МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ДНІПРОВСЬКА ПОЛІТЕХНІКА»

РАДА МОЛОДИХ ВЧЕНИХ НТУ «ДП»

РАДА МОЛОДИХ ВЧЕНИХ ДНІПРОПЕТРОВСЬКОЇ ОБЛАСТІ

ДЕСЯТА ЮВІЛЕЙНА ВСЕУКРАЇНСЬКА
НАУКОВО-ТЕХНІЧНА КОНФЕРЕНЦІЯ
СТУДЕНТІВ, АСПІРАНТІВ І
МОЛОДИХ ВЧЕНИХ,
ПРИСВЯЧЕНА 120-РІЧЧЮ НТУ "ДП"

"НАУКОВА ВЕСНА"

Секція 12 – Автоматизація та інформаційні технології

Том 12

25-26 квітня 2019 р.

Дніпро – 2019

Голова оргкомітету – Бешта Олександр Степанович – д.т.н., професор, проректор з наукової роботи.

Заступник голови:
Нікітенко Ігор Святославович – к.г.н., доцент, заступник начальника НДЧ.

Відповідальний секретар:
Деревягіна Наталія Іванівна – к.т.н., доцент кафедри гідрогеології та інженерної геології, голова Ради молодих вчених НТУ «ДП».

Секція 12 – Автоматизація та інформаційні технології

Керівник секції – Мещеряков Леонід Іванович – д.т.н, професор кафедри програмного забезпечення комп'ютерних систем.

Секретар – Мєшков Вадим Ігорович, старший викладач кафедри безпеки інформації та телекомунікацій.

ЗМІСТ

УДК 004.491.22

Кабанов А.О. студент гр. УБіт-15-1
Науковий керівник: Ковальова Ю.В., асистент кафедри безпеки інформації та телекомунікацій
(*Національний технічний університет "Дніпровська політехніка", м. Дніпро, Україна*)

ВПЛИВ КІБЕРАТАК НА ФУНКЦІОНУВАННЯ ДЕРЖАВНИХ УСТАНОВ

Анотація: Сучасний світ повністю перейшов в інформаційний простір, де IT індустрія повністю поглинула всі сфери життєдіяльності. Інформація є основним двигуном прогресу і від її надання залежить загальна картина світу. У зв'язку з цим, саме інформаційне поле є ключовим об'єктом для впливу ззовні. З огляду на тенденції розвитку інформаційно-комп'ютерної сфери саме попередження кібератак є пріоритетним напрямком для національної безпеки країни.

Статтею 1 Закону України «Про основні засади забезпечення кібербезпеки України» [1] визначено, що під кібератакою розуміється спрямовані дії в кіберпросторі, які здійснюються із застосуванням електронних пристроїв та направлені на досягнення певних цілей: порушення цілісності, доступності та конфіденційності електронних інформаційних ресурсів, порушення безпеки функціонування технологічних систем та ін. Цікаво, що цей закон вступив в дію після початку масових кібератак на території України.

Існують різні цілі і різні способи проведення кібератак. Найбільш небезпечними для державних і комерційних установ є DoS (відмова в обслуговуванні) і DDoS (розподілений DoS) мережеві атаки. Ці атаки спрямовані на те, щоб зробити неможливим обслуговування системою справжніх користувачів.

DoS-атака може призвести до великих збитків компанії, діяльність яких напряму залежить від роботи з клієнтами. Найбільш розповсюдженим методом проведення є наведення на об’єкт атаки різними протоколами, обробка яких змушує систему використовувати всі наявні обчислювальні ресурси.

DDoS-атака використовує такий самий метод, тільки в процесі атаки залучений не один комп’ютер, а множина. Архітектура DDoS-атаки зазвичай складається з 3 рівнів. Керує всіма діями 1 комп’ютер, який знаходиться на вершині так званої «піраміди». З нього проводиться несанкціоноване встановлення програми (під назвою «майстер») на декілька комп’ютерів, які працюють в Інтернеті. Несанкціоноване встановлення «майстра» відбувається через недосконалість ПЗ (наприклад за допомогою комп’ютерного хробака).

Комп’ютери, які вже заразилися цією програмою, з її допомогою, заражають програмою «демон» десятки чи сотні комп’ютерів, з яких і буде вестись DDoS-атака.

Принцип роботи цієї кібератаки полягає в наступному: з комп’ютера першого рівня подається команда «майстрам». Від них ця команда транслюється «демонам» і ті одночасно атакують заздалегідь обраний об’єкт.

Так, наприклад, одна з перших кібератак на українські державні установи відбулася в травні 2014 року на сервер ЦВК під час президентських виборів. Наслідки виявилися вагомими: DDoS-атака призвела до злому сайту ЦВК і публікуванню помилкових результатів голосування. Отримані дані одразу почали озвучувати в новинах північної країни-сусіда.

В грудні 2016 року відбулася хакерська атака на телекомунікаційні мережі Міністерства фінансів, Пенсійного фонду та Державного казначейства України. В результаті цих атак з ладу вийшов ряд комп’ютерів, а також були знищені критично важливі бази даних, які спричинили затримку бюджетних виплат загальною сумою на сотні мільйонів гривень.

Невід'ємною частиною європейської країни є функціонуюча інфраструктура. В грудні 2016 року була проведена кібератака на сайт «Укрзалізниці». Внаслідок цієї атаки робота сайту була заблокована протягом дня.

Хакерська атака червня 2017 року запам'яталася керівникам державних та комерційних установ однією з наймасштабніших. Так, 27 червня 2017 року через розповсюдження оновлення для програми «M.E.Doc» (ПЗ для подання бухгалтерської звітності в Україні) відбулося зараження вірусом Petya.A. Вірус був шифрувальником, який потрапляв через вразливість в протоколі SMB, закріплявся в системі, зашифровував вміст жорсткого диску, видаляв оригінальні файли та примусово перезавантажував комп'ютер. Після перезавантаження користувачі бачили на екрані вимагання перерахувати на рахунок біткоїн. Як пізніше стало відомо, в результаті цих дій було заблоковано функціонування ряд державних та комерційних установ таких, як «Укрпошта», «Укртелеком», «Укрзалізниця», «Нова пошта», а також зупинилась робота офіційних сайтів Кабінету Міністрів України, Київської та Львівської міської ради, Державного спеціального зв'язку та захисту інформації України.

На сьогоднішній день відповідальність за проведення кібератаки регламентує стаття 361 Кримінального кодексу України [2]. Максимальний строк обмеження волі – 5 років, при повторній спробі – позбавлення волі строком до 6 років.

