І МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

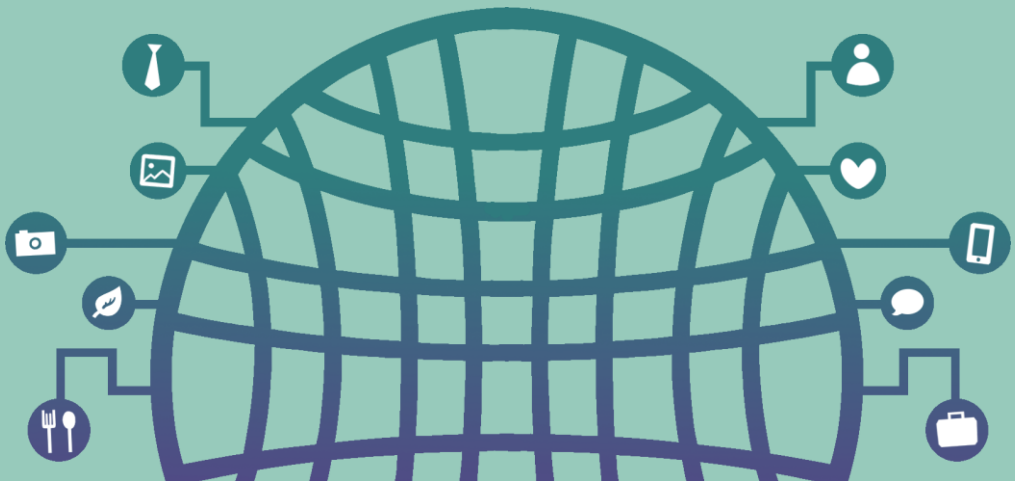
ЦИФРОВА ТРАНСФОРМАЦІЯ СУСПІЛЬСТВА

DIGITAL SOCIETY – 2022

м. Кропивницький, Україна

21-22 квітня 2022 року

ЗБІРНИК ТЕЗ ДОПОВІДЕЙ



ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ
ТЕХНІЧНИЙ УНІВЕРСИТЕТ

МЕХАНІКО-ТЕХНОЛОГІЧНИЙ ФАКУЛЬТЕТ

КАФЕДРА КІБЕРБЕЗПЕКИ ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

ЗБІРНИК ТЕЗ ДОПОВІДЕЙ

І МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

«ЦИФРОВА ТРАНСФОРМАЦІЯ СУСПІЛЬСТВА»

DIGITAL SOCIETY – 2022

21-22 квітня 2022 року

м. Кропивницький

УДК 004

Цифрова трансформація суспільства: Збірник тез доповідей І Міжнародної науково-практичної конференції, 21-22 квітня 2022 року, м. Кропивницький: ЦНТУ, 2022. – 100 с.

Збірник містить тези доповідей за матеріалами І Міжнародної науково-практичної конференції “Цифрова трансформація суспільства”, що відбулась 21-22 квітня 2022 року на базі кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ

Голова – **Левченко О.М.**, доктор економічних наук, професор, проректор з наукової роботи Центральноукраїнського національного технічного університету.

Заступник голови:

Смірнов О.А., доктор технічних наук, професор, завідувач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету.

Члени оргкомітету:

Мірошкін О.М., кандидат технічних наук, доцент, Університет Ульма, Німеччина.

Maslanka Pawel, професор, Лодзинський університет, м. Лодзь, Польща.

Milczarski Piotr, доктор технічних наук Лодзинський університет, м. Лодзь, Польща.

Карпінський М.П., доктор технічних наук, професор, м. Бельсько-Бяла, Польща.

Сєйлова Н.А., кандидат технічних наук, м. Алмати, Казахстан.

Охрименко С.А., доктор економічних наук, професор, м. Кишинів, Республіка Молдова.

Алієв А.Р., доктор наук з математики, професор, м. Баку, Азербайджан.

Мамедов Р.Г., доктор технічних наук, професор, м. Баку, Азербайджан.

Маракова І.І., доктор технічних наук, професор, Франція.

Гнатюк С.О., доктор технічних наук, професор, Національний авіаційний університет, м. Київ, Україна.

Семенов С.Г., доктор технічних наук, професор, старший науковий співробітник, Харківський національний економічний університет імені Семена Кузнеця, м. Харків, Україна.

Рудницький В.М., доктор технічних наук, професор, Черкаський державний технологічний університет, м. Черкаси, Україна.

Адреса редакційної колегії:
25030, м. Кропивницький, пр. Університетський, 8,
Центральноукраїнський національний технічний університет,
тел.: (0522)390-449.

Відповідальна за випуск: Мелешко Є.В.

Дизайн обкладинки: Мелешко Є.В., Графенюк В.О.

ЗМІСТ

СЕКЦІЯ 1. СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА ТЕХНІЧНІ АСПЕКТИ ЇХ ВПРОВАДЖЕННЯ

УДК 004.056.53

Спосіб оцінки ефективності розробленого методу підвищення безпеки програмного забезпечення

Цао Вейлінь[1], аспірант, caowl@njtc.edu.cn
Семенов С.Г.[2], д.т.н., проф., s_semenov@ukr.net
[1]*Нейцзянський педагогічний університет, Нейцзян, Сичуань, Китай*
[2]*Харківський Національний економічний університет ім. С.Кузнеця, м. Харків, Україна*

В основі запропонованого в роботі способу оцінки ефективності розробленого методу використано метод динаміки середніх, який одержав теоретичне обґрунтування у роботах [1-4]. Перевагами цього методу є простота, можливість урахування багатьох факторів (наявності засобів активного та пасивного тестування, можливості фахівців тестування на проникнення та DevSecOps та ін.), наявність аналітичних рішень [5].

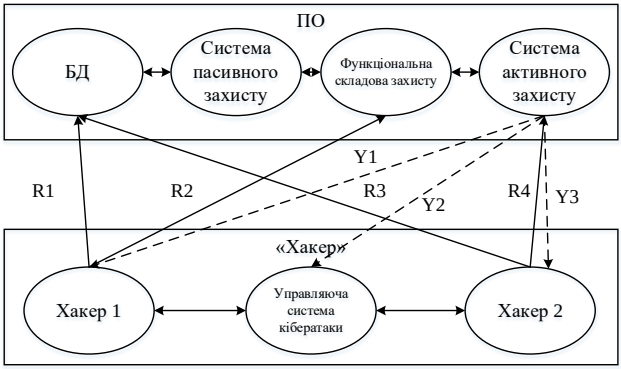
Структурна схема способу оцінки ефективності розробленого методу підвищення безпеки ПЗ та розмічений граф станів системи представлені на рис. 1.

Спосіб оцінки ефективності розробленого методу включає наступні кроки:

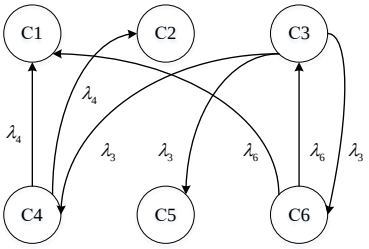
1. Аналіз можливих небезпек ПО. Змістовна постановка завдання дослідження.
2. Розробка та синтез основних компонент оцінюваної системи «ПЗ - Хакер» у структурну схему.
3. Математична формалізація процесу знаходження чисельностей станів у диференціальній формі відповідно до методу динаміки середніх.
4. Формалізація вхідних даних, і навіть додаткових умов вирішення задачи.
5. Розв'язання формалізованого завдання.
6. Фіксація та апроксимація результатів моделювання.
7. Підстановка результатів та обчислення показників ефективності розробленого методу підвищення безпеки ПЗ.

В основу вдосконаленого способу оцінки ефективності методу підвищення безпеки програмного забезпечення покладено метод динаміки середніх.

Висновки. За допомогою вдосконаленого способу доведено доцільність використання розробленого методу підвищення безпеки програмного забезпечення з урахуванням факторів невизначеності. Це дозволить знизити показник відносної шкоди на всіх етапах життєвого циклу до 6 разів, залежно від можливої тривалості кібервторгнення.



а)



б)

Рис. 1. Структурна схема способу оцінки ефективності методу підвищення безпеки ПЗ та розмічений граф станів системи

Список літератури

1. Shanahan, L., Sen, S, (2011) Dynamics of stochastic and nearly stochastic two-party competitions, Physica A: Statistical Mechanics and its Applications, Vol. 390, Issue 10, P. 1800-1810, https://doi.org/10.1016/j.physa.2010.12.041.

2. Tze Leung Lai, Haipeng Xing (2010) Statistical Models and Methods for Financial Markets, Springer New York Softcover reprint of hardcover 1st ed. 2008 356 pp.

3. Stephen Boyd, Lieven Vandenberghe (2018) Introduction to Applied Linear Algebra Vectors, Matrices, and Least Squares Cambridge University Press DOI: 10.1017/9781108583664

4. Swart., J., Winter, A. (2010) Markov processes: theory and examples, available at: https://www.uni-due.de/~hm0110/Markovprocesses/sw20.pdf

5. Semenov, S., Weilin, C., Zhang, L., & Bulba, S. (2021). Automated penetration testing method using Deep machine learning technology, Advanced Information Systems, Vol. 5, Issue 3, P. 119–127. DOI: https://doi.org/10.20998/2522-9052.2021.3.16

УДК 004.056.53

Метод підтримки прийняття рішення про безпеку програмного забезпечення

Чжан Лицзян[1] аспірант, zhanglq@njtc.edu.cn
Семенов С.Г.[2], д.т.н., проф., s_semenov@ukr.net
[1]*Нейцзянський педагогічний університет, Нейцзян, Сичуань, Китай*
[2]*Харківський Національний економічний університет ім. С.Кузнеця, м. Харків, Україна*

Проведені дослідження схеми аналізу вразливостей програмного забезпечення (ПЗ) та оцінка результатів математичного моделювання дозволили зробити висновок про комплексність даних, що піддаються аналізу у системі підтвердження потенційних уразливостей [1, 2].

Оцінювання здійснюється на підставі вектора безпеки, що поєднує в собі множину характеристик складу потенційних уразливостей, а також перелік вразливостей та недекларованих можливостей, що показують ступінь відповідності ПЗ певному критерію безпеки та закодоване значення рівня контролю відповідності [3, 4]. Виходячи з особливостей обраного математичного апарату, розв'язання задачі верифікації необхідно звести до вирішення наступних підзавдань: визначення вихідного вектора; розрахунок класифікаційних ознак вектора; вибір методу ухвалення рішення. Різноманітність вхідних даних потребує використання додаткових механізмів підвищення точності прийняття рішень. Серед таких механізмів можна виділити розробку методу підтримки прийняття рішення про безпеку ПЗ.

Розроблений метод підтримки прийняття рішення про безпеку ПЗ відрізняється від відомих синтезом удосконаленого способу генерації навчальної вибірки в процес навчання штучної нейронної мережі. Це дозволило підвищити ефективність методу підтримки прийняття рішення щодо безпеки ПЗ до 1,2 рази.

У ході дослідження було розроблено модель формування векторів вхідних даних. Відповідно до даної моделі для формування вхідних даних формується множина ознак потенційних вразливостей та недекларованих можливостей ПЗ відповідно до даних PVS-Studio Analysis Results.

Як дизайн архітектури нейронної мережі для вирішення завдання підтримки прийняття рішення про безпеку ПЗ було запропоновано за основу взяти багатошаровий персептрон.

Удосконалено метод навчання штучної нейронної мережі, який відрізняється способом генерації навчальної вибірки. Даний спосіб генерації включив три рівні генерації: генерація навчальної вибірки, генерація навчального прикладу і генерація конкретного значення характеристики безпеки. Це дозволило підвищити точність класифікації

та прийняття рішення у 1,6 рази для позитивних елементів у вибірці та у 1,2 рази для негативних елементів у вибірці.

На рис. 1. Наведено схему методу підтримки прийняття рішення про безпеку ПЗ.

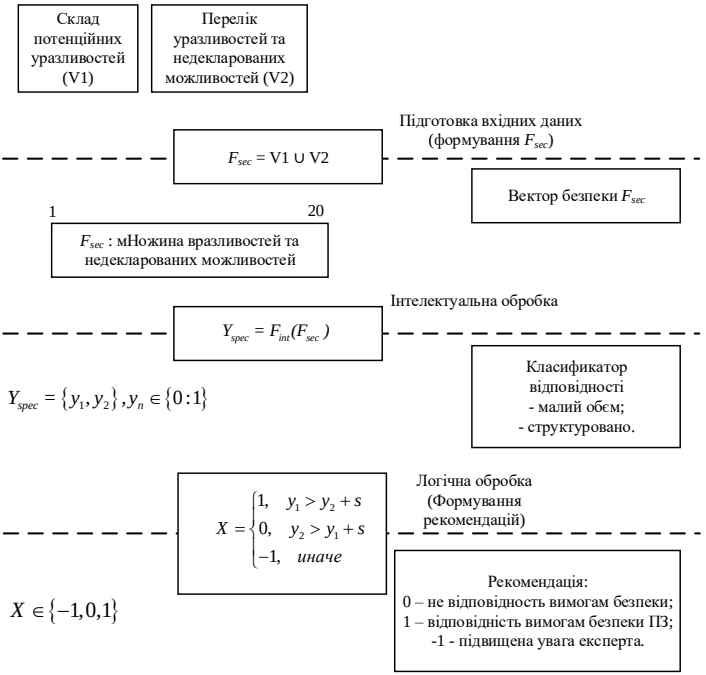


Рис. 1. Схема методу підтримки прийняття рішення про безпеку ПЗ

Список літератури

1. Semenov, S., Zhang, L., Cao, W., Bulba, S., Babenko, V., & Davydov, V. (2021). Development of a fuzzy GERT-model for investigating common software vulnerabilities. Eastern-European Journal of Enterprise Technologies, 6(2 (114), 6–18. DOI: https://doi.org/10.15587/1729-4061.2021.243715

2. Semenov, S. ., Liqiang, Z., Weiling, C., & Davydov, V. (2021). Development a mathematical model for the software security testing first stage. Eastern-European Journal of Enterprise Technologies, 3(2 (111), 24–34. DOI: https://doi.org/10.15587/1729-4061.2021.233417

3. Introduction Welcome to the OWASP Top 10 – 2021. URL: https://owasp.org/Top10/

4. Dan Sullivan Six criteria for procuring security analytics software. URL: https://www.techtarget.com/searchsecurity/feature/Six-criteria-for-procuring-security-analytics-software

УДК 519.157.2+004.021

Параметризація алгоритму для визначення квазімінімального маршруту у задачі доставки вантажів багатьма перевізниками

Романов А.Ю., аспірант, andreygorogogo@gmail.com
Науковий керівник – Романюк В.В., д. т. н., проф., romanukevadimv@i.ua
Одеський національний морський університет, м. Одеса, Україна

Вступ. Сучасний ринок доставки товарів представлений багатьма способами транспортування: наземний, водний та повітряний. Серед них найбільш популярним довгий час перебуває водний, а саме – морський вид транспортування товарів. Його перевагами над конкурентами є вартість і надійність транспортування, а також можливість доставляти будь-які типи товарів. Серед недоліків можна виділити відносно низьку швидкість доставки та залежність від погодних умов. Якщо на погодні умови та форс-мажорні обставини практично неможливо вплинути під час планування, то на швидкість доставки можна вплинути, прокладаючи максимально ефективні маршрути. Під ефективним маршрутом розуміють його довжину, виражену в одиницях відстані або часу. Такі задачі відносяться до класу транспортних задач. Зокрема, йдеться про задачу про призначення (assignment problem) та задачу комівояжера (travelling salesman problem) [1].

Задача комівояжера фактично є задачею прокладання ефективного маршруту. Для прокладання маршрутів можуть використовуватися різноманітні способи – наприклад, підхід лінійного програмування для точного розв'язання транспортної задачі з визначенням відповідного маршруту (маршрутів). Тоді кожен такий маршрут буде найбільш ефективним, але на його пошук, найімовірніше, буде витрачено багато ресурсів, головними з яких є час та гроші (як еквівалент обчислювальних засобів). Альтернативою такому способу є використання евристичних підходів, котрі дозволяють знаходити квазіоптимальні розв'язки задачі комівояжера за відносно короткий проміжок часу з використанням незначного об'єму обчислювальних засобів. Одним з найкращих евристичних підходів для розв'язування задачі комівояжера заснований на генетичному алгоритмі [2].

Генетичний алгоритм – це евристичний алгоритм пошуку, який використовується для розв'язування задач оптимізації та моделювання шляхом випадкового підбору, комбінування та варіації шуканих варіантів розв'язку. Використання такого алгоритму значно пришвидшує визначення оптимального або близького до оптимального (квазімінімального) маршруту.

Опис алгоритму. На рисунку 1 зображено спрощену схему для знаходження квазімінімального маршруту для декількох комівояжерів. В

ході роботи алгоритму генеруються нові покоління маршрутів з використанням генетичних операторів (мутацій) – обмін, переворот, здвиг і схрещення. Кожен з цих операторів по-різному впливає на визначення квазімінімального маршруту, але їх поєднання дозволяє як пришвидшити процес пошуку квазіоптимального розв'язку, так і підвищити точність [3].

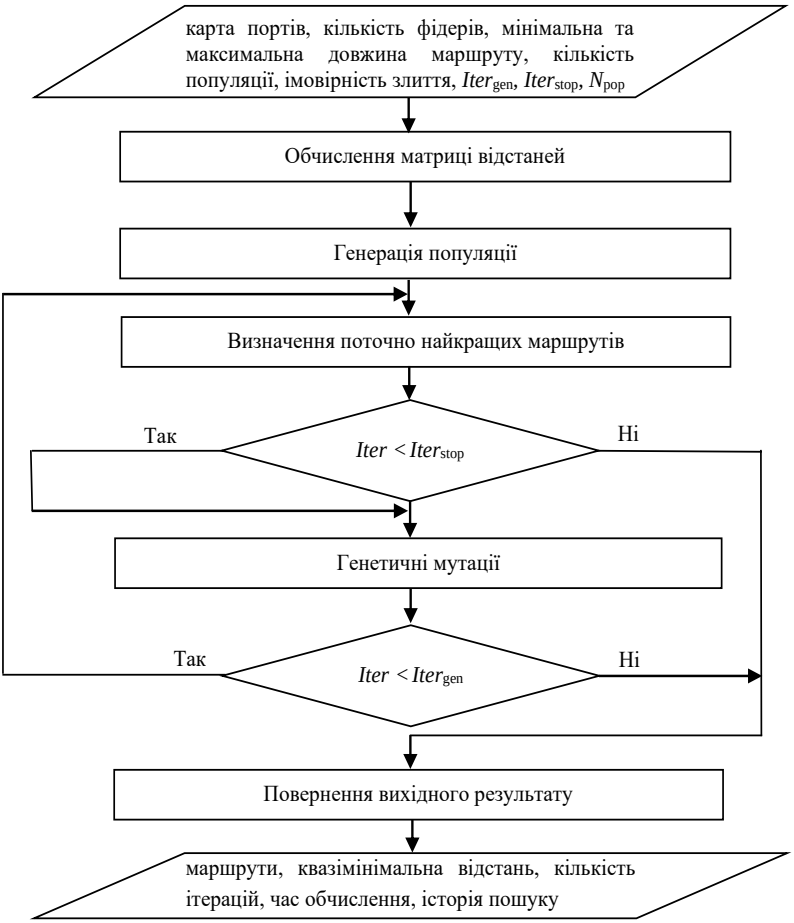


Рис. 1. Алгоритм пошуку маршрутів морських перевезень

Параметри алгоритму. Даний алгоритм передбачає наступні вхідні параметри: карта портів, кількість фідерів, розмір популяції, кількість ітерацій, ймовірність злиття, кількість ітерацій для ранньої зупинки та кількість генетичних операцій. Останні три параметри суттєво впливають на результат роботи алгоритму. Ймовірність злиття двох фідерів (в

морських перевезеннях під фідером розуміється транспортний човен) впливає на злиття двох шляхів в один, чим збільшує ймовірність до зменшення кількості фідерів. Експериментальним шляхом було визначено, що злиття впливає на швидкість пошуку квазіоптимального розв'язку, але не на значення цільової функції. Рання зупинка визначає, яку максимальну кількість поколінь може пройти алгоритм без зміни значення цільової функції – цей параметр суттєво зменшує час пошуку квазімінімального маршруту за невеликої кількості портів (до 30). Кількість генетичних операцій визначає кількість мутацій, які будуть проведені над популяцією.

Оптимізація параметрів відбувається експериментальним шляхом, тобто для кожного набору значень цих трьох параметрів проводиться запуск алгоритму, після чого аналізуються результати та робляться висновки щодо оптимальності значення вхідних параметрів. Ймовірність злиття впливає на кількість ітерацій, але не на значення цільової функції (точність квазіоптимального розв'язку). Значення ранньої зупинки має залежати від кількості портів та ітерацій – чим більше портів, тим довше знадобиться поколінь для "стабілізації" розв'язку. Кількість генетичних операцій також впливає на швидкість пошуку квазіоптимального розв'язку. Експериментальним шляхом було виявлено, що поєднання генетичних операторів в одній мутації збільшує швидкість отримання розв'язку задачі.

Висновки. Зміна значень цих параметрів завжди впливає на результат роботи алгоритму, тому основною задачею є визначення оптимального значення для кожного параметра. Відкритим залишається питання знаходження найбільш оптимального поєднання параметрів для пошуку розв'язку задачі. Оптимізація трьох основних параметрів (ймовірності злиття, значення ранньої зупинки та кількості генетичних операцій) має вплинути на якість пошуку квазіоптимального розв'язку задачі доставки вантажів багатьма перевізниками.

Список літератури

1. Greco F. Travelling Salesman Problem. – London: IntechOpen, 2008. – 212 p.

2. Michalewicz Z. Genetic Algorithms + Data Structures = Evolution Programs. – Berlin: Springer, 1996. – 388 p.

3. Király A., Abonyi J. Redesign of the supply of mobile mechanics based on a novel genetic optimization algorithm using Google Maps API // Engineering Applications of Artificial Intelligence. – Vol. 138. – 2014. – P. 9 – 12.

УДК 004.056

Кібербезпека вищого військового навчального закладу

Кива В.Ю., доктор філософії, kyvavlad30101991@gmail.com
Кошлань О.А., доктор філософії, koshlan_sasha@ukr.net
Національний університет оборони України імені Івана Черняховського, м. Київ, Україна

Нині в Україні спостерігається активне впровадження інформаційно-комунікаційних технологій (ІКТ) в освітньо-наукову діяльність закладів вищої освіти (ЗВО), зокрема і вищих військових навчальних закладів (ВВНЗ). Відповідно, впровадження ІКТ у ВВНЗ є передумовою для великого потенціалу змін консервативних підходів стосовно щоденного навчання військовослужбовців, що обумовлено його доступністю, мобільністю та ефективністю [1]. Разом з тим є і проблемні питання щодо впровадження і застосування ІКТ у ВВНЗ, а саме:

– недостатнє фінансування для закупівлі ІКТ;

– відсутність стратегічного бачення з боку керівництва ВВНЗ щодо впровадження та застосування сучасних ІКТ;

– недостатня обізнаність викладачів та навчаємих (студентів, солдатів, курсантів та слухачів) щодо застосування ІКТ під час навчання;

– відсутність або наявність невеликої кількісті фахівців (безпосередньо у ВВНЗ) яка б забезпечувала функціонування та кібербезпеку ІКТ.

У випадку з трьома першими пунктами щодо проблемних питань впровадження ІКТ у ВВНЗ, можна стверджувати про активну діяльність керівників ВВНЗ щодо їх вирішення. Тоді як четверте проблемне питання є вкрай проблематичним і спостерігається не тільки у ВВНЗ але й на державному рівні.

Крім того, незважаючи на вагомі результати досліджень щодо кібербезпеки ЗВО, доводиться констатувати, що в жодному з них не було чітко визначено та проаналізовано чинники, які впливають на кібербезпеку ЗВО, зокрема ВВНЗ. До того ж, дослідження науковців здебільшого фокусувалися на кіберзагрозах, а саме їх впливі та класифікації, які не дозволяють системно врахувати всю причинно-наслідкову систему зв'язків стосовно впливу на кібербезпеку ВВНЗ, що обумовлює актуальність дослідження.

Відповідно, метою дослідження є аналіз зовнішніх та внутрішніх чинників, які впливають на кібербезпеку ВВНЗ.

З врахуванням мети дослідження, автори виконали завдання щодо аналізу чинників, які впливають на кібербезпеку ВВНЗ [2].

Слід наголосити, що кібербезпека ВВНЗ взаємозалежна від кіберзахисту, який можна представити як комплекс взаємопов'язаних заходів, які утворюють єдине ціле і мають спільну мету щодо

забезпечення кібербезпеки ВВНЗ від впливу багатьох різноманітних чинників (умов). При цьому, по відношенню до об'єкта впливу, чинники можна розділити на внутрішні та зовнішні. Слід наголосити, що вони можуть по-різному впливати на кібербезпеку ВВНЗ, зокрема одні з них можуть мати позитивний вплив, інші ж негативний. Відповідно, домінуючий вплив негативних чинників здатний знизити позитивну дію інших.

Проведений аналіз кібербезпеки ВВНЗ дає змогу визначити такі основні **зовнішні чинники**, які впливають на неї, а саме: надзвичайні ситуації; розроблення та виробництво апаратно-програмного забезпечення; кібератаки; вербування або шантаж особового складу.

Відповідно до **внутрішніх чинників**, які впливають на кібербезпеку ВВНЗ можна віднести: підготовленість (навченість) особового складу; політика кіберзахисту; топологія (архітектура) інформаційного простору; апаратне забезпечення; програмне забезпечення.

Відповідно, вплив зовнішніх та внутрішніх чинників на кібербезпеку ВВНЗ визначає необхідність проведення постійного моніторингу його стану кіберзахищеності. Безумовно, що стан кіберзахищеності ВВНЗ буде залежати від правильно змодельованої та реалізованої моделі кіберзахисту, яка має ґрунтуватися на результатах аналізу впливу зовнішніх та внутрішніх чинників кібербезпеки ВВНЗ.

Висновки. Отже, проведений аналіз свідчить, що на кібербезпеку будь-якого ВВНЗ впливають зовнішні та внутрішні чинники. На основі декомпозиції внутрішніх та зовнішніх чинників можна встановити взаємозалежність (критичність) їх впливу на кібербезпеку ВВНЗ, що дає змогу системно врахувати всю причинно-наслідкову систему їх зв'язків. Крім того, завчасний аналіз впливу зовнішніх та внутрішніх чинників на кібербезпеку ВВНЗ дасть змогу отримати ситуаційну обізнаність сучасного стану кібербезпеки та прийняти керівництву відповідні управлінські рішення.

Список літератури

1. Кива В. Ю. Розвиток інформаційно-комунікаційної компетентності викладачів системи військової освіти у процесі дистанційного навчання: дис. … д-ра філос.: 011 – Освітні, педагогічні науки. Київ. 2020. 318 с.

2. Кива В. Ю. Аналіз чинників, які впливають на кібербезпеку вищого військового навчального закладу. Кібербезпека: освіта, наука, техніка. 2022. Том 3, № 15. С. 53–70.

