Міністерство освіти і науки України
ПОЛТАВСЬКА ДЕРЖАВНА АГРАРНА АКАДЕМІЯ
Навчально-науковий інститут економіки, управління, права та інформаційних технологій

М А Т Е Р І А Л И

студентської конференції

за результатами виробничої практики

Випуск ІІІ

кафедра інформаційних систем та технологій

21 вересня 2021 р.

Полтава – 2021

Редакційна колегія:

Матеріали студентської конференції за результатами виробничої практики кафедри інформаційних систем та технологій Полтавської державної аграрної академії. – Полтава: ПДАА, 21 вересня 2021 р. – Вип. ІІІ. – 52 с.

У збірнику надруковані матеріали студентської конференції за результатами виробничої практики кафедри інформаційних систем та технологій Полтавської державної аграрної академії (випуск ІІІ). Тези наводяться без змін та редагування. Відповідальність за зміст та редакцію тез несуть автори та наукові керівники.

Для студентів, аспірантів та викладачів вищих навчальних закладів.

ЗМІСТ

Федорченко М. Б.,
здобувач вищої освіти СВО Бакалавр,
спеціальність 126 Інформаційні системи та технології
Науковий керівник: к.т.н., доцент Уткін Ю. В.

РОЗРОБКА АЛГОРИТМУ АВТОМАТИЧНОГО ПІДРАХУНКУ ПАСАЖИРІВ В ГРОМАДСЬКОМУ ТРАНСПОРТІ З ВИКОРИСТАННЯМ ВІДЕОПОТОКУ

Дослідження пасажиропотоків є одним із пунктів програм оптимізації мережі маршрутів громадського транспорту, або дане дослідження може бути використане для оцінки ефективності функціонування окремих маршрутів. Для оптимізації цього процесу представлено алгоритм розрахунку пасажирів у відео потоці, який дозволяє автоматизувати трудомісткий процес та покращити ефективність роботи пасажирського транспорту.

Для реалізації алгоритму вирішуються три завдання: виявлення об'єктів, визначення траєкторії руху і аналіз траєкторії руху.

Автоматичний розрахунок та аналіз пасажиропотоку має багато переваг, а саме:

– поєднання поточних значень вимірів та даних минулого періоду дозволяє чіткіше уявити собі пасажиропотік. Тому, на основі даних, автоматично розрахованих пасажирами, частоту транспортних засобів, що проходять по всіх мережах, можна планувати частоту та гнучко регулювати її за потреби;

– завдяки постійному підрахунку пасажирів, транспортні компанії можуть оптимізувати та координувати свої транспортні засоби залежно від кількості пасажирів. Раціональне використання великих зчленованих та міні-автобусів, розрахунок кількості вагонів на тій чи іншій лінії. Таким чином, постачальники транспортних послуг можуть швидко та гнучко реагувати на мінливі потреби та забезпечити відповідну потужність відповідно до фактичних потреб;

– дані, отримані автоматичною системою підрахунку пасажирів, є ідеальною основою для ефективної оптимізації маршруту. Кількість пасажирів у кожному автобусі або трамваї можна легко підсумувати;

– відповідно до фактичної кількості пасажирів у кожному транспортному засобі, використовуючи фактичні дані, отримані системою автоматичного підрахунку, пасажирів можна ще на пероні розподілити оптимально, направивши їх на вільні місця. Система світлової індикації подібна до звичайних світлофорів, які можуть надійно і надійно відображати рівень навантаження відповідного поїзда. Пасажири можуть розійтися по поїзду оптимальним чином, скорочуючи час пересадок та роблячи подорож більш комфортною;

– сучасна автоматична система підрахунку пасажирів працює цілодобово, вона економічна та дуже точна.

Для того, щоб вести облік пасажирів, оптимізувати розклади руху, маршрутні мережі, тарифну політику, контролювати виручку, що здається персоналом та забезпечувати контроль оплати проїзду, необхідно створити автоматичну систему автоматичного підрахунку кількості пасажирів. Для реалізації системи автоматичного розрахунку пасажиропотоку громадського транспорту необхідно вирішити три основні завдання:

1. виявлення об’єктів (людей),
2. визначення траєкторії руху,
3. аналіз траєкторії руху.

Перший крок - визначити правильне розташування камери в автобусі. Спосіб виявлення залежить від варіантів установки камери. Тільки коли фон відеопотоку є статичним фоном, умови стабільними, а обсяг трафіку низьким, метод виділення рухомих об’єктів буде ефективним [3]. Існує багато способів виділення рухомих об’єктів у кадрі. Наприклад, визначення зміщення областей пікселів між кадрами, попіксельне визначення зміни кадрів (піксель, колір, яскравість) тощо.

Камеру рекомендовано встановити над виходом з об’єктивом, розташованим вертикально вниз. Це може вирішити відразу кілька проблем та покращити точність виявлення, що в свою чергу вплине на підведення статистики кількості пасажирів.

Проаналізувавши різні алгоритми виявлення об’єктів [4], зроблено такий висновок: за існуючого кута зйомки, коли камера спрямована на дверний отвір, нейронна мережа, придатна для будь-якої з вищезгаданих архітектур, може бути використана для виявлення людей в кадрі. Однак, щоб підвищити точність виявлення, кожну камеру необхідно встановити над дверима, що вирішує проблему виявлення небажаних об’єктів та їх перекриття. У цьому випадку може бути використаний метод Віоли-Джонса, оскільки особа в кадрі буде обличчям до камери з тієї ж сторони, що дозволить навчити каскад Хаара, а процес виявлення буде в кілька разів швидшим [2]. Встановивши камеру, також можна скористатися методом вибору рухомих об’єктів, оскільки вона добре працює при відсутності накладання.

Визначення траєкторію руху. В рамках цього завдання потрібно обробити дані, отримані в першому завданні. Траєкторія руху - це впорядкований набір точок. Коли пасажир входить або виходить з автобуса, виділяється прямокутною рамкою в кадрі. Коли людина рухається, координати кадру змінюються.

Для цього буде потрібно алгоритм відстеження центроїдів на основі OpenCV [1].

Він використовує евклідову відстань між центроїдом об’єкта в існуючому кадрі та попередньому кадрі. Він складається з декількох етапів:

- визначення координати рамки об’єкта та обчислення Центроїд;
- обчислення евклідової відстані між новими координатами центроїда та попередньо обчисленими координатами центроїда;
- оновлення координат існуючих об’єктів;
- виявлення нових об’єктів;

- скасування виявлення об’єктів, які вийшли з поля зору.

Щоб використати відстеження центроїдів для створення простого алгоритму відстеження об’єктів, першим кроком є отримання координат прямокутника від детектора об’єктів і використання їх для обчислення центроїда. Алгоритм полягає в окремому перенесенні крайніх прямокутних координат (x, y) кожного об’єкта в кожному кадрі. Рамки створюється будь - яким типом детектора (каскад Хаара, нейронна мережа тощо). Після того, як відомо координати прямокутника, можна обчислити центральні координати прямокутника. Також потрібно призначити унікальний ідентифікатор об’єкта.

Другий крок - обчислення евклідової відстані між новими обмежувальними рамками та існуючими об’єктами. Після того, як у кадрі з’являться два або більше об’єктів, було обчислено евклідову відстань між парою існуючих центроїдів та центроїдів вхідних об’єктів. Потім розраховано евклідову відстань між кожною парою вихідних центроїдів та нових центроїдів.

Третій крок - оновлення координат прямокутної рамки існуючого об’єкта. Об’єкт може переміщатися між послідовними кадрами, але відстань між центроїдами існуючих та наступних кадрів буде меншою, ніж усі інші відстані між об’єктами. Далі алгоритм вибирає центроїд, що зближається, який мінімізує евклідову відстань. Але, наприклад, жоден об’єкт поблизу об’єкта не має нічого спільного. Потрібно його зареєструвати.

Якщо виявленнь на вході більше, ніж існуючих об’єктів, що відстежуються, необхідно зареєструвати новий об’єкт. Це четвертий крок. Реєстрація полягає у призначенні ідентифікатора та збереженні центроїда прямокутної рамки. Також можна повернутися до другого кроку і повторити вищезазначені кроки для кожного кадру відеопотоку.

П’ятий крок - скасувати реєстрацію старих об’єктів. Коли об’єкт втрачається або перекривається в кадрі, алгоритм повинен вміти обробляти його. Цей алгоритм можна використовувати для розрахунку траєкторії руху пасажирів, щоб в подальшому мати змогу визначити напрямок руху під час підрахунку кількості пасажирів у майбутньому.

Аналіз траєкторії руху. Після отримання траєкторії руху її потрібно проаналізувати, щоб визначити напрямок руху. Це можна зробити, додавши вектори траєкторії. У напрямку вектора підсумовування можна розрізняти вхідних і вихідних пасажирів. Метод порівняння векторів залежить від кута установки камери. Якщо об’єкт рухається зліва направо та справа наліво, вектор має відрізнятися символом координати X. Якщо об’єкт рухається зверху вниз, знизу вгору - через символ координати Y. Якщо камера встановлена на кут, під яким об’єкт рухається під кутом, потрібно порівняти символи двох координат.

Для програмної реалізації індивідуального завдання було прийнято використати мова програмування Python та бібліотеку OpenCV. Приклад роботи програми наведено на рис. 1.

Демонстрація аналітичного підходу представлена у вигляді трьох основних завдань, виконання яких є необхідним для впровадження автоматичної системи підрахунку пасажирів у громадському транспорті.

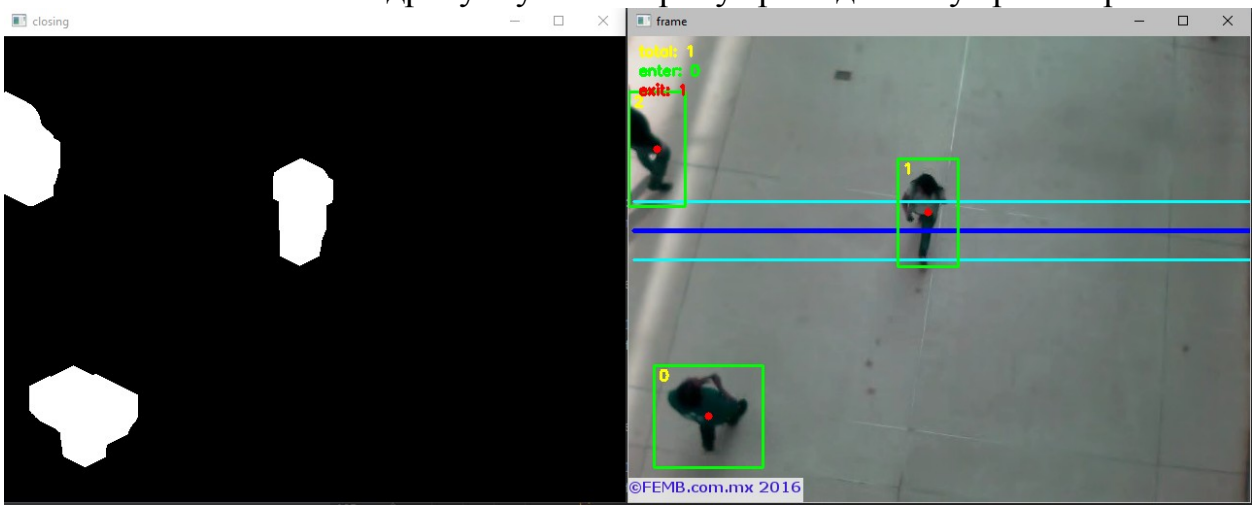

Рис. 1. Скріншот монітору с робочою програмою

У першому завданні було розглянуто кілька варіантів виявлення пасажирів та різні архітектури нейронної мережі. Залежно від того, як встановлено камеру, для виявлення пасажирів можна використовувати різні методи. Але для того, щоб покращити точність розпізнавання, камеру необхідно розмістити над входом (виходом), щоб націлити на пасажирів, що входять і виходять зверху вниз, оскільки в цьому випадку вирішується проблема перекриття людей та проблема виявлення додаткових об'єктів у кадрі.

Друге питання пропонує алгоритм визначення траєкторії пасажирів, ТОБТО необхідно розрізняти «вхідних» та «вихідних» пасажирів у громадському транспорті.

Третє завдання аналізує траєкторію методу шляхом порівняння підсумкових векторів. Найцікавіший і перспективний варіант на даний момент - використання різних методів комп'ютерного зору для розрахунку пасажиропотоку в громадському транспорті, оскільки цей метод працює автоматично і не вимагає участі людини.

В результаті проведенного аналізу та дослідженя було розроблено скрипт для автоматичного підрахунку пасажирів в громадському транспорті з використанням відеопотоку з використанням нейронної мережі, мови програмування Python та бібліотеки комп'ютерного зору OpenCV.

Список використаних джерел:

1. Буров Є. Комп'ютерні мережі. Львів: БАК, 2001. 468 с.

2. Єрьоміна Н. В. Комп'ютерні мережі: Навчальний посібник. К : КНЕУ, 2005. 230 с.

3. Уолренд Дж. Телекомунікаційні та комп'ютерні мережі: Вступний курс / Пер. з англ М : Постмаркет, 2003. 480с.

4. Семенов А. Б., Стрижаков С. К., Сунчелей І. Р. Структуровані кабельні системи: 4-е вид. : ДМК Пресс, 2002. 640 с.

Ілієш О.В.
здобувач вищої освіти СВО «Бакалавр»,
спеціальність Інформаційні системи та технології
Науковий керівник – к.т.н., доцент Одарущенко О.Б..

АНАЛІЗ МОЖЛИВИХ ДЖЕРЕЛ І КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ

Інформаційна безпека – захищеність інформації від різноманітних загроз та небезпек, для підтримки неперервності діяльності підприємства, зменшення збитків, збільшення прибутку, поліпшення і збільшення підприємницьких можливостей та збільшення сталого доходу. В межах Політики інформаційної безпеки на підприємстві, говорячи про інформаційну безпеку, мають на увазі забезпечення конфіденційності, цілісності та доступності певної інформації [1].

Але зараз мова йде про іншу частину інформаційного світу, що, хоч і безпосередньо стосується інформаційної безпеки, але і є однією із небезпек для інформаційної системи. Проводиться аналіз можливих джерел і каналів витоку інформації.

Канали витоку інформації – це методи та шляхи витоку інформації з інформаційної системи; тут грає роль також паразитний (небажаний) ланцюжок носіїв інформації, один або кілька з яких є або можуть бути правопорушниками або його спеціальною апаратурою.

