014. URL: https://zakon.rada.gov.ua/laws/show/984_011#Text (дата звернення: 15.03.2021).

УДК 004.8. 314.172

Ш.А. Мехтиев
shakir.mehtieff@gmail.com
Институт информационных технологий НАН Азербайджана, Баку

ВОПРОСЫ ИНТЕГРАЦИИ ТЕХНОЛОГИЙ ИНДУСТРИИ 4.0 ДЛЯ РЕШЕНИЯ ДЕМОГРАФИЧЕСКИХ ПРОБЛЕМ

Рост численности населения современной цивилизации существенно связан с уровнем развития производительных сил. Эта тенденция стала проявляться, начиная с эпохи неолита, отличительной чертой которой был переход от собирательства, охоты и рыбной ловли к аграрному обществу с преимущественным преобладанием скотоводства и земледелия. Относительно высокопроизводительные способы получения продуктов питания существенно ослабили зависимость человека от природы и способствовали росту его численности.

Известно, что со второй половины XVIII в. начинаются процессы перехода от аграрного общества к индустриальному обществу. В указанный период в ряде стран Западной Европы и Северной Америки в производственных целях использовались изобретения и усовершенствования, ставшие предпосылками первой промышленной революции. Для нее были характерны разделение труда, механизация, массовое производство, увеличение производительности труда. Именно в период 1750-1850 гг. население Англии, которая была пионером промышленной революции, по некоторым оценкам, увеличилось вдвое. Увеличение населения можно также связать и с улучшением медицинского обслуживания, и техническими достижениями в применяемых методах лечения, диагностики и профилактики заболеваний [1], а также увеличением производства продуктов аграрного сектора. Улучшение состояния здоровья, позволяющее большему количеству детей дожить до взрослой жизни, способствовало повышению уровня рождаемости [2].

Таким образом, исследования показывают, что именно с началом первой промышленной революции происходят устойчивый рост численности населения, высокий уровень миграции и урбанизации, которые приобрели особую актуальность и в следующих промышленных революциях.

Отметим, что систематическое изучение динамики населения, а также причин и следствий изменений в составе населения, изучаются демографической наукой, основу которой составляют данные. Данные о населении содержат различные важные детали, такие как рождение и смерть. Другими демографическими данными являются возраст, пол, годовой доход, род занятий, язык, образование и т. д. Степень социального, экономического, политического и культурного развития отдельной страны также составляется по данным о населении. Однако реальное увеличение доступности данных о населении стало происходить в периоды третьей и, в особенности, четвертой промышленных революций. Компьютерные технологии, Интернет, Всемирная паутина, Интернет вещей (ИВ), мобильные телефоны, социальные сети и др. предоставили беспрецедентные большие данные (*Big Data*) об обществе и поведении человека. В работе [3] предложены концептуальные основы формирования единой электронной демографической системы на основе этих данных.

Однако, современное общество развивается в условиях четвертой промышленной революции (Индустрия 4.0) [4], и ее основными технологическими платформами являются киберфизические системы (КФС), ИВ, искусственный интеллект (ИИ), роботы, облачные вычисления, дополненная и виртуальная реальности и др. Формирование единой электронной демографической системы в большой степени зависит от применения технологий Индустрии 4.0 и их интеграции с демографическими процессами. Рассмотрим некоторые применения этих технологий.

А. Стареющее общество.

Одной из объективных демографических тенденций современного общества является стареющее общество: рост мирового благосостояния, и медицинские достижения привели к увеличению продолжительности жизни. В то же время уровень рождаемости резко упал во всем мире, особенно в промышленно-развитых странах и странах с переходной экономикой. Согласно прогнозам, к 2050 г. людей старше 65 лет станет больше, чем подростков и молодежи вместе взятых (от 15 до 24 лет). В некоторых регионах, таких как Европа и Восточная Азия, уже возникает значительная проблема с оказанием поддержки пожилым людям и обеспечением ухода за ними [5]. Люди в пожилом возрасте могут быть зависимыми от посторонней помощи по таким причинам, как болезнь, нарушение или потеря подвижности, и могут потребовать различной степени особого ухода. В этой области управляемые ИИ роботы и дроны могут использоваться в мониторинге поведения и здоровья пожилых людей, для помощи им или опекуну в их повседневных задачах; для доставки еды и лекарств и обеспечить социальное взаимодействие [6].

Б. Охрана здоровья.

Перспективным направлением является использование носимых датчиков тела с поддержкой ИВ, облачных, туманных и краевых вычислений. Мониторинг состояния здоровья в режиме реального времени с целью прогнозирования развития болезней может снизить нагрузку на систему здравоохранения. Количество

носимых беспроводных датчиков и систем быстро растет. Одновременно проводятся исследования для достижения энергоэффективности и микроминиатюризации датчиков для сбора данных, а также по автоматическому анализу больших данных, генерируемых этими датчиками. Этот расширенный анализ данных может помочь в создании персонализированных диагнозов и предоставлении рекомендаций по лечению на индивидуальном уровне.

В. Миграция населения.

Глобальная цифровизация помогла улучшить доступ к существующим данным, таким как переписи и регистры населения и биометрические базы данных. За последние годы растущее число проектов и приложений продемонстрировало потенциал использования различных типов источников больших данных, таких как, мобильный телефон, социальные сети или спутниковые данные, для улучшения понимания явлений, связанных с глобальной миграцией и мобильностью человека. Знание того, где находятся люди, имеет решающее значение для точной оценки воздействия и планирования мероприятий, особенно тех, которые ориентированы на здоровье населения, продовольственную безопасность, изменение климата, конфликты и стихийные бедствия. Например, данные, собранные операторами сетей мобильной связи, могут с минимальными затратами предоставить точные и подробные карты распределения населения в национальном масштабе и за любой период времени, гарантируя при этом конфиденциальность пользователей телефонов [7].

Г. Дефицит квалифицированных кадров.

В ближайшие годы прогнозируется тенденция уменьшения квалифицированного персонала. Поскольку возрастает вероятность возникновения нехватки рабочей силы, это впоследствии поставит под угрозу дальнейший экономический рост страны. Решением данной проблемы могут стать коллаборативные роботы (коботы), разработанные для совместной работы с людьми. Автоматизируя монотонные, повторяющиеся и требовательные к физическим нагрузкам задачи, коботы позволяют использовать уникальные человеческие возможности в других областях.

Д. Урбанизация и "умный город".

Урбанизация относится к естественному перемещению населения из сельской местности в городские районы. В настоящее время 60% мирового населения проживает в пяти тысячах городов. Концепция "умного города" предполагает функционирование города и соответствующих служб как интеллектуальной КФС. Отметим, что КФС – это сложная система, объединяющая вычисления, связь и физические процессы. В таком "умном городе" могут быть решены следующие последствия урбанизации: транспортная проблема, здравоохранение, общественная безопасность, санитария и сбор отходов, электроснабжение, управление водными ресурсами и т. д.

Таким образом, технологии Индустрии 4.0 и вызванные ими глобальная цифровизация оказывают огромное влияние на происходящие демографические процессы во всем мире. Эти технологии создали предпосылки решения ряда проблем современной цивилизации, вызванных объективными причинами, такими как, старение, спад рождаемости, нехватка квалифицированных кадров, миграция, урбанизация и др.

Список литературы

1. Ш. Мехтиев и Б. Агаев, "Медицинская электроника: состояние, проблемы и перспективы", *I респ. науч.-практ. конф. "Мультидисциплинарные проблемы электронной медицины"*, Баку, с. 110-113, 2016.
2. R. Wilde, "Population growth and movement in the industrial revolution", 2020.
URL: https://www.thoughtco.com/population-growth-and-movement-industrial-revolution-1221640
3. Р. М. Алгулиев и др., "Формирование электронной демографии как эффективного инструмента социальных исследований и мониторинга данных о населении", *Вопросы государственного и муниципального управления*, № 4, с. 61-86, 2019.
4. H. Kagermann, W. Wahlster, and J. Helbig, Recommendations for implementing the strategic initiative INDUSTRIE 4.0. p. 80, 2013.
5. Демографические изменения, ООН, 2020. URL: https://www.un.org/ru/un75/shifting-demographics
6. T. Siripala, "Japan's robot revolution in senior care", 2018.
URL: https://www.japantimes.co.jp/opinion/2018/06/09/commentary/japan-commentary/japans-robot-revolution-senior-care/
7. P. Devillea et al., "Dynamic population mapping using mobile phone data", *Proceedings of the National Academy of Sciences*, vol. 111, no. 45, pp. 15888-15893, 2014.