УДК 004.9

Система інтерактивного вивчення ігрового рушія Unity

Абашина А.А., магістрантка
Мелешко Є.В., д.т.н., проф., elismeleshko@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна

Зараз розробка комп'ютерних ігор є достатньо перспективним напрямком у програмуванні, а, отже, існує багато інструментів для створення відеоігор, але їх вивчення потребує багато часу та не всі з аспектів є тривіальними. Тому розробка платформи, за допомогою якої можливо вивчити ігровий рушій Unity є досить актуальною.

Unity це – багатоплатформовий інструмент для розробки дво- та тривимірних додатків та ігор, що працює на операційних системах Windows I OS X. Створені за допомогою Unity застосунки працюють під системами Windows, OS X, Android, Apple iOS, Linux, а також на гральних консолях Wiu, PlayStation 3 I XBox 360. Є можливість створювати інтернет-додатки за допомогою спеціального під'єднуваного модуля для браузера Unity, а також за допомогою експериментальної реалізації в межах модуля Adobe Flash Player. Застосунки, створені за допомогою Unity, підтримують DirectX та OpenGL. Редактор Unity має простий Drag & Drop інтерфейс, який легко налаштовувати, що складається з різних вікон, завдяки чому можна проводити налагодження гри прямо в редакторі. Рушій підтримує мови: C# та JavaScript.

Розроблена система призначена для інтерактивного вивчення ігрового рушія Unity у цілях ознайомлення для подальшого вивчення.

Систему можно використати для навчання Unity, та розширених основ програмування. А саме дана система дозволяє вивчити наступні властивості Unity: створення та рух об'єктів, колайдери, управління об'єктами, взаємодія об'єктів, створення та проходження лабіринту.

У розробленій системі реалізовано наступні функціональні частини:

- *Блок створення об'єкту.* Цей блок призначений для керування створенням об'єктів використовуючи для цього методи, які описані ігровим рушієм Unity.
- *Блок руху об'єкту*. Завдяки цьому блоку можливо переміщувати об'єкти на сцені. Для переміщення об'єктів використовується аналіз вводу користувача.
- *Блок фізики Unity*. Дана функціональна частина використовується для того, щоб на об'єкти розміщенні на сцені діяла гравітація.
- *Блок обробки колайдерів*. За допомогою цієї функціональної частини є можливим визначення моментів взаємодії між об'єктами на сцені.
- *Блок обробки переміщення об'єкту мишею*. Відповідає за визначення

поточної позиції миші на екрані визначення чи знаходиться миша на об’єкті, який можливо переміщувати та переміщення об’єкту у випадку, коли користувач намагається змінити його положення.

Меню користувача програми містить шість інтерактивних завдань, в яких можна переглянути приклад програмного коду та результати його виконання, а також внести в нього свої зміни та одразу переглянути результат. У кожному завданні розглядаються окремі можливості Unity, які необхідно розглянути початківцю, а саме:

– Завдання №1 «Створення та рух об'єктів» демонструє можливості «Створення об'єкту» та «Рух об'єкту»;

– Завдання №2 «Колайдери» демонструє можливості «Фізика Unity», «Обробка колайдерів» та «Обробка переміщення об’єкту мишею»;

– Завдання №3 «Управління клавіатурою» демонструє можливості «Обробка вводу користувача», «Обробка колайдерів» та «Фізика Unity»;

– Завдання №4 «Взаємодія об'єктів» демонструє можливості «Створення об’єктів», «Обробка колайдерів», «Обробка тяжіння Unity» та «Обробка вводу користувача»;

– Завдання №5 «Створення лабіринту» демонструє можливості «Створення об’єктів» на прикладі створення лабіринту;

– Завдання №6 «Проходження лабіринту» демонструє можливості «Створення об’єктів», «Обробки вводу користувача» та «Обробка тяжіння Unity» на прикладі проходження лабіринту.

Приклад скриншоту програмного забезпечення наведено на рис. 1.

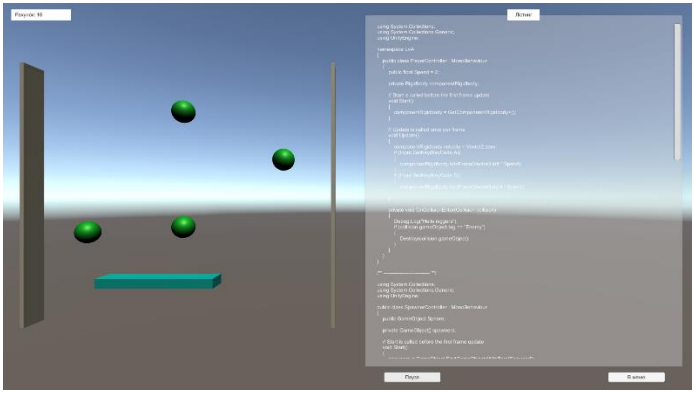


Рис. 1. Завдання №4 «Взаємодія об'єктів»

Розроблене програмне забезпечення буде корисним при інтерактивному вивченні ігрового рушія Unity.

УДК 004.9

Програмне забезпечення для конструктора нейронних мереж

Гасс М.Я., магістрант, gassxl@gmail.com
Мелешко Є.В., д.т.н., проф., elismeleshko@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна

Штучні нейронні мережі надають велике число можливостей, вони навчаються на основі досвіду, узагальнюють попередні прецеденти на нові випадки і знаходять істотні властивості у вхідних даних, що містять надмірності.

Так як розробка нейронних мереж з нуля є досить складним та трудомістким процесом, то все більшої популярності набувають різноманітні конструктори та бібліотеки для їх побудови.

На сьогоднішній день існує ряд бібліотек, що дозволяють конструювати нейронні мережі, зокрема, TensorFlow, PyTorch, Keras, FANN тощо.

Метою даної роботи була розробка конструктору нейронних мереж для класифікації та розпізнавання образів на мові програмування C++ з акцентом на можливість використання у навчальних цілях.

Розроблюване програмне забезпечення складається з чотирех блоків: блок прямого проходу, блок зворотного прохід, блок начання, блок вхідних данних начання.

Блок прямого проходу – включає в себе код, який виконує прямий прохід з вхідного шару нейронної мережі до вихідного. На вихід подається відповідь нейронної мережі.

Блок зворотного проходу – включає в себе код, який виконує зворотний прохід необхідних даних з виходу на вхід для кожного шару та обчислює помилку нейронної мережі. Також, після обчислення помилки, корегує вагові коефіцієнти зв’язків нейронів.

Блок навчання – включає в себе код, який виконує навчання нейронної мережі. Здійснює керуваняння данними, які подаються на вхід та порівняння відповідей неронної мережі з відомими вірними відповідями.

Блок вхідних даніх – містить в собі навчальну вибірку та налаштування для блоку навчання.

Створення нейронної мережі у розробленому конструкторі відбувається за наступним алгоритмом:

1. Створюється екземпляр нейронної мережі «nn::NeuralNetCahe» або «nn::NeuralNetRam».
2. Вказується кількість прошарків нейронної мережі та їх розмірність.
3. Створюються зв'язки між прошарками нейронної мережі. Зв'язки можна з’єднувати і прямим, і рекурентнім способами.

4. Використовується функція «PushIn» для передачі даних на вхід нейронної мережі.

5. Використовується функція «Calculation» для одержання відповіді нейронної мережі.

6. Отримується відповідь нейронної мережі за допомогою функції «PopOut».

Далі вже можна використовувати нейронну мережу у своїх цілях, подаючи на вхідні нейрони дані і збираючи з вихідних нейронів відповідь мережі. Якщо потрібно обучити нейронну мережу, то на вибір є декілька алгоритмів:

1. Навчання з учителем;
2. Навчання без учителя.

Нижче приведено приклад програмного коду:

```
// Створення мережі
nn::NeuralNetCahe neural(0, {{0,0,0,0}, "Test"});
// Додавання прошарків
auto l1 = neural.AddLayer(nn::NnLayerType::LayerInput, {1, 1, 1});
auto l2 = neural.AddLayer(nn::NnLayerType::LayerLinear, {100,1, 1});
auto l3 = neural.AddLayer(nn::NnLayerType::LayerLinear, {100,1, 1});
// Додавання зв’язків
neural.AddLink(nn::NnLinkType::NnLinkAll, l1, l2);
neural.AddLink(nn::NnLinkType::NnLinkAll, l2, l3);
// Додавання даних до мережі
neural.PushIn({1});
//
neural.Calculate();
```

Навчальний набір даних являє собою набір спостережень, для яких вказані значення вхідних і вихідних змінних. Перше питання, яке потрібно вирішити при створенні навчального набору даних – які змінні використовувати і скільки (і яких) спостережень зібрати. Вибір змінних (принаймні початковий) здійснюється інтуїтивно. Для більшості реальних задач буває досить декількох сотень або тисяч спостережень. Для особливо складних задач може знадобитися ще більша кількість, проте дуже рідко може зустрітися (навіть тривіальна) задача, де вистачило б менше сотні спостережень.

Розроблене програмне забезпечення тестувалося на розпізнаванні зображень та показало свою працездантість.

Функціонал розробленого програмного забезпечення створено максимально наближено до функціоналу відомих бібліотек з розробки нейронних мереж, зокрема, TensorFlow, PyTorch, Keras. Але на відміну від них, бібліотеку розроблено не на мові програмування Python, а на мові програмування C++, та можна використовувати як навчальний приклад при вивченні даної мови.

УДК 004.42:61

Удосконалена модель цифровізованого інфосервісу медичних послуг закладів охорони здоров'я міста Кропивницького

Доренський О.П., к.т.н., доцент, odorensky@gmail.com
Дробко О.С., здобувачка вищої освіти, ms.alenas@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна

Актуальність теми. Нині в Україні активно цифровізуються державні й муніципальні сервіси. Зокрема органи управління м. Кропивницького на основі суспільної потреби муніципальних послуг ініціювали створення декількох інформаційних систем (ІС), що необхідні для розвитку різних сфер діяльності [1]. Серед них – інтернетна ІС медичних послуг, які надаються закладами охорони здоров'я міста. Отже, задача цифрової трансформації сервісу надання інформації про медичні послуги муніципальними закладами охорони здоров'я є актуальною.

Мета роботи полягає у реалізації доступу до інформації про медичні послуги установ сфери охорони здоров'я міста Кропивницького за допомогою муніципальної ІС з iOS-клієнтом в офлайновому режимі. Тож об'єктом дослідження є процес забезпечення доступу до інформації про медичні послуги міських закладів охорони здоров'я з використанням інтернетних інфотелекомунікаційних технологій; предмет дослідження – технологія синтезу ІС медичних послуг муніципального рівня на основі програмного додатку для мобільної операційної системи iOS.

Удосконалення моделі ІС медичних послуг. На основі результатів аналізу існуючих систем - аналогів та технічних рішень муніципальних ІС, концептуальної моделі ІС медичних послуг [2], удосконалено модель муніципальної інформаційної системи медичних послуг [3] шляхом реалізації процесу офлайнового режиму функціонування інформаційної системи, що на відміну від існуючих моделей муніципальних систем забезпечує доступ до даних ІС за відсутності інтернету (рис. 1).

Практична реалізація удосконаленої моделі ІС. Для проектування iOS-клієнта ІС визначено функціонал компонент системи. На основі структурних елементів клієнта виконано деталізацію їх взаємозв'язків, розроблені алгоритми: узагальнений алгоритм додатку та алгоритми для роботи визначених у проекті сервісів. Також виконані необхідні розрахунки для GoogleMaps, удосконалені класи View Controller, Coordinator, ViewModel, переналаштовано взаємодію компонентів ІС. Згідно з запропонованими алгоритмами модифіковано класи сервісів, а також згідно з моделями реалізовано зв'язні, системні, програмні інтерфейси, що забезпечило компонування елементів ІС.

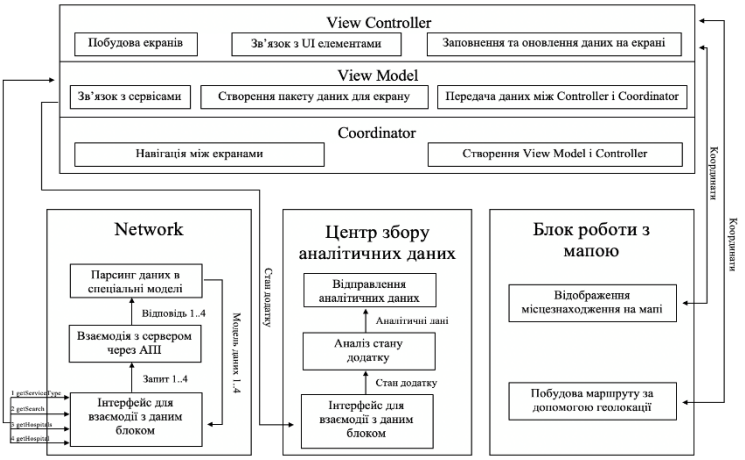


Рис. 1. Удосконалена модель муніципальної інформаційної системи медичних послуг м. Кропивницького

Висновок. Розв'язок завдань цього дослідження, зокрема розроблений на основі удосконаленої моделі мовою Swift в Xcode програмний засіб мобільного iOS-клієнта з доступом до даних ІС у період відсутності інтернету, забезпечують доступ до інформації про медичні послуги установ сфери охорони здоров'я міста Кропивницького у офлайні. Отже, поставлена науково-технічна задача розв'язана, мета роботи досягнута.

Список літератури

1. Доренський О.П., Дробко О.С. Структура і методологічні засади реалізації мобільного застосунку муніципальної інформаційної системи медичних послуг: матеріали II Всеукраїнської наук.-практ. конф. здобувачів вищої освіти й молодих учених «Комп'ютерна інженерія і кібербезпека: досягнення та інновації». Кропивницький, 2020. С. 23.

2. Дробко О.С., Доренський О.П. Модель муніципальної інформаційної системи медичних послуг: матеріали IV Міжнар. наук.-практ. конф. «Інформаційна безпека та комп'ютерні технології» / Мін-во освіти і науки України, Центральноукр. нац. техн. ун-т. Кропивницький, 2021. С. 39.

3. Дробко О.С., Доренський О.П. Функціональна модель муніципальної інформаційної системи медичних послуг міста Кропивницького // LV науково-технічна конференція «Наука в ЦНТУ: основні досягнення та перспективи розвитку» за підсумками проведення «Дня науки – 2021». Кропивницький: ЦНТУ. 2021. С. 75–76.

УДК 004.94

Розробка методу імітаційного моделювання мережевого трафіку з фрактальними властивостями

Дрєєва Г.М., аспірант, gannadreeva@gmail.com
Дрєєв О.М., к.т.н., доцент, drey.sanya@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна

Проведений аналіз публікацій [1-8] показав актуальність питання моделювання трафіку у комп'ютерних мережах. Зокрема, в [1] була проведена оцінка часу затримки пакетів в умовах зв'язку при обслуговуванні трафіку складної структури на основі розробленої імітаційної моделі. В [2] проаналізовані сучасні методи моделювання мережевого трафіку. Показано, що створення універсальної імітаційної моделі (УІМ) з їх допомогою проблемне з причини великого обсягу дослідницької роботи, необхідної для адаптації приватних моделей до всього різноманіття характеристик різних джерел мережевого навантаження і конфігурації мережі. Запропоновано застосування контекстних методів для побудови УІМ. В якості основи для побудови УІМ обраний метод динамічного марковского моделювання (ДММ). Проведена адаптація методу ДММ для УІМ і розроблена методика його застосування. У роботі [3] сформульована математична модель мультисервісного каналу зв'язку на основі експоненційної GERT-мережі. У працях [4-6] розглянуті питання генерації фрактального трафіку. У роботах [7, 8] пропонується метод агрегування фрактального трафіку телекомунікаційних мереж, його прогнозування та аналіз.

Виходячи з аналізу останніх досліджень і публікацій можна зробити висновок, що питання моделювання трафіку та використання для цих цілей генераторів фракталоподібних послідовностей є актуальним.

Таким чином, метою даної роботи є створення генератора фрактальних бінарних послідовностей на основі скінченного автомату та використання методу генерування фрактальноподібної числової послідовності на основі скінченного автомату для моделювання трафіку у мережі.

У цій роботі для реалізації методу генерування фрактального трафіку було запропоновано модель генератора на графі, а саме ланцюзі Маркова для скінченного автомату з двома станами, та вирішені наступні завдання:

– Показано актуальність задачі створення генераторів фрактальних бінарних послідовностей без використання нескінченних розподілів.

– Запропоновано використати генератор фрактальної бінарної послідовності на основі скінченного автомату.

– Показано можливість попереднього визначення фрактальної розмірності генерованого трафіку при інтенсивності $\tau = 0.5$.

– Проведено аналітичні оцінки показника Херста генерованої бінарної послідовності при інтенсивності трафіку $\tau = 0.5$.

– Показано варіативність фрактальної розмірності бінарної послідовності й при інших інтенсивностях τ.

– Виведено аналітичні вирази для отримання параметрів генератора з заданою густиною вихідних бітів з керуванням їх фрактальної розмірності.

Розроблену імітаційну модель мережевого трафіку планується використовувати у подальшому для тестування якості методів визначення фрактальної розмірності часових рядів, а також для прогнозування завантаженості мережевих пристроїв у комп'ютерних мережах.

Список літератури

1. Ушанев К.В. Имитационные модели системы массового обслуживания типа Pa/M/1, H2/M/1 и исследование на их основе качества обслуживания трафика со сложной структурой. Системы управления, связи и безопасности. 2015, №4. С.217-251.

2. Добровольский Е.В., Нечипорук О.Л. Моделирование сетевого трафика с использованием контекстных методов. Наукові праці ОНАЗ ім. О.С. Попова. 2005, № 1. С.24-32.

3. Семенов С.Г., Мелешко Є.В., Ілюшко Я.В. Математическая модель мультисервисного канала связи на основе экспоненциальной GERT-сети. Системи озброєння і військова техніка, ХУПС, 2011, № 3(27). С.64-67.

4. Tamara Radivilova, Yousef Ibrahim Daradkeh, Lyudmyla Kirichenko. Development of QoS Methods in the Information Networks with Fractal Traffic. International Journal of Electronics and Telecommunications. 2018, 64 (1). P. 27-32.

5. Mahdi Barat, Zadeh Joveini, Javad Sadri, Hoda Alavi Khoushhal. Fractal Modeling of Big Data Networks. International Conference on Pattern Recognition and Artificial Intelligence (ICPRAI 2018). Canada, Montreal: Concordia University, 2018. P. 1-4.

6. Jiang D., Huo L., Li Y. Fine-granularity inference and estimations to network traffic for SDN. PLoS ONE 2018, 13(5). Doi.org/10.1371/journal.pone.0194302.

7. Кучук Г. А, Можаєв О. О., Воробйов О. В. Прогнозирование трафика для управления перегрузками интегрированной телекоммуникационной сети. Радіоелектронні і комп'ютерні системи. 2007, № 8. С. 261–271. URL: http://nbuv.gov.ua/UJRN/recs_2007_8_48.

8. Кучук Г. А., Можаєв О. О., Воробйов О. В. Аналіз та моделі самоподібного трафіка. Авиационно-космическая техника и технология. 2006, № 9. С. 173–180. URL: http://nbuv.gov.ua/UJRN/aktit_2006_9_35.

УДК 004.056.53

Дослідження навігаційних систем, які використовують світловідбивальні маяки

Задорожний К.О., студент, kostazadorozhnij9@gmail.com
Науковий керівник – Мелешко Є.В., д.т.н., проф., elismeleshko@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна

Одним із способів навігації для автомобіля у відомому середовищі є розміщення світлоповертальних маяків на стінах. Датчик на мобільному роботі виявляє ці маяки. Маяки використовуються як фіксовані посилання в навігаційній системі. Якщо положення кожного маяка відомо, то можна розрахувати положення і курс робота.

Основи навігації за маяками. Спочатку в навколишнє середовище розміщують ряд світлоповертальних маяків. Після цього створюється карта, що описує положення кожного маяка. Точна кількість маяків і відстань між ними залежить від середовища. Однак система вимагає мінімум три маяки, які завжди мають бути видимими для навігації.

NDC8. Однією з навігаційних систем, яка використовує штучні маяки як еталони для навігації, є система NDC8, також відома як LazerWay. Навігаційна система використовується в різних промислових застосуваннях, включаючи автоматизовані транспортні засоби з LHD в підземній шахті LKAB в Кіруні, Швеція. Для виявлення штучних маяків система NDC8 використовує лазерний сканер. Коли буде виявлено необхідну кількість маяків, положення і курс автомобіля можна знайти, порівнявши розташування маяків з відомою картою.

Система NDC8 може оцінити положення транспортного засобу з невизначеністю в кілька сантиметрів при правильному налаштуванні. Для навігації під час руху транспортного засобу необхідно враховувати рух під час одного лазерного сканування. Якщо швидкість транспортного засобу не настільки низька, що нею можна знехтувати, необхідно запровадити додатковий процес обчислення шляху, щоб відстежувати рух автомобіля під час лазерного сканування.

Навігація на основі CMOS-камери. Навігаційна система на основі CMOS-камери, що використовує ті ж світлоповертальні маяки, що й система NDC8, була представлена в технологічному університеті Лулеї. Система призначена для використання в приміщеннях на короткі відстані (менше 20 м) і складається з чотирьох окремих модулів камери,

встановлених перпендикулярно один одному. Виявлення маяків здійснюється апаратно в кожному модулі камери. Вихідними є кути та відстані до виявлених маяків. Однією з переваг використання системи на основі камери замість скануючого лазера є можливість одночасного виявлення 360° маяка. При цьому рух транспортного засобу не має значення для процесу навігації. Таким чином, не потрібен процес навігаційного розрахунку.

Недоліки навігації за світлоповертаючим маяком. Оскільки навігаційна система, що використовує світловідбиваючі маяки, потребує додаткової інфраструктури в середовищі, вона підходить лише для використання добре відомих середовищ. Система не має можливості виявляти перешкоди або пересуватися по ділянках без світлоповертальних маяків. Якщо система буде використовуватися в середовищі з шорсткою поверхнею, тобто коли автомобіль, а отже, і датчик хитається, виявити маяки на великих відстанях може бути проблемою. Однак це не така велика проблема для навігаційної системи на основі камери, оскільки камери мають широке вертикальне поле зору.

Висновки. Навігаційні системи, які використовують світлоповертальні маяки підходять добре для знайомих середовищ, де немає перешкод. Для навігації потрібні мінімум 3 світлоповертальні маяки, щоб розрахувати положення і шлях робота. Світлоповертаючі маяки розміщують на стінах, наприклад в шахтах. Існують 2 основні навігаційні системи основані на світлоповертаючих маяках – NDC8 та CMOS-камери.

NDC8 використовують лазери для сканування маяків. Але при великих швидкостях потрібно додатково обчислювати шлях, під час лазерного сканування.

Навігація на основі CMOS-камери використовується на невеликих відстанях та коли рух транспорту немає значення для процесу навігації.

Список літератури

1. Навігація роботів – [Електронний ресурс]. – Режим доступу: https://uk.wikisko.ru/wiki/Robot_navigation

2. Navigation Sensors for Mobile Robots – [Електронний ресурс] – Режим доступу: http://www.diva-portal.org/smash/get/diva2:998928/FULLTEXT01.pdf

УДК 004.9

Розробка програмного забезпечення для візуалізації різних алгоритмів сортування

Золотухін Б.Є., студент, b.zolotuxin@gmail.com
Смутко В.О., студент, vitaliismutko@gmai.com
Ткаченко О.С., студент
Єремеєв М.О., студент
Науковий керівник – Босько В.В., к.т.н., доц.
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна

Алгоритми сортування впорядковують елементи за певним критерієм. Для такої простої задачі існують десятки різних алгоритмів. Причиною цьому послужив пошук ефективних способів вирішення не тільки стандартних задач, але складних випадків. Адже, вибір того чи іншого алгоритму сортування залежить відразу від декількох параметрів, які часто конфліктують один з одним, тож, треба визначатися який з них для розглядаємої задачі важливіший. Зокрема, серед основних параметрів алгоритмів сортування є швидкість роботи, об'єм потрібної додаткової пам'яті, стійкість, зрозумілість та легкість в реалізації тощо.

Візуалізація алгоритмів сортування дозволяє краще зрозуміти як вони працюють, дозволяє порівняти їх і, отже, надзвичайно корисна в процесі вивчення цих алгоритмів.

Метою даної роботи було створення програмного забезпечення для візуалізації різних алгоритмів сортування, що можна використати потім у навчальному процесі.

Принцип роботи розробленого програмного забезпечення для візуалізації алгоритмів сортування такий, що на кожній ітерації алгоритму сортування на екрані буде відображатися:

– білими лініями елементи масиву, що не беруть участь у зміні свого положення під час саме цієї ітерації;

– зеленою лінією буде відображатися елементу (елементи), що розглядається;

– синьою лінією буде відображатися елемент (елементи), з яким відбудеться зміна положення.

Довжини ліній, що символізують елементи масиву, відображають значення елементів – чим довша лінія тим більше числове значення елементу (рис. 1).

Для розробки програмного забезпечення було використано мову програмування C++ та середовище розробки Code::Blocks IDE. Для відображення роботи алгоритмів сортування було використано методи line(x1, y1, x2, y2) та setcolor(color) з бібліотеки graphics, які зображають

на екрані лінії відповідної ваги(значення) відповідного кольору. Типом даних для зберігання та виконання дій над даними було обрано вектори, а не звичайні масиви даних.

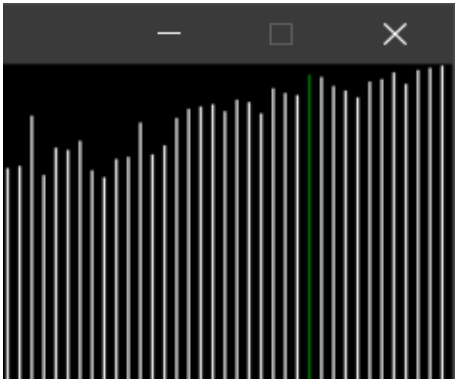


Рис. 1. Візуалізація елементів масиву під час сортування

Були реалізовані візуалізації для наступних алгоритмів сортування: сортування вибором, сортування вставкою, бульбашкове сортування, сортування методом бінарної вставки, плавне сортування, пірамідальне сортування, швидке сортування, сортування злиттям, сортування підрахунком, сортування за розрядами, сортування комірками, сортування злиттям, сортування Шелла, сортування перестановкою та випадкове сортування.

Основні кроки роботи розробленого програмного забезпечення після вибору користувачем алгоритму сортування для візуалізації:

1. Очищення екрану від залишків попередньої візуалізації;

2. Генерування та виведення випадкового масиву на екран у вигляді ліній, які потім в процесі візуалізації замальовуються певними кольорами, щоб показати які поточні елементи порівнюються (як у бульбашковому сортуванні), виділити мінімальний елемент (як у сортуванні вибором) або ж показати поточний елемент (як у сортуванні підрахунком) тощо;

3. Після кожної зміни у масиві на кожній ітерації циклу сортування перед оновленням зображення всього масиву виконується пауза, яка дозволяє користувачу побачити зміни, які відбулися, на даній ітерації циклу сортування.

Застосування того чи іншого алгоритму сортування для вирішення конкретної задачі є досить складною проблемою, вирішення якої потребує не лише досконалого володіння саме цим алгоритмом, але й всебічного розглядання того чи іншого алгоритму, тобто визначення усіх його переваг і недоліків. Візуалізація алгоритмів сортування дозволить краще розуміти принципи їх роботи.