Перелік посилань

1. Закон України «Про основні засади забезпечення кібербезпеки України»» від 21.06.2018 №2469-VIII – стаття 1
2. Кримінальний кодекс України від 05.04.2001 № 2341-III – стаття 361

УДК 303.73

Зінов'єва О.В. студентка гр. САіт-15-1
Науковий керівник: Купенко О.П., д.ф.-м.н., професор кафедри системного аналізу і управління
(Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна)

АНАЛІЗ ПОВЕДІНКОВИХ ДАНИХ ОНЛАЙН-ІГОР ЗА ДОПОМОГОЮ АЛГОРИТМІВ КЛАСТЕРИЗАЦІЇ

На меті стоїть задача про прийняття рішення щодо розвитку онлайн-гри на основі з'ясування того, як гравці поводять себе після проходження навчання. Компанія-власник гри хоче збільшити свої прибутки, для цього необхідно виявити за які додаткові функції користувачі найчастіше готові заплатити. Аналіз поведінкових даних буде проведено за допомогою двох алгоритмів кластеризації.

При розробці free-to-play ігор важливим для успіху є аналіз поведінки гравців і постійне оновлення ігрового функціоналу на основі статистики. Основний інструмент, який допомагає перетворювати дані в інформацію - це сегментація гравців. Сегментація - це виділення груп користувачів, які характеризуються будь-якою спільної особливістю, і робота з показниками додатка усередині цих груп. Тобто виділення сегмента - це створення пошукового фільтра, який дозволяє знайти всіх користувачів із заданими параметрами[1].

Для реалізації мети роботи було сформовано початкову вибірку з поведінковими даними користувачів за декілька днів, що містить інформацію про шість параметрів:

- ID гравця;
- кількість побудованих будинків;
- кількість оновлених удосконалених будинків;
- кількість проведених боїв гравця проти іншого реального користувача (pvp);
- кількість проведених боїв гравця проти оточення (pve);
- використання додаткових військ.

Наведені вище дані щодо поведінки гравців будуть використані у програмах, основаних на алгоритмах кластеризації. Кластери, отримані у результаті роботи програм, допоможуть виявити основні розбіжності у поведінці виокремлених груп користувачів під час онлайн-гри. Це у свою чергу надасть змогу сформувати рекомендації щодо додаткового функціонала або виправлення вже існуючого, який буде направлений на певні групи користувачів.

Кластерний аналіз є задачею ділення обраної вибірки об'єктів на підмножини (кластери). Data clustering відноситься до методу машинного навчання без вчителя, він дозволяє досліджувати дані та може визначати групи гравців подібної поведінки або виявляти функції (риси), що обумовлюють таку поведінку людей у грі [2]. Перелік прикладних областей, де застосовується кластеризація, широкий: сегментація зображень, маркетинг, боротьба із шахрайством, прогнозування, аналіз текстів і багато інших. На сучасному етапі кластеризація часто виступає першим кроком при аналізі даних, після виділення схожих груп застосовуються інші методи, для кожної групи будується окрема модель.

Для застосування кластеризації спочатку було підготовлено дані, які представлені лише у числовому форматі. Далі було обрано два алгоритми: перший алгоритм CURE (Clustering Using Representatives) є ієрархічним методом, тобто кластеризація виконується шляхом послідовного об'єднання менших кластерів у великі або поділом великих кластерів на менші, а другий – метод нечіткої кластеризації С-середніх, що також має назви fuzzy clustering, soft k-means, c-means.

Алгоритм CURE (кластеризація з використанням представників) виконує ієрархічну кластеризацію з використанням набору визначальних точок для призначення об'єкта в кластер.

Застосовується для дуже великих наборів числових даних (баз даних), але ефективний лише для даних низької розмірності. Даний алгоритм реалізує кластеризацію на високому рівні навіть при наявності викидів, виділяє кластери складної форми і різних розмірів, що є головними його перевагами у порівнянні з алгоритмом k-середніх. У CURE є необхідність в завданні порогових значень і кількості кластерів. При застосуванні цього алгоритму будується дерево кластерів, що складається з кожного рядка вхідного набору даних. Для кожного кластеру розраховують відстані до найближчих сусідів. Далі ближні кластери зливаються в один, що отримує усі точки, вхідних до нього даних. Для розрахунку відстані від новоствореного кластеру до інших кластери діляться на дві групи: перша група - кластери, у яких найближчими вважаються сусіди, що входять в новостворений кластер, друга група – усі інші кластери. Після цього відбувається процес оновлення об’єднаного кластера новими представниками за певними правилами, доки не буде отримано необхідну кількість кластерів. Зазвичай, даному методу необхідно до десяти сканувань бази даних для отримання фінальної кластеризації.

Метод нечіткої кластеризації C-середніх можна розглядати як вдосконалений метод k-середніх, при якому для кожного елемента з розглянутої множини розраховується ступінь його приналежності кожному з кластерів. Неієрархічні алгоритми засновано на оптимізації деякої цільової функції, в даному методі в якості цільової функції використовують суму квадратів зважених відхилень координат об'єктів від центрів шуканих кластерів. Вхідними даними для використання метода є число кластерів та ступінь нечіткості, у результаті ж отримуємо інформацію про центри кластерів та матрицю належності. Тобто буде відома ймовірність належності одного об’єкта до кожного з кластерів. Використання методів глобального пошуку (генетичні алгоритми) значно збільшить обчислювальну складність алгоритму. Алгоритм c-means має обмежене застосування через неможливість коректного розбиття на кластери, в разі коли кластери мають різну дисперсію за різними розмірностями елементів (наприклад, кластер має форму еліпса).

Результатом кластеризації є групи об'єктів, об'єднані за певною характеристикою чи характеристиками. Необхідно провести перевірку стійкості кластеризації, тобто її достовірність. Для цього застосовують інші методи кластеризації, якщо при порівнянні результатів двох різних методів групи збігаються більше, ніж на 70 % (понад 2/3 збігів), то кластерне рішення приймається.

Перелік посилань

1. Аналіз статистики у free-to-play іграх: інструменти аналітика: стаття від компанії Alawar Entertainment// [Електронний ресурс]: доступ за URL: https://habr.com/ru/company/alawar/blog/162739/ .

2. Кластерний аналіз: стаття на Вікіпедії// [Електронний ресурс]: доступ за URL: https://uk.wikipedia.org/wiki/Кластерний_аналіз.

УДК 004.946.5.056:366.6

Бардак І.А. студент гр. УБіт-15-1
Науковий керівник: Галушко С.О. старший викладач кафедри безпеки інформації
(*Національний технічний університет "Дніпровська політехніка", м. Дніпро, Україна*)

МОЖЛИВОСТІ ТЕХНОЛОГІЇ БЛОКЧЕЙН

Аннотація: У статті розкрита важливість та необхідність застосування технології блокчейн . Вивчаються засоби застосування даної технології у різних сферах життя суспільства. Підсумком роботи являється перелік переваг використання даного функціоналу.