Усі канали витоку інформації можна поділити на прямі та непрямі. Прямі відповідно вимагають доступу до апаратного забезпечення і даних інформаційної системи. Непрямі канали не вимагають безпосереднього доступу до технічних засобів інформаційної системи.

Прикладами прямих каналів витоку можна вважати [7]:

1) інсайдери (людський фактор). Витік інформації внаслідок порушення комерційної таємниці;

2) пряме копіювання.

Приклади непрямих каналів витоку представлено у вигляді:

1) крадіжка або втрата інформаційних носіїв, дослідження не знищеної інформації;

2) дистанційне фотографування або прослуховування;

3) перехоплення сигналу, наприклад електромагнітних випромінювань.

Канали витоку інформації можна також розділити за фізичними властивостями і принципам функціонування. Класифікація за цими ознаками відбувається наступним чином:

1) акустичні — методи сприйняття і/або запису звуку, наприклад підслуховування і прослуховування;

2) акустоелектричні — отримання інформації через звукові хвилі з подальшою передачею її через мережі електроживлення;

3) віброакустичні — перехоплення сигналів, що виникають за допомогою перетворення інформативного акустичного сигналу при впливі його на будівельні конструкції і інженерно-технічні комунікації приміщень, які захищаються;

4) оптичні — візуальні методи, фотографування, відеозйомка, спостереження;

5) електромагнітні — копіювання полів шляхом зняття індуктивних наводок;

6) радіовипромінювання або електричні сигнали від впроваджених в технічні засоби і приміщення спеціальних електронних пристроїв знімання мовної інформації «закладних пристроїв», які модульовані інформативним сигналом;

7) матеріальні — інформація на певних інших фізичних носіях інформації.

Залежно від виду каналів зв'язку технічні канали перехоплення інформації можна розділити на технічні та природні.

Технічні канали витоку інформації можна розділити на природні і спеціально створені.

Природні канали витоку інформації виникають при обробці інформації технічними засобами (електромагнітні канали витоку інформації) за рахунок побічних електромагнітних випромінювань, а також внаслідок наведень інформаційних сигналів в лініях електроживлення технічного засобу обробки інформації, сполучних лініях допоміжних технічних засобів і систем (ДТЗС) та сторонніх провідниках (електричні канали витоку інформації). До спеціально створюваних каналах витоку інформації відносяться канали, створювані шляхом впровадження в технічний засіб обробки інформації електронних пристроїв перехоплення інформації (закладних пристроїв) і шляхом високочастотного опромінення технічного засобу обробки інформації [9].

Також, окрім різноманіття технічних каналів витоку інформації є і цілий список технічних засобів промислового шпигування, такі як засоби акустичного контролю, апаратура для зйомки інформації з вікон, спеціальна апаратура звукозапису, мікрофони різного призначення і виконання, тощо.

За словами аналітиків, до традиційних лідерів за кількістю витоків - фінансовий сектор і ритейл - додалися інші індустрії, IT-компанії і державні організації (Звіт «Глобальне дослідження витоків конфіденційної інформації в 2016 році» компанії Infowatch, звіт «Витоку конфіденційної інформації в Росії і в світі. Підсумки 2016 року »компанії Zecurion.). Окрім вкрай очевидної, але складно вимірної шкоди діловій репутації, аналітиками відзначені й більш зрозумілі негативні наслідки витоку інформації - скасування угод, компенсація збитку третім особам, витрати на судові розгляди та інші ситуації, що, вірогідно, сприяють загибелі бізнесу.

Найбільш поширений фізичний канал витоку інформації пов'язаний з класичним документообігом - обміном документами всередині організації, з клієнтами і постачальниками послуг і товарів, а також архівним збереженням. Витік інформації може відбутися в результаті перехоплення документа після його виведення на друк (наприклад, коли принтер головного бухгалтера або генерального директора розміщений в загальному офісному просторі), внаслідок несвоєчасного знищення документів (якщо компанія не проводить відповідного навчання співробітників і економить на шредерах), вільного доступу до шаф з архівними документами (відсутність сейфів), некоректного перенесення і знищення документів при переїздах або реорганізації компаній і т. п. на жаль, всі ці випадки не відносяться до чистої теорії, це спостереження з практики роботи топ-10 організацій країни, у яких, здавалося б, все є, і всередині відбудований повний набір процесів для забезпечення безпеки.

Для припинення каналу витоку інформації шляхом виносу обладнання підприємству необхідно подбати про організацію безпечного фізичного периметра, охорони доступу в серверні приміщення і на об'єкти, в яких розміщуються резервні копії даних і електронних архівів. Ще один сумний приклад: стрічкову бібліотеку, в якій зберігалися резервні копії однієї з основних корпоративних інформаційних систем, з огляду на її великих габаритів, не вдалося розмістити в контрольованих серверних приміщеннях. Тому бібліотека «умовно тимчасово» зберігалася в офісній кімнаті. Частково рятувало ситуацію те, що прохід в організацію контролювався за допомогою СКУД. Однак служба безпеки не врахувала, що в кімнаті було кілька вікон, через які зловмисник міг проникнути і забрати декілька стрічок з даними з собою.

Канали витоків, згідно з багатьма дослідним звітам («Глобальне дослідження витоків конфіденційної інформації в 2016 році» компанії «Infowatch»), стали більш схильними до використання web-сервісів. Внутрішній порушник часто знає про існування DLP-систем на підприємстві та моніторингу поштових каналів і зовнішніх пристроїв і тому використовує web-канали, які, в силу їх різноманітності, контролювати складніше.

Більшість аналітичних джерел констатує незначний обсяг витоку інформації через мобільні пристрої. Почасти це пов'язано з обмеженістю доступною на мобільному пристрої інформації, а також з впровадженням в багатьох компаніях засобів захисту мобільних пристроїв. Але не брати в розрахунок мобільний канал витоків повністю теж неправильно: ступінь мобілізації бізнесу зростає. На закінчення відзначимо, що організація ефективного захисту від витоків інформації вимагає комплексного підходу, який передбачає аналіз основних каналів витоку даних, навчання співробітників підприємства правилам безпечної роботи з інформацією, реалізацію постійного моніторингу нових загроз, а для масштабних і різноманітних IT-ландшафтів - залучення команд професійних виконавців для проектування і впровадження рішень.

Існуючі засобів забезпечення захисту інформаційної системи поділяються на правові, організаційні та інженерно-технічні.

Захист інформації від витоку по технічним каналам здійснюється на основі конституцій і законів, наявності свідоцтв про авторське право, патентів і товарних знаків.

Наприклад, в Україні, як і в більшості інших держав, існує стандарт, що встановлює класифікацію і перелік факторів, що впливають на конфіденційну інформацію, в інтересах обґрунтування вимог захисту інформації на об'єкті реалізації інформаційної системи. Цей стандарт поширюється на вимоги щодо організації захисту інформації при створенні та експлуатації об'єктів інформатизації, які використовуються в різних галузях діяльності (оборони, економіки, науки та інших областях).

Забезпечення сукупності положень про Службу безпеки і плани заходів служби безпеки охоплюють широке коло питань, зокрема:

а) на ранньому етапі проектування приміщень і будівництві Служба безпеки розглядає і вирішує наступні питання: виділення приміщень для нарад і переговорних заходів (для таких приміщенньь виробляють спеціальні перекриття і канали повітряної вентиляції, окремі кімнати екранують), зручність контролю приміщень, людей, транспорту, створення виробничих зон за типом конфіденційності робіт з самостійним додатковим допуском;

б) служба безпеки приймає участь в підборі персоналу з перевіркою їх якостей на підставі особистих бесід (вивчення трудової книжки, отримання інформації з інших місць роботи, після прийняття на роботу, працівник повинен ознайомитись з правилами роботи з конфіденційною інформацією і порядком відповідальності);

в) служба безпеки готує положення і здійснює організацію пропускного режиму, організацію охорони приміщень і територій, організацію зберігання і використання документів, порядок обліку, зберігання, знищення документів, планові перевірки.

На рис. 1 представлено концептуальну модель небезпек інформаційної системи і забезпечення інформаційної безпеки у разі загрози.

Рис.1. Концептуальна модель інформаційної безпеки

Захист включає в себе: апаратні засоби захисту, програмні засоби захисту — це використання спеціальних програм в системах, засобах і мережах обробки даних, математичні методи захисту — застосування математичних і криптографічних методів з метою захисту конфіденційної інформації (без знання ключа неможливо дізнатися і розшифрувати вкрадену інформацію).

Список використаних джерел:

1. Войтюшенко Н. М. Інформатика і комп'ютерна техніка: навч. посібник. К.:"ЦУЛ", 2006. 568 с.
2. Галич. О. А. Управління інформаційними зв’язками та бізнес-процесами: навчальний посібник. Харків: Фінарт, 2016. 244 с.
3. Сурмин, Ю. П. Теория систем и системный анализ : учеб. пособие. Киев: МАУП, 2003. 164 с.
4. Романов А.И. Телекомуникационные сети и управление: Учебное пособие. Киев: Киевский университет, 2003. 240 с.
5. Анфилатов В.С. и др. Системный анализ в управлении: Учебное пособие. Под ред. А.А. Емельянова. М.: Финансы и статистика, 2002. 368 с.
6. Зацеркляний М. М., Мельников О. Ф. , Струков В. М. . Основи комп’ютерної техніки для економістів. К.: ВД „Професіонал”, 2007. 672 с.
7. Микитишин А.Г., Митник М.М., Стухляк П.Д., Пасічник В.В. Комп’ютерні мережі: навчальний посібник. Львів, «Магнолія 2006». 256 с.
8. Шеховцов В.А. Операційні системи. К.: Видавнича група ВНУ, 2005. 576 с.
9. Інформатика та комп’ютерна техніка: програмне забезпечення ЕОМ: навч. посібник. За ред. П. А. Щербакова. Харків, ХДАУ, 2001. 292 с.

Веременич Д.Ф.,
здобувач вищої освіти СВО Бакалавр,
спеціальність 126 Інформаційні системи та технології
Науковий керівник: к.т.н, доцент Дегтярьова Л.М.

ПОРІВНЯЛЬНИЙ АНАЛІЗ ВАРІАНТІВ АРХІТЕКТУРИ ІНФОРМАЦІЙНИХ СИСТЕМ

Стан розвинення технологій сьогодення має настільки високий рівень, що дає змогу здійснити побудову інформаційної систему будь-якої складності, масштабу й функціональності. Проте, зважаючи на потреби бізнесу, які базуються на показниках бізнес-оцінок, присутні додаткові складові, рішення яких складається з забезпечення більш раціонального підходу до процесів реалізації, подальшої експлуатації інформаційних систем й проектування. Беручи це до уваги, є можливість точно вважати відповідну архітектуру одним з головних показників ефективності інформаційної системи, що створюється, та відповідно успішності заснованого бізнесу [1]. Поняття "архітектура

інформаційної системи" можна визначити великою кількістю способів. Це пов’язано:

1. з недостатністю загальноприйнятого визначення самої інформаційної системи. З огляду на складність структури, достатнім способом описати її можливо тільки при консолідації декількох точок зору, що в кожному конкретному випадку може приводити до різних результатів.

2. з різноманіттям трактувань самого терміну "архітектура".

У результаті, архітектурну будову інформаційної системи можна здійснити, описавши її як концепцію, що визначає структуру, модель функції що виконуються й взаємозв’язки компонентів інформаційної системи.

Алгоритм обрання архітектури для інформаційної системи що проектується, в умовах ринку, зведена до визначення вартості володіння ІС. Вартість володіння ІС складається із вартості ризиків і планових витрат [3].

Витрати що є плановими містять собівартість модернізації, технічного обслуговування, заробітної плати обслуговуючого персоналу й т.д.

Загальну вартість ризиків визначають з вартості всіх типів ризиків, та їх ймовірностей і матрицею належності між ними. Відповідно, матриця відповідності обумовлюється архітектурою інформаційної системи яка була обрана. Є можливість виділити особливо важливі типи ризиків:

– проектні ризики (ризики при створенні системи);

– ризики розробки (помилки, недостатня оптимізація);

– технічні ризики (простої, відмови, втрата даних);

– бізнес-ризики (виникають через технічні ризики й пов’язані з експлуатацією системи);

– невизначеності (пов’язані з варіативністю бізнесів-процесів і складаються з необхідності внесення змін у систему й неоптимальну процедуру функціонування);

– операційні (мають на увазі невиконання набору операцій, можуть виникати через технічні ризики й бути ініціаторами бізнесів-ризиків).

Концептуальна ідея архітектурної будови інформаційної системи має формуватися ще на етапі техніко-економічного обґрунтування й обиратись такою, щоб вартість володіння нею була мінімальною.

Зважаючи на це, є змога вважати архітектуру інформаційної системи моделлю, яка дає змогу визначити вартість володіння через присутню в даній системі інфраструктуру [2].

Беручи до уваги архітектуру великих організацій або корпорацій, прийнято вживати термін «корпоративна архітектура». Її можливо презентувати у вигляді угрупування декількох типів архітектури:

– бізнес архітектура (Business architecture);
– IT-архітектура (Information Technology architecture);
– архітектура даних (Data architecture);
– програмна архітектура (Software architecture);
– технічна архітектура (Hardware architecture).

Варіативність моделей архітектури інформаційних систем представлені на рис. 1 [6].

Рис. 1 Моделі архітектури інформаційних систем.

Технічна архітектура являється першим щаблевим рівнем архітектурної структури інформаційної системи. Надає опис всіх апаратних засобів, що застосовуються при виконанні оголошеного набору функцій, а також містить засоби забезпечення мережної надійності й взаємодії. Технічна архітектура містить вказівки щодо мережевих комутаторів, периферійних пристроїв й маршрутизаторів, джерел безперебійного живлення, жорстких дисків, оперативної пам'ять, процесорів, сполучених кабелів, й т.п .

Програмна архітектура являється сукупністю комп'ютерних програм, розрахованих задля вирішення конкретних завдань. Відповідний тип архітектури призначається для проведення опису додатків, які входять до складу інформаційної системи. На даному рівні здійснюється опис програмного інтерфейсу, компонентів й поведінки [4].

Архітектура даних включає в себе засоби керування даними, і фізичні сховища даних. Зокрема, вона включає в себе логічні сховища даних, а при зосередженості компанії на роботу зі знаннями, є можливість виділити окремий рівень – архітектура знань (Knowledge architecture). На даному рівні описуються логічні й фізичні моделі даних, визначаються правила цілісності, складаються обмеження для даних.