УДК 004.05

Розрахунок параметрів ітерації проекту методом якісного аналізу вразливостей розроблення програмного забезпечення

Кобець М.О., аспірант nicko9298@gmail.com
Коваленко А.С., к.т.н., доц., annasun911@gmail.com
Коваленко О.В., д.т.н., доц., dr.kovalenkoov@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна

На теперішній час у більшості організацій і підприємств різних форм власності все більше уваги приділяється питанням аналізу й оцінки вразливостей. Удосконалений метод якісного аналізу вразливостей розроблення програмного забезпечення, що розглянуто у роботі [1], дозволив вирішити протиріччя, що виникає при розробці ПЗ, яке полягає у зневазі фірмами-розробниками ПЗ різноманітними факторами вразливості безпеки ПЗ. В процесі якісного аналізу вразливостей відбувається вироблення метрик, що відповідають за визначення граничних показників факторів, символізуючих прояви вразливості. Але практичній реалізації методу з застосуванням практичних багатокритеріальних вхідних сигналів приділено не достатньо уваги.

Було проведено низку практичних застосувань методу якісного аналізу вразливостей розроблення програмного забезпечення з застосуванням гнучкої методології розроблення програмного забезпечення Scrum та врахуванням багатокритеріальних вхідних сигналів в комплексі зі значним обсягом вибірки практичних застосувань методу дозволило підтвердити правильність застосованих підходів методу.

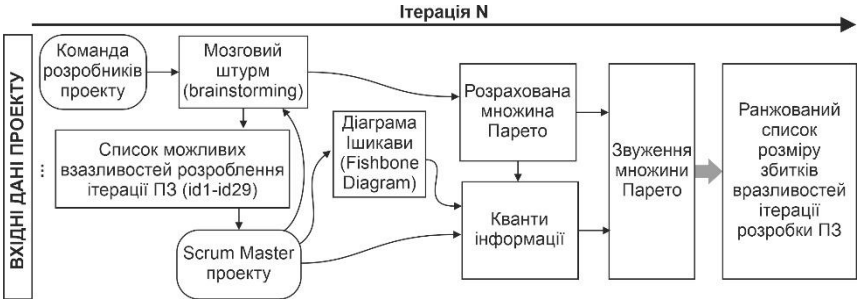


Рис. 1. Ітераційна схема розробки ПЗ з використанням методу якісного аналізу вразливостей

Scrum – це фреймворк управління, згідно з яким одна чи кілька кроссфункціональних самоорганізованих команд розробляють ПЗ поетапно [2-3]. У Scrum є система ролей, зустрічей та правил. У цій моделі розроблення ПЗ за створення і адаптацію робочих процесів відповідають команди. Використовуються ітерації фіксованої довжини, так звані спринти. Вони зазвичай займають 1-2 тижні (до 1 місяця). Scrum команди прагнуть створити готове до впровадження (якісно протестоване) програмне забезпечення.

Під час практичного застосування методу були застосовані наступні вхідні параметричні дані проекту:

1. Назва проекту.
2. Короткий опис проекту.
3. Ітерація розробки проекту та склад команди розробників.
4. Визначений набір параметрів оцінки вразливостей для проекту: Ймовірність виникнення вразливості; Збитки економічні 1 – незначний, 2 – середній, 3 – важкий; 4 – дуже важкий, погано прогнозований; 5 – критичний, крах розробки ітерації програмного забезпечення та неможливість подальшої розробки проекту; Збитки репутаційні 1 – незначний; 2 – середній, простої розробників (зняття з завдань по розробці); 3 – високий недовіра, втрата майбутніх замовлень проектів; 4 – критична, прогнозована повна втрата довіри, неможливе подальше співробітництво з замовником.

Висновки. Розглянуто практичний підхід реалізації методу якісного аналізу вразливостей розроблення програмного забезпечення. Що дозволяє звузити сукупність множин Парето та більш точно обирати пріоритетність напрямків фінансування профілактичних заходів виявлених вразливостей. Запропоновано спосіб застосування гнучкої методології розроблення програмного забезпечення Scrum з врахуванням багатокритеріальних вхідних сигналів.

Список літератури

6. Коваленко О.В. Методи якісного аналізу та кількісної оцінки ризиків розробки програмного забезпечення / О.В. Коваленко // Системи управління, навігації та зв'язку. – Випуск 3 (49). – Полтава: ПолтНТУ. – 2018. – С. 116-125.

7. Putu Adi Guna Permana Scrum Method Implementation in a Software Development Project Management/ Putu Adi Guna Permana // International Journal of Advanced Computer Science and Applications. – 2015. – Vol. 6. № 9. – P. 199-205.

8. I.F. Ashari Design and build inventory management information system using the SCRUM method / Ilham Firman Ashari, Annisa Jufe Aryani, Alief Moehamad Ardhi // Jurnal Sistem Informasi. – 2022. – Vol. 9. №1. – P. 27-35.

УДК 004.413: 004.05

Огляд та аналіз способів зменшення ризиків розробки програмного забезпечення

Константинова Л.В., викладач, liliyashel1976@gmail.com
Кривда О.С., студент 2 курсу, krivdaolse@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна

Розробка програмного забезпечення (ПЗ) – це діяльність, у якій використовуються технологічні досягнення та потрібні високий рівень знань із різних галузей. Кожен проект розробки програмного забезпечення містить елементи невизначеності, що призводить до проектних ризиків. Ризик є потенційною проблемою [1]. Це дія чи подія, яка може поставити під загрозу успіх проекту. І тому огляд й аналіз способів зменшення ризиків розробки ПЗ буде актуальною задачею.

Ризик – це можливість зазнати збитків, і загальна схильність до ризиків конкретного проекту враховуватиме як ймовірність, так і розмір потенційних збитків.

Керування ризиками означає стримування та зниження ризиків. Керування ризиками може включать наступні дії:

- Визначення ризиків та їх тригерів.
- Класифікація та визначення всіх ризиків за пріоритетами.
- Планування, що дозволить мінімізувати ризики.
- Контроль тригерів ризику під час проекту.
- Вживання заходів щодо пом'якшення наслідків, якщо будь-який ризик матеріалізується.
- Оновлення статусів ризиків протягом усього проекту.

Більшість проектів розробки ПЗ ризиковані через безліч потенційних проблем, які можуть виникнути. Проста, але ефективна схема класифікації у тому, щоб розподілити ризики зі сфер впливу. Тут важливі не елегантність чи діапазон класифікації, а, швидше, точне визначення та опис всіх реальних загроз для успіху проекту [1].

Існує планування методом «хвилі, що набігає» [2]. Команди приймають рішення щодо продукту у міру просування роботи, замість того, щоб розробляти найдокладніший план дій на самому старті проекту. Дієві рішення, прийняті з урахуванням нових знань розвитку продукту, знижують ймовірність ризиків, що до бюджету, оскільки команді не треба витрачати час і ресурси на повторне планування.

Метод розробки з урахуванням спринтів [2] надає розробникам впевненості у правильності створення продукту, і дозволяє дотримуватись потрібної швидкості виконання завдання. Спринти - це короткострокові етапи розробки з метою створення демоверсії продукту в заданий термін.

Вони служать для позначення правильних цілей та завдань для проектних команд та дозволяють побачити проміжні результати роботи.

Для зменшення ризику виникнення вразливостей, помилок при роботі ПЗ застосовують, по-перше, системи автоматичного пошуку дефектів за допомогою статичного аналізу вихідного коду програм [3], які можна використовувати на ранніх етапах розробки ПЗ, що виконує виправлення помилок з мінімальними затратами. Також, застосовують системи динамічного аналізу бінарного коду ПЗ [3], які дозволяють багаторазово запускати потрібну програму на наборі вхідних даних, що автоматично генерується, та відстежувати ситуації виникнення дефектів.

Ризики можуть змінюватись від проекту до проекту, їх завжди слід враховувати при розробці. Щоб команда розробників закінчила вчасно проект, необхідно досить часто спілкуватися з клієнтом або менеджером проекту для уточнення деталей проекту та уникнення ризиків непорозуміння [2].

Керування ризиками – це велика дисципліна. Всі дії та методи, що розглядались в роботі можуть допомогти зменшити ризики під час створення ПЗ, але треба враховувати особливості деяких програмних систем і для них застосовувати можливі специфічні технології та методи, враховуючи всі недоліки та переваги.

Список літератури

1. Risk Management in Software Development and Software Engineering Projects [Електронний ресурс]: https://www.castsoftware.com/research-labs/risk-management-in-software-development-and-software-engineering-projects

2. Риски при разработке программного обеспечения [Електронний ресурс]: https://habr.com/ru/post/423673/

3. Аветисян А.И., Белеванцев А.А., Чукляев И.И. Технологии статического и динамического анализа уязвимостей программного обеспечения [Електронний ресурс]: https://cyberleninka.ru/article/n/tehnologii-staticheskogo-i-dinamicheskogo-analiza-uyazvimostey-programmnogo-obespecheniya

УДК 004.413:004.05

Огляд та класифікація ризиків розробки програмного забезпечення

Константинова Л.В., викладач, liliyashel1976@gmail.com
Сосна О.С., студент 2 курсу, litetab387@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна

Процес розробки програмного забезпечення (ПЗ) в загальному випадку супроводжується великою кількістю невизначеностей, які здатні надавати негативний вплив на терміни випуску і якість програмного продукту [1]. Це є для проектів факторами ризику, які необхідно якомога мінімізувати. Для того, щоб керувати ризиками, необхідне вміння ідентифікації та прогнозування їх. Тому задача огляду та класифікації ризиків при розробці програмного забезпечення буде актуальною на даний час.

Ігнорування ризиків ставить під загрозу результат всього програмного проекту [2]. Якісне виявлення ризиків передбачає наявність точних даних про динаміку розвитку проекту.

На різних етапах основних процесів розробки ПЗ [3] (вибір моделі життєвого циклу; виявлення та аналіз вимог; проектування ПЗ; програмування; тестування; впровадження ПЗ; приймання ПЗ) можуть виникати помилки різної складності.

Ризики можуть відрізнятися залежно від кількох факторів, характеру проекту, команди проекту, але загалом їх можна поділити на кілька категорій. В таблиці 1 представлено ризики за видами.

Таблиця 1 – Види та наслідки ризиків

Види ризиків	**Огляд ризиків**	**Наслідки ризиків**
Управлінські ризики [1][2]	недостатня надійність апаратного та програмного інструментарію, проблема комплектації персоналу та умов праці.	Риск для всього проекту, кардинальні адміністративні заходи, аж до згортання всього проекту.
Технічні ризики, не пов'язані зі складністю ПЗ, що розробляється [1][2][3]	Деякі категорії помилок виникають просто через неуважність, внаслідок “людського фактора”.	Друкарські помилки – незначні наслідки, рідше випадкове видалення файлів - серйозна проблема.
Технічні ризики, пов'язані з недостатньою	Виготовленням ПЗ займаються спеціалісти, що не досконально	Може бути незначним, може мати наслідки у вигляді не якісного ПЗ,

кваліфікацією персоналу [1][2]	вивчили свій план робіт.	з великою кількістю помилок.
Технічні ризики, пов'язані з пізнім виправленням помилок [1][2][3]	Помилки на ранніх стадіях проекту несуть вагомий ризик за рахунок шкоди, яку вони завдають зростаючи з часом.	Чим пізніше виявляється помилка, припущена на ранній стадії проекту, тим більшою буде шкода і наслідки.

За характером наслідків ризики розробки ПЗ розділяють на дві групи: чисті й спекулятивні [2].

Чисті ризики складають:

- ризики проектного управління;
- проектні ризики;
- кадрові ризики;
- деліктні ризики.

Спекулятивні ризики складають:

- ризики фінансових обмежень;
- зміни кон'юнктури ринку;
- валютні ризики.

Виявлення та аналіз ризиків на ранніх стадіях розробки грають важливу роль для успіху проекту розробки ПЗ [1][2][3].

Висновки. В роботі було виконано огляд наявних ризиків розробки програмного забезпечення, розглянуто їх за видами та як їх уникати, представлена таблиця з основними видами ризиків та їх наслідками, що може бути корисною для створення нових методик виявлення та мінімізації ризиків.

Список літератури

1. Макаров Д. А., Розенберг М. Я., Шильников А. Б. О факторах риска в процессе разработки программного обеспечения. 2009 г. [Електронний ресурс]: https://dspace.susu.ru/xmlui/bitstream/handle/0001.74/817/9.pdf?sequence=1&isAllowed=y.

2. Бадюков В.Ф., Сыч Г.Л. Классификация и анализ рисков разработки программного обеспечения \ Вестник Хабаровской государственной академии экономики и права вып.3, 2016 г. [Електронний ресурс]: https://readera.org/klassifikacija-i-analiz-riskov-razrabotki-programmnogo-obespechenija-14319455.

3. Романова Ю.А. Основные риски в процессах разработки программного обеспечения. 2016. [Електронний ресурс]: https://cyberleninka.ru/article/n/osnovnye-riski-v-protsessah-razrabotki-programmnogo-obespecheniya/viewer.

УДК 004.056.53

Дослідження методів тестування генераторів псевдовипадкових чисел

Кривохижа В.Ю., студент, vvvetal2003@gmail.com
Науковий керівник – Мелешко Є.В., д.т.н., проф., elismeleshko@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна

Вступ

У сучасній інформатиці псевдовипадкові числа широко використовуються в безлічі додатків, від методів Монте-Карло і імітаційного моделювання до друкованої графіки. Якість використовуваного генератора псевдовипадкових чисел (ГПВЧ) впливає на якість результату у відповідних додатках. Цю обставину підкреслює відома фраза математика Кав'ю Р.: "Генерація випадкових чисел занадто важлива, щоб залишати її на волю випадку." Додатки для шифрування використовують спеціальні алгоритми для генерації випадкових чисел, зокрема, для створення ключів шифрування. Від якості таких генераторів залежить стійкість алгоритмів шифрування до кібератак.

Для перевірки якості ГПВЧ використовуються різні тести на випадковість. Було досліджено основні види тестів на якість ГПВЧ.

Частотний побітовий тест

Тест полягає у визначенні співвідношення між нулями та одиницями у всій двійковій послідовності. Мета – з'ясувати чи дійсно число нулів і одиниць у послідовності приблизно однакові, як це можна було б припустити у разі випадкової бінарної послідовності. Тест оцінює, наскільки близька частка одиниць до 0,5. Якщо обчислене під час тесту значення ймовірності $p < 0,01$, то ця двійкова послідовність не є справді випадковою. Інакше, послідовність має випадковий характер. Всі наступні тести проводяться за умови, що пройдений даний тест.

Частотний блоковий тест

Визначаються частки одиниць усередині блоку завдовжки m біт. Мета – з'ясувати чи дійсно частота повторення одиниць у блоці довжиною m біт приблизно дорівнює m/2, як можна було б припустити у разі абсолютно випадкової послідовності. Обчислене в ході тесту значення ймовірності p повинно бути не менше ніж 0,01. Якщо прийняти $m = 1$, цей тест працює аналогічно попередньому – частотному побітовому тесту.

Тест на періодичність

Цей тест обчислює частоту всіх можливих перетинів шаблонів довжиною m біт для послідовності вихідних бітів. Мета полягає в тому, щоб з'ясувати чи кількість появ 2^m шаблонів, що перекриваються, довжиною m біт, приблизно така ж як у випадку абсолютно випадкової

вхідної послідовності біт.

Тест на найдовшу послідовність одиниць у блоці

Визначається найдовший ряд одиниць усередині блоку довжиною m біт. Мета – з'ясувати, чи справді довжина такого ряду відповідає очікуванням довжини найдовшого ряду одиниць у разі абсолютно довільної послідовності.

Тест рангів бінарних матриць

У цьому тесті проводиться розрахунок рангів підматриць, що не перетинаються, побудованих з вихідної двійкової послідовності. Мета – перевірка на лінійну залежність підрядків фіксованої довжини, що становлять початкову послідовність.

Спектральний тест

Полягає в оцінці висоти піків дискретного перетворення Фур'є вихідної послідовності. Мета – виявлення періодичних властивостей вхідної послідовності, наприклад, близько розташованих одна до одної ділянок, що повторюються. Це явно демонструє відхилення від випадкового характеру досліджуваної послідовності.

Тест на лінійну складність

Цей тест заснований на принципі роботи циклу лінійного регістру зсуву зі зворотними зв’язками. Мета полягає в тому, щоб визначити, чи є вхідна послідовність досить складною, щоб її можна було вважати повністю випадковою. Абсолютно випадкова послідовність чисел характеризується довгими лінійними регістрами зсуву зі зворотними зв’язками.

Універсальний статистичний тест Маурера

Цей тест визначає число бітів між однаковими шаблонами у вихідній послідовності (міра, що має безпосереднє відношення до довжини стиснутої послідовності). Метою тесту є намагання з'ясувати, чи дана послідовність може бути сильно стиснута без втрат інформації. У випадку, якщо це можливо зробити, вона не є справді випадковою.

Висновки. У даній роботі було досліджено основні методи тестування ГПВЧ. Проблема генерації випадкових та псевдовипадкових послідовностей, що застосовуються у різних додатках і, зокрема, у криптографії, залишається актуальною на сьогоднішній день. Існує велика кількість статистичних тестів для перевірки генераторів.

Список літератури

1. Григорьев А. Ю. Методы тестирования генераторов случайных псевдослучайных последовательностей //УлГУ. Электрон. журн. 2017, № 1, с. 22-28.

2. Горбенко І.Д. Прикладна криптологія / І.Д. Горбенко, Ю.І. Горбенко. – Харків : Видавництво “Форт”, 2012. – 870 с.

УДК 629.7.02+004.056.5

Метод шифрування трафіку безпілотних літальних пристроїв квадрокоптерного типу

Майданик О.О., магістр з комп'ютерної інженерії
maidanyksmail@gmail.com
Мелешко Є.В., д.т.н., проф., elismeleshko@gmail.com
Шимко С.В., аспірант, shymko.sv@meta.ua
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна

Використання безпілотних літальних пристроїв квадрокоптерного типу для моніторингу наземних об'єктів стає все більш поширеною практикою та дозволяє ефективно вирішувати велике коло задач. В той же час квадрокоптери вразливі до інформаційних атак [1], що можуть здійснюватися з різними цілями, зокрема, для крадіжки дрону, використання його у мережі ботів для атак на інші пристрої, або для перехоплення інформації, яку він збирає для оператора пристрою. Це все зумовлює необхідність розробки дієвих методів інформаційного захисту дронів від кібератак.

У даній роботі пропонується метод шифрування трафіку квадрокоптерів через аналоговий тракт для захисту даних, якими він обмінюється з іншими пристроями, а також передає оператору. Особливу увагу при розробці методу шифрування було приділено методу генерації ключів шифрування, адже саме на них базується стійкість будь-якого алгоритму шифрування. Послідовності, отримані в результаті роботи генератора псевдовипадкових чисел повинні бути непередбачуваними та мати довгий період, щоб їх можна було використовувати в криптографічних системах захисту інформації [2, 3].

Для шифрування даних було використано шифр Вернама. А у якості ключа шифрування псевдовипадкову послідовність, що генерувалася за допомогою математичного більярду Сіная. Було запропоновано покращену математичну модель генерації ключів шифрування на основі більярду Сіная.

У 1976 році відомий математик Сінай Ю.Г. довів, що поведінка більярдної кулі у динамічному більярді, яка визначається детермінованим рівнянням, та поведінка більярдної кулі, яка керується процесом Маркова першого порядку, нерозрізнимі [4]. Оскільки марковський процес першого порядку є ймовірнісним процесом, який залежить тільки від попереднього зіткнення з перепоною, то він є як недетермінованим, так і непередбачуваним. Системи динамічного більярду виявили добре розвинену хаотичну поведінку [5].

На основі запропонованої математичної моделі було розроблено програмне забезпечення та створені робочі макети пристроїв для проведення експериментів. Для створення макету обрано модуль на основі мікроконтролера STM32F103C8T6, дані між пристроями передавалися через радіомодуль.

Для реалізації програмного забезпечення, яке повинне виконуватися на мікроконтролері, було обрано середовище розробки STM32CubeIDE від компанії STMicroelectronics – вдосконалену платформу розробки C/C++ [6] з периферійною конфігурацією, генерацією коду, складанням коду та налагодженням для мікроконтролерів та мікропроцесорів STM32.

Для побудови розроблюваної системи створено робочі макети пристроїв. Для створення макету обрано модуль на основі мікроконтролера STM32F103C8T6 [7].

Проведено тестування працездатності розробленого програмного та апаратного забезпечення, що підтвердило можливість його використання у квадрокопткрах. Було успішно здійснено обмін шифрованими даними між двома пристроями по радіоканалу. Після шифрування на одному пристрої, дані були успішно дешифровані на іншому пристрої.

Розроблене програмне та апаратне забезпечення системи шифрування трафіку квадрокоптера, що дозволяє шифрувати дані, якими квадрокоптер обмінюється з комп'ютером оператора.

Список літератури

1. Главное о безопасности дронов. Веб-сайт фирмы «Лаборатория Касперского». URL: https://www.kaspersky.ru/resource-center/threats/can-drones-be-hacked
2. Eastlake, D.E., Schiller, J.I., & Crocker, S. (2005). Randomness Requirements for Security. RFC, 4086, 1-48.
3. Barker, E. and Kelsey, J. (2015), Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.800-90Ar1
4. Sinai Y.G. Dynamical systems with elastic reflections // Russian Mathematical Surveys. – 1970. - vol. 25, no. 2, pp. 137-189.
5. Ганапольский Е.М. О природе квантового хаоса в рассеивающей бильярдной К-системе // Доповіді Національної академії наук України. - 2012. - № 3. - С. 85-91.
6. STM32CubeIDE [Електронний ресурс]. Режим доступу: https://www.st.com/en/development-tools/stm32cubeide.html
7. STM32F103C8 [Електронний ресурс]. Режим доступу: https://www.st.com/en/microcontrollers-microprocessors/stm32f103c8.html

УДК 004

Тенденції та перспективи розвитку інформаційних технологій

Марченко А.К., студентка, sanat_kumara@i.ua
Науковий керівник – Оришака О.В., канд. техн. наук, доц.,
oryhsaka@gmail.com
Центральноукраїнський національний технічний університет,
м. Кропивницький, Україна

Сьогодні людство знаходиться біля витоків Четвертої промислової революції. Розвиток інформаційних технологій є основою цієї революції, яка за масштабом, обсягом та складністю не має аналогів у всьому попередньому досвіді людства. Четверта промислова революція призводить до значних технологічних проривів у широкому спектрі областей, включаючи штучний інтелект, роботизацію, тривимірний друк, нанотехнології, біотехнології та багато іншого. Усі ці досягнення мають одну спільну особливість: вони ефективно використовують можливості інформаційних технологій [5].

Сучасні цифрові технології, які засновані на програмному забезпеченні та мережах, не є нововведенням, але з кожним роком вони стають більш удосконаленими та інтегрованими.

У наш час все більша кількість інформації обробляється за допомогою мережевих сервісів (на боці сервера). Більш того, якість такої обробки часто вище, ніж на локальному (на боці клієнта) програмному забезпеченні. Прикладом такої якості може служити розпізнавання мови та конвертація аудіо у текст, яке має клієнтську частину у вигляді програмного забезпечення Google Assistant для смартфонів і серверну частину, на якій, власне і відбувається обробка інформації.

Список сучасних ключових гравців в сегменті розпізнавання і синтезу мови в західних країнах досить значний: Amazon, Google, Apple і Microsoft. Асортимент продукції цих компаній розширюється, як в сегменті розпізнавання і синтезу мови, так і в сегменті мережевих сервісів. Список завдань, які виконуються за допомогою мережевих сервісів постійно і стійко розширюється [1, 2]. Таким чином, у світі ось уже не перший рік спостерігається тенденція розширення сегменту мережевих сервісів обробки інформації [3, 4].

Відповідно, виконання обчислювальних операцій все більше переноситься з боку клієнта на сторону сервера. Це закономірний наслідок відомого закону про спіраль розвитку. У минулому це вже було, тільки на іншому рівні, а саме: У 1970-хх роках у світі широко використовувались електронно-обчислювальні машини, де обчислювальні операції проводилися на стороні сервера, а введення-виведення даних могло здійснюватися по комп'ютерній мережі з терміналів, які не мали

обчислювальних потужностей. Приклад: ЕОМ серій System / 360 і System / 370 фірми IBM (і радянські ЕОМ серії ЄС).

Які перспективи проглядаються в цьому тренді? Оскільки все більше обчислювальних операцій переносяться на сторону сервера, то на боці клієнта (на домашніх ПК, наприклад) немає необхідності мати потужну обчислювальну техніку, отже, в найближчі роки сервери будуть збільшувати свою потужність, а клієнтські ЕОМ – навпаки, мати тенденцію до спрощення (відносно серверів). Одночасно з цим будуть удосконалюватися мережеві технології.

Висновки. Проаналізовано тенденції та перспективи розвитку інформаційних технологій, показано спіраль розвитку інформаційних технологій.

Список літератури

1. Кононенко Л.В., Юрченко О.В., Гай О.М. Теорія бухгалтерського обліку в умовах становлення глобальної економіки та інформатизації суспільства. Економічний простір: Збірник наукових праць. № 170. Дніпро: ПДАБА, 2021. С. 83-87 URL: http://prostir.pdaba.dp.ua/index.php/journal/article/view/911 (дата звернення: 20.02.2022).

2. Кононенко, Л. В., Назарова, Г. Б., Куц, В. І. Трансформація форм бухгалтерського обліку в умовах розвитку digital-технологій. Економічний простір: Збірник наукових праць. № 68. Дніпро: ПДАБА, 2021. С. 132-137. URL: https://doi.org/10.32782/2224-6282/168-22 (дата звернення: 22.02.2022)

3. Марченко К.М., Оришака О.В. Інформаційно-психологічна безпека людини в інформаційному суспільстві. Матеріали II Міжнародної науково-практичної конференції "Інформаційна безпека та інформаційні технології": тези доповідей, 2 – 3 квітня 2020 р. Кропивницький: ЦНТУ, 2020. С.15 URL: http://kbpz.kntu.kr.ua/wp-content/uploads/2020/04/ЗБІРНИК-ТЕЗ-конф-2-3-квітня.pdf#page=15 (дата звернення: 21.02.2022).

4. Оришака О.В., Селіщев В.О. Інформатизація бухгалтерського обліку: проблеми та перспективи. Напрями економічного зростання та інноваційного розвитку підприємства: матеріали всеукр. наук.-практ. конф. студ., аспірантів та молодих учених, м. Кропивницький, 16 квіт. 2020 р. Кропивницький: ЦНТУ, 2020. С. 117-118. URL: http://dspace.kntu.kr.ua/jspui/bitstream/123456789/10344/3/konferents_16-04-2020-sel-7-8.pdf (дата звернення: 22.02.2022).

5. Шваб Клаус Технологии Четвертой промышленной революции: [перевод с английского] / Клаус Шваб, Николас Дэвис. Москва: Эксмо, 2018. 320 с. : ил. (Top Business Awards).