Технологія блокчейн, яка базується на криптовалюті Bitcoin, була створена, як єдиний цифровий реєстр транзакцій. Блокчейн не має єдиного центру керування ним, а підтримкою роботоздатності займаються усі учасники мережі. Принцип умов роботи даної технології заключається у тому, що процес шифрування, котрий також має назву хешування (на базі алгоритму SHA-256), виконується великою кількістю обчислюваних машин. Після проведення розрахунків, блоку надається унікальний цифровий підпис, котрий фіксується у єдиній базі даних. Це являється однією з переваг даної технології, тому що після оновлення реєстру блок не підлягає ніяким змінам, що є гарантією безпеки. Головним аспектом технології блокчейн являється формування умови довіри у тому середовищі, у котрому ця умова може бути не виконана.

В останній час спостерігається стрімкий розвиток введення інноваційних рішень у всі сфери суспільства. Одним із таких перспективних рішень являється роботи певних сфер (медична, соціально-страхова і т.д.) на технології блокчейн.

Медицина:

Розподільчий реєстр відіграє роль єдиної бази даних для внесення медичних записів. Коли, наприклад, до медичної карти пацієнту вносяться зміни, даний запис переміщується до мережі. Такий рівень прозорості здатний поліпшити процес отримання іншими лікарями потрібної інформації щодо конкретного пацієнту. Система надає можливість отримувати більш точні діагнози із урахуванням задокументованої інформації про історію хвороби.

Засоби електронного голосування:

На даний момент йде розробка безпечної та прозорої платформи «FollowingMyVvote» анонімних онлайн голосувань. Ресурс використовує технологію блокчейн та еліптичну криптографію, щоб гарантувати точність та достовірність голосувань.

Нерухомість:

Сервіс «UBITQUITY» надає рієлторським, іпотечним та перевіряючим компаніям послуги власної платформи, котра базується на технології блокчейн для ведення записів щодо майна та пов’язаних із ним прав власності. Платформа позиціонує себе, як альтернатива паперовій системі ведення угод, котра прискорює процес юридичного аудиту нерухомості та підвищення прозорості та якості складених угод.

Блокчейн, технологія якого здатна оптимізувати бізнес-процеси, необхідно задіяти у тих сферах, де частіше за все необхідно працювати з посередниками, послуги яких являються платними та мають необхідність опрацювувати дані, які в свою чергу мають високий рівень цінності або взаємодіяти із великою кількістю незалежних учасників.

Перелік посилань:

1. Енциклопедія термінів-Режим доступу: https://en.bitcoin.it/wiki/Main_Page
2. Дешшер Д. Мета технології блокчейну/ Д.Дешшер //Основи блокчейну-2016-с.42

УДК 004.775+91

Мацайтіс Д.І. студент гр. УБіт-15-1
Науковий керівник: Тимофєєв Д.С., ст. викл. кафедри безпеки інформації та телекомунікацій
(*Національний технічний університет "Дніпровська політехніка", м. Дніпро, Україна*)

РІШЕННЯ ПО ЕЛЕКТРОННОМУ УРЯДУВАННЮ. АНАЛІЗ І ПЕРСПЕКТИВИ

Анотація: У статті розглядається важливість та доцільність електронного урядування. Пояснюється різниця між регіональним на місцевим Е-урядуванням. Проведено короткий аналіз дослідження ООН щодо ситуації з Е-урядуванням у всьому світі та місце України у цьому звіті. Розглянуто найважливіші на даний момент проблеми та важкий але перспективний шлях у досягненні надійної та сучасної системи Е-урядування.

Одним із пріоритетів України є розвиток інформаційного суспільства, його орієнтація на інтереси громадян, їх потреби та пропозиції. Систематичне вдосконалення потребує значних ресурсів, залучення міжнародного досвіду та комплексного аналізу існуючої ситуації у сфері.

Електронне урядування - форма організації державного управління, яка сприяє ефективності та прозорості діяльності органів державної влади та місцевого самоврядування з використанням сучасних технологій.

Упровадження е-урядування на місцевому та регіональному рівнях передбачає появу нових форм діяльності місцевих органів державної влади та органів місцевого самоврядування, їх взаємодію між собою, з громадянами та бізнесом шляхом надання доступу до публічної інформації, державних інформаційних ресурсів, електронних адміністративних послуг, залучення громадян до процесу вироблення і прийняття управлінських рішень в містах та регіонах.

Під «електронним регіоном» мається на увазі інфраструктура автоматизованої інформаційної системи взаємодії органів державної влади та органів місцевого самоврядування області з громадянами та суб'єктами господарювання на основі активного використання інформаційно-комунікаційних технологій для досягнення бажаних європейських стандартів якості надання електронних адміністративних послуг, відкритості та прозорості влади для громадян та суб'єктів господарювання.

Згідно досліджень ООН (United Nations E-government Survey 2016) щодо розвитку електронного урядування (E-Government Development Index) Україна посіла 62 місце серед 193 країн. Згодом у 2018 році зайняла 82 місце (загальна група індексування – високий рівень) - піднявши індекс розвитку електронного урядування та здавши позиції в якості онлайн сервісів.

Основні проблеми електронного урядування в Україні:

-відсутність ключових функцій, таких як можливість відслідкувати опрацювання Е-звернення та відсутність он-лайн платформи для зв'язку зі службою міста.

-низька якість, ефективність та результативність реалізації проектів і завдань у зазначеній сфері.

-недостатній рівень готовності державних службовців та працівників органів місцевого самоврядування, фізичних та юридичних осіб до запровадження і використання інструментів електронного урядування.

При подальшому розвитку Е-урядування маємо перспективу насамперед у зацікавленості влади та все більшій інтеграції зарубіжного досвіду, а саме: id – картки, відносна доступність та якісне оформлення закордонного паспорту.

До 2020 року Державне агентство з питань електронного урядування склало план перспективного розвитку, найголовнішим з якого на мою думку е реалізація Міжнародної хартії

відкритих даних в Україні на період до 2020 року Досягти успіху у короткі терміни неможливо – інші економічні та політичні умови, специфіку бюрократії та корупції. Важливим у даній ситуації є бажання держави до розвитку даної технології та інтеграція і адаптація міжнародних практик та досвіду у цій сфері.

Перелік посилань:

1.Електронне урядування (термін) - https://zakon.rada.gov.ua/laws/term/8419

2.Розвиток електронного урядування на місцевому та регіональному рівнях – Електронне урядування та електронна демократія (Навчальний посібник, частина 7)

3.Моніторинг впровадження інструментів електронного урядування як основи надання адміністративних послуг в електронному вигляді - http://center.kr-admin.gov.ua/100.pdf

4.Електронний уряд – звіт Об'єднаних Націй (United Nations E – Government Survey)
https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2018

5.Розпорядження від 22 серпня 2018 р. № 617-р Кабінету Міністрів України – "Про затвердження плану заходів з реалізації Концепції розвитку електронного урядування в Україні".