Необхідно виділити рівень IT-архітектури, в зв'язку з тим, що він є сполучним, на ньому здійснюється формування базового набору сервісів, використання яких проводиться як на рівні архітектури даних, так і на рівні програмної архітектури. У разі, якщо будь-яка особливість функціонування для цих двох рівнів передбачена не була, то змістовно зростає ймовірність збоїв у роботі, з урахуванням цього і втрат у бізнесі. У деякій кількості випадків відсутня можливість здійснити ділення IT-архітектури й архітектури окремого додатка. Це вірогідно при великому ступені інтеграції додатків. Зразком IT-архітектури може служити SharePoint від компанії Microsoft. Даний продукт надає сервіси задля спільної роботи й зберігання інформації, що є

дуже змістовним аспектом функціонування будь-якої компанії. Базові системні модулі сервісу відносяться до IT-архітектури, а користувачів – до програмного. Базовою функцією IT-архітектури є здійснення забезпечення функціонування бізнесів-додатків які є важливими задля досягнення визначених бізнесів-цілей. У разі, якщо деяка функція необхідна відразу в декількох додатках, то її розумно буде перенести на рівень IT-архітектури, тим самим підвищивши інтеграцію системи й знизити складність архітектури додатків [5].

Кінцевим в ієрархії являється рівень бізнес-архітектури або архітектури бізнесів-процесів. На даному рівні здійснюється визначення стратегій ведення бізнесу, віроґідні способи керування, принципи загальної організації й ключові процеси, що представляють для бізнесу величезну важливість.

Список використаних джерел:

1. Коваленко О. С., Добровська Л. М. Проектування інформаційних систем: Загальні питання теорії проектування ІС. Навч. посіб. для студ. спеціальності 126 «Інформаційні системи та технології». Електронні текстові дані. Київ : ім. Ігоря Сікорського, 2020. 192 с.
2. Авраменко В.С., Авраменко А.С. Проектування інформаційних систем: навчальний посібник. Черкаси: Черкаський національний університет ім. Б. Хмельницького, 2017. 434 с.
3. Бажин І. І. Інформаційні системи менеджменту. М.: ГУ ВШЕ. 2000. 688 с.
4. Дубаков А. А. Проектування інформаційних систем. Київ: Видання Київського Політехнічного університету, 2011. 258 с.
5. Литвин В.В., Пасічник В.В., Шаховська Н.Б. Проектування інформаційних систем. Навчальний посібник (затв. МОН України). Київ: 2021. 52 с.
6. Посилання на використану ілюстрацію (рис 1): https://elearning.sumdu.edu.ua/free_content/lectured:de1c9452f2a161439391120eef364dd8ce4d8e5e/20160217112601/170352/index.html

Кулага Б.А.
здобувач вищої освіти СВО Бакалавр
спеціальність 126 Інформаційні системи та технології
Науковий керівник к.т.н., доцент Уткін Ю.В.

ПОРІВНЯННЯ ПІДХОДІВ РОЗРОБКИ САЙТІВ ДЛЯ БІЗНЕСУ

На сьогодні все більше організацій незалежно від напряму роботи приходять до висновку що вебсторінка у всесвітній мережі інтернет має не аби який вплив для інформування користувачів та залучення клієнтів. На створення сайту витрачаються величезні ресурси, а все через те що сьогодні вебсторінка це не просто інструмент, а й обличчя компанії у всесвітній мережі.

В своєму дослідженні я порівнюю способи розробки сайтів для організації за такими критеріями як:

- швидкість розробки
- наповнюваність
- ціна розробки
- складність розробки

При розробці сайту компанії беруть до уваги декілька підходів розробки, а саме:

- створення сайту з чистого листа
- створення сайту на основі вебконструкторів

Важливо зазначити той факт що обидва з цих підходів мають право на життя оскільки повсякденно закривають ряд проблем для своїх власників тобто організацій.

У випадку коли організація переслідує мету вести продажі на своєму сайті, найчастіше використовується другий підхід, а саме залучення до розробки веб конструктори все через те що для таких сайтів не потрібно багато вкладень (Фінансових, людського часу на розробку тощо). Тобто для розробки буде достатньо вибрати шаблон який вам найбільше імпонує та модернізувати його не залучаючи код та програмістів.

Підхід з залученням вебконстуктора є найбільш вигідним оскільки не потребує уваги програмістів, вебдизайнерів, seo-аналітиків тощо, все що треба вже розроблено компанією що розробляє вебконструктор від вас потрібно лише наповнення сайту контентом та товарами, зокрема інтернет магазини це не тільки про продажі їх часто використовують для інших потреб таких як інтернет реклама, просування заходу, афіші, інформаційні сторінки, лендінги, тощо.

Лідерами ринку вебконструкторів у світі по праву вважаються компанії:

- Tilda.cc
- Wix.com
- Bitrix24.ua
- Та інші.

Недоліками вебконструкторів вважаються:

- Умовна безкоштовність - тобто при бажанні ваб сайт можна створити безкоштовно, але при значно меншому функціоналі та при відсутності власного доменного імені, здебільшого при безкоштовному тарифі, на вашому сайті з'являться рекламні елементи від вебконструктора таким чином вони можуть окупити ті ресурси які ви використовуєте.
- Не багатозадачність - тобто у ви не в змозі зробити тих функцій які присутні на сайтах з власною розробкою. Наприклад функція реєстрації користувачів чи власна логіка сайту, іншими словами при використання вебконструктора вам необхідно заздалегідь розуміти навіщо вам необхідний сайт за розуміння що саме він потрібен робити.

При розробці сайту з «чистого листа» перед вами відкриваються всі можливості, в цій ситуації ви самі вигадуєте як ваш сайт буде себе поводити з

користувачами, та що отримають користувачі при користуванні сайту та його дизайн.

Як правило до розробки сайту залучаються наступні спеціалісти

– Веброзробник;
– Веб дизайнер;
– Seo аналітик;
– Вебінженер;
– Копірайтер;
– та інші.

Недоліками розробки сайту с «чистого листа» вважаються:

– Вартість розробки що в декілька разів перевищує ціну вебконструктора;
– Тривалість розробки, як правило на розробку сайту витрачають від декількох місяців до декількох років розробки в залежності від складності продукту та функцій сайту;
– Витрати та час на підтримку серверів та ядра.

Висновок: розробка сайту являється одним із найважливіших етапом для компанії на який витрачаються значні ресурси, обидва підходи мають право на життя оскільки все залежить від часу та ресурсу і у випадках коли часу на запуск сайту немає використовують вебконструктор, який являється швидким та дешевим або умовно безкоштовним способом розробки, але не має тих можливостей які присутні в розробці сайту з «чистого листа».

Список використаних джерел:

1. Формы приема данных. Електронний ресурс. https://help-ru.tilda.cc/
2. Никсон Робин. Создаем динамические веб-сайты с помощью PHP, MySQL, JavaScript, CSS и HTML5. 5-е изд. СПб.: Питер, 2019. 816 с.

Хухро І.В.,
здобувач вищої освіти СВО «Бакалавр».
Спеціальність «Інформаційні системи та технології»
Науковий керівник – к.т.н., доцент Дегтярьова Л.М.

ШТУЧНИЙ ІНТЕЛЕКТ В СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Штучний інтелект (ШІ) дозволяє машинам вчитися на досвіді, пристосовуватися до нової інформації і виконувати завдання людини.

Використовуючи технології глибокого навчання, комп'ютери можна навчати виконанню конкретних завдань за допомогою обробки великих обсягів даних і розпізнавання закономірностей в даних.

Машинне навчання - це метод аналізу даних, який автоматизує побудову аналітичної моделі. Це область штучного інтелекту, заснована на ідеї, що

системи можуть вчитися на основі даних, виявляти закономірності і приймати рішення з мінімальним втручанням людини.

Глибинне навчання - це тип машинного навчання, який навчає комп'ютер виконувати завдання людини. Наприклад, розпізнавати мову, ідентифікувати зображення або робити прогнози. Замість того, щоб організовувати дані для роботи з заданими за замовчуванням формулами, глибинне навчання встановлює базові параметри даних і навчає комп'ютер самостійно навчатися, розпізнаючи шаблони з використанням безлічі шарів обробки.

Система автоматизації документообігу (СЕДО) - інформаційна система, що забезпечує процес створення, управління доступом і поширення електронних документів, а також забезпечує контроль над потоками документів в організації.

На сьогодні СЕДО дозволяють створювати будь-яких типи документів, передбачені діловими процесами в організації. За допомогою СЕДО реалізовано електронний документообіг (ЕДО) - єдиний механізм по роботі з документами, представленими в електронному вигляді, з реалізацією концепції «безпаперового діловодства».

Одиницею електронного документообігу є електронний документ (ЕД) - документ, створений за допомогою засобів комп'ютерної обробки інформації, підписаний електронним цифровим підписом (ЕЦП) і збережений на машинному носієві у вигляді файлу відповідного формату.

Електронний цифровий підпис (ЕЦП) є аналогом власноручного підпису, що забезпечує можливість контролю цілісності і підтвердження достовірності електронних документів.

Також, Законом України «Про електронні довірчі послуги», який набув чинності 7 листопада 2018 року передбачений новий термін - кваліфікований електронний підпис (КЕП), даний підпис створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті відкритого ключа [1].

Переваги системи електронного документообігу для бізнесу:

– зменшення витрат часу на роботу з документами;

– прозоре управління і робота внутрішніх процесів компанії. (система відображає статуси створення й редагування документів на різних етапах узгодження, дані статуси можуть бути переглянуті менеджерами, що відповідають за той чи інший документ. Також, всі зміни в документації відображаються та підписуються автоматично особою, що їх вносила);

– введення історії файлів;

– можливість роботи поза офісом;

– високий рівень захисту даних (у компанії з’являться резервні копії даних, які можуть замінити оригінали в разі їх втрати або пошкодження).

– зменшення або повна відсутність потреб витрати коштів на друк [2].

Зараз СЕДО, як правило, лише маршрутизують документи, завдання і потоки робіт між співробітниками, які і виконують всі необхідні дії.

Відповідно, такі рішення лише автоматизують наявні процеси, що добре, але вже недостатньо.

Найбільш «давня» технологія штучного інтелекту — це технологія розпізнавання тексту (OCR) і структури документів із сканованих зображень або фотографій телефонів. Сама по собі технологія OCR протягом 30 років добре економить час і гроші малих підприємців на перекладі паперових документів у цифрову форму.

Вважається, що на штучний інтелект буде покладено такі завдання, як смисловий аналіз документів і порівняння їх з корпоративними стандартами; передача в потрібну інстанцію і т. д., переходячи до самостійного створення офіційних документів і конструювання бізнес-процесів.

Виділяють такі напрями розробки штучного інтелекту, як складання анотацій до документів і короткої витримки з вмісту, класифікація фінансових документів роботом-бухгалтером, автоматичне формування авансових звітів, нормоконтроль і т. д.

Корпоративні юристи зможуть зосередитися на більш складних завданнях, а первинною експертизою договорів, їх перевіркою на відповідність закону і пошуком ризиків займуться автоматизовані системи на базі машинного навчання [3].

Можливі й інші нововведення, наприклад - голосове управління документами з мобільних пристроїв, яке дозволить продовжити працювати поза офісом. Менше рутинних завдань доведеться вирішувати і HR-фахівців. Штучний інтелект зможе самостійно перевіряти резюме здобувачів на предмет відповідності вимогам до вакансії.

Таким чином, слід зазначити, що до сфер використання штучного інтелекту (розумні сенсори, Інтернет-речей і промисловий Інтернет-речей, обробка природної мови, машинне зір, глибинне навчання, експертні системи, розпізнавання текстів, мови, зображень, бізнес-аналітика, інтелектуальні системи інформаційної безпеки, машинний переклад) можна успішно додати і системи електронного документообігу.

Список використаних джерел:

1. Система автоматизації документообігу: стаття URL: https://uk.wikipedia.org/wiki/Система_автоматизації_документообігу
2. Електронний документообіг: типи, плюси і проблеми: стаття URL: https://techexpert.ua/digital-docu-flow/
3. Роботы в канцелярии: ИИ в СЭД: стаття URL: https://dx.media/articles/analytics/roboty-v-kantselyarii-ii-v-sed/
4. Chollet, François. Deep Learning with Python. Manning Publications, 2017. 363 p.

Чорний Б.В.,
здобувач вищої освіти СВО «Бакалавр»,
спеціальність Інформаційні системи та технології
Науковий керівник – к.т.н., доцент Дегтярьова Л. М.

АНАЛІЗ ВПРОВАДЖЕННЯ ТЕХНІЧНИХ РІШЕНЬ СИСТЕМ CRM КЛАСУ

Актуальною сьогодні є проблема конкурування на ринку споживачів, що змушує бізнес здійснювати використання сучасних маркетингових розробок та технологій, проводити опрацювання питань клієнта на рівні персоналії. Персоналізація маркетингових комунікацій призводить до використання інформаційних систем (CPM). Сутність використання полягає у адресній роботі зі споживачем відповідних послуг та товарів. Розвинені світові торговельні мережі (наприклад, Епіцентр) уже давно інсталювали та використовують обрану CPM. На перше місце ставлять не піклування про загальну кількість споживачів, а про кожного споживача окремо. Оброблена та зібрана інформація про споживачів (до прикладу, історія його покупок, улюблених продуктів, переваг) використовується задля того, щоб провести формування індивідуальної пропозиції для кожного клієнта персонально. Якщо в наявності є велика кількість споживачів, даний підхід вимагає введення сучасних інформаційних технологій [6].

Підвищення ефективності результатів роботи маркетингової програми підприємства слід персоніфікувати як маркетингові комунікації для створення інформаційної бази даних людей, що споживають послуги підприємства при застосуванні CPM-системи. На ринку інформаційних систем України представлені різні CPM-системи, у них вітчизняні та зарубіжні розробники, в зв'язку з чим, їх дослідження являється актуальним під кутом реального впровадження у підприємстві [1].

Основою маркетингової діяльності в даному випадку є інформаційна база даних споживачів з використанням комп'ютерної автоматизованої системи.

Серед CRM-систем, лише три відповідають вимогам до інформаційної системи підприємства, а саме: mySAP CRM (Німеччина), Oracle CRM (США), “Парус-Менеджмент і Маркетинг” (Україна-Росія) [5].