УДК 004.94

Дослідженя методів імітаційного моделювання соціальних мереж

Мельник А.М., студентка, mselnikanna@gmail.com
Науковий керівник – Мелешко Є.В., д.т.н., проф., elismeleshko@gmail.com
Центральноукраїнський національний технічний університет,
м. Кропивницький, Україна

Віртуальні соціальні мережі у наш час відіграють досить важливі функції у комунікації людей. Використання соціальних мереж допомагає людям, які наділені додатковою інформацією розповсюджувати її, ділитися з користувачами у віддаленому режимі, також просто застосовуються для комунікації користувачів між собою.

Для дослідження соціальних мереж та соціальних процесів, що у них протікають, часто використовується імітаційне моделювання. Існує велика кількість моделей соціальних мереж. Розглянемо найбільш відомі з них. Принципи покладені в модель Барабаши-Альберт та Модель Ватса-Строгатца зараз найчастіше використовуються при побудові складних імітаційних моделей соціальних мереж.

Модель Барабаши-Альберт. Модель заснована на алгоритмі генерації випадкових мереж з використанням принципу переважного приєднання. Безмасштабні мережі широко розповсюджені в природних мережах (харчові ланцюги) і мережах, які створені людиною (Інтернет, всесвітня павутина, віртуальні соціальні мережі).

Модель Барабаши-Альберт – одна з декількох моделей з степеневою перевагою, які генерують безмасштабні мережі. Вона включає в себе дві важливі концепції:

- Ріст мережі.
- принцип переважного приєднання.

Обидві концепції широко представлені в мережах реального світу. Ріст значить, що число вузлів мережі збільшується з часом.

Принцип переважного приєднання заключається в тому, що чим більше зв'язків має вузол, тим більше переваг (ймовірності) для нього у створенні нових. Вузли з найбільшим степенем мають більше можливостей збирати для себе зв'язки, які додаються в мережу. Інтуїтивно, принцип переважного приєднання може бути зрозумілим, якщо мова йде про соціальні мережі, які об'єднують людей. Тут зв'язки від *A* до *B* означають, що людина *A* «знає» або «знайома» з людиною *B*. Сильно пов'язані вузли представлені відомими людьми з великим числом зв'язків. Коли новачок потрапляє у соціальну мережу, для нього більш корисніше налагодити зв'язки з одним з відомих людей, ніж з відносно невідомими. Схожим методом у всесвітній мережі сторінки пов'язані з хабами, до прикладу, переважно з відомими сайтами, ніж з сторінками, які

мало кому відомі. Якщо вибрати для зв'язку нову сторінку випадковим чином, то ймовірність вибору певної сторінки буде пропорційною її степеню. Це пояснює принцип переважного приєднання.

Модель Ватса-Строгатца. Ця модель ще відома під назвою «Модель малого світу». Суть моделі заключається в теорії, що кожна людина пов'язана з іншими людьми не більше, ніж через шість особистих знайомств.

Американський психолог Мілграм, задумуючись над питанням, яка "відстань" може бути між двома випадково вибраними людьми, здійснив дослід: під відстанню він мав на увазі кількість знайомств, яке необхідне для встановлення зв'язків між даними людьми. Мілграм зробив таким чином: оскільки він жив у Бостоні, то вибрав далекий шлях від Бостону – місто Небраска, і випадково обраним людям роздав конверти, які потрібно було передати в Бостон. Конверти можна було передавати лише через своїх знайомих і родичів. Мілграм отримав несподіваний результат: в середньому, кожний конверт пройшов через шість людей. Так народилася теорія про «шість рукостискань».

Модель переходу від великого світу до малого запропонував Ваттс і Строгац. Ця модель представляє собою одновимірну регулярну решітку, яка створена з N вузлів, у якій кожний вузол з'єднується тільки з своїми k найближчими сусідами, а також накладені періодичні граничні умови, тобто решітку стиснули у кільце. Після чого кожен зв'язок з ймовірністю $f << 1$ перекидують на інший випадково вибраний вузол. Правда при такій процедурі є ймовірність появи ізольованих вузлів.

Висновки. Соціальні мережі грають важливу роль у комунікації користувачів з усього світу. Імітаційне моделювання соціальних мереж дозволяє досліджувати різні соціальні процеси та перевіряти різні теорії. Моделі, які описані вище, зокрема, підтверджують теорії про існування «малого світу», та про те, що «багаті люди стають багатшими», тобто, підтверджують принцип асортативності.

Список літератури

1.Модел Барабаши-Альберт [Електронний ресурс] – Режим доступу: https://ru.wikipedia.org/wiki/Модель_Барабаши_—_Альберт (дата звернення: 20.03.2022)

2. Снарский А.А., Ландэ Д.В. Моделирование сложных сетей: учебное пособие. - К.: Инжиниринг, 2015. - 212 с. [Електронний ресурс] – Режим доступу: http://dwl.kiev.ua/art/mss/

УДК 004.056

Аналіз характеристик середовища виконання MPI-програм

Минайленко Р.М., к.т.н., доц., aron70@ukr.net
Мосольд М.І., магістрант, maximmosold@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна

Коли виконання того чи іншого алгоритму у комп'ютерній системі чи мережі вимагає великої кількості обчислювальних ресурсів, то для особливо вимогливих алгоритмічних завдань, які працюють з великою кількістю даних і вимагають мінімізувати час виконання завдання, необхідна оптимізація. Одним з основних способів такої оптимізації є розпаралелювання процесів. Паралелізація дозволяє користуватися можливостями декількох ядер процесора або декількома процесорами тощо. Це дає більше обчислювальних можливостей, але треба правильно організовувати паралельну роботу алгоритму.

Проведення паралельних обчислень в обчислювальній системі потребує встановлення середовища виконання MPI-програм, з метою забезпечення розробки, компіляції, компонування та виконання паралельних програм. Для виконання першої частини перерахованих дій, тобто розробки, компіляції та компоновки, достатньо звичайних засобів розробки програм (наприклад, Microsoft Visual Studio) необхідна лише наявність тієї чи іншої бібліотеки MPI. Для виконання паралельних програм від середовища виконання потрібно ряд додаткових можливостей, а саме:

– наявність засобів вказівки використовуваних процесорів;

– операцій віддаленого запуску програм і т.д.

Бажаною є наявність в середовищі виконання засобів профілювання, трасування та відлагодження паралельних програм. На цьому стандартизація закінчується (стандарт MPI-2 дає певні рекомендації про те, як повинно бути організовано середовище MPI-програми, проте вони не є обов'язковими).

На даний час існує декілька різних середовищ виконання MPI-програм, в більшості випадків вони створюються сумісно з розробкою тих чи інших варіантів MPI-бібліотек. Як правило, вибір реалізації MPI-бібліотек, встановлення середовища виконання і підготовки інструкцій з використання здійснюється адміністратором обчислювальної системи. Інформаційні ресурси Інтернету, на яких розташовуються вільно використовувані реалізації MPI, та промислові версії MPI містять вичерпну інформацію про процедури встановлення MPI, а виконання всіх необхідних дій є не складним.

Запуск MPI-програми також залежить від середовища виконання, але в більшості випадків ця дія виконується з використанням команди **mpirum** (стандарт MPI-2 рекомендує використовувати команду **mpiexec**). В числі можливих параметрів цієї команди:

- режим виконання - локальний або багатопроцесорний (локальний режим як правило вказується з використанням ключа - **localony**, при виконанні паралельної програми в локальному режимі всі процеси програми розташовуються на комп'ютері, з якого процеси програми розташовуються на комп'ютері, з якого був здійснений запуск програми. Такий спосіб виконання дуже корисний для початкової перевірки працездатності та відлагодження паралельної програми, частина цієї роботи може бути виконана навіть на окремому комп'ютері поза рамками багатопроцесорної обчислювальної системи);
- кількість процесорів, які слід створити під час запуску паралельної програми;
- склад використовуваних процесорів, який визначається тим чи іншим конфігураційним файлом;
- виконуваний файл паралельної програми;
- командна стрічка з параметрами для виконуваної програми.

Існує певна кількість інших параметрів, які використовуються при розробці достатньо складних паралельних програм – їх опис подається в довідково-інформаційній літературі з відповідного середовища виконання MPI-програм. Під час запуску програми на декількох комп'ютерах виконуваний файл програми слід скопіювати на ці комп'ютери тому, що він повинен знаходитися на загальному доступному для всіх комп'ютерів ресурсі.

Стандарт MPI-2 був прийнятий в 1997 р. Його використання до цих пір обмежене. Основними причинами цього є певний консерватизм розробників програмного забезпечення, складність реалізації нових стандартів, та ін.

Додатковими можливостями стандарту MPI-2 є:

- динамічне породження процесів, коли процеси паралельної програми можуть створюватися і знищуватися в ході виконання;
- однобічна взаємодія процесів, що дає змогу бути ініціатором операції передачі і прийому даних тільки одному процесу;
- паралельне введення/виведення інформації, яке забезпечує спеціальний інтерфейс для роботи процесів з файловою системою;
- розширення можливостей колективних операцій;
- інтерфейс для алгоритмічних мов типу С.

Тобто можливостей MPI-1 достатньо для реалізації багатьох паралельних алгоритмів, а сфера застосування додаткових можливостей MPI-2 виявляється не настільки широкою.

УДК 004.9

Методи зберігання даних у рекомендаційних системах

Міхав В.В., аспірант, mihaw.wolodymyr@gmail.com
Мелешко Є.В., д.т.н., проф., elismeleshko@gmail.com
Якименко М.С., к.ф.-м.н., доц., m.yakymenko@gmail.com
Бащенко Д.В., аспірант, bashchenko.dv@meta.ua
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна

Рекомендаційні системи у наш час є важливою складовою та контент-орієнтованих веб-сайтів і значним чином впливають на те, як користувачі сприймають інформаційний простір у мережі Інтернет [1]. Вибір методу представлення даних, якими оперує рекомендаційна система, має важливе значення, оскільки ефективний спосіб побудови бази даних для роботи такої системи може зменшити кількість потрібних ресурсів та збільшити кількість доступних алгоритмів для формування списків рекомендацій.

На сьогоднішній день існує багато різних систем управління базами даних, крім реляційних баз даних широке застосування отримують бази даних типу NoSQL [2]. СУБД типу NoSQL можуть бути реалізовані по-різному, зокрема, як Сховища типу «ключ-значення» (Key-value stores), Масштабовані розподілені сховища (Column Family (Bigtable) stores), графові СУБД (Graph Stores), документо-орієнтовані СУБД (Document Stores) тощо [2, 3].

Все частіше для зберігання даних рекомендаційних систем та інших додатків починають використовувати графові моделі [4, 5], також графова форма представлення даних стає поширеною у програмному моделюванні складних систем та мереж [6, 7], і це відбувається через ряд переваг графових моделей [8]. Яскравим прикладом такого підходу являється побудова рекомендаційних систем з застосуванням графової СУБД Neo4j [9]. Графові моделі СУБД надають не лише зручний формат зберігання даних, а й зручний формат запитів. В документації до Neo4j є приклади реалізації алгоритмів створення рекомендацій запитами до цієї СУБД, що ілюструє її придатність для використання в рекомендаційних системах.

Наявність великої кількості різних методів реалізації баз даних та способів представлення інформації, що можна використати при побудові рекомендаційних систем, викликає необхідність порівняльного аналізу та вибору оптимального методу і структури даних для зберігання інформації у таких системах.

У роботі було проведено дослідження різних структур даних, які можна використати для зберігання даних рекомендаційної системи. Зокрема, таких як зв'язний список, розгорнутий зв'язний список, хеш-таблиця, B-дерево, B+-дерево та бінарні діаграми рішень.

Для проведення експериментів з порівняння ефективності застосування різних структур даних за використовуваними часом та пам'ятю було розроблено програмну модель спрощеної рекомендаційної системи, в якій було виділено три основні сутності – агент, сесія та предмет. Найкращі результати показали методи зберігання даних з використанням розгорнутого та інвертованого розгорнутого зв'язних списків. Тому було вирішено також провести додаткову серію експериментів з цими структурами даних для різного розміру блоку списку. Розгорнутий список показав кращі результати за використовуваною пам'яттю в середньому в 1,54 рази та за часом генерації сесій в середньому в 1,68 разів. Інвертований розгорнутий список показав перевагу за часом генерації рекомендацій в середньому в 1,43 разів. Час генерації лайків обидва методи показали приблизно однаковим.

Список літератури

1. Recommender Systems Handbook (2010) Editors F. Ricci, L. Rokach, B. Shapira, P. B. Kantor, New York, NY, Springer-Verlag New York, Inc., USA. 842 p.

2. Meier A., Kaufmann M. (2019) SQL & NoSQL Databases. Springer Vieweg, Wiesbaden. P. 201-218. – URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.468.7089&rep=rep1&type=pdf

3. Cure O., Blin G. (2014) RDF Database Systems: Triples Storage and SPARQL Query Processing. Elsevier Science. 256 p.

4. Yi N., Li C., Feng X., Shi M. (2017) Design and implementation of movie recommender system based on graph database. 14th Web Information Systems and Applications Conference (WISA), IEEE. P. 132-135.

5. Angles R. (2012) A comparison of current graph database models. IEEE 28th International Conference on Data Engineering Workshops, IEEE. P. 171-177.

6. Берновски М.М., Кузюрин Н.Н. (2012) Случайные графы, модели и генераторы безмасштабных графов. Труды ИСП РАН. URL: https://cyberleninka.ru/article/n/sluchaynye-grafy-modeli-i-generatory-bezmasshtabnyh-grafov

7. Райгородский А.М. (2012) Математические модели Интернета. "Квант" №4. С. 12-16. – URL: https://elementy.ru/nauchno-populyarnaya_biblioteka/431792

8. Робинсон Я., Вебер Д., Эифрем Э. (2016) Графовые базы данных: новые возможности для работы со связанными данными. ДМК Пресс, Москва. 256 с.

9. Neo4j Documentation (2021), Official website of the graph database Neo4j. URL: https://neo4j.com/docs/

УДК 004.9

Розробка програмної імітаційної моделі епідемії

Мосольд М.І., магістрант, maximmosold@gmail.com
Мелешко Є.В., д.т.н., проф., elismeleshko@gmail.com
Собінов О.Г., викладач, sagcob14@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна

У цій роботі було створено програмну імітаційну модель епідемії та досліджено бібліотеки і програмні засоби, які можна використати для такого моделювання.

У розробленому програмному забезпеченні генерувався соціальний граф, вершинами якого були люди, а ребрами – можливі шляхи передачі деякого вірусу, а також моделювався процес поширення вірусу у часі після відмічення початкових уражених вузлів графу. У даній моделі вірус може бути як біологічним так і інформаційним.

Для створення графу була обрана бібліотека «NetworkX». Ця бібліотека реалізована на мові Python і призначена для створення, маніпуляції і вивчення структури, динаміки і функціонування складних мережевих структур. Основні можливості бібліотеки: робота з простими, орієнтованими і зваженими графами; висока гнучкість стосовно вибору типу вузлів (від чисел та тексту, до зображення та XML); збереження/завантаження графів в/з найбільш поширених форматів файлів зберігання графів; можна створювати графи базових типів; отримання таких характеристик графа як ступінь вершин, висота графа, діаметр, радіус, довжина шляхів, центр та ін.; візуалізація мережі у вигляді 2D і 3D графіків. І вузли, і ребра мають унікальні ідентифікатори, за якими можна отримати всю інформацію про них. Також вони можуть мати будь-яку кількість атрибутів, які зберігають різні типи даних. Зважені графи мають службовий атрибут з назвою «weight» і ця назва не може бути використано для зберігання іншої інформації для запобігання руйнування внутрішньої логіки його подання.

У розробленій моделі початковий граф може бути створений з використанням одного з трьох методів:

1. Генератор графів;
2. Завантаження даних з файлу або потоку даних;
3. Послідовне додавання вузлів і дуг.

У бібліотеці реалізовано велику кількість типових для роботи над графами алгоритмів. Реалізовані такі алгоритми як знаходження найкоротшого шляху, пошуку в висоту і в ширину, кластеризація, знаходження ізоморфізму графів і багато іншого.

Для графічного відображення результатів було використано мову програмування Python та бібліотеку Matplotlib.

Matplotlib – бібліотека на мові програмування Python для візуалізації даних двовимірною графікою. Пакет підтримує багато видів графіків і діаграм: графіки, стовпчасті діаграми і гістограми, кругові діаграми, контурні графіки, спектральні діаграми, графи. Користувач може вказати осі координат, решітку, додати написи і пояснення, використовувати логарифмічну шкалу або полярні координати.

Також в додатку використовувалися бібліотеки time та random. Бібліотека time потрібна для створення паузи між відображенням станів графу у різні моменти часу моделі, а random – для внесення випадковості в додаток.

Засобами мови Python було створено клас, який створює граф, зберігає в собі всю потрібну інформацію про роботу моделі (у вигляді змінних різних типів даних), та містить методи для обробки графу.

Приклад роботи моделі зображено на рис. 1-2. Граф, його вершини і ребра генеруються випадковим чином. Вершини графу можуть бути таких кольорів (рис. 1-2): зелений – здоровий, червоний – заражений, синій – одержав імунітет.

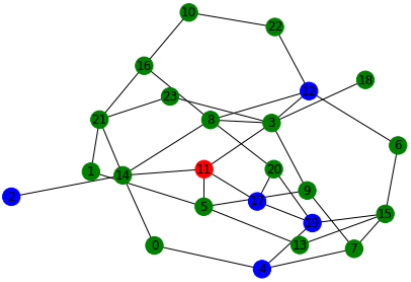


Рис. 1. Початковий стан соціального графу в моделі (один уражений вузол)

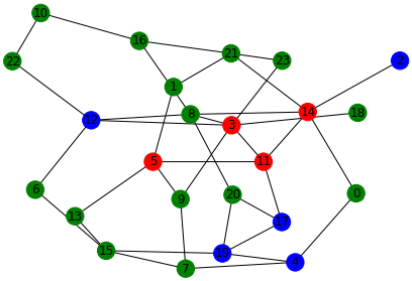


Рис. 2. Граф після першої ітерації часу моделі (чотири уражених вузлів)

Можна вказати початкову кількість червоних і синіх вершин, діапазон, в якому буде випадково обране число загальних вершин.

На кожній ітерації роботи моделі:

– всі зелені вершини, у яких є червоні сусіди, стають червоними;
– якщо вершина була *n* ітерацій була червона – вона стає синьою;
– якщо вершина була *m* ітерацій була синя – вона стає зеленою.

Робота моделі зупиняється після закінчення вказаної кількості ітерацій.

Через те, що бібліотека Matplotlib кожного разу перераховує граф – при відображенні він може приймати іншу форму, але на зв'язки це не впливає.

УДК 004.9

Дослідження можливостей мови Python для створення Telegram-ботів

Подкопаєв Д.М., магістрант, devonoset@gmail.com
Мелешко Є.В., д.т.н., проф., elismeleshko@gmail.com
Якименко Н.М., к.ф.-м.н., доц., yakimenko_n_m@ukr.net
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна

Telegram-боти – спеціальні акаунти в Telegram, створені для автоматичної обробки та надсилання повідомлень; користувачі можуть взаємодіяти з ботами за допомогою повідомлень, що надсилаються через звичайні або групові чати; логіка робота контролюється за допомогою HTTPS-запитів до Telegram API для ботів [1]. Telegram-боти відіграють роль інтерфейсу до сервісу розробника бота, який працює на віддаленому сервері. Найцікавіше в ботах це те, що для їх створення не потрібно вивчати низькорівневі методи роботи з MTProto та шифруванням – спілкування з ботом організовано за допомогою звичайного інтерфейсу HTTPS зі спрощеними методами Telegram API, що також звуться Bot API.

Python – мультипарадигмальна мова програмування, орієнтована на підвищення продуктивності розробника, а також читаності коду та його якості [2]. Дає можливість написати проект будь-якої направленості, маючи при цьому низький поріг входження. За рахунок простоти коду майбутній супровід програм стає легшим порівняно з Java або C подібних мов. Значною перевагою у використанні мови Python є наявність великого числа бібліотек, якими можна скористатися, що в свою чергу дозволяє скоротити час розробки та легко створити багато функцій у Telegram-боті.

Із корисних бібліотек Python для розробки Telegram-ботів можна виділити TeleBot [3] та Requests [4], які і були досліджені у даній роботі.

Та при всіх перевагах Python, у нього є й недоліки, це, зокрема, порівняно невисока швидкість виконання програми, але це не критичний недолік для розробки Telegram-ботів.

Метою даної роботи було дослідження можливостей мови програмування Python та її бібліотек для створення інформаційних Telegram-ботів. Було досліджено основні можливості бібліотек Python для розробки ботів – TeleBot та Requests.

Бібліотека TeleBot – це оболонка над запитами до TelegramBotAPI, що використовується для спрощення і мінімізації написаного коду.

В класі TeleBot розташовані всі методи API. Щоб слідувати загальним угодам про імена Python, вони перейменовані. Наприклад, sendMessage в send_message, editMessageText в edit_message_text. Функція, прикрашена декоратором примірника TeleBot – обробник повідомлень. Обробники повідомлень складаються з одного або декількох фільтрів. Кожен фільтр

повертає True або False для певного повідомлення і обробник отримує дозвіл на обробку повідомлення, якщо повертається True.

Типи, які можливо опрацювати через TeleBot. Усі типи визначаються у types.py. Всі вони повністю відповідають визначенню типів API Telegram, за винятком поля повідомлення from, яке перейменовано на from_user(оскільки from – це зарезервований маркер Python). Таким чином, такі атрибути, до message_id, яких можна отримати безпосередній доступ message.message_id. Слід звернути увагу, що це message.chat може бути як екземпляр, так Useri GroupChat.

Бібліотека Requests – це модуль, що виконує HTTP-запити, починаючи від передачі параметрів в URL-адресах до відправки користувацьких заголовків і перевірки SSL. Використання цієї бібліотеки дозволить Telegram-боту отримати доступ до інформації на різних веб-ресурсах. Клієнт, який використовує бібліотеку Requests, відправляє дані на URL, а сервер із цим URL зчитує дані, вирішує, що з ними робити, і надсилає клієнту відповідь. Після цього клієнт може вирішити, що робити з отриманими у відповіді даними.

У ботів Telegram є багато унікальних можливостей, які надають Bot API, зокрема, кастомізовані клавіатури, додаткові інтерфейси для команд за замовчуванням, зовнішнє зв'язування і спеціальні режими приватності для груп.

Telegram Bot API представляє собою HTTP-інтерфейс для роботи з ботами в Telegram. Документація Telegram Bot API виділяє два максимально протилежних способи отримання оновлень: 1) періодичні запити; 2) установка веб-хуків. Вхідні оновлення зберігаються до того моменту, поки сервер не обробить його, але не більш ніж 24 години. У відповідь отримуємо об'єкт Update, який серіалізовано в JSON, незалежно від способу отримання оновлень.

Telegram-бота можна створити засобами мови програмування Python і її бібліотек TeleBot та Requests, а також з використанням Telegram Bot API.

Список літератури

1. Телеграм Документация (2022) "Боты: информация для разработчиков", URL: https://tlgrm.ru/docs/bots
2. Mark Lutz (2007) "A Python Q&A Session Learning Python, 3rd Edition", O'Reilly Media, Inc. URL: https://www.oreilly.com/library/view/learning-python-3rd/9780596513986/ch01.html
3. TeleBot Documentation (2022) "The easy way to write Telegram bots", URL: https://openbase.com/js/telebot/documentation
4. Requests Documentation (2022) "Requests: HTTP for Humans™", URL: https://docs.python-requests.org/en/latest/

УДК 004.056.53

Дослідження сучасних методів захисту систем управління базами даних від інформаційних атак

Рисований М.О., студент, maxcimofficial@gmail.com
Науковий керівник – Мелешко Є.В., д.т.н., проф., elismeleshko@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна

Вступ

Дані – це найцінніший корпоративний актив для будь-якого бізнесу. Незалежно від того, в якій галузі працює підприємство, важливо дбати про фінансові звіти та медичні записи або бізнес-план для стартапу. База даних (БД) – це структурована сукупність інформації, яку можна зберігати, аналізувати та обробляти за допомогою СУБД (системи управління базами даних). Бази даних необхідно захищати та регулярно перевіряти актуальність їх захисту. Використовуючи спеціальні програми та методики, можна запобігти несанкціонованому доступу (НСД) до бази даних у локальних мережах або витоку інформації, не призначеної для широкого розголосу.

Основні загрози безпеки

Є декілька причин, за якими приватні компанії та державні установи мають витрачати великі кошти задля захисту своїх БД.

Одна з них – кіберзлочинність. Постійне вдосконалення інструменту зловмисників, поява нових програм здирників, способи проникнення та постійно існуюча можливість того, що хтось із співробітників вдасться до дій, що несуть загрозу конфіденційній інформації.

Друга причина – відповідальність за конфіденційність даних. Міжнародне законодавство, що стосується захисту персональної інформації, постійно вдосконалюється і стає більш жорстким. Відповідальність за недоторканність конфіденційних відомостей покладається на організації, які їх збирають у процесі своєї діяльності. Причому залежно від галузі та типу інформаційних активів, нормативні вимоги можуть суттєво відрізнятися. Сучасні компанії повинні відповідати відповідним стандартам.

Основні вимоги до безпеки БД

До основних вимог безпеки БД можна віднести наступні:

1. Забезпечення фізичної безпеки файлів даних.

2. Безпека програмного забезпечення користувача, забезпечення йому безпечних механізмів доступу до даних.

3. Безпечна організація роботи з даними, контроль цілісності, доступності та конфіденційності даних.

Розглянемо основні методи забезпечення циз вимог до баз даних.

Розділення сервера БД та веб-сервера

У традиційному розумінні це означає збереження сервера БД у захищеному, заблокованому середовищі з контролем доступу для запобігання доступу неавторизованих людей. Але це також означає збереження бази даних на окремій фізичній машині, видаленій з машин, на яких запущені програми або веб-сервери. Веб-сервер, швидше за все, піддасться атаці, оскільки він розташований у DMZ і, отже, загальнодоступний. І якщо веб-сервер зламано, а сервер бази даних працює на тій же машині, зловмисник матиме доступ як користувач root до вашої бази даних і даних.

Безпечний доступ користувачів до БД

Необхідно прагнути того, щоб якомога менше людей мали доступ до БД. Адміністратори повинні мати лише мінімальні привілеї, необхідні для виконання своєї роботи, і лише в періоди, коли їм потрібен доступ.

Стандартні процедури безпеки облікових записів повинні бути такі:

- Необхідно застосовувати надійні паролі;
- В БД слід зберігати не паролі, а їх хеш-значення;
- Хеш-значення паролів слід зберігати в зашифрованому вигляді;
- Облікові записи повинні бути заблоковані після трьох або чотирьох спроб входу до системи.

Використання брандмауера веб-додатків

Сервер баз даних має бути захищений від кіберзагроз брандмауером, який за замовчуванням забороняє доступ до трафіку. Єдиний доступний трафік має надходити від певних програм або веб-серверів, яким потрібен доступ до даних. Брандмауер також повинен захищати базу даних від ініціювання вихідних з'єднань, якщо в цьому немає особливої потреби.

Висновки. Забезпечення кібербезпеки баз даних є складним завданням, яке повинне використовувати всі аспекти технологій і практик забезпечення інформаційної безпеки. Вирішння цієї задачі також, природно, зменшує зручність використання баз даних. Чим доступніша та зручніша база даних, тим вона вразливіша до загроз безпеці; чим більш невразлива база даних для загроз, тим складніше її зламати та вкрасти дані.