УДК 004.85

М.О. Бубела, В.О. Шевчук, Л.І. Поліщук
ya.bubela@gmail.com, vlad3032002@gmail.com, pli_80@ukr.net
Центральноукраїнський національний технічний університет, Кропивницький

АНАЛІТИЧНИЙ ОГЛЯД ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В МЕДИЦИНІ

У сучасному світі медицина відіграє важливу роль у житті людства. Завдяки досягненням у галузі медицини людство досягло збільшення тривалості життя та покращило її якість. Однак різке збільшення обсягу інформації в сфері медицини призвело до необхідності якісної та швидкої її обробки, оскільки люди не завжди в змозі справитися з цією проблемою, «людський фактор» не дозволяє обробляти інформацію зі 100% точністю. Подібна ситуація спостерігається у повсякденній роботі лікаря: є лікарська помилка, частоту якої наукове співтовариство намагається зменшити. Штучний інтелект (ШІ) та системи машинного навчання повинні допомогти у цьому питанні. Ще одним фактором, який робить системи штучного інтелекту надзвичайно перспективними, є відносна економічна ефективність та переваги використання цих систем. За прогнозами, до 2024 року ринок штучного інтелекту для медицини зросте до 10 мільярдів доларів. Крім того, впровадження систем штучного інтелекту зменшить витрати у ключових сферах розвитку ринку штучного інтелекту для медицини. Інвестиції в програмні платформи ШІ, що надають інструменти, технології та послуги на основі структурованої та неструктурованої інформації, оцінюються у 2,5 мільярда доларів на рік.

Штучний інтелект дозволяє комп’ютерам вчитися на власному досвіді, пристосовуватися до заданих параметрів та виконувати завдання, які раніше могли виконувати лише люди. У більшості реалізацій ШІ, починаючи від комп'ютерних шахістів і закінчуючи автомобілями без водіїв, вміння глибоко вивчати та обробляти природну мову є вирішальним. Завдяки цим технологіям комп’ютери можна «навчити» виконувати певні завдання, обробляючи велику кількість даних та виявляючи в них закономірності.

Експертні системи - це застосування систем штучного інтелекту, в яких база знань являє собою формалізовані практичні знання висококваліфікованих спеціалістів у вузькій предметній області. Експертні системи призначені для заміни експертів при вирішенні проблем через їх недостатню кількість, недостатню ефективність у вирішенні проблеми або в небезпечних умовах. Зазвичай експертні системи розглядаються з точки зору їх застосування у двох аспектах: для яких завдань вони можуть бути використані та в якій галузі діяльності. Ці два аспекти накладають свій відбиток на архітектуру експертної системи, що розробляється. Можна виділити наступні основні класи завдань, які можна вирішити за допомогою експертних систем: діагностика; передбачення; управління; дизайн (конфігурація).

Розробка ШІ можлива лише за наявності експертів у цій галузі, і експерти повинні погодитись у своїй оцінці запропонованого рішення; проблема повинна належати до досить структурованої області.

Компетентність людини з часом слабшає, і перерва в діяльності може вплинути на професійні якості. Передача знань від однієї експертної особи до іншої є складною, на відміну від передачі інформації між ШІ. Це простий процес копіювання даних з однієї системи в іншу, без необхідності перекладу даних та тривалого навчання, як у людей. Також впливає так званий «людський фактор», через який прийняття рішення людиною може бути ускладненим, що може призвести до критичних ситуацій, особливо в медицині.

Для моделювання процесів, що відбуваються в мозку людини, використовують нейронні мережі. Штучні нейрони об'єднуються в мережі, з'єднуючи виходи одних нейронів з входами інших. Спрощено кажучи, нейронна мережа - це просто програма, яка отримує дані на вході і дає відповіді на виході. Побудована з дуже великої кількості простих елементів, нейронна мережа здатна вирішувати надзвичайно складні проблеми. Існують також більш складні моделі, в яких вихід однієї мережі спрямовується на вхід іншої. Ці моделі створюють каскади нейронних мереж, так званих багатошарових нейронних мереж.

Іншим цікавим типом нейронної мережі є нейронна мережа зі зворотним зв'язком (RNN, рекурентна нейронна мережа), коли вихід з мережевого рівня надходить назад на один із входів. Такі платформи мають «ефект пам'яті», це означає, що інформація не втрачається при переході від одного «нейрона» до іншого, що робить такі системи неймовірно ефективними. Такі системи можна використовувати для прогнозування поведінки живого об’єкта, який активно використовується в медицині.

УДК 004.031 42

Т.Х. Фаталиев, Ш.А. Мехтиев
t.fataliyev@gmail.com, shakir.mehtieff@gmail.com
Институт информационных технологий НАН Азербайджана, Баку

О ВОЗМОЖНОСТЯХ ПРИМЕНЕНИЯ РЕШЕНИЙ INDUSTRY 4.0 В НАУКЕ

Термин “Индустрия 4.0” (*Industry* 4.0) был введен для описания масштабного применения информационных технологий в промышленном производстве [1]. С 2011 года по всему миру появились инициативы, касающиеся совмещения промышленного производства, цифровых технологий и Интернета. Главный экономический потенциал *Industry* 4.0 заключается в ее способности ускорить корпоративные процессы принятия решений и адаптации. Это касается как процессов повышения эффективности в проектировании, производстве, обслуживании, продажах и маркетинге, так и основной деятельности отдельных структурных подразделений и изменения бизнес-модели. *Industry* 4.0 можно определить через цифровизацию и объединение технических систем на базе технологий беспроводных сенсорных сетей (*Wireless Sensor Networks, WSN*), Интернета вещей (*Internet of Things, IoT*), больших данных (*Big data*), облачных сервисов (*cloud computing*), озер данных (*data lake*), искусственного интеллекта (*Artificial Intelligence, AI*) и др. В то же время стало возможным слияние физического и виртуального мира через киберфизические системы (*Cyber-Physical Systems, CPS*). *CPS* могут осуществлять мониторинг и управление социальными, производственно-технологическими или экологическими объектами с целями выполнения возложенных на них функций и недопущения аварийных ситуаций или чрезвычайных происшествий (неисправности, поломки, экологические риски и т.п.). Другие группы *CPS* могут функционировать в “умном городе” (*smart city*), т.е. существует некая гипотетическая инфраструктура (распределенная или централизованная), в которой все ее активы (узлы или модули) объединены в сеть.

Можно выделить следующие основные характеристики *Industry* 4.0 [2]:

- Вертикальное объединение интеллектуальных производственных систем (интеллектуальные фабрики, интеллектуальные города, интеллектуальные датчики).
- Горизонтальная интеграция посредством глобальных сетей нового поколения для создания стоимости, включая интеграцию деловых партнеров и клиентов.
- Сквозное проектирование по всей цепочке создания стоимости, включая не только производственный процесс, но и весь жизненный цикл продукта.
- Ускорение с помощью экспоненциальных (*IoT, WSN, AI* и др.) технологий, что обеспечивает индивидуальные решения, гибкость и экономию в производственных процессах.

Огромный потенциал *Industry* 4.0 для научной среды привел к появлению и развитию концепции *Science* 4.0 [3]. В этом контексте актуальными стали вопросы сбора, хранения, обработки, передачи и анализа научных данных, организация научной деятельности и управление наукой, объединенных концепцией *Science* 4.0 с широким использованием технологической платформы *Industry* 4.0.