MySAP CRM пропонує широкий функціонал для планування маркетингової діяльності, проведення управління маркетинговими кампаніями, здійснення генерації нових можливостей продажу і сегментації клієнтської бази. Щоб був проведений пошук потенційних клієнтів, залучені всі джерела інформації які можливі, проводиться моніторинг клієнтів. Зі даними клієнтів що були знайдені проводять використання в будуванні багаторівневих маркетингових компаній націлених на чітко визначені сегменти ринку. Недоліком, який є суттєвим являється висока вартість CRM-системи, що перешкоджає її впровадженню у підприємстві. Перевага що є основною у Oracle CRM полягає у зменшенні витрат, які пов'язані з

встановленням, оновленням та підтримкою працездатності обладнання і програмного забезпечення, що працює на ньому. Сервіс не вимагає попередніх інвестицій в IT, легко розгортається, автоматично оновлюється, забезпечуючи високий рівень рентабельності, і дозволяє організаціям оптимізувати продуктивність відповідно до власних вимог.

У застосунках реалізовано прогресивні технології, методи контролю, планування, обробки та аналізу одержаних результатів маркетингових програм, які розраховані на збільшення віддачі від інвестицій, одержання більш вагомої кількості відгуків і ріст обсягів продажів. Покладаючись на це, як і у попередній CRM-системі вагомим недоліком виступає висока вступна ціна [2].

CRM-система "Парус-Менеджмент і Маркетинг" орієнтована на підприємства, які працюють у сфері послуг, торгівлі, виробництва та сервісного обслуговування. Існує кілька галузевих конфігурацій системи. Багатофункціональність даної системи компенсує відсутність можливості програмування. Цінова політика прийнятна для українських малих та середніх підприємств. Вартість проекту для 5 робочих місць від 280 дол. США, сюди входить: установка, 5 годин навчання, обслуговування протягом року. Базова конфігурація "Парус-Менеджмент и Маркетинг" дозволяє автоматизувати наступні завдання:

– ведення єдиної структурованої бази клієнтів;
– планування та обліку продажів;
– маркетингових досліджень і опитувань;
– формування звітності та аналізу даних. Позитивні сторони "Парус-Менеджмент і Маркетинг":
– не вимагає застосування сторонніх СУБД;
– гнучкість налаштування інтерфейсу;
– зручність і дружність інтерфейсу;
– великий перелік функціональних розділів;
– сумісність з пакетами «MS Office» і «Open Office»;
– широка мережа представників в Україні і Росії за ліцензійною супроводу ПЗ;
– наявність навчального центру навчання та сертифікації користувачів системи.

Узагальнюючи, серед трьох вищерозглянутих інформаційних систем CRM-система "Парус-Менеджмент і Маркетинг" є оптимальним результуючим варіантом задля впровадження її у діяльності певного підприємства та використання при формуванні і реалізації маркетингової стратегії [3].

Правильний вибір CPM-системи здатний призвести не тільки до збільшення продажу послуг та товарів, а також підвищення лояльності відвідувачів, покращення якості обслуговування споживачів відповідного підприємства, додатково вирішить наступний перелік завдань: облік клубних і бонусних систем, планування та облік продажів, облік маркетингових заходів і

акцій, облік завантаження персоналу, ведення проектів та маркетингових досліджень і опитувань, формування звітності та аналіз даних [4].

Список використаних джерел

1. Мегаплан – корпоративна CRM-система [Електронний ресурс] Офіційний сайт. – https://megaplan.ru/

2. Wolenik Marc Microsoft Dynamics CRM 2013 Unleashed // Marc Wolenik, Sams Publishing; 1 edition, 2014, p. 1176;

3. Уолренд Дж. CRM – мета використання: Вступний курс / Пер. з англ М : Постмаркет, 2003. 480с.

4. Руденко О.Г., Бодянський Є. В. Впровадження CRM в організаціях. Харків: Компанія СМІТ, 2006. 284 с.

5. Новиков Ю. В., Кондратенко С. В. Впровадження CRM. М : Вид-во ЕКОМ, 2000. 312 с.

6. Оліфер В.Г., Оліфер Н.А. CRM мережі. Принципи, технології, протоколи / В.Г. Оліфер, Н.А. Оліфер. - СПб.: Пітер, 2002 .- 672 с.

Соломка В.О.,
здобувач вищої освіти СВО «Бакалавр»,
спеціальність Інформаційні системи та технології
Науковий керівник – к.т.н., доцент Дегтярьова Л. М.

СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

Під інформаційною безпекою підприємств слід розуміти загальну захищеність середовища, спрямованого на формування, застосування та розвиток інформації (даних).

Конфіденційна інформація, пов'язана з діяльністю конкретної компанії може викликати непідробний інтерес у конкурентів, стаючи об'єктом зазіхань.

Неналежна увага захисту корпоративних даних здатна привести до фінансових та іміджевих втрат, а також стати причиною банкрутства підприємства. Катастрофічні наслідки може мати незначна недбалість всього лише одного співробітника. Особливий інтерес для зловмисників представляють дані під охороною, розкрадання і розголошення яких може завдати максимального збитку [1]. Види загроз інформаційної безпеки:

- втрата конфіденційності даних і програм;
- пошкодження даних;
- відсутність доступу до інформації;
- відмова користувача від інформації, що передається;
- внутрішні загрози (некомпетентність керівництва і співробітників, організація навмисної витоку відомостей).

Автоматизація доступу і робочих процесів - перше, що необхідно зробити для забезпечення інформаційної безпеки підприємства. Для цього

використовується цілий комплекс систем, що здійснюють захист даних, які знаходяться на електронних носіях щоб уникнути несанкціонованого використання і впливу вірусів. Найважливішими опціями спеціалізованих систем є: створення резервних копій і відновлення пошкоджених даних.

Повноцінний захист неможливий без цілодобового контролю за інформацією, який повинен здійснюватися до того моменту, поки дані не втратять актуальність або не будуть повністю вилучені [2].

Системи інформаційної безпеки повинні бути максимально технологічними, здатними ефективно протистояти загрозам усіх типів. Тільки так вони зможуть стати надійним захистом для інформаційного середовища підприємства.

При встановленні системи автоматизації та захисту необхідно враховувати її функціональне призначення і економічну ефективність, що дозволить підібрати оптимальне обладнання та програмне забезпечення. Впоратись з цим завданням можуть лише висококваліфіковані фахівці. Активно використовуватися в забезпеченні інформаційної безпеки повинні інтернет-ресурси, засоби і рішення, розробники яких здатні запропонувати ефективні та доступні онлайн-сервіси [3].

Функціональні можливості систем інформаційної безпеки спрямовані на виконання дій:

– моніторинг, виявлення і визначення спрямованості загроз;

– створення умови для максимально безпечного використання даних;

– оперативне виявлення та усунення наслідків несанкціонованого доступу до інформації.

– класифікація засобів інформаційного захисту:

– технічні; програмні; організаційні; криптографічні;

– законодавчі.

Інформаційна доступність і конфіденційність - основа успішності будь-якої комерційної діяльності. Розробка якісного багаторівневого захисту включає облік видів, форм і способів виникнення можливих загроз.

Найбільшою ефективністю відрізняється криптографічний метод захисту, шифрує не тільки канали доступу, але і дані безпосередньо. Багаторівнева система дозволяє використовувати інформацію обмеженому колу осіб [4]. Визначати ступінь конфіденційності відомостей повинен безпосередній керівник організації. Технології та моделі захисту повинні відповідати ряду галузевих нормативів.

Важливо застосовувати програми, які здійснюють цілодобовий моніторинг доступу в мережу, а також уникати використання недорогих систем бездротового доступу в інтернет, що не володіють належними характеристиками захищеності. Необхідно навчати співробітників роботі з системами автоматизації та захисту даних в цілях зниження ризиків випадкової втрати або розголошення корпоративної інформації. Найвища ринкова конкуренція змушує сучасних підприємців адекватно реагувати на

існуючі економічні реалії, що і призвело до бурхливого розвитку і масового проникнення інформаційних технологій практично в усі сфери бізнесу [5].

Віртуальна складова комерційної діяльності випереджає по ефективності реальну. Недооцінення загроз інформаційній безпеці дорого обходиться багатьом організаціям.

Захист корпоративних даних повинен мати найголовніше значення для підприємств, що прагнуть досягти довгострокового економічного успіху.

Список використаних джерел

1. Горбатюк, О. М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть О. М. Горбатюк Вісник Київського університету імені Т. Шевченка. 1999. № 14 : Міжнародні відносини. С. 46-48.

2. Щербина, В. М. Інформаційне забезпечення економічної безпеки підприємств та установ В. М. Щербина Актуальні проблеми економіки. 2006. № 10. С. 220-225.

3. Маракова, І. Захист інформації: підручник Маракова І., Рибак, А., Ямпольский Ю. Одеса : ОдНПУ, 2001. 164 с.

4. Остроухов, В.В. Проблеми забезпечення інформаційної безпеки України В. В. Остроухов. Політичний менеджмент. 2008. № 4. С. 135–141.

5. Баринов, А. Інформаційний суверенітет чи інформаційна безпека? А. Барсуков. Національна безпека і оборона. 2001. № 1. С. 70-76.

Тищенко А.В.,
здобувач вищої освіти СВО Бакалавр,
спеціальність 126 Інформаційні системи та технології
Науковий керівник – к.т.н., доцент Дегтярьова Л.М.

СПЕЦІАЛІЗОВАНІ ЗАСОБИ ДЛЯ БОРОТЬБИ З ВІРУСАМИ, НЕСАНКЦІОНОВАНИМИ РОЗСИЛКАМИ ЕЛЕКТРОННОЇ ПОШТИ, ШКІДЛИВИМИ ПРОГРАМАМИ

Сучасне життя людини складно уявити без можливості зберегти велику кількість інформації та мати доступ до неї. Однак, людина не здатна впоратись із швидкими потоками інформації, тому і був винайдений комп’ютер, що наразі є найбільш ємним сховищем даних. Але разом з великими можливостями комп’ютер породив великі проблеми захищеності, цілісності, можливості довго зберігати інформацію. Причиною всіх цих проблем став комп’ютерний вірус. Користуючись вірусами, зловмисники можуть зламувати комп’ютерні мережі, грабувати банки, красти інтелектуальну власність. Існують віруси, які можуть самовідтворюватись. Такі віруси заважають комп’ютеру нормально працювати, шкодять інформації яка знаходиться на ньому. Попри те, що багато країн приймають закони для боротьби з комп’ютерними злочинами і для створення програмних засобів для захисту від вірусів, кількість останніх тільки збільшується. Все це вимагає від людини, що

користується комп'ютером великої кількості знань про віруси, шляхи зараження і способи захисту від них.

Комп'ютерний вірус – це програма невеликого розміру, що може записувати себе в кінець виконуваних файлів, драйверів. Також вона здатна розміщувати себе в завантажувальному секторі диска. Під час запуску зараженого драйвера або програми першим спочатку відбувається виконання вірусу, після чого цій програмі передається управління.

Останнім часом все більше трапляються випадки зараження так званими макровірусами. Такі віруси передаються шляхом обміну документами, в яких виконуються макрокоманди (документи текстового редактора Word), цим і зумовлена їх назва. Макровіруси це макрокоманди, що наказують переносити вірус в інші файли і виконувати в них різноманітні шкідливі процеси. В даний час найбільш поширені макровіруси, що заражають файли текстового процесора Word і табличного процесора Excel для операційної системи Windows

Антивірусна програма (антивірус) – спеціальна комп'ютерна програма, призначення якої полягає в знаходженні та знищенні шкідливого програмного забезпечення та вірусів різного роду, з метою коректної роботи вашого пристрою та забезпечення цілісності ваших даних [1].

Антивірусне програмне забезпечення почало з'являтися майже одразу після появи найперших вірусних програм. Наразі над створенням антивірусного програмного забезпечення працюють цілі компанії та тисячі людей.

Антивіруси працюють за двома основними принципами усунення шкідливого програмного забезпечення:

– сканування та виявлення програм, що виконують підозрілі дії і можуть класифікуватись як віруси;

– сканування всього комп'ютера і пошук відповідного все існуючого вірусу у базі даних виробника.

Визначають також класифікацію модулів антивірусу, що є частиною різноманітних антивірусних програм:

1. Сканери – модуль антивірусу, що працює по принципу зіставлення, тобто проводить пошук відповідного вірусу по базі сигнатур. Якість пошуку залежить від актуальності бази даних;

2. Ревізорний модуль – може запам'ятати стан файлів на вашому комп'ютері, щоб надалі мати можливість порівняння для виявлення змін.

3. Монітори – спеціальні помічники, що в разі появи потенційно небезпечного програмного забезпечення пропонують користувачеві виконати перелік певних дій на вибір, серед яких завжди буде функція для видалення.

4. Вакцини – цей модуль діє таким чином, що коли вірус хоче заразити якусь програму, то вакцина показує вірусу, що ця програма вже заражена. Однак в наш час такий метод досить застарів, адже в глобальній мережі існують вже мільйони вірусів.

Багато компаній, розуміючи актуальну проблему поширення вірусів та шкідливого програмного забезпечення через електронну пошту почали

створювати спеціалізовані антивіруси для захисту поштових серверів. Особливість таких антивірусних програм це можливість аналізувати дані, що проходять через сервер пошти, при цьому не допускаючи передачі листів із зараженими файлами. Також існує варіант підключення звичайних антивірусів для перевірки файлів до серверів електронної пошти.

Варіант антивірусного захисту для серверів пошти типу POP3 і SMTP показує себе більш ефективно ніж антивірусний захист пристроїв користувачів. Зазвичай процесом налагодження антивірусної програми на сервері займається адміністратор з досвідом, що не буде робити помилок під час налаштування. Користувачі серверів із захистом POP3 і SMTP можуть не думати про небезпеку поширення вірусів через пошту, повідомлення до них будуть надходити вже очищені, тобто без вірусів [2].

Під час проходження виробничої практики на підприємстві «Солвер-Трейд», де для захисту інформації та підтримання працездатності обладнання встановлена антивірусна програма було проведено ознайомлення з програмними засобами, що забезпечують захист від вірусів і проаналізовано проблему швидкості розвитку антивірусних програм на фоні самих вірусів. Також було проведене самостійне встановлення антивірусних програм на комп'ютерах підприємства для захисту мережі.

Проаналізувавши все вище сказане, можна зробити висновок, що незважаючи на швидкий та широкий розвиток антивірусних програм, самі віруси все більше поширюються. Для протидії останнім, необхідне створення більш якісних та універсальних програм, що будуть мати всі вдалі рішення своїх попередників. Однак, в даний момент немає такого антивірусу, який би гарантував 100% захист ваших даних та вашої системи. Важливим моментом є необхідність вчасно оновлювати ваші антивірусні програми та регулярно перевіряти їх на актуальність.

Список використаних джерел

1. Филин С.А. Информационная безопасность. М .: «Альфа-Прес», 2006. 412 с.