УДК 004.415.5

Бобошко М.А. студентка гр. УБіт-15-1
Науковий керівник: Галушко С.О. старший викладач кафедри безпеки інформації та телекомунікацій
(Національний технічний університет "Дніпровська політехніка", м. Дніпро, Україна)

БЕЗПЕКА DOCKER КОНТЕЙНЕРІВ

Анотація: Мета та головна тема статті розповісти про безпеку при використанні приладу автоматизації налаштування кластерів, за допомогою docker. Показати базові вразливості, а також методології протидії ним. Головною ідеєю є показання та надання практичних навичок для забезпечення безпеки кластерів на docker.

Зі стрімким розвитком IT-індустрії, людям що не пов’язані з нею користуватися комп’ютером становиться все важче и важче. Здавалось би це проблема тих хто не має достатніх навичок та знань у цій сфері але психологія людина така, що людині легше поскаржитись та перекласти проблему на інші плечі. Саме для подолання непорозумінь та полегшення праці програмістів була створена програма Docker.

Docker вирішує такі питання як передача готового продукту користувачу, якому не потрібно притримуватися правил встановлення програми, цей процес повністю автоматизован[1]. В той самий час Docker дозволяє програмісту автоматизувати свою роботу, наприклад йому потрібно підняти 50 однакових серверів, то за допомогою Docker йому не потрібно робити однакову монотонну роботу.

Головна особливість Docker полягає в тому, що для роботи програми потрібно лише один раз налаштувати у Docker оточення та залежності, а потім можна тиражувати на будь-які пристрої та системи. Для бази на якій буде працювати програма потрібен образ будь то Unix подібні системи, або усім добре відомі версії Windows.

Проблема полягає в тому, що образи можна отримати через інтернет у відкритому доступі, тому дізнатися був використаний безпечний чи небезпечний образ не можливо. Вирішенням є практика обирати те, що є популярним, закритим або перевіреним (trusted repositories)[2].

Ще один інструмент, яким варто скористатися - Docker Content Trust. Це нова функція, доступна в Docker Engine 1.8. Вона дозволяє верифікувати власника образу.

Наступною загрозою є звичні лінощі, нащо змінювати конфігурацію якщо усе добре працює. Але як можна з настройками по defaulty гарантувати повну безпеку кінцевого продукту?

Оскількі Docker така ж складна як і багатофункціональна програма усі вразливості неможливо перерахувати але вони майже всі відомі його творцям і Docker постійно вдосконалюється. Docker створювався з урахуванням вимог безпеки, і деякі його особливості допомагають в її забезпеченні.

Однак не варто забувати про обережність, оскільки тут немає іншого шляху, окрім як постійно стежити за сучасними тенденціями і застосовувати кращі практики, які склалися в цій сфері[3].

Із цього можна зробити висновок, що найкраще всього буде використання специфічних для контейнерів інструментів забезпечення безпеки, які допомагають боротися з вразливостями та загрозами, пов'язаними з використанням Docker[4].

Перелік посилань

1. Р. Моисеев (2017) Рекомендации по безопасности при работе с Docker Електронний ресурс https://habr.com/ru/post/333402/
2. Southbridge (2017) Проблемы безопасности Docker Електронний ресурс https://habr.com/ru/company/southbridge/blog/339126/

3. Amit Sharma (2018) Five Docker Security Best Practices Електронний ресурс https://thenewstack.io/5-docker-security-best-practices/
4. Офіційна документація Docker. (2019) Docker security Електронний ресурс https://docs.docker.com/engine/security/security/

УДК 004.771

Палій В.В. студент гр. УБіт-15-1
Науковий керівник: Галушко С.О. старший викладач кафедри безпеки інформації та телекомунікацій
(*Національний технічний університет "Дніпровська політехніка", м. Дніпро, Україна*)

ВРАЗЛИВОСТІ МОВИ ПРОГРАМУВАННЯ НА ПРИКЛАДІ PYTHON

Анотація. Ключовою темою статті є найчастіші вразливості в сфері розробки програмного забезпечення, наведення їх прикладів, методів реалізації, методи протидіяння вразливостям та загрозам, що можуть виникнути. Стаття має за мету попередити появлення базових вразливостей при розробці коду.

У зв’язку з тенденцією останніх двох років, у сфері розвитку штучного інтелекту та машинного навчання, стали потрібні у великій кількості розробники. Також ця тенденція схожа і для створення WEB сервісів. Але збільшення кількості коду написаному на цій мові може приводити до появи сервісів з більшою кількістю вразливостей. Основною ідеєю буде розповісти про найчастіші та найпопулярніші вразливості на прикладі мови Python.

Найбільш розповсюдженою вразливістю, як і в усіх інших мовах, є мовна ін’єкція. Python, як і всі мови, що працюють з WEB та SQL, вразлив до SQL ін’єкцій. Вони використовуються для маніпулювання даних у базі. Для запобігання слід використовувати ORM, а також фреймворки мови. Другим типом є командна ін’єкція – це вид атаки, цілю якої є виконання довільної команди в операційній системі сервера. Виконується за допомогою вбудованих бібліотек popen, subprocess, os.system[1]. Для запобігання слід не виконувати явних програм через код або використовувати бібліотеки, котрі екранують небажані символи.

Другою вразливістю, є наявність великої кількості сторонніх бібліотек або як їх ще називають site-packages. Система імпортування пакетів в Python є дуже гнучкою, що дозволяє швидко писати патчі або змінювати основний функціонал тих, чи інших модулів. Вразливість є в тому, що зловмисники публікують пакети зі схожими іменами модулів, що потрібні для ваших потреб або ж взагалі ідентичні, але все «інфіковані». Тому одна неуважність може привести до появи вразливості або загрози. Для запобігання використовувати віртуальне середовище Python або сторонні сервіси, що допомагають тестувати написаний код.

Третьою найчастішою є вразливість використання старої середи виконання мови Python та старі пакети мови. Зараз більшість POSIX систем надаються з Python 2, що є старою та ненадійною версію. Найбільшою вразливістю цього є, як і в мові програмування C, переповнення буферу або вихід за границі буфера[2]. Реалізацією цього було переповнення цілого числа, що дозволяло використовувати довільний код. Більшість старих пакетів базуються на старих версіях мови, що не є безпечним. Рішенням цього є оновлення пакетів та середовища виконання мови Python.

Для написання безпечного та високо продуктивного коду можна порекомендувати вивчити основні загрози, що можуть бути присутні у вашому коді, використовувати останні версії фреймворків або утиліт, перевіряти достовірність інстальованих пакетів, а також робити моніторинг на наявність нових вразливостей, оскільки з кожним новим патчем може з’явитися нова вразливість.

Перелік посилань

1. T. O'Коннор (2013) Жестокий Python: настольная книга хакеров, аналитиков и инженеров по безопасности. Waltham, MA: Elsevier.
2. С. А Бабин (2014) Инструментарий Хакера. Санкт-Петербург: БХВ-Петербург.