Рассмотрим научную среду с точки зрения интеграционных процессов в *smart city* [4]. Известно, что понятие *smart city* постоянно развивается, широко используется в инновационных технологиях. Применение базовых технологий *Industry* 4.0 актуально для решения следующих задач в этой среде:

• В отношении зданий – бесперебойное электроснабжение и водоснабжение; климат-контроль; контроль доступа; охрана зданий и видеонаблюдение; управление материалами и оборудованием; мониторинг оборудования; управление зданием, обнаружение и предупреждение об опасности и т.д.

• Сетевая и вычислительная инфраструктура – обслуживание сетевых ресурсов, средств и оборудования; сетевой мониторинг и безопасность; электронные услуги; постоянная диагностика и защита и др.

• Управление и безопасность информационного обеспечения науки.

• Интеграция *Industry* 4.0 в среду научных исследований.

В этой среде генерируются большие потоки данных. Здесь следует отметить, что традиционные данные можно классифицировать следующим образом [5]:

• Данные наблюдений – полученные с телескопов, спутников, социальных сетей, демографических исследований, исторической информации или одноразовой записи событий. В большинстве случаев эти данные не могут быть повторены и поэтому должны быть сохранены.

• Экспериментальные данные – полученные в результате высокопроизводительных решений клинических, биомедицинских и фармацевтических экспериментов или других контролируемых экспериментов. Особенно важно хранить некоторые данные, которые невозможно перепроверить по этическим или другим причинам, например, данные о людях и исчезающих видах.

• Вычислительные данные – генерируются в результате крупномасштабных вычислений в суперкомпьютерах, центрах обработки данных и т. д., хранятся в течение определенного периода и обрабатываются с помощью технологий интеллектуального анализа.

• Информационные данные – используются научными обществами для различных целей. К таким данным относятся геном человека, сейсмология, океанография, клинические исследования, данные об исчезающих видах.

В контексте *Industry* 4.0 открываются новые возможности для сбора, хранения, обработки, передачи и анализа перечисленных данных. Эти данные приобретают универсальный характер, циркулируя в территориально-распределенной структуре научного *smart city*.

Таким образом, базовые технологии *Industry* 4.0, которые включают *CPS, IoT, AI, cloud computing, Big data* аналитику и др., делают возможной взаимосвязь, а также обеспечивают интеллектуальность отдельных составляющих и целой системы.

IoT представляет собой интеграцию датчиков и вычислений в интернет-среде посредством *WSN*, что позволяет обнаруживать любые объекты и их подключение к более широкой сети.

Cloud computing обеспечивают сетевой доступ по запросу к общему пулу вычислительных ресурсов. Эта технология позволяет хранить данные в центрах обработки данных через удаленный доступ. Таким образом, *cloud computing* облегчают интеграцию различных устройств, поскольку им не нужно физически находиться рядом.

Комбинация использования *IoT* и *cloud computing* позволяет подключать различное оборудование, собирая огромный объем данных, что приводит к проблеме *Big data*. Они включают данные систем и объектов, такие как, показания датчиков, и совместно с аналитикой, например, интеллектуального анализа данных и машинного обучения, представляют один из наиболее важных факторов *Industry* 4.0. *Big data* так же необходимы для создания цифровых двойников (*digital twin*), и, следовательно, аналитика обеспечивает расширенные возможности прогнозирования, выявляя события, которые могут повлиять на среду, до того, как они произойдут. Сочетание *Big data* с аналитикой может поддерживать самоорганизацию процессов и оптимизировать функции принятия решений во всех аспектах управления

В заключении отметим, что в рамках *Science* 4.0 можно предложить следующую структуру обработки данных:

• На уровне физических объектов данные собираются с датчиков, установленных для измерения различных физических параметров.

• На начальном вычислительном уровне происходит первичная обработка данных в соответствии с ее назначением и получение оперативной информации о характеристиках отдельных компонентов или формирование сигналов управления обратной связью.

• Проведение сложных расчетов на прикладном уровне на основе данных, обрабатываемых на нижних уровнях, и создание различных типов физических моделей объектов.

• Проведение анализа больших данных в центрах обработки данных. На этом уровне новые знания приобретаются за счет применения технологий *AI*, создается обратная связь из киберпространства в физическое пространство для корректировки системы и проведения превентивных мер.

Таким образом, реализация *Science* 4.0 представляет сложный процесс и должна претворяться в жизнь поэтапно.

Список литературы

1. H. Kagermann, W. Wahlster, and J. Helbig, Recommendations for implementing the strategic initiative INDUSTRIE 4.0. p. 80, 2013.

URL: https://www.din.de/blob/76902/e8cac883f42bf28536e7e8165993f1fd/recommendations-for-implementing-industry-4-0-data.pdf

2. Industry 4.0. Challenges and solutions for the digital transformation and use of exponential technologies. URL: https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/manufacturing/ch-en-manufacturing-industry-4-0-24102014.pdf

3. As the world changes, science does too – and that’s a good thing.

URL: https://theconversation.com/as-the-world-changes-science-does-too-and-thats-a-good-thing-152688#:~:text=The%20term%20%E2%80%9CIndustry%204.0%E2%80%9D%20has,virtual%2C%20physical%20and%20biological%20domains.

4. T. Kh. Fataliyev, Sh. A. Mehdiyev. Integration of Cyber-Physical Systems in E-Science Environment: State-of-the-Art, Problems and Effective Solutions, I.J. Modern Education and Computer Science, № 9, pp. 35-43, 2019.

5. T. Kh. Fataliyev, Sh. A. Mehdiyev. Research of the technology for the management and processing of big scientific data, Problems of Information Society, №2, pp. 60–70, 2019.

УДК 331.45, 614.8

О.В. Оришака, К.М. Марченко, А.К. Марченко
oryhsaka@gmail.com, k_marchenko@i.ua,a26052001@i.ua
Центральноукраїнський національний технічний університет, Кропивницький

ОХОРОНА ПРАЦІ, ЯК СКЛАДОВА ЧАСТИНА БЕЗПЕКИ ЖИТТЕДІЯЛЬНОСТІ ПІД ЧАС ПАНДЕМІЇ SARS-COV-2

Проблеми безпеки життєдіяльності людини і охорони праці, як їх складової частини були, є і будуть самими актуальними, тому що без їх вирішення неможливо існування людства.

Згідно нормативним документам «Охорона праці - це система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження життя, здоров'я і працездатності людини у процесі трудової діяльності» [1].

А безпека життєдіяльності включає санітарно-епідеміологічне благополуччя, охорону здоров'я [2].

Таким чином питання вакцинації, як лікувально-профілактичний захід, є складової частиною охорона праці, яка, в свою чергу є складовою частиною безпеки життедіяльності в тому числі під час пандемії (SARS-CoV-2).

З початку пандемії SARS-CoV-2 пройшло вже більше року, що дозволяє зробити певні висновки.

Нами були проаналізовані дані з відкритих джерел по трьом країнам: Україна [3], Ізраїль [4] і Швеція [5]. Згідно з цими даними, лідируюче місце в світі з вакцинації населення від SARS-CoV-2 займає Ізраїль де станом на 16.03.2021 близько 60% населення вакціновано від SARS-CoV-2 [3].

У Шеції станом на 16.03.2021 вакціновано приблизно 8% населення [5].

Україна за цим показником займає одне з останніх місць в світі, а відсоток вакцинованих людей станом на 16.03.2021 в країні близький до нуля [3].

Статистика смертності від SARS-CoV-2 в Ізраїлі, за даними порталу JHU CSSE COVID-19 Data [6], дані якого використовує і всесвітній сервіс Google, становить 67 осіб (середнє значення за 7 діб на верхньому екстремумі кривої смертності), що з урахуванням чисельності населення країни 8,88 млн. людей відповідає показнику смертності 7,3 людини на 1 тис. населення країни.