2. Ярочкин В.И. Информационная безопасность.: Учебник для сту дентов вузов. И М.: Академический Проект; Гаудеамус, 2 -е изд. 2004. 544 с .

Городянин А.В.,
здобувач вищої освіти СВО «Бакалавр»,
спеціальність 126 Інформаційні системи та технології
Науковий керівник к.т.н., доцени Уткін Ю.В.

ВАЖЛИВІСТЬ ВПРОВАДЖЕННЯ АНАЛІТИКИ ДЛЯ САЙТУ

Кожне підприємство, або кожен бізнес який має свій сайт, хоча б раз у житті задавалось питанням поліпшення свого сайту. В цьому їм допоможе аналітика сайту.

Аналітика - основа інтелектуальної, логіко-мисленевої діяльності, спрямованої на рішення практичних завдань. У її основі лежить не стільки принцип констатації фактів, скільки принцип «випередження подій», що дозволяє організації або індивідові прогнозувати майбутній стан об'єкту аналізу [1].

Сутність аналітики полягає в тому, що вона дає більш чітке уявлення про користувача сайту, його поведінку. Завдяки цьому покращення сайту, його вміст, зручність користування, весь час буде змінюватись на краще. Користувачу буде легше знаходити потрібну інформацію, легше взаємодіяти з сайтом. Завдяки карті подій є можливість проаналізувати поведінку користувача, які саме сторінки сайту він оглядав, на які посилання переходив. Аналітика дає можливість навіть знати з якого регіону або країни заходить користувач, що дає змогу вчасно впровадити свій бізнес в тій чи іншій країні.

Аналітика допомагає повністю корегувати сайт, змінюючи код сторін для швидкого завантаження, адже чим довше завантажується сторінка тим менша конверсія. Немає конверсії – немає прибутку.

Для кращого розповсюдження сайту використовується реклама, в якій аналітика дає змогу персоналізувати рекламу для більш якісного приросту клієнтів. Адже якщо сайт розрахований на певний вік клієнтів, або на певну діяльність то іншим людям цей сайт не потрібен і не дасть ніякої користі новим користувачам, а гроші вже не повернути.

Інформація утворюється шляхом перетворення первинних даних. Природою появи даних, як джерела інформації, прийнято вважати надходження сигналів оточуючого нас світу та реєстрацію їх певним способом. На основі фундаментальних законів природничих наук можна стверджувати, що фізичні об’єкти знаходяться в стані неперервного руху та змін, які супроводжуються обміном енергії і переходом її з однієї форми в іншу. Всі види обміну енергією між матеріальними об’єктами викликають зміни їх властивостей. Такі зміни можна спостерігати, вимірювати або фіксувати Отже, дані – це зареєстровані сигнали змін енергетичного стану матеріальних об’єктів.

Особливим аспектом управління є вибір відповідного програмного та апаратного забезпечення інформаційних систем, яке дозволило б інтегрувати й реалізовувати комплекс управлінських задач, включаючи як документообіг, так і управління бізнес-процесами в цілому.

Процес впровадження інформаційних систем є складним і повинен відбуватися у певній послідовності, оскільки всі етапи взаємопов’язані та взаємозалежні. При прийнятті рішення адміністрацією компанії про впровадження інформаційних систем, як правило, розробляється план його реалізації. Порушення хоча б одного елементу плану реалізації та термінів його виконання може призвести до порушення налагоджених зв’язків [2]. В цьому допоможе додаток Google analytics, який надасть можливість прослідкувати за поведінкою користувача. Додаток має багато можливостей в допомозі бізнесу. Починаючи від часу утримання користувача на певній сторінці до зацікавленості користувача, які саме сторінки зацікавили

користувача. Google analytics надає можливість перегляду користувачів які перейшли за посиланням інших інтернет-ресурсів або реклами в інтернеті. В порівнянні з сайтами які не використовують Google analytics сайти, які його використовують набагато якісніші та зручні у використанні.

Збільшити трафік на сайт можна без підвищення рекламного бюджету. Якщо використовується кілька каналів залучення трафіку (наприклад, рекламу в Facebook і Instagram, пошукову рекламу в Google, банерну рекламу), веб-аналітика допомагає визначити скільки конверсій приносить кожен канал, і відмовитися від фінансування неефективної реклами. За допомогою веб-аналітики також можна визначити прийнятну вартість залучення клієнта за кожним каналом трафіку [3].

Таким чином ми дійшли висновку, що аналітика грає дуже важливу роль в бізнесі та запобігає зайвим витратам. Допомагає більш якісно опрацювати стратегію розвитку на ринку.

Список використаних джерел:

1. Савченко І. М. Інформаційно-аналітична діяльність педагогічних працівників професійно-технічних навчальних закладів: термінологічний посібник. «Київ», 2014. 127 с.

2. Галич О. А. Управління інформаційними зв’язками та бізнес-процесами: навчальний посібник. Харків: Фінарт, 2016. 244 с.

3. https://ag.marketing/blog/vidpovidi-yaki-ne-otrimati-bez-veb-analitiki/ Електронний помічник для бізнесу.

Савченко. О. А,
здобувач вищої освіти СВО Бакалавр,
спеціальність 126 Інформаційні системи та технології
Науковий керівник: к.т.н., доцент Уткін Ю. В.

АНАЛІЗ ПОТЕНЦІЙНИХ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА

З розвитком Internet-технологій і електронної комерції з кожним днем з'являється все більше загроз безпеки інформації.

Сьогодні організації все частіше використовують інформацію в бізнес-процесах, для полегшення управлінських рішень і ведення бізнесу. Залежність від інформації в бізнес-середовищі вкрай велика, адже безліч торгових операцій здійснюється в електронному вигляді через Internet.

Загроза інформаційної безпеки - сукупність умов і факторів, що створюють небезпеку порушення інформаційної безпеки.

Під загрозою (в загальному) розуміється потенційно можлива подія, дія (вплив), процес або явище, які можуть призвести до заподіяння шкоди чиїм-небудь інтересам.

Беручи до уваги типову фірму, загрози її інформаційній безпеці можна класифікувати за такими критеріями:

- за аспектом інформаційної безпеки (доступність, цілісність, конфіденційність), на що спрямовані загрози передусім;
- за компонентами інформаційних систем, на які спрямовані загрози (дані, програми, апаратура, підтримуюча інфраструктура);
- за способом здійснення (випадкові/навмисні дії природного/ техногенного характеру);
- за розміщенням джерела загроз (всередині/ззовні інформаційної системи).

В якості приклада використано систему відеоспостереження.

Провівши аналіз безпеки об’єктів вважаємо що можна поєднати системи відеоспостереження з датчиками руху, системою контактного розмикання дверей, що дозволить вивести на новий рівень методи сповіщення про порушення на інтерфейс користувача використовуючи мережні технології. Цю систему можна підключити до відео реєстратора і він буде автоматично передавати сповіщення на електронну пошту підприємства.

Таким чином система відеоспостереження як складова системи безпеки об’єкта дозволяє істотно підвищити рівень ефективності її роботи, що покращує рівень безпеки всіх присутніх і збереження набутого майна.

Основні переваги та недоліки існуючих моделей оцінювання ризиків інформаційної безпеки відображено в табл. 1.

Таблиця. 1.

Підходи	Переваги	Недоліки
Модель на основі побудови «Матриці СУІБ»	- повнота опису інформаційної системи, її ресурсів іуразливостей; - можливість виділити найбільш уразливі ресурси; - можливість оцінки існуючої системи захисту інформації.	- наявність суб'єктивної думки щодо визначення важливості активів і частоти реалізації загроз.
Модель оцінювання ризиків інформаційної безпеки на основі нечітких множин	- застосування апарату нечіткої логіки; - можливість розрахувати ймовірність реалізації загрози; - визначає ризики реалізації відповідної загрози.	- неможливо розрахувати час, щовитрачається зловмисником на реалізацію загрози, атакож час виявлення атаки.
Пробіт-аналіз	- забезпечує єдину методологічну базу обліку особливостей пар загроза/наслідок; - основа для вирішення завдання кількісної оцінки у сфері безпеки інформації.	- замало практичних прикладів.
Кількісний аналіз ризиків інформаційної безпеки	- відносна простотавпровадження; - зрозумілість для менеджерів; - є приклади успішного застосування.	- відносно дорогий; - краще застосовуєтьсядо існуючих інформаційних активів.

Стандарти ISO	- спільний підхід до організації управління ризиками.	- концептуальний характер стандартів.
Методи експертних оцінок	- відносна простота; - можливість якісні оцінювання	- суб'єктивність думок експертів; - обмеженість суджень.
Методологія "Facilitated Risk Analysis Process (FRAP)" Методологія RiskWatch	- надає кількісний аналізризиків; - забезпечує симуляційну модель системи. - Відносна простота впровадження; - зрозумілість для менеджерів; - можливість створення своїх профілів захищеності	- Занадто “науковий” метод; - тільки для відносно великих підприємств. - відносно дорогий; - краще застосовується до існуючих інформаційних активів.
Методологія CRAMM	- є універсальною і підходить для організацій як державного, так та комерційного сектору; - використовує кількісні і якісні способи оцінки ризиків; - розроблені комерційні програмні продукти, що реалізовують положенняCRAMM.	

Розглянувши описані вище підходи, можна зробити висновок, що жоден з методів не дає докладних рекомендацій з приводу складання розкладу проведення повторних оцінок ризиків, і в методологіях не приділено уваги оновленню величин ризиків. У разі якщо потрібно виконати тільки разову оцінку рівня ризиків в компанії будь-якого розміру, доцільно застосовувати методологію CORAS. Для управління ризиками на базі періодичних оцінок на технічному рівні найкраще підходить CRAMM.

Методологія OCTAVE краща для використання у великих компаніях, де передбачається впровадження управління ризиками на базі регулярних оцінок на рівні не нижче організаційного і потрібна розробка обґрунтованого плану заходів щодо їх зниження.

Список використаних джерел

1. Кавун С.В., Шубина Г.В. Методика построения политики безопасности организации. Бизнес Информ. 2005. № 1–2. С. 96–102.

2. Види інформаційних загроз. Електронний ресурс- https://sites.google.com/site/vidiinformacijnihzagrozinform/

3. Погребняк А.В. Технології комп’ютерної безпеки. Монографія. МЕГУ, Рівне, 2011. 117 с.

Пилипенко В.О.
здобувач вищої освіти СВО «Бакалавр»,
спеціальність Інформаційні системи та технології
Науковий керівник – к.т.н., доцент Дегтярьова Л. М

ШТУЧНИЙ ІНТЕЛЕКТ В СУЧАСНОМУ ЖИТТІ ТА ПОБУТІ

Штучний інтелект (ШІ)- розділ комп'ютерної лінгвістики та інформатики, що опікується формалізацією проблем та завдань, які подібні до дій, що виконує людина. Штучний інтелект - здатність інженерної системи здобувати, обробляти та застосовувати знання та вміння.

Те, що вчені назвали «штучним інтелектом», сьогодні виглядає як звичайна комп'ютерна програма, та й новітні розробки у вигляді технологій та функцій являються, за великим рахунком, імітацією окремих функцій інтелекту людини. Намагаючись знайти вирішення проблеми, спеціалісти створили нейронні мережі, які в ідеалі повинні були функціонувати по аналогії з людським мозком.

Штучні нейронні мережі (ШНМ) - це обчислювальні системи, натхнені біологічними нейронними мережами, що складають мозок тварин. Такі системи навчаються задачам (і поступально покращують свою продуктивність на них), розглядаючи приклади, загалом без спеціального програмування під задачу.

ШНМ ґрунтується на сукупності з'єднаних вузлів, що називають штучними нейронами (аналогічно до біологічних нейронів у головному мозку тварин). Кожне з'єднання (аналогічне синапсові) між штучними нейронами може передавати сигнал від одного до іншого. Штучний нейрон, що отримує сигнал, може обробляти його, й потім сигналізувати штучним нейронам, приєднаним до нього. Нейронні мережі можуть реалізовуватися як програмно, так і апаратно [1, с. 8-10].

Для написання ШІ використовують таки мови програмування як Lips, Java, Prolog, Python.

В наші дні ШІ використовується в багатьох сферах суспільного життя, промисловості та наукових дослідах. Переглянемо п’ять найбільших областей застосування ШІ:

- медицина (визначає відхилення в будові клітин, звіряє септоматику, оцінює данні отримані з медичної техніки, тестування та моделювання нових ліків);
- фінанси (регуляція базових транзакцій, прогнози, розпізнавання шахрайських дій, загальна автоматизація процесів);
- консультування (консультування клієнтів с залученням ШІ, обробка значного числа запитів одночасно, моментально звертається до баз даних);
- освіта (адаптивна система навчання);
- автомобілі та дорожні рухи (регулювання дорожніх рухів, логістка, система автоматичного керування автомобіля) [2, с. 25-26].

Розглянемо приклад роботи ШНМ на основі розпізнавання голосових команд для розумного будинку. В будинку будуть розташовані мікрофони, є управління кондиціонером, світлом і т.д. за допомогою програмного забезпечення. В цьому будинку живе дві людини, задача полягає в тому, щоб розумний будинок реагував на їх команди та не приймав команди від інших людей. Також, щоб він розпізнавав десять команд, наприклад: увімкнути світло, вимкнути світло, увімкнути кондиціонер, вимкнути кондиціонер, поставити чайник, закрити двері, увімкнути музику, увімкнути телевізор, вимкнути телевізор.

Для успіху в подальшому потрібна навчальна вибірка. Дві людини повинні говорити десять команд по сто екземплярів. Окремо записується фонова розмова власників будинку та сторонніх людей. Це і буде навчальною вибіркою. Завжди процентів двадцять з начальної вибірки береться на тестову вибірку. Завдяки тестовій вибірці можна перевірити ШНМ і що вона не бачила в процесі навчання.

Для роботи з аудіозаписами потрібно перевести їх в спектор (спектральну характеристику). Спектральна характеристика - перетворення в аудіокартинку, де з часом змінюється частоти та їх амплітуда. Саме в цьому спектрі ШНМ розпізнають аудіозаписи. Береться розмова однієї людина, поділяється на маленькі фрагменти по 100 мс.

Таким чином перетворюється вся вихідна база. ШНМ працює безперервно, розділяючи розмову людей на 100 мс, при кожній бесіді для розпізнавання фонової розмови та команди. Іноді 100 мс замало, тоді для коректної роботи ШМ передбачено інші дії.