УДК 681.518.54

Голота М.В., Демчук А.О., Удовик М.О., студенти гр. 125-18-1
Науковий керівник: Саксонов Г.М., ст. викл. кафедри безпеки інформації та телекомунікацій
(*Національний технічний університет "Дніпровська політехніка", м. Дніпро, Україна*)

BIG DATA

General provisions

Big data is various tools, approaches and methods for processing both structured and unstructured data in order to use it for specific tasks and purposes.

Structured data:

XML Schemas

Scalar data types (strings, numbers, dates)

Sequences

Complex data types

Restrictions

Unstructured data:

Natural Language Text

Missing explicit structure definition

Automatic selection of structures, as a rule, cannot be performed unambiguously

May contain data such as dates, numbers and facts.

In general, Big Data is data storage and processing.

Huge amounts of data are processed so that a person can get specific and necessary results for their further effective use.

In fact, Big Data is a solution to problems and an alternative to traditional data management systems.

Regular databases cannot store and process unstructured data. Big data solves this main task. Successfully stores and manages large-volume information;

Structures information coming from various sources (video, images, audio and text documents) into one single, understandable and digestible form;

Formation of analytics and the creation of accurate forecasts based on structured and processed information.

Big data: application and possibilities

Volumes of heterogeneous and rapidly arriving digital information cannot be processed with traditional instruments. The very analysis of the data allows you to see certain and imperceptible patterns that a person cannot see. This allows you to optimize all areas of our life - from government to production and telecommunications.

For example, some companies a few years ago defended their clients from fraud, and taking care of a client’s money took care of their own money.

Big Data defines three main types of tasks.

Storing and managing data in hundreds of terabytes or petabytes that conventional relational databases do not allow for efficient use.

The organization of unstructured information, consisting of texts, images, video and other types of data.

Big Data analysis, which raises the question of how to work with unstructured information, the generation of analytical reports, as well as the introduction of predictive models.

Three signs that big data should have:

Volume - volume (data are measured by the size of the physical volume of documents).

Velocity - the data is regularly updated, which requires their continuous processing.

Variety - a variety of data can have heterogeneous formats, to be unstructured or partially structured.

Big Data Analysis Techniques

There are many different methods of analyzing data arrays, which are based on tools borrowed from statistics and computer science. The list does not claim to be complete, but it reflects the most popular approaches in various industries.

A / B testing. A technique in which a control sample is compared in turn with others. Thus, it is possible to identify the optimal combination of indicators to achieve, for example, the best response of consumers to a marketing proposal.

Big data allows you to spend a huge number of iterations and thus obtain a statistically reliable result.

Association rule learning. A set of techniques for identifying relationships, i.e. associative rules between variables in large data arrays. Used in data mining.

Classification. A set of techniques that allows you to predict consumer behavior in a particular market segment (making purchasing decisions, outflows, consumption, etc.). Used in data mining.

Cluster analysis. The statistical method of classifying objects into groups by identifying in advance unknown common features. Used in data mining.

Crowdsourcing. Methods of collecting data from a large number of sources.

Data fusion and data integration. A set of techniques that allows you to analyze the comments of users of social networks and compare with sales results in real time.

Data mining. A set of techniques that allows you to identify the most susceptible categories of consumers for a promoted product or service, identify the characteristics of the most successful employees, and predict the behavioral model of consumers.

Ensemble learning. This method involves a lot of predictive models, which improves the quality of the predictions made.

Genetic algorithms. In this technique, possible solutions are presented in the form of `chromosomes', which can be combined and mutated. As in the process of natural evolution, the most adapted individual survives.

Machine learning. The direction in computer science (historically, the name `artificial intelligence` was fixed to it), which aims to create self-learning algorithms based on the analysis of empirical data.

Natural language processing (NLP). A set of methods of recognition of human natural language borrowed from computer science and linguistics.

Network analysis. A set of techniques for analyzing connections between nodes in networks. With regard to social networks, it allows analyzing the relationships between individual users, companies, communities, etc.

Optimization. A set of numerical methods for redesigning complex systems and processes to improve one or more indicators. Helps in making strategic decisions, for example, the composition of the product line to be launched on the market, investment analysis, and so on.

Pattern recognition. A set of techniques with elements of self-learning to predict the behavioral model of consumers.

Predictive modeling. A set of techniques that allow you to create a mathematical model in advance of a given likely scenario. For example, analysis of the CRM-system database for possible conditions that will push subscribers to change the provider.

Regression. A set of statistical methods to identify patterns between changes in the dependent variable and one or more independent ones. Often used for prediction and prediction. Used in data mining.

Sentiment analysis. At the heart of methods for assessing consumer attitudes are the technologies of recognition of human natural language. They allow you to isolate from the general information flow messages related to the subject of interest (for example, a consumer product). Next, evaluate the polarity of judgment (positive or negative), the degree of emotionality, and so on.

Signal processing. A set of techniques borrowed from radio engineering, which pursues the goal of recognizing a signal against noise and its further analysis.

Spatial analysis. A set of methods for analyzing spatial data, partly borrowed from statistics — topology of terrain, geographic coordinates, geometry of objects. The source of big data in this case is often geographic information systems (GIS).

Statistics. The science of collecting, organizing and interpreting data, including developing questionnaires and conducting experiments. Statistical methods are often used for evaluative judgments about the relationship between certain events.

Supervised learning. A set of techniques based on machine learning technologies that allow you to identify functional relationships in the analyzed data arrays.

Simulation. Modeling the behavior of complex systems is often used to predict, predict, and work through different scenarios when planning.

Time series analysis. A set of methods for analyzing repetitive over time data sequences borrowed from statistics and digital signal processing. Some of the obvious uses are tracking the stock market or the incidence of patients.

Unsupervised learning. A set of techniques based on machine learning technologies that allow you to identify hidden functional relationships in the analyzed data arrays. It has common features with Cluster Analysis.

Visualization. Methods for graphing the results of big data analysis in the form of diagrams or animated images to simplify the interpretation make it easier to understand the results.

Big Data in CyberSecurity

Technology develops evolutionarily, until it reaches a certain limit, and then there is a revolution, a paradigm shift. Today, we are on the verge of such a revolution in cyber security. Many approaches that seemed universal and unshakable lose their relevance, and new concepts arise in their place. What today is seen as a fashionable topic in a narrow professional field, tomorrow it becomes an ordinary, habitual phenomenon not only in cyber security, but also in the life of every person.

Even if a person does not have any accounts in social networks, the universal transition of commercial services to online almost forces you to leave "digital traces". Buying tickets, online shopping, ordering a pizza, calling a taxi - all these are situations when you send very sensitive personal information to the World Wide Web - passport data, full name, home and work address, map of regular movements around the city.

Does a person know where this data goes, who stores it, processes it and for what purpose does it use? No, in most cases, not only does not know, but does not even think. The digital world is so closely intertwined with the real that people no longer make a big difference between telling friends a funny story at a party and posting it on Facebook.