За даними того ж джерела [6], статистика смертності від SARS-CoV-2 у Швеції становить 138 осіб (середнє за 7 діб на верхньому екстремумі кривої смертності), що з урахуванням чисельності населення країни 10,23 млн. людей відповідає показнику смертності 13,5 осіб на 1 тис. населення країни.

Статистика смертності від SARS-CoV-2 на Україні, за даними порталу JHU CSSE COVID-19 Data [6], становить 234 осіб, що з урахуванням чисельності населення країни 40 млн. чоловік відповідає показнику смертності 5,85 чоловік на 1 тис. населення країни.

Таким чином, вищеназвані показники смертності від SARS-CoV-2 на Україні, в Ізраїлі та Швеції одного порядку, та істотно не відрізняються, чого не можна сказати про показники ступеня охоплення вакцинацією населення.

Вищенаведені факти свідчать про те, що щеплення від інфекції SARS-CoV-2 під час пандемії SARS-CoV-2 не призводять до зменшення смертності від інфекції SARS-CoV-2.

Список літератури

1. Сайт Верховної ради України [Електронний ресурс] // Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2694-12#n13.

2. Сайт Верховної ради України [Електронний ресурс] // Режим доступу до ресурсу: https://zakon.rada.gov.ua/rada/show/v-482729-14#Text

3. Сайт МинФин [Електронний ресурс] // Режим доступу до ресурсу: https://index.minfin.com.ua /reference/coronavirus/vaccination

4. Сайт МинФин [Електронний ресурс] // Режим доступу до ресурсу: https://index.minfin.com.ua /reference/coronavirus/vaccination/israel

5. Сайт МинФин [Електронний ресурс] // Режим доступу до ресурсу: https://index.minfin.com.ua /reference/coronavirus/vaccination/sweden

6. Сайт JHU CSSE COVID-19 Data [Електронний ресурс] // Режим доступу до ресурсу: https://github.com /CSSEGISandData/COVID-19

УДК 004.62

В.В. Прокопов, Є.В. Мелешко
prostoemail97@gmail.com
Центральноукраїнський національний технічний університет, Кропивницький

ДОСЛІДЖЕННЯ СПОСОБУ ПРИВЕДЕННЯ ТЕКСТОВИХ ДАНИХ ДО ЗРУЧНОЇ ДЛЯ ОБРОБКИ АЛГОРИТМАМИ КЛАСТЕРИЗАЦІЇ ФОРМИ ДЛЯ АНАЛІЗУ ДАНИХ З ВЕБ-РЕСУРСІВ

Разом із стрімким накопиченням даних у мережі Інтернет починають поставати проблеми стосовно їх аналізу, фільтрації, класифікації та пошуку. Одним із способів їх дослідження є кластерний аналіз.

Метою даної роботи є дослідження способу приведення текстових даних до зручної для обробки алгоритмами кластеризації форми, який можна застосувати для аналізу відкритих даних з веб-сайтів.

Одним із найважливіших моментів у процесі аналізу даних є проблема їхнього представлення у формі, яка буде зрозуміла для алгоритмів, які будуть займатися їх подальшою обробкою. Алгоритми для обробки даних потребують їх представлення у чітко визначеному форматі – цифровому. Тож, коли йде мова про оброку текстових даних, логічно випливає питання щодо їх перетворення у зрозумілу та прийнятну для алгоритму форму. Одним із ефективних підходів до вирішення такої задачі є векторизація (або векторне представлення слів).

Під векторним представленням слів розуміється сукупність різних підходів до моделювання мови та навчання представлень в обробці природної мови, спрямованих на зіставлення зі словами, узятими із деякого словника векторів невеликої розмірності [1]. Інакше кажучи, відбувається відображення деякого набору тексту в векторний простір *n*-розмірності.

Для виконання задачі векторизації найчастіше звертаються до методу term frequency-inverse document frequency (TF-IDF), тобто техніки пошуку інформації, яка дозволяє виявити відносну важливість слів у документі [2]. Загалом, якщо слово багато разів зустрічається в документі, то робиться припущення, що воно, мабуть, може бути важливим (надається певна вага). Вага (значимість) слова пропорційна кількості вживань цього слова у документі, і обернено пропорційна частоті вживання слова в інших документах колекції. Однак, якщо досліджуване слово також часто зустрічається в декількох документах, це може бути просто загальним словом і насправді не дуже значущим. TF-IDF намагається це врахувати і повертає загальний бал важливості для кожного слова.

TF-IDF поділяється на дві частини: TF та IDF. TF відповідає за частотність терміну та вимірює наскільки часто термін зустрічається в документі. Логічно припустити, що в довгих документах термін може зустрітися в більших кількостях, ніж в коротких, тому абсолютні числа тут не проходять. Тому застосовують відносні – ділять на кількість разів, коли потрібний термін зустрівся в тексті, на загальну кількість слів у тексті. Частина IDF – зворотна частотність документів, вона вимірює безпосередньо важливість терміну. Після підрахунку TF, всі терміни вважаються рівними за важливістю один одному. Але відомо, що, наприклад, прийменники зустрічаються дуже часто, хоча практично не впливають на зміст тексту. Тож IDF розраховується як логарифм від загальної кількості документів, поділеній на кількість документів, в яких зустрічається певний термін. При обході певного тексту, для нього підраховується TF всіх слів, які перебувають в ньому. Потім для кожного слова розраховується IDF і множиться на TF. Кінцевий результат може бути представленій у вигляді словника, відсортованого за частотою появи слів, де ключами будуть терміни, а значеннями – підраховані TF-IDF для них.

Такий відхід до векторного представлення слів, зробив метод TF-IDF одним із найефективніших підходів, які найчастіше використовується для представлення документів колекцій у вигляді числових векторів, що відображають важливість використання кожного слова з деякого набору слів (кількість слів набору визначає величину вектора) у кожному документі [3]. Подібна модель називається векторною і дає можливість порівняти тексти, представлені у тій чи іншій метриці (напр., евклідовому просторі, косинусній мірі тощо), тобто проводячи кластерний аналіз.

Список літератури

1. Векторное представление слов // Веб-сайт вики-конспектов Университета ИТМО – [Электронный ресурс]. – Режим доступа: http://neerc.ifmo.ru/wiki/index.php?title= Векторное_представление_слов

2. Котюбеев Р. 4 метода векторизации текстов // Веб-сайт специализированного учебного центра обучения и повышения квалификации специалистов Big Data «Python School» [Электронный ресурс]. – Режим доступа: https://python-school.ru/nlp-vectorization-methods

3. Орельен Ж. Прикладное машинное обучение с помощью Scikit-Learn и TensorFlow: концепции, инструменты и техники для создания интеллектуальных систем. – СПб.: Альфа-книга: 2018. – 688 с.

УДК 004.031.4

Т.Х. Фаталиев
tfataliyev@gmail.com
Институт Информационных Технологий НАНА, Баку, Азербайджан

О РОЛИ ГРАЖДАНСКОЙ НАУКИ В РАЗВИТИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Проблема интеграции науки и образования в принципе не нова и ее решения всегда были в центре внимания общества. Одним из основных направлений этой интеграции является усиление участия ученых в обучении, а преподавателей и студентов в научных исследованиях. В результате повышаются эффективность исследований и использования бюджетных средств; качества обучения и подготовки научно-технических кадров; и обеспечивается приток молодежи в области исследований, проектирования и т.д. В процессе интеграции применение современных информационных технологий (ИТ) развивается в значительной степени и охватывает различные аспекты деятельности в науке и образовании. Следует отметить, что гражданская наука (ГН), которая характеризуется широким участием граждан в научных исследованиях и считается новым направлением электронной науки (э-науки), также оказывает значительное влияние на эти достижения [1].