На разі сфера використання штучного інтелекту стрімко розвивається, можна бути впевненими, що за нею стоїть вирішення та спрощення багатьох проблем людства: побутових, економічних, математичних, фізичних і т.д. Також можуть виникнути певні недоліки: зменшення робочих місць, вихід з ладу приладів, які використовують ШІ, вузька направленість, навіть можливий апокаліптичний сценарій.

Список використаних джерел:

1. Глибовець М.М., Олецький О.В. Системи штучного інтелекту. Київ: Вид. "КМ Академія", 2002. 366 с.
2. Гнатієнко Г.М., Снитюк В.Є. Експертні технології прийняття рішень. К.: ТОВ «Маклаут», 2008. 444с.
3. Рассел С., Норвиг П. Искусственный интеллект: современный подход. М.: Изд-ский дом "Вильямс. 2006.

Красюк А.О.,
здобувач вищої освіти СВО «Бакалавр»,
спеціальність Інформаційні системи та технології
Науковий керівник – к.т.н., доцент Дегтярьова Л. М..

АНАЛІЗ СУЧАСНИХ МЕТОДІВ БЕЗПЕЧНОГО ЗБЕРІГАННЯ ДАНИХ У МЕРЕЖІ ІНТЕРНЕТ

Іформаційна безпека - це захищеність інформації та інфраструктури, що її підтримує, від випадкових або навмисних дій природного чи штучного характеру, які можуть завдати сильного збитку суб'єктам зберігання даних [1].

Цілісністю інформації є такі фактори:

- достовірність;
- актуальність ;
- захищеність інформації від впливу та змоги її змінення;
- конфіденційність являє собою:;
- захищеність баз даних;
- актуальне технічне, апаратне та програмне забезпечення для захисту даних;
- шифрування даних.

Шифрування на рівні бази даних - використання технології шифрування для перетворення інформації, що зберігається в базі даних, в шифротекст, що робить її прочитання неможливим для осіб, що не володіють ключами шифрування.

Одним із прикладів шифрування на рівні бази даних є шифрування на рівні стовпців, яке записує в базу даних вже зашифровані дані, а саму базу даних - без подальшого шифрування - в сховище.

Найбільш сучасним і універсальним типом хмарних сховищ є об'єктне сховище, яке дозволяє працювати з даними найбільш узагальненим способом. Для більшості прикладних користувачів мережевий диск або мережева папка - поняття близькі, якщо не ідентичні. Але в частині системного адміністрування вони істотно розрізняються.

Симетричне шифрування є найстарішим і найвідомішим методом. У контексті бази даних він включає в себе закритий ключ, який застосовується для шифрування та дешифрування інформації, що зберігається в БД і викликається з неї. Цей спосіб виділяється простотою використання та швидкістю роботи, але недоліком є те що, при отриманні ключа сторонньою особою може статися витік інформації яка є конфіденційною, однак ця проблема вирішена за допомогою асиметричного шифрування, в якому є два пов'язаних між собою ключа.

Асиметричне шифрування значно повільніше ніж симетричне, однак є більш безпечним за рахунок того що, відкритий ключ який є абсолютно доступним а також ідентичним для всіх використовується для шифрування даних, а для розшифрування використовується закритий ключ, який є унікальним для кожного користувача [2].

Хмарні сховища - модель онлайн-сховища, в якому дані зберігаються на численних розподілених в мережі серверах, що надаються в користування клієнтам, в основному, третьою стороною. На відміну від моделі зберігання даних на власних виділених серверах, придбаних або орендованих спеціально для подібних цілей, кількість або будь-яка внутрішня структура серверів клієнту, в загальному випадку не помітна.

Дані зберігаються і обробляються в так званій «хмарі», яка представляє собою, з точки зору клієнта, один великий віртуальний сервер. Фізично ж такі сервери можуть розташовуватися віддалено один від одного географічно.

Google диск був представлений 24 квітня 2012 року, який являє собою 15 ГБ пам'яті для безкоштовного збереження даних, та можливість покупки додаткової пам'яті в розмірі від 100 ГБ до 2 ТБ, а вже 13 травня 2013 року Google заявила про об'єднання лімітів і користувач отримував загалом 15 ГБ, на всі сервіси збереження даних Google.(рис. 1,зображено логотип сервісу).

Рис. 1.Логотип Google диску

В даний час існує велика кількість хмарних сервісів, які схожі між собою за якістю надання послуг та своєю роботою в цілому, але також можна звернути увагу на сервіс хмарного зберігання даних від компанії Microsoft під назвою OneDrive.(рис. 2, зображено логотип сервісу)

Рис. 2. Логотип OneDrive

OneDrive представляє собою файловий хостинг створений компанією Microsoft як частина набору онлайн-послуг, що дозволяє користувачам зберігати файли, а також інші особисті дані як ключі відновлення BitLocker або налаштування Windows у хмарі.

Список використаних джерел:

1. Близнюк І.М. Інформаційна безпека України та заходи її забезпечення Науковий вісник Національної академії внутрішніх справ України. 2008. № 5. С. 206-214.

2. Остроухов В.В. До проблеми забезпечення інформаційної безпеки України. Політичний менеджмент. 2008. № 4. С. 135–141.

Кошеленко О. В.,
здобувач вищої освіти СВО «Бакалавр»,
спеціальність Інформаційні системи та технології
Науковий керівник – к.т.н., доцент Дегтярьова Л. М.

ВПРОВАДЖЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СИСТЕМІ УПРАВЛІННЯ ПІДПРИЄМСТВОМ

Стратегію будь-якого підприємства слід встановлювати на основі ефективного управління виробничим процесом з метою отримання найбільшого прибутку. Використання штучного інтелекту в цій галузі може забезпечити найбільш ефективне, швидке та якісне управління всіма бізнес-процесами.

Впровадження комп'ютерних технологій знижує ризик неправильних операцій в організації виробничого процесу. Однак таке впровадження потребує значних інвестицій, що може бути економічно невиправданим за будь-яких обставин. Зараз усі компанії намагаються перенести відповідальні операції на комп'ютери [1].

Штучний інтелект - це наука і технологія, яка може відтворювати процес мислення людського мозку та направляти його до створення та обробки різних комп'ютерних програм, а також інтелектуальних машин, які можуть повністю замінити та спростити роботу людини [2].

У наш час впровадженню штучного інтелекту приділяється багато уваги. Його переваги перед людським інтелектом очевидні, але всі проблеми, пов'язані із впровадженням штучного інтелекту в систему управління підприємством, його роль у ефективності виробничого процесу не до кінця зрозумілі.

В останні роки світова економіка зазнала серйозних динамічних змін, а стрімке зростання потоку інформації вплинуло на рівень розвитку підприємств. Вільний час став більш цінним, інтелект активно копіюється та використовується, зростає попит на високоякісні таланти, здатні виконувати різноманітні завдання, і загалом зростає частка розумової праці. Інтенсифікація цих процесів призводить до змін матеріально-технологічного оновлення сучасного суспільства, а інформаційні системи на основі комп'ютерних технологій та мереж є особливо корисними.

Кожна компанія повинна підтримувати необхідний рівень розвитку для забезпечення своєї ефективної роботи. Для того, щоб організація мала змогу пристосуватися до зовнішніх умов існування, що динамічно змінюються, підприємства повинні постійно перепроектовувати та реорганізовувати свою діяльність, змінювати стратегію, ставити перед собою нові цілі. Важливим елементом ефективної діяльності є стратегічне планування роботи всіх її підрозділів з метою передбачення можливих перешкод або труднощів. Планування підприємства дозволяє сформулювати подальші стратегії, можливості розширення, масштаби збільшення тощо, а також оцінити ефективність кожного підрозділу. Реалізація цих ідей вимагає своєчасного

впровадження інноваційних технологій, які пов'язані з адаптацією всіх відділів та структур до технологічних змін, що відбуваються в сучасному комп'ютеризованому середовищі [3].

У нашій країні більшість компаній, що займаються цим видом робіт, є висококваліфікованими експертами, які можуть передбачити розвиток компанії на основі свого досвіду, знань та здібностей. Однак, оскільки це завдання вирішує одна людина, існує певний ступінь ризику, що експерти можуть помилитися. Тому ми можемо визначити, що основними недоліками людського інтелекту порівняно з швидкісним посібником (комп'ютером) є:

– неможливо виконати велику кількість розрахунків, якщо одна людина аналізує великий обсяг інформації, це збільшує ймовірність пропуску важливих деталей після обробки великої кількості даних одна особа впорядковує інформацію та отримує загальний результат.

– великий обсяг інформації потребує якісної обробки протягом тривалого періоду часу, крім того, для кращої оцінки потрібно більше часу;

– експерти можуть загубитися при роботі з великими обсягами даних, що може призвести до не найефективніших, але, можливо, неправильних рішень;

– відсутність бачення перспектив розвитку, так як вони в умовах високої конкуренції не є очевидними;

– необхідність людського організму у відпочинку;

– неможливість виконання безперервного процесу аналізу, розрахунку чи оцінки тривалого процесу;

– необхідність постійного заохочення працівника до роботи;

– помилковість визначення пріоритетів та цілей під час реорганізації структури чи підприємства в цілому.

– ймовірність негативного впливу емоційного чи фізичного стану людини на якість проведеної роботи.

У повсякденній діяльності виникає проблема вдосконалення систем управління бізнесом, що заохочує використання сучасних комп'ютерних технологій для обробки інформації. Це те, що називається впровадженням технології штучного інтелекту в організацію виробничого процесу.

Застосування комп'ютерних технологій у сфері управління бізнесом, що за допомогою експертних систем управління керівники сучасних провідних підприємств можуть передбачати події та їх результати на основі отриманих даних. Наприклад, аналіз ринку, отримання інформації про характеристики продажу, попиту та пропозиції конкретних видів послуг чи продуктів, моніторинг коливань валютних курсів, оцінка ефективності заходів корпоративного управління та аналіз економічного стану компанії.

Ці системи широко використовуються для контролю, організації та управління виробничим процесом підприємств. Такі комп'ютерні системи управління необхідні для ефективного контролю фінансово - господарської діяльності та швидкої розробки рішень та методів усунення негативних ситуацій.

Основними вимогами сучасних інтелектуальних систем є:

– висока гнучкість та простота взаємодії між системою та користувачем, яка забезпечує розширення системних функцій, щоб охопити більший вміст та збільшити складність завдань, покладених користувачем на систему, що реалізується за допомогою більш потужних інноваційних даних технологічне обладнання, а його логіка;

– найбільш персональні характеристики, придатні для користувачів;

– покращення та спрощення інтерфейсу програми з його наближенням його до природного рівня;

– підвищення рівня автономності проведення операцій, а саме самостійне вирішення проблем з заданої області з можливістю подальшого роз'яснення ходу розрахунку та прийнятих в процесі допущень;

– підвищення наочності обробленого матеріалу з використання мультимедійних засобів;

– можливість синтезу, сумісності, синхронізації та інтегрованості різних комп'ютерних систем;

– забезпечення функціонування системи у режимі реального часу;

– можливість подальшого обновлення та вдосконалення інтелектуальної системи, підтримка нових модифікацій та збереження великого об'єму інформації для можливості аналізу попередніх даних й створення прогнозу на основі попередньо отриманих показників.

Впровадження інтелектуальних систем управління підприємствами та розробка нових комп'ютерних методів організації виробничих процесів є необхідними умовами для виживання та швидкого розвитку окремих підрозділів, структур та цілих організацій на сучасному рівні економічної конкуренції.

Список використаних джерел:

1. Винарик Л.С., Щедрин А.Н., Васильева Н.Ф. Информаційна економика: становленння, развиток, проблеми. Донецьк: ИЭП НАН України, 2002. 311 с.

2. Кизим М. О. Матюшенко І. Ю., Шостак І. В. Перспективи розвитку інформаційно-комунікаційних технологій і штучного інтелекту в економіках країн світу та України : монографія / ВД «Інжек», 2012. 492 с.

3. Саймон Г. Науки об искусственном. М.: УРСС, 2004. 144 с.

Коваль Д.М.,
здобувач вищої освіти СВО «Бакалавр»,
спеціальність Інформаційні системи та технології
Науковий керівник: к.т.н, доцент Дегтярьова Л.М.

АНАЛІЗ МОЖЛИВОСТЕЙ ІНТЕГРАЦІЇ INTERNET OF THINGS І UNMANNED AERIAL VEHICLE

Інтернет речей (Internet of Things, IoT) можна охарактеризувати як мережа, що складається з взаємозв'язаних пристроїв, що містять в собі вбудовані передавачі, а також ПЗ, що здійснює між фізичним світом і комп'ютерними системами передачу і обмін даними в автоматичному режимі, за допомогою використання стандартних протоколів зв’язку. Окрім передавачів, мережа може мати виконавчі пристрої, вбудовані у фізичні об'єкти і пов'язані між собою через дротові чи бездротові мережі. Взаємопов'язані пристрої мають можливість зчитування та приведення в дію, функцію програмування та ідентифікації, а також за рахунок використання інтелектуальних інтерфейсів дозволяють виключити необхідність участі людини.

IoT-системи, Інтернету речей, а також особливості інтеграції різного периферійного обладнання на замовлення поширене в різних організаціях та підприємствах. Спираючись на досвід фахівців різних сфер діяльностей, багато компаній готові впровадити можливості по налагодженню взаємодії на базі COM і USB портів, бездротової технології Bluetooth Low Energy (BLE), в тому числі як основи для IoT систем. А також для створення та залучення в роботу компактних і доступних рішень на базі різних мікрокомп'ютерів [1]. Найбільші програмно-апаратні комплекси, включають понад 10 000 пристроїв від спеціалізованої компанії. Підтримується і онлайн-взаємодія, збір і обмін даними між усіма пристроями і апаратними компонентами той чи іншої компанії, яка надає цей продукт. Наявні технології і можливості щодо забезпечення мережевої взаємодії можуть бути використані для розробки IoT пристроїв в ритейлі, логістиці, промисловості (як основа для Індустрії), розумних будинках, офісах і міських просторах. Слідом за розширенням кількості проектів, сфер застосування обладнання, стає дедалі більше інтегрується периферії. Фахівці компаній завжди готові до кастомной інтеграції в інтересах існуючих і нових замовників. Компанія будучи досвідченим розробником з конкурентоспроможними ПО власної розробки, активно виступає за кооперацію з надійними партнерами.