The more information about the user is available to the security officer, the more accurate the employee profile. It follows from this that behavioral analysis in corporate systems will inevitably seek to take into account the actions of an employee outside the company and its business processes. It follows that large-scale data collection and analysis technologies will be developed (Big Data). From an information security point of view, a user's portrait based on such complete information that big data can provide is a real breakthrough. Already, we are seeing a great interest of corporations to this topic.

The analysis of big data provides unique opportunities for the predictive analysis of the conduct and, as a result, the possibility of a preemptive, rather than after the fact, reacting to information security threats. The average employee has many accounts in a variety of systems - corporate email, several public email services, instant messengers and cloud storage. As a rule, the actions of a person in each individual account look innocent, but their comparison instantly creates an obvious picture of the planned violation. The problem is that for the majority of modern systems all of this is scattered information, from which a person is forced to manually fold a single picture.

If all this information about each employee were not summarized in a single personal dossier, the information security service would most likely have missed the incident. After all, a security officer in a company of about 500 people receives hundreds of notifications of potential violations every day. In such a flow of information, it is almost impossible to single out the “same” notification, especially if by itself it does not look critical. When it comes to manually comparing the logs of various systems, the task becomes overwhelming.

Similarly, big data is used to protect against external cyber attacks. One of the employees of our other customer at some point began to behave unusually - he began to turn to corporate resources that he had not used before. Such a deviation from the standard profile of behavior is an excuse to be wary, by convention, the “yellow” level of threat.

The data from various sources, collected together, made it possible to identify the cyber attack and, most importantly, take timely measures to counteract it.

However, while analyzing big data poses several major problems. The first is that its storage and processing requires large hardware capacities. Even if we discard this problem, the fact remains that the aggregated information about users is very heterogeneous. These are videos, images, geotags, text and more. Technologies for their automatic analysis and search for correlations are still very imperfect.

The new concept of information security is based on monitoring human actions, rather than information movements, and now it is obvious that it will become the driver of the development of many technologies that are now at the very beginning.

Перелік посилань:

1. Что такое Big data: собрали всё самое важное о больших данных [https://rb.ru/howto/chto-takoe-big-data/].

2. Работа с Big Data: основные области и возможности [https://www.marketing.spb.ru/lib-around/stat/Big_Data.htm]

3. Большие данные (Big Data). [http://www.tadviser.ru/index.php/Статья:Большие_данные_(Big_Data)]

4. Дырявый щит и большие данные: как меняется кибербезопасность в эпоху слияния онлайн и оффлайн? [https://www.forbes.ru/tehnologii/341795-dyryavyy-shchit-i-bolshie-dannye-kak-menyaetsya-kiberbezopasnost-v-epohu-sliyaniya]

УДК 004

Агашкова К.О., студентка гр. 125-18-1
Науковий керівник: Саксонов Г.М., старший викладач кафедри безпеки інформації і телекомунікації
(Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна)

РОЗУМНІ ВКАЗІВНИКИ

Метою даної роботи є звертання уваги читачів на необхідність і зручність використання розумних вказівників під час програмування на С++.

У роботі описані основні види розумних вказівників і особливості їх використання.

Як відомо, після використання динамічної пам'яті вона повинна бути звільнена. І бажано робити це кожен раз, коли в програмі використовується виділення цієї пам'яті. Після оператора new мови програмування С ++, який забезпечує виділення динамічної ділянки пам'яті з купи, потрібно використовувати оператор delete, який повертає назад в купу виділену оператором new пам'ять. У випадку, коли пам'ять не була звільнена, існує ймовірність виникнення таких критичних помилок:

- видалення вже видаленого об'єкта;
- витік пам’яті;
- розіменування нульового вказівника;
- звернення до неініціалізованої області пам'яті і ін.

У загальному випадку, витік пам’яті не грає важливої ролі, якщо програма не працює постійно, однак це непрофесійно.

Існує техніка управління ресурсами за допомогою локальних об'єктів, що називаються RAII. При отриманні будь-якого ресурсу, він ініціалізується в конструкторі, і, працюючи з ним в функції, коректно звільняється в деструкції.

Ресурсом може бути що завгодно, наприклад, файл, мережеве з'єднання, пристрій пам'яті і т.д.

Якщо в нашій програмі багато динамічних об'єктів, то в деструкторі доведеться багаторазово використовувати оператор delete з метою повернення пам'яті в купу. Якщо ж ми, створивши динамічну область пам'яті, не звільнимо її в кінці, то наслідки роботи програми можуть привести до серйозних помилок. В результаті з'явиться нова структура, навантажена операція виділення / звільнення пам'яті.

Саме тому зручніше використовувати розумні вказівники - об'єкти, що зберігають в собі вказівники на динамічно розподілені ділянки пам'яті різних типів даних. Розумні вказівники автоматично їх видаляють по закінченню роботи програми без явної вказівки delete.

Розглянемо наступні види розумних вказівників:

• boost :: scoped_ptr;

• std; auto_ptr;

• std :: tr1 :: shared_ptr;

boost :: scoped_ptr

Цей вказівник знаходиться у біблотеці boost. У нього є одна особливість: його не можна скопіювати, так як у нього є особистий оператор присвоювання і конструктор копіювання.

std :: auto_ptr

Даний вказівник є доопрацьованим варіантом попереднього. Більш того, він є частиною стандартної бібліотеки С ++

std :: shared_ptr

Вказівник, що підраховує посилання. Це означає, що існує змінна, яка зберігає в собі певну кількість вказівників, що посилаються на об'єкт.

Лічильник збільшується на одну одиницю при кожному виклику оператора присвоювання або копіювання.

Тепер і p2 і p1 вказують на один об'єкт, а лічильник посилань дорівнює 2. По виходу з функції лічильник обнуляється, і об'єкт знищується автоматично.

Перелік посилань:

1. Smart pointers для начинающих. [https://habr.com/ru/post/140222/]
2 Умный_указатель [https://ru.wikipedia.org/wiki/Умный_указатель]

УДК 303.732.4

Мілінчук Г.С. студентка гр. САіт-15-1
Науковий керівник: Хом'як Т.В., к.ф.-м.н., доцент кафедри системного аналізу та управління.
(Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна)

РОЗРОБКА ЕКСПЕРТНОЇ СИСТЕМИ ДЛЯ ПРИЙНЯТТЯ УПРАВЛІНСЬКИХ РІШЕНЬ В АГАРНОМУ ПІДПРИЄМСТВІ

Робота присвячена практичному обґрунтуванню впровадження експертної системи для розробки управлінських рішень на агарному підприємстві. Розроблено експертну систему (ЕС) у середовищі Mini Expert System, яка використовує Байєсову систему логічного висновку. Дана експерта система дозволяє прийняти рішення щодо подальшого розвитку аграрних підприємств в залежності від поточного стану полів та оцінки ситуації експертами.