ГН - это концепция добровольного вовлечения в научные исследования большого количества граждан-любителей, большинство из которых не имеют начальной подготовки по специальности. Следует отметить, что наиболее известным решением в реализации ГН является волонтерство. Участие добровольцев (волонтеров) в проектах ГН характеризуется инклюзивностью, т.е. независимостью от уровня образования; физического состояния; возраста; социализации и т.д. К основным целям ГН можно отнести [2]:

•Участие добровольцев в сборе больших объемов данных в широком диапазоне пространства и времени создает возможности для более эффективных решений поставленных вопросов.

•Содействие гражданскому участию в научных исследованиях и науке в целом.

•Реализация нового подхода к неформальному образованию.

Участие добровольцев в исследованиях имеет давнюю истории. Они участвовали в изучении взаимосвязи между климатом и биоразнообразием на протяжении сотен лет. Так, еще в 1874 году британское правительство профинансировало специальный проект по привлечению астрономов-любителей со всего мира к измерению расстояния между Землей и Солнцем [3].

В последнее десятилетие наблюдается массовое увеличение проектов ГН и численности ее участников. Это объясняется развитием ИТ, особенно сетевых технологий, Интернета, обработки и хранения данных, появления графических пользовательских интерфейсов и географических информационных систем на основе веб-технологий, мобильных технологий, смартфонов, планшетов и других портативных устройств. В связи этим, также особую актуальность приобретают применения инструментов концепции Industry 4.0.

В настоящее время пандемия COVID-19 повлияла на исследования во всем мире. Эта ситуация уникальна в своем роде, так как текущие исследования разрушаются, а запланированные исследования не могут начаться, пока они не будут адаптированы к новой реальности. В связи с этим, например, портал volunteerscience.com работает над тем, чтобы помочь преподавателям проводить свои курсы онлайн. Студенты могут участвовать в экспериментах по ГН и получить соответствующие сертификаты. На сайте есть библиотека, состоящая из более чем 100 экспериментов и опросов, которые студенты и преподаватели могут использовать в своих проектах. Портал citizenscience.org также занимается разработкой собственных ресурсов, связанных с пандемией. Эти проекты могут быть полезны как гражданам, желающих помочь в борьбе с вирусом, так и школьникам, студентам, исследователям, будучи в изоляции.

Отметить, что существует множество проектов ГН по различным аспектам исследуемой проблемы. Рассмотрим некоторые из них. Программа *BioBlitzes*–это краткосрочные мероприятия, продолжающиеся обычно в течение дня, во время которых добровольцев просят найти и сфотографировать как можно больше видов растений или животных в определенном месте и времени [4]. В онлайн-проектах таких, как *Zooniverse (zooniverse.org)* и *iNaturalist (inaturalist.org)* представлены задачи определения живых существ или классификации галактик. Эта деятельность приносит пользу, как ученым, так и волонтерам: ученые проводят трудоемкие и дорогостоящие проекты, которые невозможно реализовать без поддержки тысяч добровольцев, а волонтеры могут лучше понять науку и научные методы, оценить природу и поддержать природоохранные инициативы.

В зависимости от уровня участия добровольцев проекты ГН можно классифицировать на: 1) контрактные проекты; инициированные учеными для удовлетворения потребностей сообщества; 2) совместные проекты для сбора данных, разработанные учеными для общественности; 3) совместные проекты, в которых общественность, в дополнение к сбору данных, уточняет дизайн, анализ и распространение проекта; 4) совместно созданные проекты, разработанные в сотрудничестве с общественностью и 5) коллективные вклады;

инициированные непрофессиональными членами общественности, которые самостоятельно проводят исследования [5].

ГН вызывая большой интерес, получает более широкую поддержку на международном уровне. Примером среди многочисленных организаций, рассмотрим Европейскую ассоциацию гражданской науки (*European Citizen Science Association, ECSA, https://ecsa.citizen-science.net/*). Рабочая группа ECSA по обучению и образованию объединяет учителей школ и высших учебных заведений; исследователей в области образования; ученых; и другие сообщества, заинтересованные в развитии неформального обучения и образовательных аспектов своих проектов ГН. Таким образом, углубляется отношения между наукой и обществом и укрепляется общественные уверенности в науке.

Хотя ГН это новая практика массового участия общественности в научных исследованиях, но она имеет достаточной степени потенциал в образовательной среде. ГН имеет возможности в качестве инновационного образовательного инструмента. Ее интеграция в образовательную среду приводит к новым достижениям в области современных образовательных технологий, повышает знания и осведомленность, научную грамотность, навыки мышления и совместного сотрудничества добровольных участников этой среды. Проекты ГН могут обогатить научно-практические достижения в исследуемой области, предлагая студентам возможность получить ранний опыт, который в противном случае может быть слишком сложным, дорогостоящим или непрактичным для повторения после окончания учебы. Следовательно, существует потребность в раскрытии образовательных преимуществ ГН, особенно в практике высшего образования.

Реализация проектов ГН сопровождается использованием современных ИТ, в частности, приложений для сбора, обработки и анализа данных. Поэтому обучение этим технологиям позволит повысить профессиональные навыки и образовательный опыт студентов. ГН имеет высокий потенциал для улучшения учебных программ, позволяет учесть дополнительные факторы, влияющие на правильный выбор талантливыми студентами специальностей, усиливает их веру в собственные способности, а также помогает в приобретении академического опыта, например, практический характер, и адекватность подготовки к будущей карьере.

Как известно, по сравнению с традиционных форм обучения, активное обучение увеличивает успеваемость студентов. Следует отметить, что иногда решение студентов прекращать обучения связано с множеством факторов, таким, как потеря интереса к учебной программе, убеждения относительно своей компетентности и недостатком знаний о науке. Таким образом, увеличивается вероятность того, что поддержка преподавателей в преобразовании их методов обучения с включением ГН в практику не только может иметь потенциал для повышения успеваемости студентов, но также может повысить их интерес к специальностям.

Проекты ГН также включают возможности для социализации через межведомственные команды, так как общение студентов с членами команд дает возможности улучшения социальных навыков.

В заключении отметим, что растущий прогресс ИТ, а также возможности решений Industry 4.0 сыграет важную роль в становлении ГН как нового направления э-науки. Участие в проектах ГН миллионов добровольцев наряду с учеными повышает их знания и осведомленность, научную грамотность, навыки мышления и совместного сотрудничества. В этом контексте интеграция ГН и образования приведет к развитию науки и образования в новом качестве, повысит эффективность научных исследований, образования и подготовки кадров.

Список литературы

1. R.M. Alguliyev, R.G. Alakbarov, T.Kh. Fataliyev, Electronic science: current status, problems and perspectives, Problems of information technology, №2, pp. 4–14, 2015.

2. T.Kh. Fataliyev, Citizen science as a new direction in the development of eScience, Problems of information society, №1, pp. 57-64, 2014.

3. T.H. Sparks, P.D. Carey, The responses of species to climate over two centuries - an analysis of the Marsham Phenological Record, 1736-1947, Journal of Ecology, Vol. 83, №2, pp. 321-329, 1995.

4. C. Herodotou, M. Aristeidou, G. Miller, H. Ballard, L. Robinson, What Do We Know about Young Volunteers? An Exploratory Study of Participation in Zooniverse. Citizen Science: Theory and Practice, 5(1), 2020, article no. 2, http://doi.org/10.5334/cstp.248

5. J.L. Shirk and etc., Public Participation in Scientific Research: a Framework for Deliberate Design, Ecology and Society, Vol. 17, №2, article no. 29, pp. 1-20, 2012. http://dx.doi.org/10.5751/ES-04705-170229

УДК 373.3:004

В.В. Кіш[1], О.Л. Канюк [2]
kish.viktor@student.uzhnu.edu.ua,
[1]студент 1 курсу
[2]завідувач кафедри іноземних мов,кандидат педагогічних наук, доцент
ДВНЗ «УжНУ», Ужгород

АЛГОРИТМ ДИДАКТИЧНОГО ПРОЕКТУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ НАВЧАННЯ МАЙБУТНІХ ФАХІВЦІВ

Для підготовки і перепідготовки висококваліфікованих фахівців у вищих навчальних закладах необхідно застосовувати нові системи управління та нові технології навчання. Цій проблемі сьогодні приділено достатньо велику кількість робіт. Так Г.Л. Чепуренко і І.Г. Захарова відзначають, що для управління процесом підготовки фахівців у ВНЗ необхідно створити умови впровадження інформаційного середовища на базі комп'ютерних систем. С.В. Арженовський вказує на іншу модель управління, в основу якої, як він вважає, повинні бути покладені математичні методи і моделі. К.Г. Кречетніков і О.В. Гончарова вказують на необхідність застосування в освіті креативних і когнітивних технологій. У дослідженнях Л.О. Горовенко значне місце приділено проблемі побудови інформаційно-освітнього середовища з елементами штучного інтелекту [1].