Список літератури

1. Скакун В.В. Защита информации в базах данных и экспертных системах: пособие для студентов фак. радиофизики и комп. технологий / В.В. Скакун. – Минск: БГУ, 2015. – 140 с.

2. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. — М.: ИД «ФОРУМ»: ИНФРА-М, 2011. – 416 с.

УДК 004.056

Стійка функція шифрування удосконаленого модуля криптографічного захисту інформації

Смірнова Т.В., к.т.н., sm.tetyana@gmail.com
Буравченко К.О., к.т.н., buravchenkok@gmail.com
Смірнов О.А., д.т.н., проф., dr.SmirnovOA@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна

На сучасному етапі розвитку хмарних технологій, існує завдання захисту даних, які зберігаються у відповідних інформаційно-комунікаційних системах. Останні події, пов'язані з атаками на різні хмарні сервіси потребують розроблення нових або удосконалення існуючих механізмів захисту інформації. Одними з таких механізмів є програмні модулі криптографічного захисту даних, у яких необхідно реалізовувати вибір стійких методів шифрування та гешування, а також синхронізацію секретного ключа. У якості зазначених процедур можуть використовуватись відомі криптографічні методи і засоби, стійкі до лінійного, диференціального, алгебраїчного, квантового та інших відомих видів криптоаналізу.

Сьогодні серед множини методів захисту інформації особливе місце займають криптографічні методи. У теперішній час в месенджерах і інших застосунках використовуються наступні відомі програмні модулі криптографічного захисту даних: MTProto 1.0 – модуль, який використовується для шифрування повідомлень при передаванні клієнтами Telegram; Signal Protocol – використовується для шифрування миттєвих повідомлень Facebook Messenger; TLS Skype – для миттєвих повідомлень використовується TLS (безпека на рівні транспорту) для шифрування повідомлень між клієнтом Skype та службою чату, коли вони надсилаються безпосередньо між двома клієнтами Skype. Проведений порівняльний аналіз розглянутих модулів захисту інформації у сучасних інформаційно-комунікаційних системах та мережах (ІКСМ). за такими критеріями, як використовувані криптоалгоритми, швидкість роботи (ШР), зручність для користувачів (ЗК) і кросплатформеність (КП), показав, що розглянуті програмні модулі мають низку недоліків і можуть бути удосконалені за рахунок використання сучасних процедур безпеки. Зважаючи на зазначене, важливим завданням є удосконалення модуля криптографічного захисту інформації для забезпечення конфіденційності та цілісності даних у сучасних ІКСМ. На теперішній час розробляється удосконалений модуль криптографічного захисту інформації, який за рахунок фіксування інформації про ідентифікатор користувача, ідентифікатор сесії, час відправлення, довжину повідомлення та його

порядковий номер, а також використання нової процедури формування сеансового ключа для шифрування, дозволить забезпечити конфіденційність і цілісність даних в ІКСМ. Опис удосконаленого модуля криптографічного захисту інформації буде наведений у наступних роботах. Для ефективного використання цього модуля важливим є вибір криптостійких методів шифрування F_{enc} та гешування F_{hash}, а також синхронізація секретного ключа *authKey*. У якості функцій F_{enc} та F_{hash} можуть бути використані зокрема й алгоритми, стійкі до лінійного, диференціального, алгебраїчного, квантового та інших відомих видів криптоаналізу. Областю застосування запропонованих підходів є хмарні системи.

Управління ключовими даними

Алгоритми шифрування зазвичай не є секретними і публікуються відкрито або майже відкрито (у деяких випадках). Основне навантаження щодо захисту інформації методами шифрування несуть ключі. Адміністрування ключів покликане додати їм необхідні властивості і забезпечити нормальне функціонування на всіх стадіях життя (використання) ключів. Стадіями життя ключів є: генерація або формування; розподіл; верифікація і автентифікація; зберігання; використання; модифікація; ліквідація або утилізація.

Криптостійкість деяких алгоритмів шифрування (або майже всіх) сильно залежить від того наскільки непередбачувані числа, що видає ГПВЧ, який використовує той або інший алгоритм шифрування. У зв'язку цим виникає поняття криптостійкості ГПВЧ, чим більше непередбачуваний ГСВЧ, тим вище його криптостійкість. Тому для розробленої системи був запропонований новий метод генерації криптографічних ключів.

Для удосконалення прототипу, яким є алгоритм шифрування RC6, пропонується наступна методика:

1. *Ускладнити процедуру обрахунку U і T.*

У даних процедурах пропонується ввести блок підстановок (вибраний із множини, так званих , гранично-нелінійних бієктивних перетворень; побудований на основі конструкції Ніберг-Дінга), операцію додавання за модулем 2^{32} і множення за *модулем* 2^{32}, що забезпечить захист від алгебраїчних атак, лінійного та диференціального криптоаналізу, інтерполяційної атаки. Також пропонується ввести операції динамічного-циклічного зсуву (залежить від розширених ключів)– це дозволить динамічно керувати процесом розсіювання інформаційних даних.

2. *Збільшити кількість підключів.*

Для забезпечення динамічного керування процесом розсіювання інформаційних даних, також це ускладнить диференціальний та лінійний криптоаналіз.

3. Замінити часткове вхідне та вихідне відбілювання – повним.

Це ускладнить проведення лінійного та диференціального криптоаналізу.

4. *Змінення раундової функції.*

Після кожних двох раундів добавлена операція *RoundColumns*, що призведе до ще більшого лавинного ефекту запропонованого алгоритму.

5. Зменшена кількість раундів

Це дозволяє підвищити швидкість шифрування даних без втрати криптостійкості.

Представлення вхідних та вихідних даних алгоритму шифрування

До вхідних даних алгоритму належать: відкритий текст; ключ шифрування (секретний ключ у відповідності з яким виконується розширення підключів).

На виході отримуємо шифротекст. Вхідні, вихідні блоки даних алгоритму представляються у вигляді чотирьох 32-бітних підбоків *A, B, C* і *D*.

Параметри алгоритму

Розмір блоку та довжина ключа шифрування. Запропонований метод шифрування підтримує довжину блоку даних у 128 бітів з підтримкою ключа шифрування довжиною 128.

Алгоритм шифрування – це складна процедура, що складається з попередньої та фінальної рандомізації, між якими відбуваються ітеративні (циклові) перетворення шифрування (зашифрування та розшифрування). Мінімальне допустиме число раундів шифрування (r), а отже і кількість циклів ($n = r/2$) залежить від довжини ключа шифрування. При довжині ключа 128 бітів ($r = 12$), відповідно кількість циклів ($n = 6$).

Процедура зашифрування

На вхід процедури подаються підключі K_i і відкритий текст, який розбивається на підблоки *A, B, C, D*. Спочатку виконується повне початкове відбілювання (рандомізація) підблоків *A, B, C* і *D*. Потім виконуються r раундових перетворень. Далі виконується повне кінцеве відбілювання підблоків *A, B, C* і *D*. Отримані у результаті зашифрування підблоки об'єднують у шифротекст.

Початкове та кінцеве відбілювання

Перед початком шифрування даних всі підблоки відбілюють за допомогою відповідних підключів: $A = (A \oplus K_0)$, $B = (B + K_1)$, $C = (C \oplus K_2)$, $D = (D + K_1)$. Для підблоків *A* і *C* ця операція виконується додаванням за модулем 2 кожного байту вказаного підблоку з кожним байтом вказаного підключа, а для *B* і *D* – додаванням за модулем 2^{32}. Така ж операція виконуються наприкінці шифрування, але для *A* і *C* вже використовується додаванням за модулем 2^{32}, а для *B* і *D* – додаванням за модулем 2: $A = (A + K_{6r+4})$, $B = (B \oplus K_{6r+5})$, $C = (C + K_{6r+6})$,

$D = (C \oplus K_{6r+7})$.

Раундові перетворення

Для кожного раунду *i* ($i = \overline{1,..,r}$) виконується наступне:

1) Послідовності *B* і *D* подаються на вхід функцій *Ft*() і *Fu*() відповідно. В результаті отримують допоміжні 32-ох бітні послідовності *T* і *U*.

2) Додають кожний байт блоків *A* і *C* з кожними байтом послідовностей *T* і *U* використовуючи додавання за модулем 2^{32} та за модулем 2 відповідно: $A = (A + T) \bmod 2^{32}$, $C = (C + U) \bmod 2$.

3) Виконують циклічний по бітний зсув елементів блоків *A* і *C* в залежності від елементів блоків *U* і *T*: $A = (A <<< U)$, $C = (C <<< T)$.

Приклад при зсуві *x* на *y* (для оптимізації беремо *y* mod32): $Z = (X <<< Y) \bmod 32$.

4) Додають кожний байт блоків *A* і *C* з кожними байтом підключів K_{6i+4} і K_{6i+6}, ($0 \le i \le (r\text{-}1)$ використовуючи додавання за модулем 2 та за модулем 2^{32} відповідно: $A = (A + K_{6i+4}) \bmod 2$, $C = (C + K_{6i+6}) \bmod 2^{32}$.

5) У кінці раунду підблоки зсуваються вліво: $(A, B, C, D) = (B, C, D, A)$.

Процедура розшифрування

При розшифруванні підключі використовуються в зворотному порядку, накладання підключів замість додавання по модулю 2^n виконується відніманням, зрушення субблоків виконується на початку раунду і у зворотний бік, а також замість процедури *RoundColumns* використовується зворотня до неї – *InvRoundColumns*. Перетворення *f()* не зазнало змін.

Висновки. У роботі проведено аналіз вимог до побудови систем забезпечення конфіденційності даних на базі криптоалгоритмів, визначено ключові аспекти і шляхи удосконалення існуючих методів і систем шифрування даних. Розроблено метод генерації криптографічних ключів, щоб покращити швидкість генерації ключів, з його використанням удосконалено функцію шифрування (для забезпечення удосконаленого модуля) на основі відомого і ефективного алгоритму RC6, що дозволило підвищити швидкість криптографічної обробки даних та перевірити криптостійкість алгоритму проти спеціалізованих атак лінійного та диференціального криптоаналізу.

УДК 004.9

Метод колаборативної фільтрації на основі аналізу тональності текстів коментарів

Шингалов Д.В., аспірант, dimashingalov@gmail.com
Босько В.В., к.т.н., доцент, victorvv2@ukr.net
Резніченко В.А., викладач, upsbilly2017@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна

Для створення рекомендаційної системи на основі колаборативної фільтрації необхідною умовою є наявність інформації про оцінки (або лайки/дизлайки, або покупки), яка дає змогу зрозуміти попередні вподобання користувача та на основі цього знання створити для нього рекомендації. Не на всіх веб-ресурсах ця інформація є у достатній кількості, тому доцільно доповнювати її, аналізуючи наявні дані, зокрема, тексти коментарів. Визначивши тональність коментаря, можна співставити її з оцінкою, наприклад, негативний коментар – низька оцінка, позитивний коментар – висока оцінка. Для коректного співставлення необхідно використати нечітку логіку.

У роботі досліджено можливість побудови рекоменлаційної системи на основі колаборативної фільтрації з використанням аналізу текстів коментарів.

Сучасна теорія аналізу та керування великими даними (Big Data) виокремлює два основних методи автоматичного аналізу настроїв – це метод на основі використання лексем і метод машинного навчання. При машинному навчанні застосовуються класифікатори на базі юніграмм або їх комбінацій (N-грам) в якості ознак. Методи машинного навчання для аналізу текстів – це сукупність методів, заснованих на алгоритмах штучного інтелекту, які використовують для навчання дані, в даному випадку, коментарі раніше помічені як позитивні, негативні або нейтральні.

Найпопулярніші алгоритми навчання для класифікації тексту – це метод опорних векторів, наївний баєсів класифікатор, дерева прийняття рішень, метод максимальної ентропії та нейронні мережі.

У лексемному ж методі в основі лежать юніграмми, які знаходяться в словнику і мають відповідні бали полярності. Словники можуть бути створені з використанням різних методів:

- Вручну побудовані словники (простий, але не дуже швидкий метод). Наприклад General Inquire, який складається зі слів суспільствознавчих категорій для контент-аналізу. Ці категорії аналізу контенту намагаються охопити тон, ставлення, зовнішній вигляд.
- Словники з підготовлених даних бувають напівавтоматичними

(наприклад, використовують такі ресурси, як WordNet або UNL), або автоматичними, коли словник може бути отриманий автоматично через асоціацію, де оцінка для кожного нового прикметника розраховується з використанням частоти близькості від прикметника до одного або більшої кількості затравочних слів.

VADER (Valence Aware Dictionary Sense Reasoner) – це словник, який спеціально налаштований задля оцінки настроїв повідомлень в соціальних мережах. Застосування даного словника дозволяє розпізнати:

– типові заперечення виду «не добре» і «було не дуже добре»;

– використання знаків пунктуації для посилення настрою (наприклад, «Добре!!!»);

– використання всіх прописних букв в написанні тексту для акцентування уваги;

– використання ступенів порівняння (наприклад, «дуже»);

– розуміння сленгових слів;

– розуміння смайликів, схожих на емоції, записаних текстовими символами;

– дозволяє аналізувати складні речення та довгі тексти на інших мовах (відмінних від англійської).

Лексика почуттів VADER чутлива як до полярності, так і до інтенсивності почуттів, що дуже виражені в контексті соціальних мереж. Оцінка висловлювання відбувається шляхом сумування валентних оцінок кожного слова в лексиконі, який скоректовано у відповідності з правилами, а потім нормалізовано, щоб результати були в діапазонах від -1 (самого краю негатива) і до +1 (самого крайнього позитива). Це сама зручна метрика, у випадку, якщо потрібна єдина одномірна міра почуттів для подальшої побудови рекомендацій. Це також корисно для дослідників, котрі хотіли би встановити стандартизовані порогові значення для класифікації речень як позитивні, нейтральні, так і негативні.

Для аналізу текстів коментарів користувачів соціальних мереж було вирішено застосовувати словник Vader, який побудовано з використанням даних Amazon Turk.

Розроблений метод складається з наступних етапів:

Етап 1. Аналіз тональності коментарів лексемним методолом, який здійснюється з використанням словника VADER. На початку програма відкидає усі незначущі слова, та сполучні слова, відбувається перетворення емодзі у текстові значення. Крім того відбувається перевірка модифікаторів та заперечень, обчислення акцентів на пунктуаційних знаках у тексті. Після цього відбувається присвоєння поляризованих балів з огляду на те, які слова мають позитивне чи негативне значення, відбувається оцінка кортежів за силою настрою. Також програма обчислює кількість слів, що мають нейтральний відтінок та не несуть емоційного забарвлення у тексті та обраховує кількість слів,

що повторюються. На прикінцевій стадії обчислюється нормалізована сума балів, яка надає можливість визначити полярність тексту.

Етап 2. Переведення тональності коментарів в оцінки методами нечіткої логіки. На цьому етапі на основі отриманих попередньо балів полярності, відбувається обчислення середніх балів (зірочок) для подальшого надання рекомендацій користувачеві. Використовується база правил за якими, враховуються параметри полярності, її розмір та відносність. Для кожного параметра задані максимальний та мінімальний поріг приналежності. В кінцевому результаті кожному тексту можна присвоїти деяку кількість балів 1-5, де 5-це дуже добре, а 1- дуже погано. Визначена на основі коментаря оцінка для об'єкту контенту додається у матрицю оцінок для колаборативної фільтрації.

Етап 3. Здійснюється колаборативна фільтрація та користувачу надається список рекомендацій. Безпосередньо користувач може дізнатися наскільки цікавий об'єкт контенту (або товар) на веб-сайті для нього, на основі прогнозованих оцінок та визначитися стосовно його перегляду (придбання).

У подальшому користувач може отримувати рекомендації стосовно найбільш цікавих об'єктів контенту не тільки на основі його оцінок та оцінок інших користувачів цим об'єтам, а також на основі написаних коментарів.

Було проведено експерименти для перевірки ефективності розробленого методу. Для оцінки якості його роботи використано наступні метрики – Precision, Recall та F-міру.

Міра точності Precision характеризує, скільки отриманих від класифікатора позитивних відповідей є правильними. Чим більше Precision, тим менше число помилкових влучень. Однак, міра точності не дає уявлення про те, чи всі правильні відповіді повернув класифікатор. Для цього існує так звана міра повноти Recall

Precision і Recall дають досить вичерпну характеристику класифікатора, причому «з різних кутів». Але найбільш зручно для характеристики класифікатора використовувати одну величину, так звану метрику F1, що є гармонійним поєднанням попередніх двох.

У ході експерименту було проаналізовано сто коментарів, половина з яких представляла собою позитивні відгуки людей відносно різних фільмів, а інша половина – негативні відгуки, кожен з яких було попередньо проаналізовано вручну. Тобто до експерименту кожен з коментарів був оцінений двома людьми незалежно один від одного, які переконалися в позитивному чи негативному настрої тексту, що і є попереднім маркуванням.

Тестування розробленого методу показало наступні результати: precision = 0,96, recall = 0,8727, F1-measure = 0,914. А отже точність запропонованого методу досить висока для розглянутого набору даних.

UDC 004.94

Divorce prediction using ARIMA model

Hajirahimova M.[1], Ph.D. in tech. sciences, ass. prof., hmakrufa@gmail.com
Aliyeva A.[2], senior researcher, aliyeva.a.s@mail.ru
[1,2]Institute of Information Technology of ANAS, Baku, Azerbaijan Republic

In recent years, the number of divorce cases are increasing very rapidly all over the world. From last few decades, the number of divorces has gone up from 0.7 in 1000 to 1.7 in 1000 in Azerbaijan [1]. Today, the increasing rate of divorce cases is a concerning issue.That is why the issue of divorce forecast has been considered. In this work, have been applied the ARIMA(Auto-Regressive Integrated Moving Average) time series forecasting model and predicted the number of divorced cases for the next decade in Azerbaijan (from 2022 to 2031). ARIMA is a prediction algorithm based on the idea that information about the past values of a time series can be used alone to predict future values. ARIMA model is specified by three parameters: (p, d, q). Where, p is the order of the Auto Regressive (AR) term. It refers to the number of lags of Y to be used as predictors.q is the order of the Moving Average (MA) term. It refers to the number of lagged forecast errors that should go into the ARIMA model. The value of d is the minimum number of differencing needed to make the series stationary. If the time series is already stationary, then d = 0 [2] .

Statistics 1935 to 2021 from the State Statistical Committee of the Republic of Azerbaijan source [1] are used for the study.The divorce dataset is divided into training (85%) and testing (15%). This data was plotted on a graph to see the trend, as shown in figure 1.

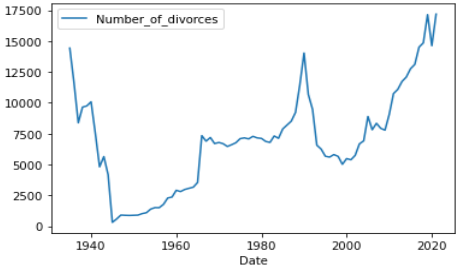


Figure 1 – Time series plot of divorce (1935-2021)

The ARIMA model consists of four steps. The first step is the identification of the model. This includes identifying the most suitable lags for the components of the AR and MA, and deciding whether the variable needs first differentiation to induce stationary. The model identification is made by the

Auto Correlation (ACF) and the Partial Auto Correlation (PACF) (figure 2 a) and b)). Model parameters were estimated using Python.

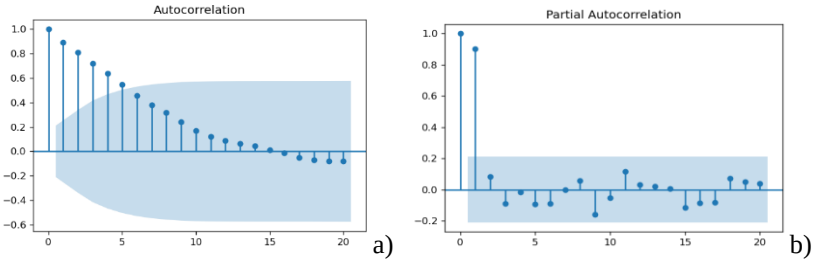


Figure 2 – a) PACF function, b) ACF function

In Python, it is possible to automate the ARIMA prediction process by using the auto_arima () function. The auto_arima() function uses a stepwise approach to search multiple combinations of p,d,q parameters and chooses the best model that has the least AIC [3].

Table 1 –Evaluation based on AIC

Model	AIC criterion
ARIMA(2, 2, 1)	1239.194
ARIMA(2, 2, 2)	1241.149
ARIMA(3, 2, 1)	1240.749
ARIMA(3, 2, 2)	1243.045
ARIMA(4, 2, 1)	1242.684

The smaller the AIC criterion, the better the model. Therefore, a final fitted model chosen for divorce data is ARIMA(2,2,1) which give the lowest AIC (1239.194) among all models from the table above (table 1). This model can be considered as the best fit model and can be further used to generate the forecasts. Based on the ACF and PACF, the daily prediction of divorce cases is calculated, as shown in figure 3.

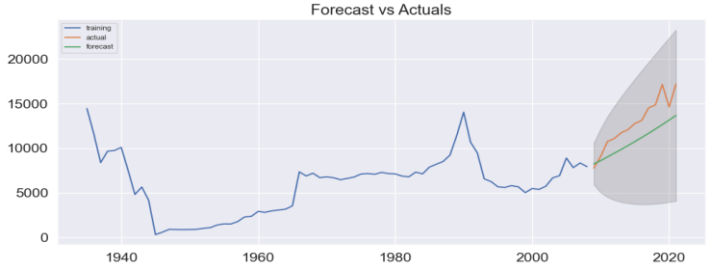


Figure 3 – Actual and forecasted cases

Figure 4 shows the forecasting results of divorces in Azerbaijan over the next decade using the ARIMA model.

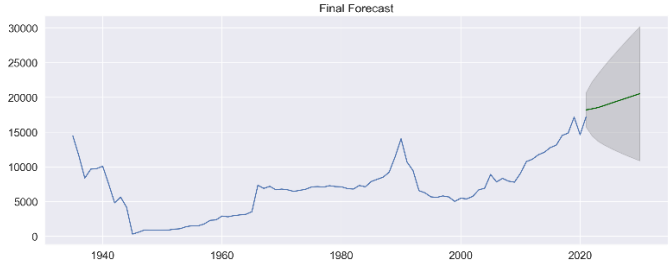


Figure 4 – Prediction the number of divorces for the next decade

Table 2 shows the forecasting of divorce for the next decade in Azerbaijan (from 2022 to 2031). The model has revealed an increasing pattern in the number of divorce cases.

Table 2 – Forecasting the number of divorces

Predicted date	Forecated value of divorces(fc_series)	Minimum prediction (lower_series)	Maximum prediction (upper_series)
2022	18195	15708	20682
2023	18350	14449	22250
2024	18530	13674	23386
2025	18810	13158	24461
2026	19105	12716	25493
2027	19391	12303	26480
2028	19675	11916	27434
2029	19958	11552	28365
2030	20242	11205	29279
2031	20526	10871	30181

Conclusions. In this research, we used ARIMA model to predicting the number of divorced cases in Azerbaijan for the next decade. The MAPE error of forecast prediction is 0.15 for this model which is very low means we have acquired high accuracy from this model. For future studies, the machine learning algorithms will be tested for forecasting the divorced cases.

References

1. State Statistical Committee of the Republic of Azerbaijan: Demographic indicators of Azerbaijan, Statistical yearbook , Baku, 2021, stat.gov.az

2. ARIMA Model for Time Series Forecasting, https://www.kaggle.com/code/ /arima-model-for-time-series-forecasting

3. Time Series Analysis using ARIMA Model, https://www.analyticsvidhya.com/

UDC 378.147

Introduction of electronic resources in the learning process

Axmedova Zulxumor, master, srustam1979@gmail.com
Bukhara Engineering and Technology Institute, Uzbekistan

An important role in the development of modern education in the world is played by the process of its informatization, which involves improving the quality and accessibility of the educational process through the creation of a unified information environment that performs educational functions.

Problems of informatization of education are the most important problem

XXI century due to the following main reasons [1]:

– the rapid development of the process of informatization of society, which entails many global changes and significantly affects almost all aspects of people's lives;

– Functionality and technical characteristics of informatics tools, information and telecommunication technologies have been growing exceptionally rapidly in recent years, while their cost has been steadily declining, which makes these tools accessible to the mass user;

– further rapid development of information and communication technologies and the widespread introduction of its achievements into social practice led to the formation of a completely new information environment of society, which modern philosophers call the infosphere. It is the infosphere that will determine the main features of the information society, that new civilization that is already being formed today in developed countries and will, with historical inevitability, spread from them all over the world.

The tool for informatization of education is the means of informatization, including electronic educational resources (hereinafter referred to as EER). EERs are a fundamental component of the information and educational environment and are focused on the implementation of the educational process with the help of information and communication technologies and on the use of new methods and forms of education, such as e-learning, mobile learning, network training, offline learning, blended learning, cooperative learning.

An electronic educational resource may include educational content, software components, and metadata.

Educational content - structured subject content used in the educational process, informationally significant content of the EER.

Software components provide the presentation of content elements to the user in certain combinations, and also provide an interactive model of working with content.

EER metadata is structured data intended to describe the characteristics of an EER, a data object or a component of an educational technological system.

In general, they are information that characterizes or explains other information.

Metadata solves the following tasks [2]:

– accelerate the search for the necessary resources;

– give users an idea about the content of the resource, its educational and innovative qualities.

The following electronic resources can be used in higher education institutions:

– resources of the country's educational portals provided for non-commercial use in the education system;

– resources of commercial educational portals and electronic educational publications on magnetic media purchased by educational institutions to replenish electronic libraries at their own expense;

– educational resources of regional portals;

– resources developed by educators.

The functionality of using ESM is largely determined by their didactic properties. Currently, EORs are able to provide:

– support for all stages of the educational process - practical exercises, obtaining information, certification and monitoring of students' achievements;

– increasing the possibility of independent work of students;

– changing the roles of the teacher (providing and coordinating the educational process) and students (active participation in the educational process);

– ability to manage the course of events and responsibility for the result;

– the use of fundamentally new methods and forms of education, including self-study.

Various literary sources covering the topic of using electronic educational resources are similar in their conclusions about the benefits of introducing EER into the system of organizing the educational process. These include:

– activation of the development and implementation of new organizational forms and teaching methods that motivate the active creative work of both students and university teachers to the maximum;

– ensuring the procedure for continuous quality control of knowledge and acquired competencies;

– the possibility of predicting student performance;

– ensuring the flexibility of the educational process in accordance with the program goals and taking into account the results obtained at each stage;

– ensuring the possibility of rational distribution by students of their time, physical and mental resources, and hence favorable conditions for the active acquisition of knowledge by them;

– motivation of students to study by introducing the principle of competitiveness in the learning process;

– identification of strong and lagging students at an early stage in order to implement an individual approach.

Among the listed positive qualities of the use of EER, increasing the motivation of students for independent work is the advantage that is mentioned in one way or another in all the literature sources studied during the study.

The problem of low motivation among students at the moment is really relevant, as students often ignore homework and control tasks, or do them by copying other people's work, not thinking about the low quality of performance, and most importantly, the lack of acquiring the necessary competencies.