Але, щоб розпочати дані застосовувати, потрібно налагодити їх правильну обробку. Недостатньо викидати інформацію у великих обсягах у внутрішні системи компанії. Потрібна повноцінна інтеграція даних. Дані потрібно зібрати і перемістити в якусь систему зберігання або в додаток. Там вони оцінюються в контексті бізнес-процесу або контексті використання для прийняття рішень. По суті, інтеграція даних - це те, що по-справжньому дозволяє інтернету речей приносити користь. Але ті, хто використовує IoT,

знають про неї дуже мало. Навіщо інтегрувати дані в інтернет речей Безсумнівно, планування впровадження інтернету речей потрібно починати з бізнес-задач, але рухатися варто в сторону даних. В процесі планування необхідно встановити, які основні дані потрібно зібрати і як їх ефективно використовувати. Дуже часто виявляється, що здатність переміщати і обробляти дані - головна проблема, яку потрібно вирішити. Інтеграція даних - це основа і центр більшості стратегій інтернету речей, які мені доводилося розробляти. Моя порада - сфокусуватися на інтеграції даних як основної частини стратегії використання інтернету речей в компанії. Не важливо, з яких пристроїв ви зібрали ці дані: з носяться пристроїв або з сенсорів на турбінах літаків. Якість даних також має велике значення для IoT.

Можливості IoT коли ми говоримо про можливості інтернету речей, не можна бути гранично точним і конкретним. Цілком можливо, поки ви читаєте це речення, можливості ще збільшилися. Я б в свою чергу сказав, що тут немає конкретних рамок. IoT тільки зараз здатен покрити автономне управління цілим містом, що вже й казати про можливості в побуті чи бізнесі. Можна брати найсміливіші, і, здавалося б, неможливі ідеї та реалізувати їх за допомогою інтернету речей. Також є висока ймовірність того, що всі ваші задумки можна втілити – питання тільки в затраченому часі, засобах і фахівцях, що цим займаються [2].

Безпіло́тний аппарат, а саме (unmanned aerial vehicle, UAV), який працює без наявності людини на борту може мати дистанційне керування або бути автономним апаратом, що здатні аналізувати зовнішнє оточення за допомогою сенсорів та здійснювати самостійно навігацію.

Як і будь-які інші новітні технології, розвиток безпілотної промисловості передбачає певні ризики:

- безпекові (при безконтрольному приземленні в громадських місцях, атомних об’єктах, посольствах, туристичних та пам’ятних місцях, що може спричинити пошкодження майна або поранення людей);

- порушення конфіденційності і таємниці особистого життя, адже безпілотники зазвичай містять відеокамери, мікрофони, різноманітні датчики в т.ч. GPS та системи реєстрації місцерозташування осіб. Оскільки безпілотними відносяться до авіації, вони повинні дотримуватися міжнародних правил безпеки польотів [3].

Для нормативного регулювання використання безпілотних апаратів визначаються наступні категорії:

1.Дистанційно пілотовані авіаційні системи (ДПАС / RPAS) – системи, що містять: літальний апарат, який управляється пілотом з віддаленої пілотної станції (наприклад на землі або в будівлі); одну або кілька пов'язаних з ними віддалених станцій контролю, командування і управління зв'язку та інші компоненти, необхідні для роботи (наприклад злітний трамплін).

2. Безпілотні автономні системи (БАС / UAS) – безпілотні авіаційні системи, які функціонують автономно і керуються за допомогою комп'ютера без втручання пілоту після зльоту. БАС виключені з поля правового регулювання, оскільки на даний час вони заборонені для використання, а

державні органи , у т. ч. в ЄС, не намагаються регулювати їхнє використання на даному етапі. Отже, в подальшому будемо розглядати правове використання дистанційно пілотованих авіаційних систем (ДПАС / RPAS). Технічні характеристики безпілотних літальних апаратів UAV розрізняються за розміром, продуктивністю і типом. Вони можуть бути майже непомітними, як комахи, або великі, схожі на пілотовані літаки. Вони можуть зависати у повітрі або розвивати швидкість до 1000 км/год.

Управління безпілотниками може здійснюватись за допомогою смартфона, планшета або програмного забезпечення супутникового зв’язку. Вони можуть бути запущені за допомогою ракет, катапульт або вручну і переносити різні види матеріалів, наприклад відеокамери або добрива. Сучасні технології дозволяють літати UAV на значні відстані протягом тривалого часу, однак переважна більшість не піднімається більш ніж на 150 м над землею. Повітряний простір на цій висоті використовується здебільшого для польотів планерів та легкомоторної авіації.

Використання IoT, досконало підходить для розвитку та модернізації інформаційної системи департаменту, тому що автономне управління, яке не займає людського ресурс буде покривати велику частку роботи з документообігом та економити бюджет.

Так само UAV може внести великий внесок в сучасну технологію організаційного харакутеру. Наприклад при задіянні департаменту за для облаштування заходу та пітримки в інформаційній сфері UAV, який спроможний обробляти та фіксувати інформацію, щодо проведення заходу та передавати на проекцію вихідні данні допоможе органічно та дисципліновано підтримувати її.

IoT – концепція мережі, що складається із взаємозв'язаних фізичних пристроїв, які мають вбудовані давачі, а також програмне забезпечення, що дозволяє здійснювати передачу і обмін даними між фізичним світом і комп'ютерними системами в автоматичному режимі, за допомогою використання стандартних протоколів зв'язку. Окрім давачів, мережа може мати виконавчі пристрої, вбудовані у фізичні об'єкти і пов'язані між собою через дротові чи бездротові мережі. Ці взаємопов'язані пристрої мають можливість зчитування та приведення в дію, функцію програмування та ідентифікації, а також дозволяють виключити необхідність участі людини, за рахунок використання інтелектуальних інтерфейсів. Набуває поширення також термін Internet of Everything, IoE - всеохопний, або всеосяжний інтернет. Це явище спричинило занепокоєння в конфіденційності інформації й сприяло появі нового терміну безпека інтернету речей.

IoT дуже перспективна концепція мережі. Насамперед тому що:

1.IoT тільки зараз здатен покрити автономне управління цілим містом, що вже й казати про можливості в побуті чи бізнесі

2.Великий прогрес, коли ми говоримо про можливості інтернету речей, не можна бути гранично точним і конкретним. Цілком можливо, поки ви читаєте це речення, можливості ще збільшилися.

3.Реально можливо брати найсміливіші ідеї та реалізувати їх за допомогою інтернету речей.

4.Широкий спектр використання, наявні технології і можливості щодо забезпечення мережевої взаємодії можуть бути використані для розробки IoT пристроїв в ритейлі, логістиці, промисловості (як основа для Індустрії), розумних будинках, офісах і міських просторах.

5.Компанії будучи досвідченими розробниками IoT з конкурентоспроможним ПЗ власної розробки, мають можливість активно виступати за кооперацію з надійними партнерами.

Безпілотний апарат (англ. unmanned vehicle) – це рухомий апарат, який працює без наявності людини (водія або пілота) на борту. Безпілотні засоби можуть мати дистанційне керування, або бути автономними апаратами, які здатні аналізувати зовнішнє оточення за допомогою сенсорів і здійснювати навігацію самостійно [4]. Unmanned aerial vehicle (UAV) це майбутнє сфери авіації та зменшення рисків, невдачі виконання авіа задач.

1.Людська безпека - дистанційно пілотовані авіаційні системи які управляються пілотом з віддаленої пілотної станції.

2.Безпілотні авіаційні системи, які функціонують автономно і керуються за допомогою комп'ютера без втручання пілоту після зльоту.

3.Сучасні технології дозволяють літати UAV на значні відстані протягом тривалого часу

4.Комунікативність, а саме вони можуть бути майже непомітними, як комахи, або великі, схожі на пілотовані літаки. Вони можуть зависати у повітрі або розвивати швидкість до 1000 км/год.

5.Широкий спектр використання, такий як: здійснювання польотів над закритими садами, стеження за людьми на вулицях, підраховувати кількість людей, що заходять і виходять з будівель і т.д.

6.Відносно легке управління безпілотниками може здійснюватись за допомогою смартфона, планшета або програмного забезпечення супутникового зв’язку.

7.Запуск та можливість в перенесені. Вони можуть бути запущені за допомогою ракет, катапульт або вручну і переносити різні види матеріалів, наприклад відеокамери, добрива і т.д.

Таким чином слід зазначити, що IoT так само як і UAV можна в певній мірі впроваджувати в роботу департаменту. Наприклад, можна розглядати IoT, як концепцію мережі, що допоможе здійснювати передачу і обмін даними між фізичним світом і комп’ютерними системами в автоматичному режимі, за допомогою використання стандартних протоколів зв’язку. А UAV насамперед для організацій, контролю та аналізу проведених заходів. Організація заходу за залученням безпілотних апаратів проходила більш організовано та збирала інформацію для аналізу та вдосконалення її контролю проведення.

Список використаних джерел:

1. 3C deps https://deps.ua/ua/katalog/iot.html

2. Б.Ю. Жураковський, І.О. Зенів Технології інтернту речей навч. посібник. КПІ ім. Ігоря Сікорського 2021. 271с.

3. Корольова О. В. Пулим О. В. Туранський М. О. Історія розвитку та застосування розвідувальних і розвідувально-ударних безпілотних комплексів військово-науковий вісник 2021. 301с.

4. Закон і норматив https://www.zakon-i normativ.info/index.php/component/lica/?href=0&view=text&base=24&id=46588&menu=46746

Говоров І.С.,
здобувач вищої освіти СВО «Бакалавр»,
спеціальність Інформаційні системи та технології
Науковий керівник – к.т.н., доцент Дегтярьова Л. М.

АНАЛІЗ СУЧАСНИХ МЕТОДІВ БЕЗПЕЧНОГО ЗБЕРІГАННЯ ДАНИХ У ХМАРНИХ СХОВИЩАХ ДАНИХ

Хмарне сховище даних - це свого роду віртуальний носій інформації, який зберігає і обробляє дані на численних серверах, розкиданих у всесвітній павутині.

Існує три типи хмарних сховищ даних, кожен з яких пропонує унікальні переваги і власні приклади використання [1]:

- об'єктне сховище;
- файлове сховище;
- бочне сховище.

Розміщувати в інтернеті можна різні дані, по-різному організовані, тому і сховища теж можуть бути різними.

Найбільш сучасним і універсальним типом хмарних сховищ є об'єктне сховище, яке дозволяє працювати з даними найбільш узагальненим способом. Для більшості прикладних користувачів мережевий диск або мережева папка - поняття близькі, якщо не ідентичні. Але в частині системного адміністрування вони істотно розрізняються.

Покласти файл в хмарну папку можна або через браузер і веб-інтерфейс, або через спеціальну локальну папку, яка автоматично синхронізується з хмарним сховищем. У другому випадку на комп'ютер користувача потрібно встановити відповідну утиліту.

Сучасні хмарні об'єктні сховища забезпечують високий рівень надійності зберігання даних, гнучкість їх розміщення і опису, високу масштабованість і низьку питому вартість зберігання.

Середовища тестування і розробки програмного забезпечення часто вимагають створення, використання і подальшого видалення окремих, незалежних і дублюючих середовищ зберігання. Крім тимчасових витрат, з цими процесами можуть бути пов'язані серйозні початкові капіталовкладення.

Принцип роботи будь-якого «хмарного» сховища приблизно наступний: на персональний комп'ютер або ноутбук ставиться програма-клієнт

«хмарного» сховища, прописується шлях до папок розташованим на жорсткому диску, які планується помістити в це «хмара». Програма-клієнт копіює інформацію з зазначених папок в сховище, і в подальшому відстежує будь-які зміни в цих папках і автоматично вносить корективи в «хмарне» сховище даних [1].

Покласти файл в хмарну папку можна або через браузер і веб-інтерфейс, або через спеціальну локальну папку, яка автоматично синхронізується з хмарним сховищем. У другому випадку на комп'ютер користувача потрібно встановити відповідну утиліту.

Крім доступу до файлів з різних пристроїв, хмарні папки забезпечують зберігання резервних копій цих файлів. Як правило, хмарна інфраструктура будується на обладнанні з дуже високою надійністю.

В об'єктному сховище прикладної користувач може ефективно зберігати як безліч відносно невеликих об'єктів, так і величезні, наприклад, відеофільми.

Створення резервних копій та відновлення критично важливі для забезпечення захисту та доступності даних, однак дотримання відповідності зростаючим потребам в області ресурсів може стати постійною проблемою. Хмарне сховище забезпечує низьку вартість, високу надійність і практично безмежні можливості масштабування для рішень резервного копіювання та відновлення.

Традиційні локальні рішення для зберігання даних можуть виявитися непередбачуваними в питаннях вартості, продуктивності і масштабованості, особливо з плином часу. Проекти, пов'язані з великими даними, вимагають наявності великомасштабних, доступних і надійних пулів сховищ даних з високою доступністю. Часто подібні пули називають «озерами даних».

Безпека при зберіганні і пересилання даних є одним з основних питань при роботі з «хмарою», особливо щодо конфіденційних і приватних даних. Так, наприклад, провайдер має можливість переглядати дані клієнта (якщо вони не захищені паролем), які також можуть потрапити в руки хакерів, які зуміли зламати системи захисту провайдера.

Питання забезпечення надійного зберігання, безпеки та доступності критично важливих корпоративних даних мають першорядну важливість. При розгляді варіанту зберігання даних в хмарі існує кілька фундаментальних вимог [2]:

- надійність;
- доступність;
- безпека.

Надійність, своєчасність отримання і доступність даних в «хмарі» дуже сильно залежить від багатьох проміжних параметрів, таких як: канали передачі даних на шляху від клієнта до «хмари», надійність останньої милі, якість роботи інтернет-провайдера клієнта, доступність самого «хмари» в даний момент часу.

Список використаних джерел:

1. Микитишин А.Г., Митник М.М., Стухляк П. Д, Пасічник В.В. Комп'ютерні мережі: навчальний посібник. Львів: «Магнолія 2006», 2013. 256 с.
2. Козловський А.В., Паночишин Ю.М. Комп’ютерна техніка та інформаційні технології (навчальний посібник), 2012. 463 ст.

Мандаліна О.С.,
здобувач вищої освіти СВО «Бакалавр»,
спеціальність Інформаційні системи та технології
Науковий керівник – к.т.н., доцент Дегтярьова Л. М.

АНАЛІЗ ПОТЕНЦІЙНИХ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА

Загрози інформаційній безпеці - це різні дії, які можуть привести до порушень стану захисту інформації. Іншими словами, це - потенційно можливі події, процеси або дії, які можуть завдати шкоди інформаційним та комп'ютерним системам.