Однак будь-яке завдання цілеспрямованого управління, планування, іншими словами, будь-яке завдання управління освітнім процесом у ВНЗ зводиться до вибору кращого варіанту з будь-яких наявних альтернатив управління і відповідних технологій навчання студентів. Загальна теорія дослідження оптимальних систем управління передбачає вивчення процесів інформаційної взаємодії елементів, що входять у систему управління освітнім процесом. Це обумовлено тим, що процеси збору та передачі керуючої інформації вимагають обліку інформаційних особливостей функціонування кожного елемента системи управління. На даний час питання про наукове обґрунтування системи комплексного управління освітнім процесом у ВНЗ, її оптимальності приділено недостатньо уваги. Найчастіше ця проблема згорталася до процедури інформаційного дослідження кожного об'єкта (процесу) управління. Щоб підійти раціонально до вирішення проблеми синтезу оптимальної структури управління освітнім процесом у вузі, необхідно розглянути і питання закономірностей інформаційної взаємодії всіх елементів, що входять в структуру управління. Тому будемо розглядати систему управління освітнім процесом як систему, в основі якої лежить використання інформаційних технологій навчання. Характерною особливістю такої системи є наявність в ній визначених частин, причому для кожної частини можна з'ясувати мету функціонування, підпорядковану спільній меті всієї системи управління, участь у системі людей, машин та природного середовища, існування внутрішніх матеріальних, енергетичних та інформаційних зв'язків між частинами системи.

Аналізуючи проблеми використання інформаційних технологій в освіті слід, в першу чергу, відзначити, що процес їх впровадження в систему освіти передбачає розробки розвиненої системи телекомунікацій, глобальних і локальних освітніх мереж.

Інформаційна технологія навчання (ІТН) - це певна логіка організації навчально-пізнавального процесу, заснованого на використанні комп'ютерних та інших інформаційних засобів.

Вона передбачає досягнення заданих цілей підготовки фахівців - професіоналів, активне включення студентів у свідоме освоєння змісту освіти, забезпечує творче оволодіння основними способами майбутньої професійної діяльності, сприяє формуванню особистісного становлення майбутніх фахівців. Відповідно до цього її проектування повинно підпорядковуватися законам створення комплексу навчально-методичного забезпечення дидактичного процесу, при побудові якого найбільшою мірою повинні бути враховані відмінності в початковій підготовці майбутніх фахівців, варіюватися наочність, повнота і конкретність подачі матеріалу, забезпечуватися системність і варіативність представлення інформації, передбачатися можливість опрацювання матеріалу до отримання запланованого результату, що забезпечить адекватність ІТН процесу оволодіння знаннями [1].

Проектування ІТН має бути організовано відповідно до таких принципів:

- принцип цілісності, згідно з яким вона повинна в інтегрованому вигляді представляти систему цілей, методів, засобів, форм, умов навчання, забезпечуючи тим самим реальне функціонування і розвиток конкретної дидактичної системи;
- принцип відтворюваності, згідно з яким відтворення ІТН із урахуванням характеристик даного педагогічного середовища гарантує досягнення заданих цілей навчання;

- принцип нелінійності педагогічних структур, який встановлює пріоритет факторів, які безпосередньо впливають на механізми самоорганізації і саморегулювання відповідних педагогічних систем;

- принцип адаптації процесу навчання до особистості учня, що полягає в тому, що навчальний процес повинен мати властивість поділу на підпроцеси, кожен з яких має специфічні, тільки йому притаманні особливості, що відповідають пізнавальним потребам конкретного студента;

- принцип потенційної надмірності інформації, що вимагає розробки такої технології процесу передачі майбутнім фахівцем інформації, яка створює для них оптимальні умови для узагальненого засвоєння знань.

Названі принципи визначають специфічні риси проектування використання ІТН в умовах підготовки професіоналів, серед яких можна виділити наступні:

- розробка цілей і завдань навчання орієнтується на заздалегідь виділену еталонну модель конкретного фахівця;

- логіко-змістовний аналіз інформації дисциплін та службової діяльності проводиться з позиції виокремлення в ній провідних ідей і способів дії в контексті вирішення професійних завдань фахівця;

- орієнтація всіх навчальних процедур на гарантоване досягнення навчальних цілей, повне рішення дидактичних завдань;

- проектування завдань-процедур, завдань-операцій, завдань орієнтацій, алгоритмів пізнання здійснюється в таких діях студентів, які можна виміряти і оцінити за заданими критеріями (інтелектуальної, операціонально, ціннісно-смисловий, нормативної готовності фахівця);

- оперативний зворотний зв'язок, оцінка і самооцінка поточних і разом підсумкових результатів навчання і розвитку особистості майбутнього фахівця здійснюється як із позицій предметного змісту професійного навчання (знання, вміння, навички), так і з позицій зміни особистісного досвіду, ціннісних орієнтацій і якостей студента, заданих еталонною моделлю фахівця [1]..

Стрижнем проектування і використання ІТН є постановка і реалізація в навчальному процесі дидактичної задачі, сформульованої в контексті майбутньої професійної діяльності. Її визначення включає наступні послідовні етапи:

- завдання мети вивчення конкретної навчальної дисципліни;

- відбір і структурування змісту навчання, адекватного заданої мети;

- завдання рівнів засвоєння навчальних тем дисципліни, що вивчається;

- вибір використовуваних комп'ютерних та інформаційних засобів навчання; - розробка тестів і завдань для контролю за засвоєнням змісту навчальної дисципліни;

- розробка структури планування і проведення навчальних занять;

- визначення сукупності способів і прийомів організації пізнавальної діяльності студентів, побудова схеми її управління.

Слід вказати, що це складний багаторівневий процес, що складається з ряду взаємообумовлених етапів, кожен з яких є об'єктом розробки і реалізації фахівців різного профілю (педагог-методист, психолог, програміст і т.д .), що спираються при цьому на фундаментальні знання в галузі педагогіки, психології, художнього дизайну, системного аналізу, теорії систем, теорії управління та ін. у кожній галузі знань вироблені свої поняття, свою мову, відкриті певні закони, складові її базис. Це означає, що в ідеалі колектив, який розробляє конкретну ІТН, повинен бути багатопрофільним, тобто «багатомовним». Тому до технолога (в даному випадку викладачеві-предметнику), який виступає центральною фігурою при передпроектній розробці, проектуванні та експлуатації ІТН, пред'являються підвищені вимоги в світлі рівня і різноплановості володіння інформацією, що відноситься до різних етапів її проектування.

Завдання мети навчання

Відбір і структурування змісту навчальної дисципліни

Вибір використовуваних комп'ютерних та інформаційних засобів навчання

Розробка структури планування і проведення навчальних занять

Розробка тестів і завдань для контролю за засвоєнням змісту навчальної дисципліни

Отже, першим і найбільш важливим етапом проектування ІТН, від якого залежить результативність усього подальшого технологічного процесу, є етап завдання мети навчання. Під результативністю в цьому випадку слід розуміти ступінь досягнення студентом соціально значущих дидактичних цілей, трансформованих у систему критеріїв, що відповідає специфіці конкретного виду навчальних занять.