Of course, in addition to the described advantages, one can also highlight the disadvantages of ESM, such as:

– the need to use special equipment and programs, as well as to connect to the Internet/Intranet to access the electronic information and educational environment. Both can have interruptions in work, turn off or break down, which makes the ESM not the most reliable learning tool;

– the development of the speech, graphic and written culture of students is not ensured, since the dialogue with the teacher is conducted mostly through the LMS in electronic form;

– the need to improve the skills of scientific and pedagogical workers in the use of EER in the educational process and in their development, since the creation of high-quality electronic educational content is a complex, creative work that requires authors to spend a lot of time, a variety of knowledge, and skills in using various teaching methods using the system learning management, knowledge of the potential of the system for which materials are being developed, as well as new information processing technologies;

– the problem of copyright: when acquiring or creating any EER, it is necessary to understand on what legal basis the use of a particular resource is made and to monitor the fulfillment of the conditions laid down in the license for a particular product.

Conclusions. From the foregoing, we can conclude that electronic educational resources have great practical value: providing students with information in a variety of ways and at any time convenient for them, they provide more opportunities for independent work, and planning all types of work and setting deadlines for the implementation of activities increases motivation for learning and contributes to the activation of cognitive activity. Thus, a well-created electronic resource is able to improve the quality of education, thereby increasing the level of training and competitiveness of graduates.

References:

1. Prokudin D.E. Informatization of domestic education: results and prospects. Internet project "Philosophical Anthropology". [Text]: 2006

2. Bobomuradovich S.R., Integration of education, science and production as a basis of an innovative educational process, European Journal of Research and Reflection in Educational Sciences, 2020 8/12.

UDC 378.147

Software for creating and placing electronic educational resources

Saidova Nargiza, master, srustam1979@gmail.com
Bukhara Engineering and Technology Institute, Uzbekistan

For the creation and placement of electronic educational resources, the control of the educational process, as well as the accounting and analysis of learning outcomes, distance learning information systems are used.

A distance learning system (hereinafter referred to as LMS) is software for organizing distance learning, an additional support system for the educational process, electronic document management, for creating electronic learning materials, administering and evaluating progress within the discipline under study, and conducting consultations [1].

LMS is able to solve the following tasks:

– ensure the management of e-learning, face-to-face and blended learning;
– implement the preparation of training courses and training programs;
– ensure the development and testing of knowledge, various practical tasks;
– evaluate and analyze learning outcomes;
– provide management of the library of educational materials.

Currently, due to increasing demand, the market for distance learning systems is actively expanding and replenished with new products. Consider the following most relevant LMS of foreign production: Hypermethod, Media Transformer, Blackboard, Moodle.

A popular example of a foreign distance learning system is Moodle (Modular Object-Oriented Dynamic Learning Environment). This software product is used in more than 100 countries by universities, schools, companies and independent teachers.

The system is free, but its capabilities are not inferior to well-known commercial analogues. It is distributed in open source codes, which makes it possible to remake it for the specifics of each educational project, supplement it with new services. Thanks to the developed modular architecture, Moodle's capabilities can be easily expanded [2].

Moodle contains a rich set of resources such as text, a web page, an audio or video file, and course elements that include a glossary, lecture, quiz, assignment, forum, wiki, and more.

All downloadable educational material in the system can be divided into didactic units, at the end of each of them give control questions, based on the results of the answers to which the system will transfer students to the next level of studying the material, or return to the previous one. Evaluation of work can be carried out automatically by setting the evaluation parameters. The system enters the estimates into the statement.

Various types of tests are used to quickly check knowledge. Test questions are stored in a database and can be reused in the same or different courses.

Completing a task in Moodle is a student's activity, which usually results in the creation and upload of a file of any format to the server or the creation of text directly in the system.

The forum function is useful for academic discussion of problems and consultations. Moodle supports a very useful feature of collaborative editing of texts (a wiki element of the course).

The system supports the exchange of files of any format both between the teacher and the student, and between the students themselves, in particular - in real time.

An important feature of Moodle is the preservation of all work performed by the student, grades and comments of the teacher on the submitted work, all messages on the forum. The system controls the "attendance", the activity of students, the time of their real educational work in the network.

Conclusions. Thus, the following advantages of Moodle can be distinguished:

– open source code - the possibility of "sharpening" for the specifics of a particular educational project, the development of additional modules, integration with other systems;

– focus on collaborative learning technologies – allows you to organize learning in an active form, in the process of joint solution of educational problems, mutual exchange of knowledge;

– wide opportunities for communication: exchange of files of any formats, mailing, forum, chat, the ability to review students' work, internal mail, etc.;

– possibility to use any evaluation system (point, verbal);

– complete information about the work of students (activity, time and content of educational work, portfolio);

– complies with the developed standards and provides an opportunity to make changes without total reprogramming;

– programming interfaces provide the opportunity to work for people of different educational levels, different physical abilities (including the disabled), different cultures.

References:

1. Bobomuradovich S.R. Integration of education, science and production as a basis of an innovative educational process, European Journal of Research and Reflection in Educational Sciences, 2020 8/12.

2. Sodikova F.S., Sariev R.B. Learning with Moodle in Higher Education, Young Scientist, 19/2019.

UDC 004.9

Computer model of information influence dissemination in social networks by different strategies

Ulichev O.S.[1], Candidate of Engineering Sciences, askin79@gmail.com
Meleshko Ye.V.[1], Doctor of Engineering Science, Professor,
elismeleshko@gmail.com
Al-Oraiqat A.M.[2], Doctor of Engineering Science, Professor
Smirnov O.A.[1], Doctor of Engineering Science, Professor
Polishchuk L.I.[1], Senior Lecturer
[1]*Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine*
[2]*Taibah University, Medina, Kingdom of Saudi Arabia*

Currently, there is an increase in the individual active influence of social network users on public opinion formation. This fact has become the basis of various studies in different fields including public communications, sociology, psychology, and information security. Many researchers have studied the role of social networks' active users in the processes of forming public opinion and information manipulation. The possibilities of exploiting such users in various information campaigns are also being investigated. Such active users have a large number of contacts with an influence on their audience and are often called opinion leaders. Acting as a mediator between the information flows and the audience, the opinion leader is involved in the formation of public opinion. Especially during the informational confrontation, when the recipient needs truthful and objective information to determine his position.

The work's goal is to compare the effectiveness of information dissemination strategies that can be proposed for disseminating informational influences in a social network. As a rule, opinion leaders in target network segments are used to disseminate information on social media among a maximum number of users in a minimum time interval. Experiments made it possible to compare the effectiveness of disseminating methods information using opinion leaders, and methods of disseminating information with some other winning structural positions in a social network were evaluated on the developed computer models. The experiments conducted on the model confirm the high effectiveness in attracting opinion leaders to the dissemination processes. At the same time, they show that more effective ways are possible due to the involvement of nodes with other best structural positions during the process of information dissemination in a social network.

In the developed model, a network node is characterized by a set of parameters that determine its behavior and the current state:

$$V_i =< Av_i,\ Rv_i,\ Ov_i,\ Iv_i, \{Vj_i\} >, \quad (1)$$

where Av_i (Active) is the user activity, the number of active dialogs (calls to

other users) for one model iteration; Rv_i (Reputation) is the user's reputation, the newsletter impact, the persuasion power; Ov_i (Opposite) denotes the information resistance, criticality concerning the idea that is spreading; Iv_i (Involvement) - involvement degree in the idea, trust level in the idea; $\{Vj_i\}$ - the set of contacts (nodes) with which there is an information exchange at the node V_i.

The social network nodes in a model can be of two types: ordinary and idea generators. Ideas generators are active nodes and they are the information dissemination centers. The model considers the idea of dissemination of specific content or direction. We will further denote its α- idea. The model may include counter-generators, by which we denote (-α), that is, the idea is opposite to α. The generator unit is formally described as follows:

$$Gen_{\alpha i} =< V_i, | Av_i \sim 1, I\alpha v_i = Ig >, \quad (2)$$

where Ig is the involvement in the idea at the level of the idea generator.

That is, generators are nodes with high activity, the maximum degree of involvement in the α-idea (involvement of the generator level). All generators of the social network segments form many generators - *Gen*. The main idea of the model is to formalize the behavioral strategies of the active nodes in a network segment. A node begins to spread the α-idea, that is its involvement parameter in the α-idea $I\alpha v_i > 0{,}5Ig$. The information messages quantity to nodes from the set of available nodes (contacts V_i) per one iteration of the model is proportional to the node activity $|\alpha_i| \sim Av_i$.

The social network structure is generated based on a random combination of clusters given the number of different types. The available types of clusters in the model are present: clique, group and leader group. In the manual mode, we can edit the generated structure by adding or adding or remove nodes and links. The process of information exchange in the model is presented in the form of iterations sequence, where each iteration corresponds to a certain time interval (for example, 1 iteration = 1 day).

The dissemination of information in a social network is evaluated by the integral criterion:

$$I_\alpha(G) = \sum_{i=1}^{n} I\alpha v_i. \quad (3)$$

Involvement in the α-idea of a separate node is determined by the additive principle. The engagement rate is equal to the sum of accumulated α-sends for the current iteration:

$$I\alpha v_j = \sum_{m=1}^{x} \sum_{i=1}^{n} k_{ij} * \alpha_i, \quad (4)$$

where Iv_j involvement level of the j^{th} node in the α-idea; x is the current simulation iteration; n is the quantity of the contacts for the j^{th} node; α_ia message from the ith node fixes the presence of a message. The parameter value is defined as:

$$\alpha_i = \begin{cases} 1, \ \alpha - message\ from\ V_i \text{exist} \\ 0, \ \alpha - message\ from\ V_i\ not \text{ exist'} \end{cases} \quad (5)$$

where k_{ij} is an information exposure coefficient, determined by the ratio (6):

$$k_{ij} = \frac{Rv_i}{Opv_j}. \quad (6)$$

The behavior and involvement in the idea is determined by the parameter Iv_j, if a certain threshold value is exceeded, the node is considered involved in the idea. Since the level of trust (mistrust) in the model is already fixed to a specific idea, it is proposed to determine the information weight (IW) of an idea as a coefficient obtained from the relation:

$$IW = \frac{Reputation}{Mistrust}. \quad (7)$$

At each iteration, the rate of increase in engagement is determined by equation (6). The function is monotonically non-decreasing. The maximum value of the function is the generator level defined in the models' parameters.

In the experiment, we compare the effectiveness of target nodes' attack strategies with the "tree" and "bush" strategies that were proposed in [1, 2].

The experiments conducted on the program model confirmed the high efficiency of disseminating information influences when attracting opinion leaders (the "Tree" strategy by the quantity of the connections). The "Tree" strategies generally show stability regardless of the best level of the idea generator's initial position. The advantages of attracting opinion leaders for information impacts are the availability of developed methods and tools for selecting and evaluating such nodes in real networks.

At the same time, under certain conditions, the strategies of attacking the target site (in experiments, the target site was selected according to the criterion of a winning structural position) gave a significant advantage. According to the multi-stage theory flow of information, information reaches the general public in several stages. At the last stage, it is the sources (nodes) with a large audience that are decisive. However, at the attracting initial stages, nodes with a winning structural position can give a significant advantage. The effectiveness of the attack strategy on the target node substantially not only depends on the generator initial position and the available paths (communication connections) to the target node. Methods for assessing the node value and methods for their selection in real networks require further research and improvement.

References

1. Ulichev O. and Meleshko E., "Software modeling of the spread of information-psychological influences in virtual social networks," Scientific-technical journal "Modern information systems", Vol. 2, № 2, Kharkiv, pp. 35-39, 2018. URL: http://nbuv.gov.ua/UJRN/adinsys_2018_2_2_8.

2. Ulichev O., "Mathematical model of distribution of information and psychological influences in the segment of social network," Scientific works collection of Central Ukrainian National Technical University, №. 30, pp. 165-174, 2018. URL: http://nbuv.gov.ua/UJRN/znpkntu_2018_31_22.

UDC 004.056.53

Some questions of computer literacy in the field of computer viruses and anti-virus programs

Kondrashenko I.S., student, andr0911171@gmail.com
Scientific adviser – Konoplitska-Slobodenyuk O.K., teacher
Central Ukrainian National Technical University, Kropyvnitskyi, Ukraine

Computer virus is a type of malicious program that can be embedded in the code of other programs, system memory areas, boot sectors and distribute its copies through various communication channels.

The main purpose of the virus is its spread. In addition, often its accompanying function is a violation of software and hardware - deleting files, deleting the operating system, unsuitable data structures, disruption of network structures, theft of personal data, extortion, blocking users and more. Even if the author of the virus did not program malicious effects, the virus can cause computer crashes due to errors, ignored subtleties of interaction with the operating system and other programs.

Viruses are spread mainly through the Internet, local networks, and removable media, such as flash drives, memory cards, and so on. As for the mechanism of virus distribution, viruses spread by copying their "body" and ensuring its subsequent execution: entering themselves into the code of other programs running, replacing other programs, registering to start the operating system through the registry and more. A virus or a carrier can be not only programs that contain machine code, but also any information that contains commands that run automatically, such as batch files and Microsoft Word and Excel documents that contain macros. Once a virus has successfully entered the code of a program, file, or document, it will remain in a so-called "sleep" state until circumstances force the computer or other device to execute its code. In order for the virus to infect your computer, you need to run an infected program, which in turn will execute the virus code.

Now, about the types of computer viruses that exist.

1) Worm – a program that makes copies of itself. The downside is that the computer gets cluttered and slows down. A distinctive feature of the worm is that it cannot be part of another harmless program.

2) Rootkit viruses – these viruses are used to hide harmful activity. They mask malware to prevent it from being detected by anti-virus programs. Rootkits can also modify the operating system on a computer and replace its basic functions to hide their own presence and the actions of an attacker on an infected computer.

3) Spyware – Spyware collects information about user behavior and actions. Most of them are interested in information - addresses, passwords, credit card details.

4) Zombies – Zombie viruses allow an attacker to control a user's computer. Zombie computers can be networked (bot-net) and used for mass attacks on sites or spam. The user may not even know that his computer is being zombied and used by an attacker.

5) Adware viruses (Adware) – advertising programs, without the knowledge of users are embedded in various software to display advertisements. Typically, adware is built into software that is distributed for free. Advertising is located in the working interface. Most often, such programs also collect and forward to their developer personal information about the user.

6) Trojan viruses (Trojan) – Trojan program is the most dangerous type of virus, as it is disguised in other harmless programs. And as long as the user does not run this most harmless program, the Trojan is not dangerous and it is not easy to detect. A Trojan can do a lot of damage to your computer. Trojans are mainly used to steal, modify or delete personal user data. A distinctive feature of the Trojan virus is that it cannot reproduce on its own.

7) And probably the most famous type of virus – Virus-blocker (Winlock) – such programs block the user's access to the operating system. When the computer boots, a window appears accusing the user of downloading unlicensed content or infringing copyright. And under the threat of complete deletion of all data from the computer, or "criminal liability" require to send an SMS to a phone number or top up his account. Of course, after the transfer of money to the account of the attacker, the banner does not disappear.

Now, about the antivirus programs that are able to detect such threats. Modern anti-virus programs have the necessary functionality to detect and neutralize various virus programs and provide reliable protection for the user's computer. It should be noted that viruses are ahead of anti-virus programs in their development, so even in the case of regular use of anti-viruses there is no 100% guarantee of security. Anti-virus programs can detect and destroy only known viruses, and when a new computer virus appears, protection against it does not exist until an anti-virus is developed for it. However, many modern anti-virus packages include a special software module called a heuristic analyzer, which is able to examine the contents of files for the presence of code specific to computer viruses. This makes it possible to detect and warn about the danger of contracting a new virus in time. When choosing an antivirus program, you should pay attention to such a parameter as the number of recognizable signatures (a sequence of characters that are guaranteed to recognize the virus). The second parameter is the presence of a heuristic analyzer of unknown viruses, its presence is very useful, but significantly slows down the program. To date, there are many different antivirus programs.

Conclusions. Because new viruses are appearing at breakneck speed, it is recommended that use an anti-virus program with a good reputation and regularly update it, to make your information system more secure.

УДК 004.9+378.147

Переваги інноваційних засобів навчання як інструменту дистанційного навчання у ЗВО

Бугай В.В., студент 2 курсу, balik.bugai@gmail.com
Науковий керівник – Ісак Л.М., ст. викладач, заступник декана з навчальної роботи, isakluda@ukr.net
Університет Григорія Сковороди в Переяславі,
м. Переяслав, Україна

Останніми роками освітяни у всьому світі все частіше використовують інформаційні технології для підготовки до занять, для інструктування студентів та адміністрування інформації. Спостерігається тенденція до активного впровадження онлайн-курсів, персоналізації, інтерактивності онлайн-навчання, яке також називається електронним навчанням, яке поряд з різними інтеграціями e-learning з традиційними класами швидко розвивається. Flip teaching, або flipped classroom, є хорошим прикладом інтеграції e-learning та традиційного навчання. Термін «flipped classroom» означає, що метод навчання відвертається або відхиляється від традиційного методу. У flipped classroom інструкція подається в Інтернеті, а час у класі можна ефективно використовувати для виконання домашніх завдань, вправ, проектів, обговорень чи інших інтерактивних заходів, що ілюструють концептуальний зміст навчання. Це нововведення залучає студентів до уроку і дає їм більше можливостей отримати практичні навички та знання. Наприклад, студенти у flipped classrooms можуть переглядати уроки за допомогою відео- чи аудіозаписів, а потім виконувати різні завдання та вправи під наглядом викладача.

Розвиток сучасної світової та вітчизняної освіти та тенденції до впровадження нових технологій і сучасних моделей навчання вимагають не тільки розвитку інформаційно-комунікаційних технологій, але й відповідних організаційних змін, запровадження оновлення у кадровій політиці навчального закладу, удосконалення нормативно-методичної бази освітнього процесу, розвитку педагогічних інструментів та методик, які відповідають завданням сучасної освіти та рівню сучасних інформаційно-комунікаційних технологій (ІКТ) [1] та переосмислення ролі педагогів – педагог має бути партнером у процесі навчання, володіти інноваційними навичками викладання, проявляти технологічний ентузіазм, зацікавленість і майстерність [3].

Шеріл Нуссбаум-Бич (член Ради директорів Міжнародного товариства з технологій в галузі освіти, США) сказав: «Технології ніколи не замінять викладача, але викладач, який ефективно застосовує технології для розвитку своїх студентів, замінить того, хто ними не володіє» [2].

Серед існуючих технологічних платформ, доступних для забезпечення flipped classrooms, системи управління навчанням (Learning Management Systems – LMS) виділяються як найбільш поширені через їх перевагу в наданні контенту курсу та для керування величезною кількістю інформаційних онлайн- курсів. Зокрема, MOODLE (модульне об'єктно-орієнтоване динамічне навчальне середовище) з відкритим кодом є найпопулярнішою LMS. Луцький національний технічний університет оголосив про використання MOODLE як єдиної платформи з відкритим кодом для спільного середовища співпраці та навчання з 2019 року.

MOODLE – Modular Object-Oriented Dynamic Learning Environment, (вимовляється «Мудл»), або – модульне об'єктно-орієнтоване динамічне навчальне середовище – це система управління навчанням, орієнтована насамперед на організацію взаємодії між викладачем і студентами, хоча підходить і для організації традиційних дистанційних курсів, а також для підтримки очного навчання. Більш докладно про MOODLE можна дізнатися на офіційному сайті проекту: http://moodle.org/.

Використовуючи MOODLE викладач може створювати курси, наповнюючи їх вмістом у вигляді текстів, допоміжних файлів, презентацій, тестів, анкет, опитувальників і т.п. Для роботи в MOODLE досить мати будь- який web-браузер, що робить використання цього навчальної середовища зручним як для викладача, так і для тих, хто навчається. За результатами виконання студентами завдань, викладач може виставляти оцінки і давати коментарі. Таким чином MOODLE є як центром створення навчального матеріалу так і центром забезпечення інтерактивної взаємодії між учасниками навчального процесу.

Таблиця 1. Можливості, які система дистанційного навчання MOODLE надає користувачам

Студенти	**Викладачі**	**Адміністрація**
навчаються в будь-який час, в будь-якому місці, в зручному темпі	підтримують курс в актуальному стані	ефективно розподіляє навантаження на викладачів
витрачають більше часу на глибоке вивчення цікавих тем	змінюють порядок і спосіб подачі матеріалу в залежності від роботи групи	аналізує результати навчання
знання краще засвоюються	витрачають більше часу на творчу роботу і професійне зростання, тому що рутинні процеси можна довірити СДН	знижує витрати на управління навчальним процесом
	підтримують зворотний зв'язок з учнями, в тому числі і після закінчення навчання	

Як припускали деякі дослідники, широка популярність MOODLE значною мірою залежить від його переваг. Наприклад, для Moodle немає ліцензійної плати, і, щоб мати змогу користуватися MOODLE, вищим навчальним закладам потрібно лише змінити її систему, щоб вона відповідала процедурам та політиці навчального закладу. Широке залучення ресурсів MOODLE передбачає додаткові економічні, технологічні, педагогічні та філософські переваги.

Таблиця 2. Основні причини збільшення залучення технологій з відкритим кодом у домені вищої освіти

Сфера	**Перевага Learning Management Systems – LMS**
економічна	– полегшує навантаження на управління ліцензіями на програмне забезпечення
	– знижує витрати на придбання та запуск програмного забезпечення нижчі ніж розробка власного програмного забезпечення
	– незалежність
	– технологічний продукт
загальна	– надійні та безпечні технології
	– відкрита архітектура
	– взаємодія
	– відкриті, але добре захищені авторські права та ліцензії
педагогічна	– дозволяють використовувати різні сценарії навчання
	– веб-навчання
	– модульна та багатомовна структура
	– різноманітність інструментів
філософська	– спільний підхід
	– антимонопольний підхід
	– безкоштовний доступ до навчання

Навчальне середовище MOODLE відкриває нові можливості не тільки для навчального закладу в цілому, а й для кожного викладача. Висновки зроблені Iwasaki та іншими дослідниками [5] свідчать, що викладачі, які базували свої курси на конструктивістській філософії, вважали, що знання здобуваються тоді, коли інформація контактує з існуючими знаннями, здобутими з досвідом. Результати вказували на те, що в курсах, що використовують конструктивістський підхід, інтерактивні функції в LMS використовувались для посилення активного навчання студентів; курси, що застосовували традиційні способи викладання, як правило, використовували вікторини та завдання для проектів для посилення основних знань та практичних навичок студентів; викладачі в змішаних

курсах скористалися як «будівельними» класами, так і «передавальними» класами, використовуючи комунікаційну функцію LMS, щоб розвивати студентські здібності та можливості самостійного навчання.

Слід зазначити, що MOODLE, як система управління навчанням (LMS), надає студентам можливість багаторазового повторення навчального матеріалу, оскільки він постійно доступний через Інтернет. Для самостійного опрацювання дисципліни навчально-методичний матеріал подається логічно, структуровано та послідовно. MOODLE пропонує широкий спектр засобів для само тестування та для самоконтролю. Варто зазначити, що виконання завдань та їх оцінювання проходить незалежно від людського чинника. Головною перевагою MOODLE є можливість організації дистанційного навчання для самостійного опанування навчальним матеріалом, інтерактивного навчання та комунікації з викладачем. MOODLE, який має високий рівень налаштувань в інтерфейсі, змісті та можливостях взаємодії, дає змогу викладачам використовувати ефективні методи навчання, для ефективного студентів.

Список використаної літератури

1. Байдалюк Я. Середовище навчання Moodle: його переваги та недоліки. URL: http://irznanii.com/a/115399/seredovishche-navchannya-moodle-yogo-perevagi-ta-nedolki (дата звернення: 10.02.2020)

2. Ломакович А. М. Впровадження модульного об'єктно-орієнтованого динамічного навчального середовища Moodle в освітній процес вищої школи / А. М. Ломакович, Н. В. Бабій, О. А. Фурман. *Науковий вісник Кременецької обласної гуманітарно-педагогічної академії ім. Тараса Шевченка.* Серія: Педагогіка. 2017.Вип.7.С. 63-71. URL: http://nbuv.gov.ua/UJRN/nvkogpth_2017_7_11 (дата звернення: 10.02.2020)

3. Теорія та практика змішаного навчання: монографія/В. М. Кухаренко,С. М. Березенська, К. Л. Бугайчук, Н. Ю. Олійник, Т. О. Олійник, О. В. Рибалко, Н. Г. Сиротенко, А. Л. Столяревська. Харків: НТУ «ХПІ», 2016. 284 с.

4. Distance Education, 6(1), Retrieved on February 9th. URL: http://tojde.anadolu.edu.tr/tojde17/articles/carlos.htm

5. Iwasaki, C., Tanaka, T., & Kubota, K. Analysis of relating the use of a learning management system to teacher epistemology and course characteristics in higher education. Knowledge Management & E-Learning: An International Journal. 2011. 3(3). P.478-490.

6. Machado, C., & Thompson, K. The adoption of open sources within higher education in Europe and a dissemination case study. Turkish Online Journal of Distance Education. 2015 6(1), Retrieved on February 9th from http://tojde.anadolu.edu.tr/tojde17/articles/carlos.htm

7. Moodle. URL: http://moodle.org/ (дата звернення: 10.02.2020)

УДК 004:613

Проблеми інформаційної гігієни у сучасному суспільстві

Марченко К.М., канд. техн. наук, доцент, k_marchenko@i.ua
Оришака О.В., канд. техн. наук, доцент, oryhsaka@gmail.com
Марченко А.К., студентка
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна

Збільшення обсягів оброблюваної інформації в сучасному інформаційному суспільстві зумовлює значне зростання інформаційного навантаження не лише на комп'ютерні системи та комунікації, а й на людей, які забезпечують інформаційні процеси в цих системах. Розвиток та поширення інформаційних технологій призводить до збільшення номенклатури професій, пов'язаних з обробкою інформації.

Професійні захворювання в галузі інформаційних технологій мають свою специфіку. Крім фізичних та фізіологічних порушень, спостерігається підвищине психічне навантаження, особливо на робочих місцях з підвищеною відповідальністю та щільним інформаційним потоком, оперативним прийняттям рішень, стрес, нервова втома тощо [1]. Тому розробка норм інформаційної гігієни є актуальною задачею.

Аналіз досліджень [2-5] показав наявність проблеми з кількісними оцінками інформаційного навантаження та порогових значень дії цих навантажень на людину як учасника інформаційних процесів. Зокрема, існують санітарні норми при роботі з комп'ютером, але вони торкаються лише фізичної взаємодії з пристроями і зовсім не враховують інформаційне навантаження.

Таким чином задачею досліджень є вивчення та розробка кількісних показників впливу інформаційного потоку на стан людини.

Список літератури

1. Марченко К.Н., Пестунов В.М., Свяцкая Л.П., Марченко Т.К.. Влияние информации на состояние злоровья человека. Наукові записки, вип.10, ч. 2, Кіровоград: КНТУ, 2010. – С. 224-229.

2. Дружилов С.А. Современная информационная среда и экология человека: психологические аспекты. Гигиена и санитария. 2018; 7: 593-603.

3. Еремин А.Л. Влияние информационной среды на здоровье населения. Проблемы социальной гигиены, здравоохранения и истории медицины, №6. 2000; С. 21-4.

4. Бухтияров И.В., Денисов Э.И., Еремин А.Л. Основы информационной гигиены: концепции и проблемы инноваций. Гигиена и санитария, №4. 2014. С.5-9.5. Еремин А.Л. Природа и физиология информационной экологии человека. Экология человека. 2000; 2: 55-60.