Сучасне сільськогосподарське виробництво характеризується різноманітністю форм землеволодіння та землекористування, складністю технологічних процесів та високою конкуренцією серед сільськогосподарських товаровиробників. Це вимагає збільшення обсягів інформаційної забезпеченості користувачів, створення інтелектуальних систем, застосування для цього пріоритетних інформаційних технологій – ГІС-технологій, банків і баз даних, мережевих технологій, а також інтелектуальних технологій, у тому числі експертних систем, що дозволяють моделювати різні сценарії поведінки, мислення і комунікації в аграрних виробничих структурах. Доведено, що використання експертних систем для аналізу господарської діяльності суттєво впливає на підвищення ефективності управління в агарних підприємствах.

Mini Expert System - це експертна система, яка використовує систему логічного висновку на основі теореми Байєса про повну ймовірність. Вона призначена для проведення консультації з користувачем в будь-якій прикладній області (на яку налаштована завантажена база знань) з метою визначення вірогідності можливих результатів і використовує для цього набір оцінок правдоподібності деяких передумов, що отримуються від користувача.

На першому етапі створення експертної системи сформульовано базу знань про дану область у вигляді двох наборів: набір питань та набір варіантів результату [1]. Після цього сформульовані вірогідності отримання позитивної відповіді та вірогідності отримання негативної відповіді. Крім того, кожному результату ставиться у відповідність апріорна вірогідність цього результату, тобто вірогідність результату у разі відсутності додаткової інформації.

В процесі роботи ЕС вирішувач, користуючись даними наборами, матрицями і теоремою Байеса, визначає апостеріорну ймовірність кожного результату, тобто ймовірність, скориговану відповідно до відповідей користувача на кожне питання:

- при позитивній відповіді

$$P_{\text{апостер}} = \frac{P_{y_{ij}} P_i}{P_{y_{ij}} P_i + P_{n_{ij}} \cdot (1 - P_i)},$$

- при негативній відповіді

$$P_{\text{апостер}} = \frac{(1 - P_{y_{ij}}) P_i}{(1 - P_{y_{ij})} P_i + (1 - P_{n_{ij}}) \cdot (1 - P_n)},$$

- при відповіді "не знаю" апостеріорна ймовірність дорівнює апріорній.

Наступним кроком створення ЕС є завантаження бази знань у форматі .DAT до середовища експертної системи програми MiniES.exe та безпосередньо консультація користувача [2-4]. Завантажена база знань має вигляд, представлений на рис.1.

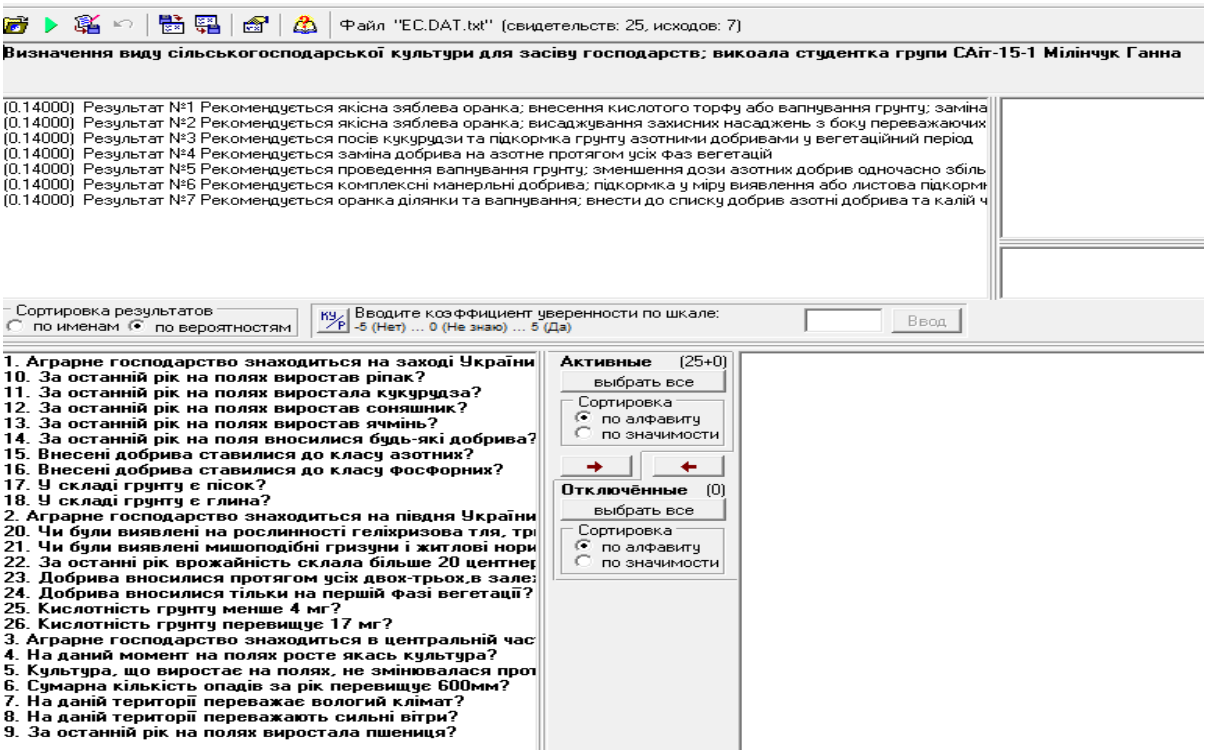

Рисунок 1 - Завантажена до MiniES.exe база знань

Після проведення консультації експертна система надає рекомендації для подальшого розвитку аграрного господарства з метою збільшення прибутку.

Таким чином, розроблена програма вирішує проблему низького прибутку в аграрних господарствах та надає рекомендації щодо стратегій розвитку сільськогосподарських угідь. Після консультації система отримає від фермера, який звернувся за послугою до ТОВ «Спейс Агро Моніторинг», інформацію щодо стану господарства на даний момент та пропонує найоптимальніший план розвитку.

Перелік посилань

1. Гаврилова, Т. А. Базы знаний интеллектуальных систем / Т.А. Гаврилова. - СПб.: Питер, 2000.
2. Писаревська Т. А. Інформаційні системи і технології в управлінні трудовими ресурсами: Навч. посібник. - 2-ге вид., перероб. і доп. - К.: КНЕУ, 2000. - 279 с.
3. Субботін С.О. Подання й обробка знань у системах штучного інтелекту та підтримки прийняття рішень. - Запоріжжя: ЗНТУ, 2008. - 341 с.
4. Ситник В. Ф. Системи підтримки прийняття рішень / Ситник В. Ф. – К.: КНЕУ, 2004. – 614 с.