Список літератури

1. Водопьянова М. Ю. Дидактическое обеспечение информационных технологий обучения в профессиональном образовании : дис. ... канд. пед. наук : 13.00.08 / Водопьянова Мария Юрьевна. – Краснодар, 2005. – 167 с.

УДК 519.1

В.І. Петренюк
petrenjukvi@i.ua
Центральноукраїнський національний технічний університет, Кропивницький

МОДЕЛЬ ГРАФІВ-ОБСТРУКЦІЙ ДЛЯ НЕОРІЄНТОВАНОЇ ПОВЕРХНІ

Основні визначення та позначення узяті з [1,2].

Розглянемо задачу побудови моделей графів-обструкцій неорієнтованого роду на основі множини відомих графів-обструкцій, а саме, повної для проективної площини чи неповної для поверхні Клейна. Моделлю графа-обструкції G неорієнтованого роду 2 будемо називати граф більшого неорієнтованого роду, отриманий шляхом приклеювання в доступних частинах частини чи підграфа, гомеоморфного K_5 чи $K_{3,3}$, принаймні однієї копії площинного підграфа H граф-обструкції G проективної площини [3], чи іншого графа аналогічному цьому підграфу H. Для цього використаємо метод φ-перетворень та метод рекурсивних аналогій [4,5], чи їх комбінацію та додаткової перевірки побудованого таким чином графа на предмет наявності несуттєвих ребер відносно роду при операції видалення чи стискання в точку . Приклади використання метода аналогій та метода φ-перетворень наведено на рис. 1, 2, відповідно.

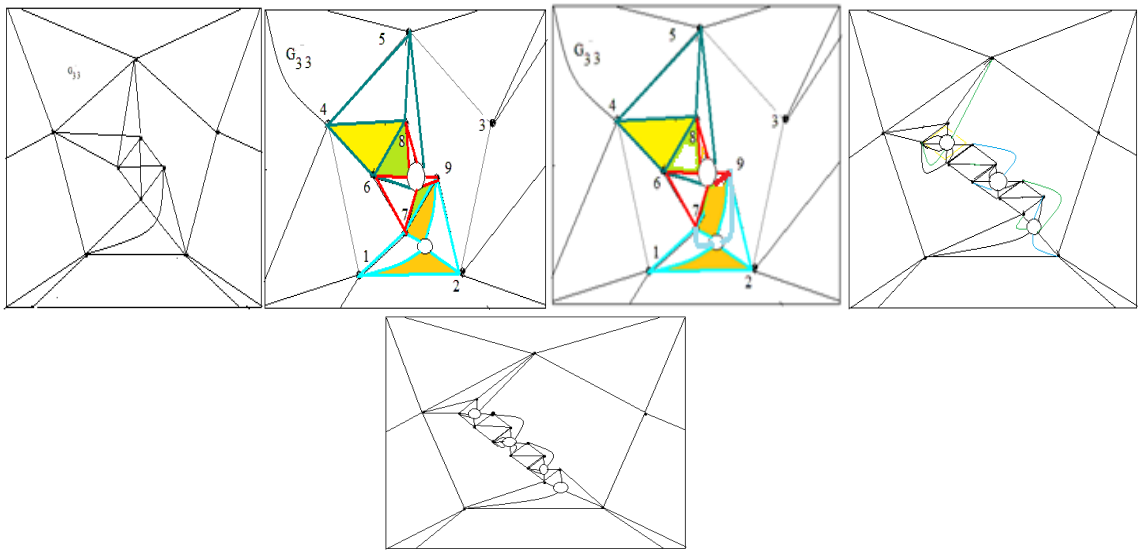


Рис. 1. Граф-обструкція G_{33} мінімально вкладений на N_3, де клітки з границями (1,7,9,2) та (4,6.8) мають кліткову відстань 1.

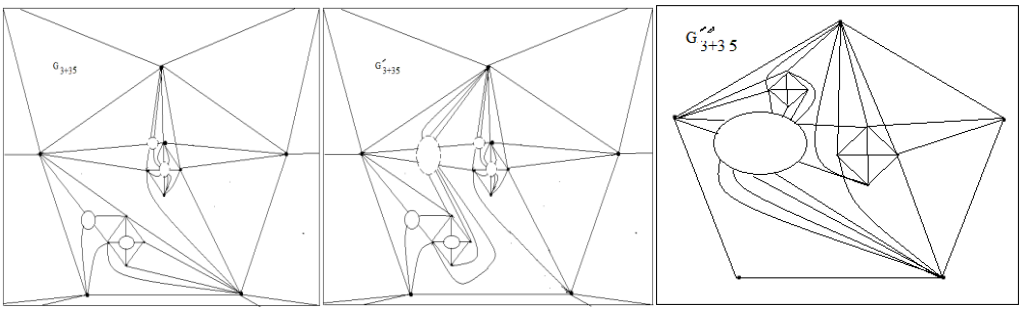


Рис 2. Графи неорієнтованого роду 6, отримані шляхом склейки графів G_3 та G_{35} по підграфу K_5.

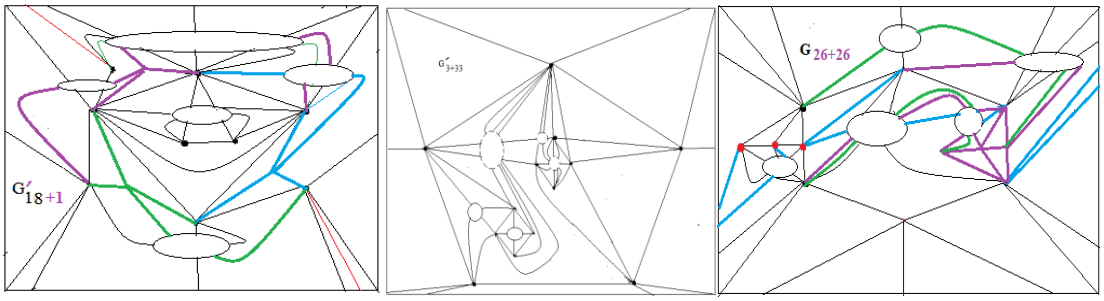


Рис 3. Графи неорієнтованого роду 6, отримані шляхом склейки графів G_1 та G_{18} по підграфу K_5 (перша карта), графів G_3 та G_{33} по підграфу K_5 (друга карта), двох копій графа G_{26} по підграфу K_6, (третя карта) зліва направо.

Лема 1. Мають місце наступні твердження:

1. Дві зірки, що перетинаються на площині елементарного диску висячими ребрами, можливо вкласти на приклеєній до диску ленті Мебіуса без перетину у внутрішніх точках;

2. Нехай ребро e перетинає на евклідовій площині елементарного диска ребра трикутника K_3.

а). Ребра графа K_4 можливо вкласти на ленті Мебіуса, приклеєній до елементарного диска так, щоб пара зхрещених на евклідовій площині ребер та одне з двох паралельних ребер розташувалися на ленті Мебіуса:

б). Якщо ребро e перетинає ребро-основу трикутника, то на приклеєну ленту Мебіуса можливо вкласти як ребро e так і всі ребра трикутника, в іншому випадку можливо вкласти на приклеєну ленту Мебіуса ребро e та два суміжних з ним ребра трикутника, а ребро-основу трикутника ні;

3. Нехай два графи G_1, G_2 мають n_1, n_2 неізоморфних мінімальних вкладень до неорієнтованої поверхні. Якщо граф G -φ-образ графів G_1, G_2 при склейці по вершинам повних підграфів одного порядку, то граф G матиме $n_1 \cdot n_2$ неізоморфних вкладень до неорієнтованої поверхні.

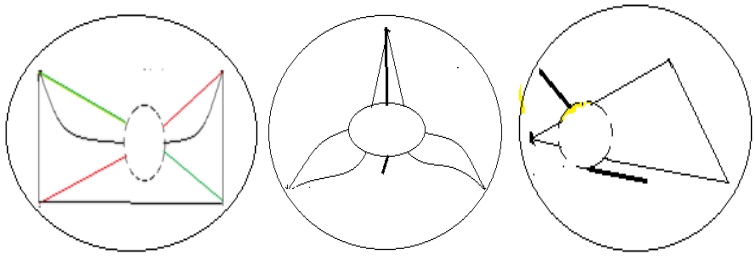


Рис 4. На першій карті граф K_4 вкладено на ленту Мебіуса, на двох інших проілюстровано співвідношення б) твердження 2 леми 1.