УДК 32.019.5+004.77

Дослідження інформаційно-психологічних впливів на основі цифрового газлайтингу у мережі Інтернет

Мелешко Є.В., д.т.н., проф., elismeleshko@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна

Газлайтинг – метод інформаційно-психологічного впливу, що має на меті змусити об'єкт впливу сумніватися у своїй здатності адекватно сприймати оточуючу реальність через застосування брехні, заплутування, залякування, звинувачень, знецінення та різних багатокрокових комбінацій цих стратегій, а також створення переконання у жертви, що з нею щось не так і тільки суб'єкт впливу адекватно сприймає реальність і треба сприймати інформацію від нього як правильну.

Цей термін в основному використовується для опису одної з форм міжособистісних маніпуляцій, зокрема, у проблемних сімейних відносинах, як один з різновидів психологічного насильства. Але в наш час публіцистичне використання терміну газлайтинг все частіше використовується для опису сучасної політичної тактики [1-3]. Зокрема:

– Перші, контрольовані та ретельно сплановані випадки політичного газлайтингу приписують Східній Німеччині у 1970-х та 80-х років [2-4].

– «Газлайтинг» використовувався для опису стилю зовнішньо-політичної пропаганди Російської Федерації [1, 2, 5].

– Американські журналісти широко використовували слово «газлайтинг» для опису дій Д. Трампа під час президентських виборів у США 2016 року та його перебування на посаді президента [1-3, 6].

В цих випадках використовують термін «політичний газлайтинг».

При використанні інформаційних технологій та Інтернету для реалізації як міжособистісних, так і групових (політичних) маніпуляцій такого роду доречно використовувати термін «цифровий газлайниг».

Цифровий газлайтинг – це використання інформаційних технологій та мережі Інтернет для спотворення сприйняття світу як однієї людини, так і деякої категорії користувачів Інтернету на основі методів звичайного газлайтингу. Зокрема, Синтія М. Дуденхоффер, доцент та директор з інформаційних ресурсів та оцінювання у Центральному методистському університеті у Фейеті, штат Міссурі, відзначає зростання домашнього насильства, пов'язаного із системами домашнього моніторингу, такими як Google Nest. Вона називає цей вид впливу «цифровим газлайтингом» [7].

Термін «газлайтинг» походить від п'єси «Gas Light» 1938 р. та фільму «Gaslight» 1944 р. [1, 2], у яких чоловік використовує хитрість, щоб переконати свою дружину, що вона психічно хвора, з метою привласнення її майна. З 1960-х рр. психологи почали використовувати

цей термін для позначення реального еквіваленту явища, зображеного в п'єсі та фільмі. Американське діалектне товариство визнало слово gaslight «найкориснішим» новим словом року у 2016 р. [2, 8], а Oxford University Press надало йому ІІ місце у своєму списку найпопулярніших нових слів 2018 р. [2, 9].

Головною особливістю газлайтингу є заплутування жертви та намагання знищити в її свідомості причинно-наслідкові зв'язки, а також викликати відмову від власних цілей, думок та навіть відчуттів і емоцій. Існує один важливий фактор газлайтингу, що сприяє його ефективності: жертва довіряє своєму маніпулятору та/або певним чином залежить від нього [1, 2]. Автор [1] виділяє 3 підтипи політичного газлайтингу, що можна віднести і до групового цифрового газлайтингу:

1. **Введення контрнаративів.** Вони можуть бути реалістичними або надуманими, але завжди суперечать домінантній існуючій історії.

2. **Дискредитація експертів.** Підривання авторитету експертів та здійснення інформаційної ізоляції їх від суспільства, з подальшим пропонуванням інших «експертів», вигідних газлайтеру.

3. **Заперечення більш-менш зрозумілого факту.** Найбільш вражаючими є випадки, коли політик заперечує, що сказав чи зробив щось, що насправді було зафіксовано в записі лише днями раніше.

Є два різні типи жертв політичного газлайтингу: 1) ті, якими успішно маніпулюють, 2) і ті, хто дотримується протилежних поглядів (журналісти та дослідники), тобто, не ошукані але дискредитовані.

Знання того, що таке газлайтинг, дозволяє об'єктам цього впливу помітити його, даючи їм можливість протистояти йому.

Список літератури

1. Rietdijk, N. (2021). Post-truth Politics and Collective Gaslighting. Episteme, 1-17. URL: https://www.cambridge.org/core/journals/episteme/article/posttruth-politics-and-collective-gaslighting/88BDC6B5D1540817086E1027A0FF1B5A

2. Gaslighting. URL: https://en.wikipedia.org/wiki/Gaslighting (дата звернення 20.03.2022)

3. Naraharisetty R. (2021) How 'Political Gaslighting' Undermines the Truth. URL: https://theswaddle.com/how-political-gaslighting-undermines-the-truth/

4. Лора Уильямс (2020) 10 фактов о тайной полиции Восточной Германии. URL: https://mises.in.ua/article/10-faktov-o-tainoi-policii-gdr/

5. Caldwell A. (2016). How Russia Successfully Gaslighted the West. Huffington Post, 16 December. https://www.huffingtonpost.ca/adam-caldwell/the-gaslighting-of-the-west_b_13657466.html

6. Gibson C. (2017) What we talk about when we talk about Donald Trump and 'gaslighting'. The Washington Post. ISSN 0190-8286. URL: https://www.washingtonpost.com/lifestyle/style/what-we-talk-about-when-we-talk-about-donald-trump-and-gaslighting/2017/01/27/b02e6de4-e330-11e6-ba11-63c4b4fb5a63_story.html

7. Marcotte A. (2019) Tech Trends. American Libraries. URL: https://americanlibrariesmagazine.org/2019/03/01/tech-trends-libraries/

8. Metcalf A. (2017) 2016 Word of the Year (PDF). American Dialect Society. Most useful word of the year. URL: https://www.americandialect.org/wp-content/uploads/2016-Word-of-the-Year-PRESS-RELEASE.pdf

9. Word of the Year 2018: Shortlist. Oxford University Press. URL: https://languages.oup.com/word-of-the-year/2018-shortlist/

УДК 004.056.53

Використання мемів з метою інформаційно-психологічномих впливів у інформаційних війнах

Ружин В.Ю., бакалавр, why1703i@gmail.com
Науковий керівник – Мелешко Є.В., д.т.н., проф., elismeleshko@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна

Меми – це смішні зображення чи відео з надписами, які швидко поширюються в соціальних мережах та медіа. Часто їх пересилають друзям та знайомим, збільшуючи популярність та впізнаваність. Найчастіше меми слугують лише для підняття настрою людини, проте також їх можна використовувати і для інформаційно-психологічного впливу.

Інформаційно-психологічний вплив – це вплив на свідомість та підсвідомість особистості й населення з метою внесення змін у їхню поведінку і світогляд.

В умовах повномаштабної війни, яка була розпочата 24 лютого армією РФ, необхідно звернути увагу на інформаційно-психологічний вплив під час інформаційних війн та інформаційних протиборств.

Інформаційна війна (ІВ) – форма ведення інформаційного протиборства між різними суб'єктами (державами, неурядовими, економічними або іншими структурами), що передбачає здійснення комплексу заходів із завдання шкоди інформаційній сфері конфронтуючої сторони й захисту власної інформаційної безпеки.

Основне завдання ІВ (між державами) – здійснення безпосереднього негативного руйнівного впливу на сукупну політичну могутність держави шляхом послаблення її реальних і потенційних можливостей щодо забезпечення власної безпеки, створення труднощів у внутрішньому розвитку й проведенні активної зовнішньої діяльності, а також у підтриманні міжнародних зв'язків; завдання шкоди політичному іміджу, тобто послаблення панівної еліти, установленого нею соціально-політичного режиму чи навіть сприяння усуненню останньої від влади.

Меми, які зараз використовують для інформаційно-психологічного впливу можна поділити на два види, а саме:

1. Меми, що дискредитують армію противника;
2. Меми, що піднімають дух українців.

З перших днів війни українці почали висміювати так звану "другу армію світу", що породило, наприклад, такі меми: "Найвеличніша армія світу могла б перетворити Америку на ядерний попіл, але не мала часу, бо відгрібла в селі на Сумщині", "Ой вей, грізний воїн! В Одесі ти ледь-ледь поц!", "Друга армія світу? Ой, я вас благаю".

Варто виділити головні меми, які були народжені під час цієї війни:

1. “Русский военный корабль” – цей мем став символом незламності нашого народу. Кожен громадянин України та, певно, більша частина цивілізованого світу знає лише один вірний шлях для окупантів.

2. “Заспокійливий засіб Арестович М” – мем пов’язаний з дивовижним спокоєм радника Офісу Президента України. Здається що Олексій Арестович буде таким же спокійним навіть, якщо все населення Росії (140 млн) в один момент нападуть на Україну.

3. “Кадиров шукає Бандеру” – серія публікацій, у яких стверджується, що Кадиров оголошує «полювання» на головного ворога Росії – Степана Бандеру, за голову якого він готовий заплатити 250 млн. рублів з бюджету республіки Чечні і, одже, йому невідомо, що Бандера помер в 1959 році. А українці відразу відреагували на цей курьйозний випадок та створили велику кількість мемів, зокрема, такі – “Друзі! Прохання не поширювати інформацію про місцезнаходження Степана Андрійовича Бандери!”, “За деякими оперативними даними Бандера переховується у львівському метро”, “Передайте Кадирову, що Бандера не проти зустрітися з ним, хіба що на своїй території”.

4. “Чорнобаївка” – це мем про селище в Херсонській області, яке стало Бермудським трикутником для окупантів. Саме тут більше десяти разів “загубилися” війська та техніка РФ.

5. “Паляниця” – найкращий спосіб виявити російського диверсанта. Окрім того, що вони не можуть правильно вимовляти це слово, вони також не знають його пекладу. Адже по россійському телебаченні кажуть, що це “клубніка”, певно через схожість зі словом полуниця.

Висновки: Інструментом інформаційно-психологічного вплову під час інформаційних протиборств можуть бути, навіть, смішні картинки в Інтернеті. Прикладом цього є висміювання “другої армії світу” в мережі Інтернет. Багато українських мемів допомагають нам не впасти духом в цей тяжкий час.

Список літератури

9. Історія інформаційно-психологічного протиборства : підруч. / [Я.М.Жарков, Л.Ф.Компанцева, В.В.Остроухов, В.М.Петрик, М.М.Присяжнюк, Є.Д.Скулиш] ; за заг. Ред. д.ю.н., проф., засл. юриста України Є.Д.Скулиша. – К. : Наук.-вид. відділ НА СБ України, 2012. – 212 с.

2. Інформаційна безпека (соціально-правові аспекти) : Підручник / [Остроухов В.В., Петрик В.М., Присяжнюк М.М. та ін.; за заг. ред. Є.Д.Скулиша]. – К. : КНТ, 2010. – 776 с.

УДК 32.019.5+ 004.77

Соціальна інженерія як засіб обходу систем захисту інформації з використанням людського фактору

Сніховський А.О., магістр, twixielulamoon99@gmail.com
Кірєєв С.М., магістр, kireevsergey3627@gmail.com
Шевченко О.О., магістрант, shev4enos@gmail.com
Чабан О.О., магістрант, visardvalimar@gmail.com
Науковий керівник – Якименко М.С., к.ф.-м.н., доц.
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна

Соціальна інженерія – сукупність прийомів, методів і технологій створення такого простору, умов і обставин, які максимально ефективно призводять до конкретного необхідного результату стосовно обходу систем захисту інформації, з використанням соціології та психології.

У переважній більшості систем захисту інформації, людина є найменш надійною ланкою. Саме тому для досягнення найбільш надійної інформаційної системи потрібно поєднувати апаратні та технічні засоби з урахуванням людського фактору. Для того, щоб убезпечити себе від впливу соціальної інженерії, необхідно зрозуміти, як вона працює.

Всі техніки соціальної інженерії засновані на когнітивних викривленнях (стереотипи, упередження). Ці помилки в поведінці використовуються соціальними інженерами для створення атак, спрямованих на отримання конфіденційної інформації, часто за згодою жертви.

Претекстінг – це набір дій, відпрацьованих за певним, заздалегідь складеним сценарієм, в результаті якого жертва може видати будь-яку інформацію або вчинити певну дію. Найчастіше даний вид атаки передбачає використання голосових засобів, таких як Skype, телефон і т.п.. Для використання цієї техніки зловмисникові необхідно спочатку мати деякі дані про жертви (ім'я співробітника; посаду; назва проектів, з якими він працює; дату народження). Зловмисник спочатку використовує реальні запити з ім'ям співробітників компанії і, після того як увійде в довіру, отримує необхідну йому інформацію.

Фішинг – техніка інтернет-шахрайства, спрямована на отримання конфіденційної інформації користувачів – даних для авторизації різних систем. Це найпопулярніша схема соціальної інженерії на сьогоднішній день. Жоден великий витік персональних даних не обходиться без хвилі фішингових розсилок, що передують їй. Основним видом фішингових атак є підроблений лист, відправлений жертві по електронній пошті, яке виглядає як офіційний лист від платіжної системи або банку. У листі міститься форма для введення персональних даних (PIN-кодів, логіна і

пароля тощо) або посилання на web-сторінку, де розташовується така форма. Причини довіри жертви подібним сторінок можуть бути різні: блокування облікового запису, поломка в системі, втрата даних та інше.

Троянський кінь – це техніка грунтується на цікавості, страху або інших емоціях користувачів. Зловмисник відправляє лист жертві за допомогою електронної пошти, як додаток до якого знаходиться «оновлення» антивіруса, ключ до грошового виграшу або компромат на співробітника. Насправді ж у вкладенні знаходиться шкідлива програма, яка після того, як користувач запустить її на своєму комп'ютері, буде використовуватися для збору або зміна інформації зловмисником.

Кві про кво (послуга за послугу) – дана техніка передбачає звернення зловмисника до користувача по електронній пошті або корпоративному телефону. Зловмисник може представитися, наприклад, співробітником технічної підтримки та інформувати про виникнення технічних проблем на робочому місці. Далі він повідомляє про необхідність їх усунення. У процесі «рішення» такої проблеми, зловмисник підштовхує жертву на вчинення дій, що дозволяють атакуючому виконати певні команди або встановити необхідне програмне забезпечення на комп'ютері жертви.

Дорожнє яблуко – цей метод є адаптацію троянського коня і полягає у використанні фізичних носіїв (CD, флеш-накопичувачів). Зловмисник зазвичай підкидає такий носій в загальнодоступних місцях на території компанії (парковки, столові, робочі місця співробітників, туалети). Для того, щоб у співробітника виник інтерес до даного носія, зловмисник може нанести на носій логотип компанії і якийсь підпис. Наприклад, «дані про продажі», «зарплата співробітників», «звіт в податкову» і інше.

Зворотня соціальна інженерія – даний вид атаки спрямований на створення такої ситуації, при якій жертва змушена буде сама звернеться до зловмисника за «допомогою». Наприклад, зловмисник може вислати лист з телефонами і контактами «служби підтримки» і через деякий час створити оборотні неполадки в комп'ютері жертви. Користувач в такому випадку подзвонить або зв'яжеться по електронній пошті з зловмисником сам, і в процесі «виправлення» проблеми зловмисник зможе отримати необхідні йому дані.

Плечевий серфінг – спостереження особистої інформації про жертву через її плече. Цей тип атаки поширений в громадських місцях, таких як кафе, торговельні центри, аеропорти, вокзали, а також в громадському транспорті.

Застосування технік соціальної інженерії вимагає не тільки знання психології, а й уміння збирати про людину необхідну інформацію. Відносно новим способом отримання такої інформації став її збір з відкритих джерел, головним чином з соціальних мереж. Наприклад, соціальні мережі, містять величезну кількість даних, які люди й не намагаються приховати. Як правило, користувачі не приділяють належної

уваги питанням безпеки, залишаючи у вільному доступі дані і відомості, які можуть бути використані зловмисником.

Немає єдиної універсальної схеми злому з використанням соціальної інженерії. В кожному окремому випадку хакер розробляє власний шлях до досягнення конкретного результату. Вибір тієї чи іншої техніки залежить не тільки від уже відомого знання про об'єкт впливу, а й від безпосередньої ситуативної практики взаємодії з ним, оскільки найчастіше соціальний інженер має справу зі сформованими умовами та обставинами, які можуть вже ніколи не повторитися в майбутньому.

Для проведення своїх атак зловмисники, які застосовують техніки соціальної інженерії, часто експлуатують довірливість, лінь, люб'язність і навіть ентузіазм користувачів і співробітників організацій. Захиститися від таких атак непросто, оскільки їхні жертви можуть не підозрювати, що їх обманули. Зловмисники, які використовують методи соціальної інженерії, переслідують, в загальному, такі ж цілі, що і будь-які інші зловмисники: їм потрібні гроші, інформація або IT-ресурси компанії-жертви. Для захисту від таких атак потрібно вивчити їх різновиди, зрозуміти, що потрібно зловмисникові, і оцінити збиток, який може бути заподіяний організації. Володіючи всією цією інформацією, можна інтегрувати в політику безпеки необхідних заходів захисту.

Соціальні інженери часто використовують для атак телефони, пошту чи месенджери.

Забезпечення захисту від соціальної інженерії потребує скептичного ставлення до будь-яких повідомлень та деякі принципи наведені нижче.

Заходи для забезпечення безпеки при одержанні телефонних дзвінків: 1) перевірка особистості абонента, 2) використання послуги визначення номера, 3) ігнорування невідомих посилань в sms-повідомленнях;

Заходи для забезпечення безпеки при одержанні електронних листів передбачають створення конкретних принципів використання електронної пошти, що охоплюють такі елементи: 1) вкладення в документи, 2) гіперпосилання в документах, 3) запити особистої або корпоративної інформації, які виходять із середини компанії, 4) запити особистої або корпоративної інформації, які виходять із-за меж компанії.

Для забезпечення захисту від атак під час обміну повідомленнями в корпоративному середовищі слід виконати кілька вимог: 1) вибрати одну платформу для миттєвого обміну повідомленнями, 2) визначити параметри захисту, що задаються при розгортанні служби миттєвого обміну повідомленнями, 3) визначити принципи встановлення нових контактів, 4) задати стандарти вибору паролів, 5) скласти рекомендації по використанню служби миттєвого обміну повідомленнями.

Фахівці з соціальної інженерії виділяють наступні основні захисні методи для організацій:

1) розробка продуманої політики класифікації даних, яка враховує ті здаються нешкідливими типи даних, які можуть привести до отримання

важливої інформації;

2) забезпечення захисту інформації про клієнтів за допомогою шифрування даних або використання управління доступом;

3) навчання співробітників навичкам для розпізнавання соціального інженера, проявам підозри при спілкуванні з невідомими людьми;

4) заборона персоналу на обмін паролями або використання спільного;

5) заборона на надання інформації з відділу з секретами кому-небудь, не так знайомому особисто або не підтверджені будь-яким способом;

6) використання особливих процедур підтвердження для всіх, хто запитує доступ до конфіденційної інформації;

Для захисту великих компаній і їх співробітників від шахраїв, що використовують техніки соціальної інженерії, часто застосовуються комплексні багаторівневі системи безпеки. Нижче перераховані деякі особливості і обов'язки таких систем:

1) Фізична безпека. Бар'єри, що обмежують доступ в будівлі компанії і до корпоративних ресурсів.

2) Дані. При аналізі загроз і плануванні заходів щодо захисту даних потрібно визначити принципи поводження з паперовими і електронними носіями даних.

3) Програмне забезпечення. Для захисту середовища необхідно врахувати, як зловмисники можуть використовувати в своїх цілях поштові програми, служби миттєвої передачі повідомлень і інші додатки.

4) Комп'ютери. Захист користувачів від прямих атак на їх комп'ютери, шляхом визначення строгих принципів, які вказують, які програми можна використовувати на корпоративних комп'ютерах.

5) Внутрішня комп'ютерна мережа. В останні роки через широке використання віддаленої роботи, кордони внутрішніх мереж стали багато в чому умовними. Співробітникам компанії потрібно роз'яснити, як вони повинні забезпечувати інформаційну безпеку роботи в будь-якому мережевий середовищі.

6) Периметр мережі. Кордон між внутрішніми мережами компанії і зовнішніми, такими як Інтернет або мережі партнерських організацій.

Найбільшою проблемою є неможливість створення ідеальної універсальної системи захисту. Якщо зловмисники захочуть отримати вашу інформацію, то вони знайдуть метод як це зробити, питання лише в часі та витрачених на це коштах. Тому важливо постійно оновлювати методи захисту та політики безпеки в організації. А звичайним користувачам треба підвищувати свою обізнаність в IT сфері.

В роботі наведено класифікацію та аналіз основних методів соціальної інженерії, а також методи захисту від них.

Отже, жертвою соціальної інженерії може стати будь хто, тому потрібно підвищувати рівень обізнаності людей в питаннях інформаційної безпеки.

УДК 004.8

Дослідження можливостей застосування штучного інтелекту для створення творів мистецтва

Ховренко Є.Д., студентка, x-e-d@ukr.net
Конопліцька О.К., викладач, ksucha80@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна

Термін «штучний інтелект» протягом десятиліть був науковою фантастикою, де машини, які здатні вільно мислити, автономно навчатися і, можливо, навіть відчувати емоції, були переосмислені у різних формах. Можливо через це, коли ми чуємо про мистецтво створене штучним інтелектом, зокрема створення художніх картин, то можемо уявити щось, що не відповідає дійсності.

Художники, що працюють з обчислювальними системами, мають набагато більше впливу на результати, ніж можна було б припустити: вони надають вхідні дані, спрямовують процес та фільтрують вихідні дані. Використання штучного інтелекту у своїй роботі цікавило художників з різних причин. Одних приваблює робота з найфутуристичнішими технологіями, інші використовують їх як спосіб інтеграції випадковості у свою роботу, а треті бачать у цьому потенціал для розширення елементів їх існуючих практик.

Штучний інтелект спочатку застосовувався до мистецтва не як творець, а як наслідувач. Цей метод називається передачею стилю, і він використовує глибокі нейронні мережі для відтворення та змішування стилів творів мистецтва, навчаючи штучний інтелект розуміти існуючі витвори мистецтва.

Багато критиків вважають, що штучний інтелект зруйнує художню індустрію, тому що він дозволить художникам легше висловлювати себе. Це також усуває деякі дорогі завдання, такі як малювання або живопис, що залишають художникам менше часу, щоб мати змогу заробляти на життя своїм мистецтвом.

В 1973 художник Гарольд Коен розробив алгоритм, який дозволяв комп'ютеру малювати з нерівномірністю, схожею на малювання від руки. Аарон – один з найперших прикладів повністю автономного творця зображень. Замість того, щоб створювати випадкові абстракції попередників, Аарон був запрограмований малювати певні об'єкти, і Коен виявив, що деякі з його інструкцій генерували форми, які він не уявляв собі раніше, та він встановив команди, які дозволяли машині приймати щось на зразок художніх рішень. Хоча Аарон був закодований лише на абстрактний власний стиль Коена, він був здатний створювати нескінченну кількість зображень у цьому стилі.

У 2015 році у блозі Google опубліковано розповідь групи дослідників про те, як штучні нейронні мережі навчилися писати свої картини. Для цього використовувалися нейромережі, призначені для розпізнавання зображень: отримавши фотографію або малюнок, вони з'ясовують, які об'єкти на ній зображені. Щоб отримувати «картини», дослідники змушують працювати ці нейронні мережі в зворотньому напрямку: вони показують мережі випадковий шум і просять «поліпшити» його таким чином, щоб на виході була одержана певна інтерпретація. Наприклад, якщо попросити нейромережу «знайти» в шумі банан, мурах або морську зірку, та справді підкоригує зображення, щоб у ньому виявилися відомі риси вказаного об'єкту.

Існує багато додатків, які за допомогою спеціальних фільтрів побудованих на штучному інтелекті перетворюють фотографії користувачів на витвори мистецтва. Наприклад, завдяки Google, у користувачів з 2020 року з'явилася можливість зробити фото у стилі улюбленого художника. Art Transfer – нова функція програми Google Arts & Culture, яка дозволяє застосовувати стиль відомих картин до вибраних фотографій, від сміливих завитків Вінсента Ван Гога до сюрреалістичних полотен Фріди Кало. Art Transfer заснована на алгоритмічній моделі, яка не просто змішує зображення, а робить унікальне «перескладання» зображення на основі конкретного художнього стилю.

Виникає дискусія, чи мають твори мистецтва, створені штучним інтелектом, культурну цінність і чи є це мистецтвом взагалі. З одного боку, не маючи сенсу та ідеї, яку хотів донести митець, картина втрачає свою цікавість для глядачів, залишаючи лише естетичне задоволення. З іншого ж боку, це надає змогу глядачеві уявити себе митцем та відшукати ідею для самого себе.

Деякі люди вважають, що цей новий тип технологій здатен замінити справжніх митців. Однак інші люди думають, що це лише один з інструментів для художника, який хоче розширити світогляд. Штучний інтелект допомагає творчим людям у різний спосіб, у тому числі допомагає їм імітувати стилі відомих художників минулого. Ця здатність наслідувати і відтворювати може бути корисною як при створенні, так і при відновленні твору.

Висновки. Подібно до того, як пензель відноситься до живопису, а фортепіано до музики, роль штучного інтелекту у створенні мистецтва – це лише інструмент для творчості, а не творець. Штучний інтелект надає художнику нові можливості, зокрема, дозволяє стилізувати зображення за допомогою різних фільтрів. І його творчий потенціал залежить від того, як його використовує людина.

УДК 004.77+32.019.5

Дослідження поняття, видів та методів протидії кібербулінгу

Шовкопляс Ю.С., магістрант, yshovkopluas@gmail.com
Мельник С.О., магістрант
Сушков В.В., магістрант
Пономаренко А.С., магістр
Науковий керівник – Якименко М.С., к.ф.-м.н., доц.
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна

Кібербулінг або інтернет-мобінг – це сучасна форма агресії, яка набула поширення з появою мобільних телефонів та Інтернету. Будь-які її форми мають на меті дошкулити, нашкодити чи принизити людину дистанційно, без фізичного насильства (на відміну від булінгу). «Зброєю» булера стають соціальні мережі, форуми, чати, мобільні телефони тощо.

Кібербулінг представляє собою напади з метою завдання психологічної шкоди, які здійснюються через електронну пошту (і-мейл), миттєві повідомлення, переписки в чатах, на веб-сайтах, в соціальних мережах; здійснюється через текстові повідомлення або через зображення (фото, відео); до кібербулінгу відносять також терор за допомогою мобільного телефонного зв'язку.

Відмінності кібербулінгу від булінгу зумовлюються особливостями Інтернет-середовища: анонімністю, можливістю підмінити ідентичність, охоплювати велику аудиторію одночасно, (особливо дієво для поширення пліток), здатність тероризувати та тримати у напрузі жертву будь-де і будь-коли. Якщо у випадку цькування агресора можуть зупинити не скільки моральні аргументи, скільки ймовірні наслідки його дій, то у випадку здійснення кібербулінгу майже неможливо виявити кіберпереслідувача. Також здійснення кібернасильства не передбачає переривання основної діяльності, або відволікання від неї.