УДК 519.252

Мозолєва А.В., студентка гр. САіт-15-2
Науковий керівник: Ус С.А., к.ф.-м.н., проф. каф. системного аналізу і управління НТУ «Дніпровська політехніка»
(Національний технічний університет «Дніпровська політехніка», м. Дніпро, Україна)

ЗАСТОСУВАННЯ МЕТОДУ АНАЛІЗУ ІЄРАРХІЙ ДЛЯ ВИЗНАЧЕННЯ АВТОБУСУ ДЛЯ ЗАМІНИ

Автомобіль є дуже складним механізмом, у якому всі його частини повинні працювати злагоджено. Для цього завжди необхідно проводити регулярний техогляд, аби упевнитись у надійності системи. Особливо важливим є технічний стан громадського транспорту, адже від справності автобуса нерідко залежить безпека пасажирів. Звичайно, після знаходження пошкоджень, необхідно їх ліквідувати якнайшвидше, аби не зазнати великого збитку від простою транспорту, проте, буває так, що іноді транспортний засіб потребує повної заміни. Здається, що це доволі легко - прийняти рішення про заміну транспортного засобу, зрозумівши, що деякі з його показників у дуже поганому стані, але що ж робити, якщо необхідно обрати з декількох одиниць транспорту, наприклад на транспортному підприємстві? Саме це питання і буде розглядатись у даній роботі на прикладі транспортного підприємства.

На приватному підприємстві, організованому в 2003 році, запланована заміна одного з восьми автобусів. Ці автобуси використовують для пасажирських перевезень по місту, де розташоване підприємство, та по території усієї України. Також транспорт підприємства використовується для щоденного надання перевезень шахтарів на місце та з місця роботи і для сезонних перевезень у курортні містечка. Через активне використання ресурсів транспорту, деякі автобуси застаріли, тому виникла необхідність заміни транспорту, починаючи з того, що має найгірший стан.

Для визначення автобусу у найгіршому стані, у даній роботі був використаний метод аналізу ієрархій. Завдяки цьому методу відбувається спрощення пошуку рішень шляхом представлення складної задачі у вигляді послідовного рішення більш простих задач. Також, метод, що використовується, є доволі універсальним, адже порівнювати альтернативи можна за критеріями, що не належать до одної системи вимірювань.

MAI базується на експертних оцінках, за допомогою яких було описано стан кожного з автобусів за певними критеріями:

A – кількість років в експлуатації;
B – пробіг (тис. км.);
C – вартість необхідного ремонту (тис. грн.);
D – витрата палива на 100 км. (літри);
E – відсоток іржі на кузові автобуса.

У результаті експертного оцінювання кожного з автобусів за критеріями, що наведені вище, була отримана матриця експертних оцінок (табл. 1).

Першим етапом аналізу була побудова ієрархічної структури (рис. 1), де ціль складала найвищий рівень ієрархії (перший рівень), на наступних рівнях представлені критерії, за якими були порівняні об’єкти, та альтернативи (автобуси) на найнижчому рівні. [1]

Таблиця 1. Матриця експертних оцінок

		Критерії				
		A	B	C	D	E
Автобуси	I	3	300	7	20	0,02
	II	4	150	17	35	0,01
	III	10	580	5	25	0,055
	IV	5	180	15	36,7	0,015
	V	1	50	0	29	0,005
	VI	2	145	10	33	0,008
	VII	1	65	0	29	0,006
	VIII	8	640	54	35	0,05

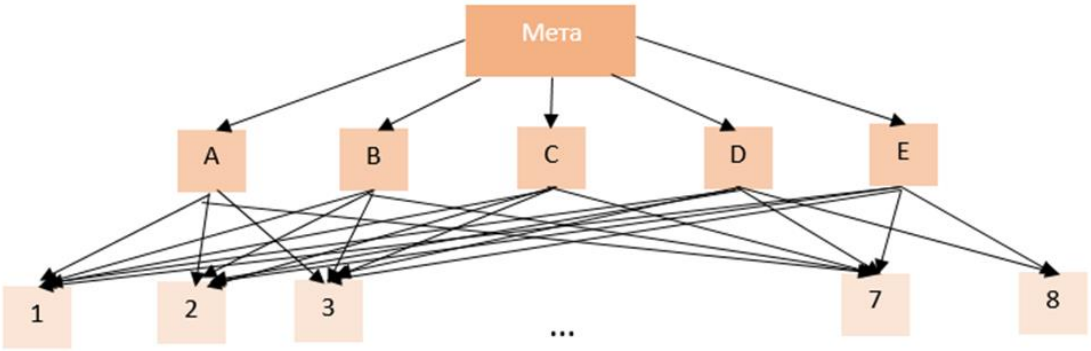

Рис. 1. Трьохрівнева ієрархія «ціль – критерій –альтернативи»

Далі була створена матриця парних порівнянь для другого рівня ієрархії, після розрахування локальних пріоритетів для якої, стало очевидним, що найважливішим критерієм є пробіг автомобіля, а найменш важливим є показник відсотка іржі на кузові.

Наступним кроком було складання матриць порівнянь елементів третього рівня (табл. 2) для кожного з критеріїв другого рівня, з якими вони пов'язані. В результаті таких обчислень були отримані показники пріоритетності кожного автобусу відносно усіх критеріїв. Варто зауважити, що чим більше у автобусу є показник пріоритетності, відносно певного критерію, тим більш ймовірно те, що цей автобус необхідно буде замінити.

Таблиця 2. Матриця парних порівнянь для критерія А

Критерій А								
	I	II	III	IV	V	VI	VII	VIII
I	1	1/2	1/7	1/3	3	2	3	1/6
II	2	1	1/6	1/2	4	3	4	1/5
III	7	6	1	5	9	8	9	3
IV	3	2	1/5	1	5	4	5	1/4
V	1/3	1/4	1/9	1/5	1	1/2	1	1/8
VI	1/2	1/3	1/8	1/4	2	1	2	1/7
VII	1/3	1/4	1/9	1/5	1	1/2	1	1/8
VIII	6	5	1/3	4	8	7	8	1

Останнім кроком даного методу є обчислення глобальних пріоритетів критеріїв третього рівня. У результаті обчислень стає очевидно, що замінити необхідно саме восьмий автобус, адже саме він має найвищий показник пріоритетності (0,28), далі на заміну претендуватимуть четвертий та третій автобуси з показниками пріоритетності 0,2 та 0,19 відповідно.

Підводячи підсумки, можна сказати, що MAI є систематичною процедурою ієрархічного представлення елементів, що визначають суть будь-якої проблеми. Значення в результаті використання цього методу не залежать від одиниць вимірювання, що дуже полегшує роботу з визначенням пріоритетів, та добре підходить для визначення якісної оцінки. В результаті проведеної роботи стало зрозумілим, що найбільше потребує заміни восьмий автобус, адже показник пріоритетності в нього вийшов найбільший.

Перелік посилань

1. Сааті Т. Л. Про вимір неосяжного. Підхід до відносних вимірах на основі головного власного вектора матриці парних порівнянь // Електронний журнал "Cloud Of Science". 2015. Т. 2. №1. (http://cloudofscience.ru/sites/default/files/pdf/CoS_2_5.pdf)