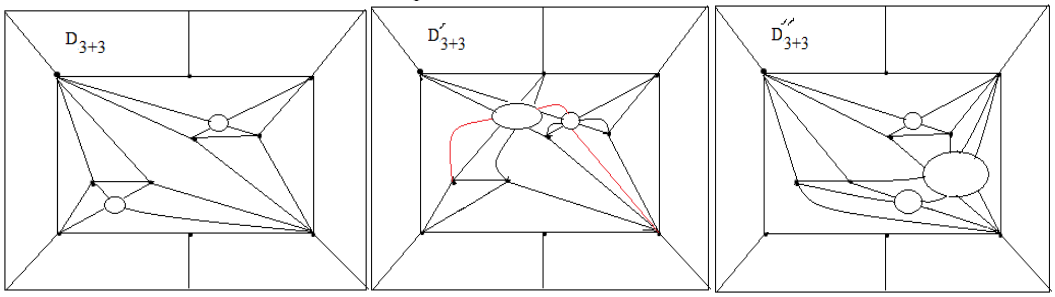


Рис 2.4. Графи та граф-обструкції неорієнтованого роду 3 та 4, отримані шляхом склейки по підграфу K_{33} двох графів G_3.

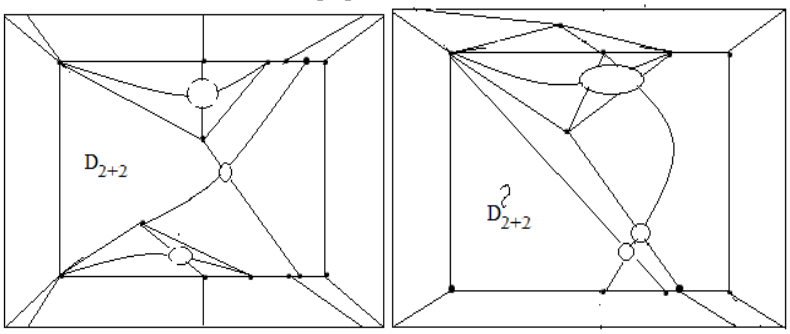


Рис 2.5. Графи та граф-обструкції неорієнтованого роду 3 і 4, отримані шляхом склейки графів G_2

Сисок літератури

1. Хоменко М. П. φ-перетворення графів. препринт ИМ АНУ, Киев, 1973, 383 с.

2. Хоменко М. П. Топологические аспекты теории графов. препрнт ИМ АНУ, Киев, 1970, 299 с.

3. Mohar B., Thomassen C., Graphs on Surfaces, Johns Hopkins University Press, 2001- 412 p.

4. Hur S. The Kuratowski covering conjecture for graphs of order less than 10. Phd, Ohio State University, (2008).

5. D. Archdeacon P. Huneke, A Kuratowski Theorem for Nonorientable Surfaces , Journal of combinatorial theory, Series B 46, 1989, 173-231.

УДК 004.056, 004.75

О.К. Савеленко, К.О. Буравченко
elena.savelenko@gmail.com
Центральноукраїнський національний технічний університет, Кропивницький

ШТУЧНІ ІМУННІ СИСТЕМИ І ЇХ ВИКОРИСТАННЯ ДЛЯ РІШЕННЯ ЗАДАЧІ СИМВОЛЬНОЇ РЕГРЕССІЇ

Інформаційні системи, побудовані на принципах роботи імунітету, маютьвеличезний потенціал у багатьох областях. На даний момент штучні імунні системивикористовуються переважно як різновид систем штучного інтелекту, протевельми перспективним бачиться використання систем захисту, що працюють за принципомімунітету, для боротьби з комп'ютерними вірусами, виявлення мережевих вторгнень і т. д.

При створенні штучної імунної системи необхідно представити модель функціонування імунної системи людини. Це складний механізм, що складається з безлічірізних компонентів. Використовуючи досягнення генної інженерії, позначимо деякіосновні елементи, які переносяться в комп'ютерні мережі.

У деякому роді імунні системи можна вважати спадкоємцями генетичних алгоритмів і нейронних мереж, що володіють певною специфікою. Судячи з різних публікацій, їх намагаються застосовувати для вирішення наступних завдань: розпізнавання (поряд з імунними системами), створення антивірусів (що логічно, виходячи з основної функції біологічних імунних систем), різних завдань оптимізації.

Лімфоцити - клітини, з яких складається імунна система.

Дану задачу можна розбити на следующиепідзадачі:

а) виділення підмножини істотних рис і особливостей природної імунної системи, необхідних для вирішення даного завдання;

б) опис штучної імунної мережі та її компонентів з урахуванням вимог, отриманих на попередньому етапі;

в) побудова навчальної вибірки - набору зображень букв для навчання мережі;

г) розробка власне алгоритму для отриманої штучної імунної мережі;

д) розробка інтерфейсу користувача.

У нашій задачі (пошуку символьного представлення функції) лімфоцит буде являти собою одне з можливих рішень задачі – деякуфункцію, представлену деревом вираження (наприклад, таким як на рисунку 1). У цьому дереві можуть використовуватися різні операції (+, -, *, /, sin, cos), числа, змінні, максимальна кількість яких задано (щоб обмежити глибину пошуку). Якщо користуватися термінами генетичних алгоритмів, лімфоцит - це просто особина.

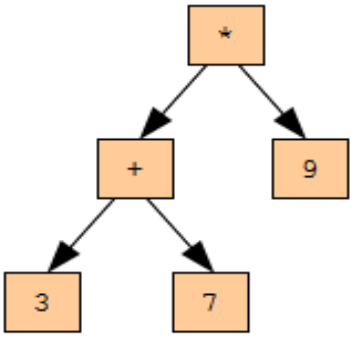


Рис. 1 Дерево визначення функції рішення задач

Спочатку створюється деякий безліч випадковим чином згенерованих лімфоцитів. Потім протягом усього циклу функціонування системи з поточного безлічі лімфоцитів вибираються кращі, до них застосовуються різні операції гіпермутація (для створення краще пристосованих клітин - еволюція в дії). Потім зі старих і знову отриманих клітин вибирається нова поточна множість, і цей крок повторюється заново до тих пір, поки не буде знайдено рішення с достатньою точністю, або ми проведемо максимально допустиму кількість ітерацій. В якості оцінки рішень використовується раніше розглянута цільова функція.

Список літератури

1. Искусственныеиммунныесистемы и ихприменение / [под ред. Дасгупты] – М.: Физматлит 2006 – 344 с.
2. Colin G. JohnsonArtificialImmuneSystemsProgrammingforSymbolicRegression / Colin G. Johnson // GeneticProgramming: 6th EuropeanConference. – 2003. – P. 345–353 – ISBN=3-540-00971-X

ЗМІСТ

СЕКЦІЯ 1. ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ, СУСПІЛЬСТВА ТА ОСОБИСТОСТІ

СЕКЦІЯ 2. ПРОГРАМУВАННЯ ТА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ

СЕКЦІЯ 3. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ, МЕДИЦИНІ ТА ОСВІТІ

НАУКОВЕ ВИДАННЯ

ТЕЗИ ДОПОВІДЕЙ

IV Міжнародної науково-практичної конференції “Інформаційна безпека та комп’ютерні технології”

15–16 квітня 2021 р.

Відповідальний за випуск: *О.А. Смірнов*

Комп`ютерна верстка: *Р.М. Минайленко*

Електронне видання

Центральноукраїнський національний технічний університет
пр-кт Університетський, 8, м. Кропивницький, 25006.
тел. (0522) 559-245, www.kntu.kr.ua