На відміну від традиційного цькування, де агресор відомий в обличчя і його можна спробувати уникнути, в кіберпросторі переслідувач часто анонімний. Жертва не знає, чи один переслідувач або їх кілька; чоловік це чи жінка; старий або молодий; чи знайомі вони, чи ні. Така невизначеність посилює тривогу, жертва може починати фантазувати про могутність і силу агресора і в зв'язку з цим – про власну беззахисність і вразливість, спираючись на свій особистий минулий досвід, персональні життєві переживання. Таким чином, кібербулінг може бути особливо небезпечний.

Сучасні дослідники виділяють різні типи поведінки, які характерні для кібербулінгу, зокрема:

Суперечки, або флеймінг (від англ. flaming – пекучий, гарячий, полум'яний) – обмін короткими гнівними і запальними репліками між двома чи більше учасниками, використовуючи комунікаційні технології. Частіш за все розгортається в «публічних» місцях Інтернету, на чатах, форумах, дискусійних групах, інколи перетворюється в затяжну війну. На перший погляд, флеймінг – це боротьба між рівними, але в певних умовах вона теж може перетворитися на нерівноправний психологічний терор. Так, неочікуваний випад може привести жертву до сильних емоційних переживань, особливо на тому проміжку часу, коли вона не знає, хто серед учасників яку займе позицію, наскільки її позиція буде підтримана значущими учасниками.

Нападки, постійні виснажливі атаки (англ. harassment) – найчастіше це залучення повторюваних образливих повідомлень, спрямованих на жертву (наприклад, сотні смс-повідомлень на мобільний телефон, постійні дзвінки) з перевантаженням персональних каналів комунікації. На відміну від перепалки, атаки більш тривалі і односторонні. В чатах чи на форумах нападки теж трапляються, в онлайн-іграх нападки найчастіше використовують гріфери (grieffers) – група гравців, які за мету ставлять не перемогу в певній грі, а руйнацію ігрового досвіду інших учасників.

Обмовлення, зведення наклепів (denigration) – розповсюдження принизливої неправдивої інформації з використанням комп'ютерних технологій. Це можуть бути і текстові повідомлення і фото, і пісні, які змальовують жертву в негативній манері. Жертвами можуть ставати не тільки окремі особи, трапляється розсилка списків, створюються спеціальні «книги для критики» (slam books), в яких розміщуються жарти, де також можуть розміщуватись наклепи, перетворюючи гумор на техніку «списку групи ненависті», з якого вибираються мішені для тренування власної злоби, зливання роздратування, переносу агресії тощо.

Самозванство, втілення в певну особу (impersonation) – переслідувач позиціонує себе як жертву, використовуючи її пароль доступу до її акаунту в соціальних мережах, блогу, пошти, системи миттєвих повідомлень тощо, а потім здійснює негативну комунікацію. Організація «хвилі зворотних зв'язків» відбувається, коли з адреси жертви без її відому відправляються ганебні провокаційні листи її друзям і близьким за адресною книгою, а потім розгублена жертва не очікувано отримує гнівні відповіді. Особливо небезпечним є використання імперсоналізації проти людей, включених до «списку груп ненависті», адже наражає на реальну небезпеку їхнє життя.

Ошуканство, видурювання конфіденційної інформації та її розповсюдження (outing&trickery) – отримання персональної інформації в міжособовій комунікації і передача її (текстів, фото, відео) в публічну зону Інтернету або поштою тим, кому вона не призначалась.

Відчуження (остракізм), ізоляція. Будь-якій людині, особливо в дитинстві, притаманно сприймати себе або в якійсь групі, або поза нею.

Бажання бути включеним у групу виступає мотивом багатьох вчинків підлітків. Виключення із групи сприймається як соціальна смерть. Чим в більшій мірі людина виключається із взаємодії, наприклад, в грі, тим гірше вона себе почуває і тим більше знижується її самооцінка. У віртуальному середовищі виключення також наражає на серйозні емоційні негаразди, аж до повного емоційного руйнування дитини. Онлайн відчуження можливе в будь-яких типах середовищ, де використовується захист паролями, формується список небажаної пошти або список друзів. Кіберостракізм проявляється також через відсутність швидкої відповіді на миттєві повідомлення чи електронні листи.

Кіберпереслідування – це дії з прихованого вистежування переслідуваних і тих, хто пересувається без діла поруч, зазвичай зроблені нишком, анонімно, з метою організації злочинних дій на кшталт спроб згвалтування, фізичного насильства, побиття. Відстежуючи через Інтернет необережних користувачів, злочинець отримує інформацію про час, місце і всі необхідні умови здійснення майбутнього нападу.

Сексуальні посягання – з появою інтернету сексуальні збочення вийшли на новий рівень. Замаскувавшись під фейковим ім'ям чи прикинувшись другом, агресор може запросити жертву на зустріч чи вивідати в неї час та місце, коли вона буде сама.

Хепіслепінг (від англ. happy slapping – щасливе ляскання) – відносно новий вид кібербулінгу, який починався в англійському метро, де підлітки прогулюючись пероном раптом ляскали один одного, в той час як інший учасник знімав цю дію на мобільну камеру. В подальшому за будь-якими відеороликами, в яких записано реальні напади, закріпилась назва хепіслепінг. Відеоролики нападів з метою ґвалтування чи його імітації інколи ще називають хопінг – наскок. Ці відеоролики розміщують в Інтернеті, де його можуть продивлятись тисячі людей.

Якщо людина потерпає від знущань кібербулера, їй часто дуже складно зізнатися у цьому близьким. На це є декілька причин:

– страх, що інші не зрозуміють сенсу проблеми;

– страх бути висміяним через буцімто незначну проблему;

– страх бути покараним за «донос» на булера, особливо, якщо цькування зайшли далеко і людина під контролем агресора;

– страх з'ясувати, що «сам винен» і знущання цілком справедливі.

Причини кібербулінгу є психологічні (у нападників: схильність до агресії, схильність до використання образ, пригнічень, неврівноваженість; у жертв: чутливість, закомплексованість, боязкість, тривожність та пригніченість), соціальні (у нападників: самоствердження через образу іншого; у жертв: соціальна ізольованість, спілкування переважно з дорослими) та культурні (у нападників: низький рівень духовних цінностей; у жертв: гуманізм, високий рівень духовних цінностей).

Корисні правила-поради для профілактики і подолання кібербулінгу, з якими потрібно бути ознайомленими:

– Не виплескувати свій негатив у кіберпростір. Важливо вчитись домовлятись. Не поспішати. Перед тим, як писати і відправляти повідомлення, потрібно заспокоїтись, притишити роздратування, злість, образу, гнів. Емоції – погані порадники, вони минають, а написане і відправлене в Інтернет продовжує нести і помножувати негатив уже без волі і контролю автора.

– Будувати свою власну онлайн-репутацію, не провокуватися ілюзією анонімності. Інтернет – це особливе середовище із своїми правилами поведінки - «нетикетом» (новоутворення від англ. net -мережа і «етикет»). Хоча кібер-простір і надає додаткові можливості відчути свободу і розкутість завдяки анонімності, існують способи довідатись, хто саме відправив повідомлення, хто стоїть за певним ніком (анонімним псевдонімом). І якщо некоректні дії у віртуальному просторі призводять до реальної шкоди – від анонімності залишається лише ілюзія: все тайне стає явним. У віртуальному просторі, як і в реальному, діє золоте правило: стався і дій стосовно інших так, як хотів би, щоб ставились до тебе.

– Поважати факти. Зберігати підтвердження факту нападів. Потрібно розуміти: якщо тебе неприємно вразило якесь повідомлення чи картинка на сайті (фото, відео, будь що), правильна реакція – вимкнути екран (щоб зупинити негативний вплив, але не комп'ютер) і негайно звернутись за порадою чи допомогою.

– Доречно ігнорувати поодинокий негатив. Одноразові образливі повідомлення найкраще ігнорувати, часто в результаті цього кібербуллінг на початковій стадії і зупиняться. Якщо ж реагувати на негативні коментарі, комунікація продовжується. В інших випадках ігнорувати не варто, наприклад, не дивлячись на те, що відправник не відомий, якщо листи систематично містять загрози життю і здоров'ю, варто поставити до відома телефонного або Інтернет-провайдера, інспектора місцевого відділку міліції із роботи з неповнолітніми, для цього й важливо копіювати повідомлення із загрозами. Якщо образлива інформація розміщена на сайті, варто зробити запит адміністратору щодо видалення цієї інформації.

– Можливе тимчасове блокування. Програми, що забезпечують миттєвий обмін повідомленнями, мають можливість тимчасового відключення, можна заблокувати отримання повідомлень з певних адрес, навіть змінити телефонний номер. Пауза в спілкуванні руйнує взаємопідсилювані автоматизми кібербулінгу, особливо якщо він мотивований втечею буллерів від нудьги і не супроводжується буллінгом у реальному житті.

Отже, явище кібербулінгу на сучасному етапі розвитку суспільства досить поширене і його може застосувати будь-яка особа як зброю. Проте необхідно чітко усвідомлювати його психологічний вплив на людське суспільство та ту шкоду, яку це явище приносить суспільству.

УДК 004.738.5: 334.72

Сучасні тенденції застосування Інтернет-технологій у бізнесі

Марченко К.М., к.т.н., доцент, k_marchenko@i.ua
Мельник А.М., студентка, mselnikanna@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна

Інтернет-технології в наш час грають велику роль у формуванні нових способів взаємодії бізнесу з користувачами, партнерами, а також для впровадження шляхів купівлі-продажу товарів.

Інформаційні технології призначені для вирішення конкретних функціональних задач, серед яких чільне місце відводиться обґрунтуванню рішення про нарощування виробничих потужностей підприємства. Тобто збільшення можливого обсягу випуску продукції відповідної якості й асортименту за умови найбільш повного використання сучасних технологій виробництва, підвищення ефективності капіталовкладень і раціональної організації виробництва. ІТ-технології збільшують можливості для реалізації прав на отримання інформації, самореалізацію, здобуття нових знань, проведення дозвілля, розширюють сфери потенційного працевлаштування людей за межами території проживання тощо.

Використання мережі Інтернет допомагає підвищити конкурентоспроможність товарів, розширити ринки збуту, знаходити нових постачальників, посередників та споживачів. Це відповідає бізнес-процесам залучення клієнта, вивчення його потреб, самого акту вчинення правочину (транзакції) і післяпродажного обслуговування, тобто система повинна охоплювати всі без винятку бізнес-процеси взаємодії компанії з клієнтом. Таку систему функціонування може забезпечити використання Інтернет-технологій, що є актуальним для ведення бізнесу і стає невід'ємною частиною функціонування будь-якого підприємства у сучасному світі.

Принцип роботи Інтернет-технологій полягає у моніторингу роботи, та збору інформації для подальшого опрацювання. Збір здійснюється за допомогою датчиків та контролерів, які підключаються на ключові частини обланання.

Найсуттєвішими перевагами Інтернет-технологій для ведення бізнесу є:

1. Нова економічна система: розвиток Інтернету створив новий вид економіки, темпи зростання якої настільки колосальні, що вона уже встигла змінити саме традиційне поняття ведення бізнесу. Сьогодні

економіка являє собою систему, що використовує сучасні технології, і її основу складають підприємства, що активно переводять свій бізнес в Інтернет. Для того, щоб бізнес у Інтернеті був успішним, не обов'язково бути великою компанією.

2. Інтернет є ідеальним середовищем для ведення бізнесу, оскільки всі його користувачі можуть виступати потенційними клієнтами.

3. Створення і підтримка іміджу через web-сайт.

4. Розширення можливостей для клієнта, в першу чергу це забезпечення його необхідною інформацією.

5. Мінімізація витрат.

6. Доступність інформації. Завдяки Інтернету, є можливість донести інформацію до споживача за кілька годин, опублікувавши її на вітрині власного web-сайту.

7. Можливість працювати 24 години на добу.

8. Мінімальні початкові вкладення: для створення web-сайту немає необхідності у великих фінансових витратах, які, крім того, є значно нижчими порівняно з витратами на відкриття звичайного магазину.

9. Можливість глобалізації: суміщення технологій і можливостей Інтернету і рекламної справи відкриває широкі можливості для реклами у мережі.

10. Постійний та оперативний доступ до отримання і пошуку ділової інформації.

11. Можливість одночасної централізації та децентралізації управління об'єктом господарювання.

12. Забезпечення інтерактивного контакту з потенційними партнерами та споживачами.

13. Можливість дистанційного навчання для формування професійної компетентності керівників, управлінського персоналу тощо.

14. Управління розвитком середовища міст і регіонів, а також окремих будинків і помешкань.

Список літератури

1. Заморьова Д.В. Актуальність використання інтернет-технологій в бізнесі / Д.В. Заморьова // Економіка. Менеджмент. Бізнес. – № 2(8). – 2013. – С. 72-79.

2. Сучасні IT-рішення для управління бізнесом – [Електронний ресурс] – Режим доступу: https://www.it.ua/

3. Економічна безпека. Інформаційна безпека підприємства – [Електронний ресурс] – Режим доступу: https://stud.com.ua/21678/ekonomika/informatsiyna_bezpeka_pidpriyemstva

УДК 004.056:330

Забезпечення фінансової безпеки при використанні криптовалюти

Норов А.О., студент, alonzomer13@gmail.com
Науковий керівник – Конопліцька О.К., викладач, ksuha80@gmail.com
Центральноукраїнський національний технічний університет,
м. Кропивницький, Україна

Криптовалюта – це форма оплати, яку можна обміняти в Інтернеті на товари та послуги. Багато компаній випускають власні валюти, які часто називають токенами, і їх можна обмінювати за товар або послугу, які надає компанія. Звичні для нас гроші випускають центральні банки різних країн. На їхню вартість впливають рішення уряду, економіка та міжнародна торгівля.

Криптовалюта є принципово новим інструментом взаєморозрахунків. Для генерації монет, або майнінгу, необхідно розробити певний математичний алгоритм розрахунків. Кожен криптоблок – це послідовність блоків, а кожен із блоків – складна математична формула. Щоб створити нову монету, потрібно згенерувати новий ланцюжок блоків транзакцій. Криптовалюта випускається безпосередньо в мережі Інтернет і жодним чином не пов'язана з жодною валютою чи національною валютною системою. На даний момент кількість видів криптовалют у світі наближається до тисячі, і ринок продовжує зростати. Біткойн є першою і найвідомішою з багатьох інших віртуальних електронних валют.

Криптовалюти працюють за допомогою технології, яка називається блокчейн. Блокчейн – це повна і незмінна історія транзакцій користувачів, з якою погоджується кожен, хто є учасником. Криптогаманці автоматично оновлюються в регулярні проміжки часу, приймається спільнотою як факт і зберігається на комп'ютері кожного учасника.

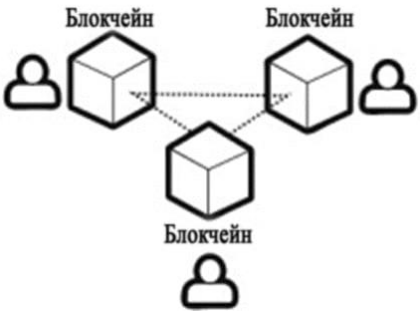


Рис. 1. Схема системи блокчейн

Технологія блокчейн забезпечує інфраструктуру для існування цифрової валюти без центрального банку. Оскільки під час реєстрації не існує централізованої бази даних, замість того, щоб вибирати обліковий запис, користувач просто отримує випадкове число (зване закритим ключем або початковим кодом), яке представляє собою рядок літер і цифр або набір випадкових слів.

У випадку біткойна, який є найвідомішою криптовалютою, користувач отримує випадкове число з 2^{256} можливостей. Це число з цифрою 1, за якою слідують 80 нулів:

100.000.000.000.000.000.000.000.000.000.000.000.000.000.
000.000.000.000.000.000.000.000.000.000.000.000.000.000

У криптовалютах не можна зберігати монети. Монети завжди записуються в блокчейн і ніколи не відходять звідти. Ви використовуєте так звані гаманці для зберігання приватного ключа, який дозволяє надсилати монети, підписавши криптографічну функцію в блокчейні.

Типи гаманців для криптовалюти:

1. Paper-wallet – приватні ключі просто створювалися генератором випадкових чисел, а потім записувалися на аркуші паперу.

2. Mind-wallet – повний ключ запам’ятовується і ніде не записується.

3. Soft-wallet – приватний ключ кодується паролем на комп’ютері або у програмі.

4. Hard wallet – приватний ключ на USB-накопичувачі, але до нього неможливо отримати доступ з комп’ютера.

5. Біржі – обмінюють криптовалюти між собою або на фіатні валюти.

Висновки. Криптовалюта – додаток, що використовує технології блокчейн, за допомогою яких історія транзакцій і, отже, точна кількість валюти, якою володіє кожен, зберігається через блокчейн. Блокчейн – незмінна історія транзакцій децентралізованої спільноти. Шифрування приватним ключем є оригінальним типом шифрування. Криптогаманець зберігає приватні та відкриті ключі користувача. Це дозволяє та полегшує відправку та отримання монет. Крім того криптогаманець також діє як особиста книга операцій.

Список літератури

1. Cryptocurrencies simply explained - by Co-Founder Dr. Julian Hosp: Bitcoin, Ethereum, Blockchain, ICOs, Decentralization, Mining & Co Paperback – December 21, 2017. – 176 p.

2. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. – 9 p.

3. The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order (PICADOR USA) Paperback – January 12, 2016.- 384 p.

УДК 004.9+658.5

Система підтримки прийняття рішень в питаннях заміни обладнання на підприємстві

Прокопенко Є.С., студент, prokopenko19712002@gmail.com
Науковий керівник – Улічев О.С., к.т.н., askin79@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна

Завданням дослідження є реалізація програмного комплексу на основі оптимізації розв'язку задачі заміни обладнання. Така задача особливо гостро стоїть, наприклад, для автотранспортних підприємств, які мають дуже розрізнений транспортний парк: машини куплені в різні часи, частина машин куплена не новими, транспортні одиниці істотно відрізняються як за ціною, так і за бюджетом обслуговування. Враховуючи експлуатаційне зношення машин, періодично виникає задача оцінки та вибору – які машини підлягають заміні, а які ще доцільно ремонтувати і продовжувати експлуатацію. Оптимізація окремих процесів – необхідна умова ефективного управління будь-якої комерційної структури. Найчастіше керівник (або відповідальна особа) робить це на інтуїтивному рівні. Однак, вирішення даної проблеми з використанням математичного апарату, реалізованого у вигляді програмної системи, дозволяє звести до мінімуму час аналізу, втрати, помилки, ризики.

З часом зростають виробничі витрати на поточний та капітальний ремонт і обслуговування, знижуються продуктивність праці, тощо. Тому у певний час виникає потреба заміни старого обладнання на нове. Критерієм оптимальності є, як правило, прибуток від експлуатації обладнання (задача максимізації) або сумарні витрати на експлуатацію протягом запланованого періоду (завдання мінімізації). Задача полягає у знаходженні плану-графіка заміни старого обладнання на нове протягом планованого періоду експлуатації. При побудові моделі прийнято вважати, що рішення про заміну виноситься на початку кожного проміжку експлуатації (наприклад, на початку року) і, що обладнання можна використовувати необмежено довго.

Для визначення оптимальної стратегії заміни обладнання треба заздалегідь знати певну інформацію про нього: його вік на початок періоду експлуатації, бажаний період експлуатації, прибуток і витрати на одиницю обладнання, ціну нового обладнання.

Для опису моделі введемо такі позначення:

N – кількість років планування заміни обладнання;

T – часовий параметр;

Y_t – змінна – вік обладнання у t-ий рік планування;

F – цільова функція – загальний дохід від використання обладнання під час планування;

$f(t)$ – дохід від використання обладнання, вік якого t років;

R_t – вартість продукції, виробленої протягом року одиниці устаткування, вік якого t років;

U_i – витрати на обслуговування одиниці обладнання протягом одного t-го року;

$s(t)$ – залишкова вартість обладнання, вік якого t років;

P – вартість нового обладнання;

$f_T(t)$ – максимальний прибуток у T років, що залишилися від використання обладнання, вік якого t років.

Математична модель

Математична модель завдання заміни обладнання має вигляд функціонального рівняння:

$$F = \sum_{t=1}^{T} f(Y_t) \to \max \tag{1}$$

$$\begin{cases} Y_0 \geq 0 \\ Y_t \in \{0;\ Y_{t-1} + 1\} \forall t \in N_T \end{cases} \tag{2}$$

$$\begin{cases} f_1 = \max \begin{cases} R_1(t) - U_1(t) \\ R_1(0) - U_1(0) + s_1(t) - P \end{cases} \\ f_T = \max \begin{cases} R_T(t) - U_T(t) + f_{T-1}(t+1) \\ R_T(0) - U_T(0) + s_T(t) - P + f_{T-1}(1) \end{cases} \end{cases}, T \in N \tag{3}$$

Результатом роботи математичної моделі стає таблиця TxT, згідно якої буде прийнято рішення про заміну обладнання. Автоматизація аналізу можлива за умови використання програмного комплексу прийняття рішень в питаннях заміни обладнання.

Висновки. Вибір оптимального часу заміни обладнання допоможе максимізувати прибуток будь-якого підприємства, але інтуїтивне прийняття рішення, що базується на особистому досвіді керівника займає багато часу та може призводити до помилок, що, в свою чергу, призводять до економічних втрат. Для вирішення цієї проблеми пропонується використовувати програмний комплекс підтримки прийняття рішень в питаннях заміни обладнання, що базується на розглянутій вище моделі.

Список літератури

1. Шумейко О. А. Динамічна модель оптимального розподілу інвестицій при замінні обладнання. Економіко-математичне моделювання соціально-економічних систем. 2020. №17. С. 255−267.

2. Андрейцев А. Ю., Вяля Ю. Э., Гейлик А. В., Ляшко О. В., Смирнов И. В. Задача о замене оборудования: некоторые специальные случаи. Вісник Херсонського національного технічного університету. 2019. №2(69). С. 153–159.

УДК 004.9+519.872

Методи комп'ютерного імітаційного моделювання систем масового обслуговування

Ткачук Р.О., аспірант, ro.tkachuk@outlook.com
Шуліка Я.П., аспірант, yar.shulika@gmail.com
Рудяк Р.А., аспірант, rudiak.ra@gmail.com
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна

Імітаційне моделювання – метод дослідження, при якому вивчаєма система замінюється моделлю з достатньою точністю опису функціонування реальної системи, і над моделлю проводяться експерименти з метою отримання шуканої інформації про цю систему [1].

До імітаційного моделювання вдаються, якщо:

– дорого чи неможливо експериментувати на реальному об'єкті;

– неможливо побудувати аналітичну модель: у системі є час, причинно-наслідкові зв'язки, нелінійні процеси, стохастичні змінні тощо.

Методи імітаційного моделювання можна розділити на групи [1-2]:

– *Дискретно-подійне моделювання*. Пропонує абстрагуватися від безперервної природи подій і розглядати лише основні події моделі, що моделюється, такі, як: «очікування», «обробка замовлення», «рух з вантажем» тощо.

– *Безперервне імітаційне моделювання*. Створюється шляхом задання рівнянь для сукупності змінних станів, динамічна поведінка яких імітує реальну систему. Моделі часто визначаються в термінах похідних змінних стану.

– *Системна динаміка.* Для досліджуваної системи будуються графічні діаграми причинно-наслідкових зв'язків та глобальних впливів одних параметрів на інші в часі, а потім створена модель імітується на ЕОМ.

– *Агентне моделювання*. Дослідження децентралізованих систем, динаміка функціонування яких визначається не глобальними правилами та законами, а результатом індивідуальної активності елементів системи.

– *Статистичне імітаційне моделювання*. Дозволяє відтворювати на ЕОМ функціонування складних випадкових процесів.

Імітаційна модель відтворює поведінку системи, що моделюється, у часі. При розробці практично будь-якої імітаційної моделі необхідно оперувати трьома увидами часу:

– *реальний час*, у якому існує система, що моделюється;

– *модельний (системний) час*, в масштабі якого відбувається робота моделі системи;

– *машинний час*, що відображає витрати часу ЕОМ на проведення імітації системи.

За допомогою використання модельного часу вирішуються такі задачі:
– відображається перехід імітації системи з одного стану в інший;
– здійснюється синхронізація роботи елементів моделі системи;
– змінюється масштаб часу функціонування досліджуваної системи;
– виконується управління ходом модельного експерименту;
– моделюється квазіпаралельна реалізація подій у моделі.

У процесі імітаційного моделювання (рис. 1) дослідник має справу з чотирма основними елементами: реальна система, логіко-математична модель модельованого об'єкту, імітаційна модель та ЕОМ, на якій здійснюється імітація – спрямований обчислювальний експеримент [3].

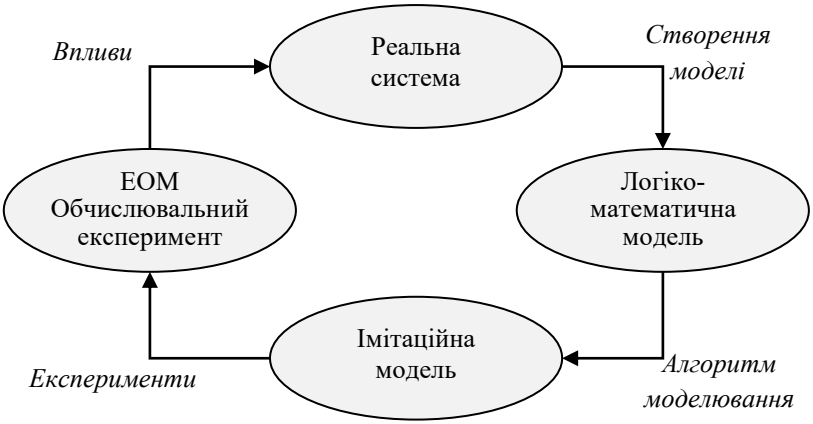


Рис. 1. Процес імітаційного дослідження системи

Дослідник вивчає реальну систему та розробляє її логіко-математичну модель. Потім створює моделюючий алгоритм та використовує його для проведення обчислювальних експериментів на ЕОМ.

Список літератури

1. Строгалев В. П., Толкачева И. О. Имитационное моделирование. – МГТУ им. Баумана, 2008. – С. 697-737.

2. Borshchev A., Filippov A. “From System Dynamics and Discrete Event to Practical Agent-Based Modeling: Reasons, Techniques, Tools”, The 22nd International Conference of the System Dynamics Society, July 25 - 29, 2004, Oxford, England

3. Лычкина Н.Н. Имитационное моделирование экономических процесов: учебное пособие для слушателей программы eMBI. – Академия АйТи. – 2005.

Все буде Україна!

НАУКОВЕ ВИДАННЯ

ЗБІРНИК ТЕЗ ДОПОВІДЕЙ

І МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

“ЦИФРОВА ТРАНСФОРМАЦІЯ СУСПІЛЬСТВА”

DIGITAL SOCIETY – 2022

21-22 квітня 2022 року

Тези доповідей надруковано в авторській редакції.
Відповідальність за зміст несуть автори.

Відповідальна за випуск: Мелешко Є.В.

Дизайн обкладинки: Мелешко Є.В., Графенюк В.О.

Підписано до друку 25.04.2022
Тираж 50 прим.

©Кафедра кібербезпеки та програмного забезпечення ЦНТУ,
м.Кропивницький, пр.Університетський, 8.
Тел. (0522) 39-04-49