Загрози ІБ можна розділити на два типи: природні та штучні. До природних відносяться природні явища, що не залежать від людини, наприклад урагани, повені, пожежі і т.д. Штучні загрози залежать безпосередньо від людини і можуть бути навмисними і ненавмисними. Ненавмисні загрози виникають через необережність, неуважність і незнання. Прикладом таких загроз може бути встановлення програм, що не входять в число необхідних для роботи і в подальшому порушують роботу системи, що і призводить до втрати інформації. Навмисні загрози, на відміну від попередніх, створюються спеціально. До них можна віднести атаки зловмисників як ззовні, так і зсередини компанії. Результат реалізації цього виду загроз - втрати коштів та інтелектуальної власності організації [1].

Залежно від різних способів класифікації всі можливі загрози інформаційної безпеки можна розділити на наступні основні підгрупи:

- небажаний контент.
- несанкціонований доступ.
- витоки інформації.
- втрата даних.
- шахрайство.
- кібер-війни.
- кібер-тероризм.

Небажаний контент - це не тільки шкідливий код, потенційно небезпечні програми і спам, але і сайти, заборонені законодавством, також небажані ресурси з інформацією, що не відповідає віку споживача.

Несанкціонований доступ - перегляд інформації співробітником, який не має дозволу користуватися нею, шляхом перевищення посадових

повноважень. Несанкціонований доступ призводить до витоку інформації. Залежно від того, які дані і де вони зберігаються, витоку можуть організовувати різними способами, а саме через атаки на сайт, злом програм, перехоплення даних по мережі, використання несанкціонованих програм.

Витоки інформації можна розділяти на умисні й випадкові. Випадкові витоку відбуваються через помилки обладнання, програмного забезпечення та персоналу. Умисні, в свою чергу, організовуються навмисно з метою отримати доступ до даних, та завдання шкоди [2].

Втрату даних можна вважати однією з основних загроз інформаційній безпеці. Порушення цілісності інформації може бути викликано несправністю обладнання або навмисними діями людей, будь то співробітники або зловмисники.

Не менш небезпечною загрозою є шахрайство з використанням інформаційних технологій «фрод». До шахрайства можна віднести не тільки маніпуляції з кредитними картами «кардинг», а також і злом онлайн-банку. Цілями цих економічних злочинів є обхід законодавства, політики безпеки або нормативних актів та привласнення майна.

Щорічно у всьому світі зростає терористична загроза, поступово переходячи при цьому в віртуальний простір. На сьогоднішній день нікого не дивує можливість атак на автоматизовані системи управління технологічними процесами (АСУ ТП) різних підприємств. Але подібні атаки не проводяться без попередньої розвідки, для цього застосовується кібер-шпіонаж, який допомагає зібрати необхідні дані. Існує також таке поняття, як «інформаційна війна», вона відрізняється від звичайної війни тим, що в якості зброї виступає ретельно підготовлена інформація.

Порушення режиму інформаційної безпеки може бути викликано як спланованими операціями зловмисників, так і недосвідченістю співробітників. Користувач повинен мати хоч якесь поняття про ІБ, шкідливий програмному забезпеченні, щоб своїми діями не завдати шкоди компанії і самому собі. Такі інциденти, як втрата або витік інформації, можуть також бути обумовлені цілеспрямованими діями співробітників компанії, які зацікавлені в отриманні прибутку в обмін на цінні дані організації, в якій працюють або працювали.

Основними джерелами загроз є окремі зловмисники «хакери», кібер-злочинні групи і державні спецслужби (кібер-підрозділи), які застосовують весь арсенал доступних кібер-засобів, перерахованих і описаних вище. Щоб пробитися через захист і отримати доступ до потрібної інформації, вони використовують слабкі місця і помилки в роботі програмного забезпечення і веб-додатків, вади в конфігураціях мережевих екранів і налаштуваннях прав доступу, вдаються до прослуховування каналів зв'язку і використання клавіатурних шпигунів [3].

Те, що буде проводитися атака, залежить від типу інформації, її розташування, способів доступу до неї і рівня захисту. Якщо атака буде розрахована на недосвідченість жертви, то можливо, наприклад, використання спам-розсилок.

Оцінювати загрози інформаційної безпеки необхідно комплексно, при цьому методи оцінки будуть відрізнятися в кожному конкретному випадку. Так, щоб виключити втрату даних через несправність обладнання, потрібно використовувати якісні комплектуючі, проводити регулярне технічне обслуговування, встановлювати стабілізатори напруги. Далі слід встановлювати і регулярно оновлювати програмне забезпечення (ПЗ). Окрему увагу потрібно приділити захисному ПЗ, бази якого повинні оновлюватися щодня [4].

Навчання співробітників компанії основним поняттям інформаційної безпеки і принципам роботи різних шкідливих програм допоможе уникнути випадкові витоки даних, виключити з використання випадкове встановлене потенційно небезпечне програмне забезпечення на комп'ютері. Також в якості запобіжного заходу від втрати інформації слід робити резервні копії. Для того щоб стежити за діяльністю співробітників на робочих місцях і мати можливість виявити зловмисника, слід використовувати DLP-системи [5].

Організувати інформаційну безпеку допоможуть спеціалізовані програми, розроблені на основі сучасних технологій:

– захист від небажаного контенту (антивірус, анти-спам, веб-фільтри, анти-шпигуни);
– мережеві екрани і системи виявлення вторгнень (IPS);
– управління обліковими даними (IDM);
– контроль привілейованих користувачів (PUM);
– захист від DDoS; захист веб-додатків (WAF);
– аналіз вихідного коду; анти-фрод;
– захист від націлених атак;
– управління подіями безпеки (SIEM);
– системи виявлення аномальної поведінки користувачів (UEBA);
– захист АСУ ТП;
– захист від витоків даних (DLP);
– шифрування;
– захист мобільних пристроїв;
– резервне копіювання;
– системи відмовостійкості.

Таким чином можна зазначити, що інформаційна безпека – це комплексна багаторівнева система, яка охоплює інтереси людини, суспільства і держави. В науці питання інформаційної безпеки досліджуються безпекознавством, правовими науками (насамперед, інформаційним правом), теорією управління, соціологією, політологією та психологією.

Список використаних джерел:

1. Горбатюк О.М. Сучасний стан та проблеми інформаційної безпеки України на рубежів// Вісник Київського університету імені Т.Шевченка. 2009. Вип. 14: Міжнародні відносини. С. 46-48.

2. Близнюк І.М. Інформаційна безпека України та заходи її забезпечення// Науковий вісник Національної академії внутрішніх справ України. 2008. № 5. С. 206-214.

3. Остроухов В.В. До проблеми забезпечення інформаційної безпеки України // Політичний менеджмент. 2008. № 4. С. 135–141.

4. Гуцалюк М.О. Інформаційна безпека України: нові загрози // Бизнес и безопасность. 2007. № 5. С. 2–3.

5. Харченко Л.С., Ліпкан В.А., Логінов О.В. Інформаційна безпека України: Глосарій. К.: Текст, 2004. 136 с.

Побережний Р.Д.,
здобувач вищої освіти СВО Бакалавр,
Спеціальність Інформаційні системи та технології
Науковий керівник: к.т.н., доцент Дегтярьова Л.М.

ЗАСОБИ ДІАГНОСТИКИ ПІДКЛЮЧЕННЯ ДО МЕРЕЖІ ІНТЕРНЕТ

На сьогодні багато користувачів підключені до мережі Інтернет, й не виключенням є збої в підключенні до нього. Причини переривання з'єднання можуть бути різні: програмні, апаратні та технічні. Для кожної проблеми є своє рішення, але щоб виявити проблему потрібно провести діагностику [1].

Діагностика - це сукупність дій направлених на пошук несправності в системі тощо.

Технічна діагностика - галузь науково-технічних знань, сутність якої складають теорія, методи і засоби постановки діагнозу про стан технічних об'єктів.

Метою технічної діагностики є підвищення надійності та ресурсу технічних систем. Основним завданням технічної діагностики є розпізнавання стану технічної системи в умовах обмеженої інформації. Діагностика також може проводитися без розбору приладу. Діагностування здійснюється людиною, програмою або апаратурою.

Діагностика інтернету – це тест або серія тестів, які допомагають користувачу оцінити фінкціональність комп'ютера.

До діагностики Інтернету належить тест швидкості інтернету, тест налаштувань, тест якості лінії, тест ping, тест програмного та апаратного забезпечення. Тести пропускної здатності вимірюють як швидко машина може отримувати і передавати дані в Інтернет. Тести Ping допомагають користувачам визначити, чи може низька продуктивність комп'ютера бути віднесена до комп'ютера, його інтернет з'єднанню або інтернет трафіку. Тести налаштувань допомагають користувачам оптимізувати настройки мережі для забезпечення стабільного з'єднання. Точно так же діагностичний тест Інтернет може допомогти мережевим адміністраторам оптимізувати мережеву безпеку [2].

Перше можна провести діагностику за допомогою стандартної програми Windows «Діагностика неполадок»(рисунок 3 та рисунок 4). Після проведення діагностики система покаже ймовірну причину поломки (наприклад відмова DNS-серверу).

Інтернет з'єднання можна перевіряти в консолі за допомогою команди PING + адреса сайту.

Ще один із способів це підключення іншого пристрою до мережі. Якщо підключення є то це програмна помилка в першому пристрої. В цьому випадку може допомогти скидання налаштування мережі.

Якщо використовується бездротова мережа Wi-fi, варто спробувати підключення через кабель Ethernet. Якщо провідний Інтернет з'являється то проблема в налаштуваннях роутера.

Також це може бути програмний збій або апаратна поломка. Це можна продіагностувати в «Диспетчер пристроїв». Якщо в списку немає мережевої то вона вийшли з ладу і потребує ремонту, а якщо навпроти неї горить індикатор то слід оновити драйвери.

Однією з причин можливе механічне пошкодження кабелю скрученої пари. Це можна діагностувати за допомогою спеціального приладу або візуально.

Також з'єднання може зупинитись за виною провайдера. Це може бути наприклад пошкодження кабелю чи мережевого обладнання.

Отже проблема переривання з'єднання є досить поширеною та має різні причини та способи вирішення. Причинами можуть стати як і програмне забезпечення комп'ютера так і його апаратне оснащення. Для уникнення розривів потрібно своєчасно оновлювати драйвери та слідкувати за технічним станом обладнання.

Несправності фізичного рівня можуть виникнути в мережевому пристрої, в середовищі передачі або в місці їх контакту. Вони найбільш легко піддаються виявленню, так як носять постійний характер (природно, до моменту їх усунення). Локалізувати несправність можна, зокрема, за допомогою найпростіших тестерів для локальних мереж. Такі тестери перевіряють роботу каналу в одну сторону (від тестера до концентратора або до мережевої плати комп'ютера). Якщо дефект має місце в середовищі передачі, то його можна виявити за допомогою кабельного тестера.

Плаваючі помилки, обумовлені поганим контактом в місцях з'єднання, діагностувати трохи складніше. Але навіть такі несправності можна виявити за допомогою кабельного тестера - досить бути уважним. Найкращий спосіб профілактики утворення дефектів в середовищі передачі - використання якісних матеріалів і виконання професійного монтажу.

Інструментальна діагностика виконується за допомогою досить дорогих приладів - мережевих тестерів і аналізаторів протоколів.

Мережеві тестери займають проміжне положення між кабельними тестерами і аналізаторами протоколів. Вони незамінні для пошуку несправностей в мережах. Виробники випускають широку гаму таких приладів, що відрізняються набором контрольованих параметрів і сервісних

функцій, здатністю працювати в тих чи інших мережах (наприклад, Ethernet і /або Token Ring), конструктивним виконанням і ціною. Ці прилади дозволяють вимірювати безліч різних параметрів, наприклад пікову і усереднену завантаженість, частку широкомовного трафіку, збої в роботі протоколів верхніх рівнів. У мережах Ethernet деякі з них здатні підраховувати число конфліктів (колізій), ідентифікувати адреси DLC-пакетів (з помилками CRC, коротких і довгих), відрізняти фрагменти від пакетів з помилками CRC і коротких пакетів. У мережах Token Ring вони підключаються до кільця, в якому запущений процес аварійної сигналізації, і можуть визначити станцію з перевантаженим буфером прийому, виявити порядок станцій в кільці, заміряти час обходу маркера і т. п.

Деякі сучасні моделі мережевих тестерів можуть працювати як сервери Web, тому вони дозволяють як призначеного для користувача інтерфейсу використовувати звичайний браузер. Але найефективнішими пристроями є прилади, що поєднують функції портативного мережевого і кабельного тестера.

Список використаних джерел:

1. Скотт Хогдал Дж. Анализ и диагностика компьютерных сетей. М., Лори, 2001. 354 с.
2. Олифер В.Г.,Олифер Н.А. Основы компьютерных сетей. СПб.: Питер, 2009. 352 с.

Ростовський Н.М.,
здобувач вищої освіти СВО Бакалавр,
Спеціальність 126 Інформаційні системи та технології
Науковий керівник к.т.н, доцент Дегтярьова Л.М.

МОЖЛИВОСТІ ОПТИМІЗАЦІЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ПІДПРИЄМСТВА

Перед сучасним приватним підприємством завжди актуальним буде питання комп'ютерної мережі, тобто питання про її вибір, встановлення, налагодження.

Це пов'язано з розвитком інформатизації підприємства.

Потрібно дуже обґрунтовано і вивірено підійти до питання вибору комп'ютерної мережі, щоб отримати ідеальне співвідношення ціни якості і зручності.

Але потім цю мережу потрібно ще оптимізувати для максимально продуктивної її роботи.

Отже, для початку постає питання вибору мережі, для цього потрібен аналіз всіх актуальних видів топологій, від «шини», до комбінацій «дерева» з «зіркою». Після ретельного аналізу потрібно обрати топологію яка буде найзручнішою для підприємства вашого виду.

Щоб обрати комп’ютерну мережу потрібно повністю проаналізувати можливості підприємства, апаратне забезпечення, розміри робочих приміщенн, а також звичайно фінансові можливості компанії, бо економити на комп’ютерній мережі недоцільно.

Морально застаріла «шина», яка вже не актуальна, одразу не підходить для будь якого типу компаній. Для великої комп’ютерної мережі краще обирати якісь комбінації топологій. Коли ж, для менших підприємств вистачить і звичайної «зірки».

Після установки мережі, повної її настройки, потрібно перейти до питання її оптимізації.

Основним моментом в оптимізації мережі є повний і постійний контроль за роботою локальної мережі, це необхідно для підтримки її постійно працездатною. Це також потрібно для зберігання продуктивності підприємства. Часто контроль відокремлюють від інших функцій систем управління і реалізують спеціальними засобами. Такий поділ функцій контролю необхідний для невеликих і середніх мереж, для яких установка системи управління недоцільна через велику ціну і складність обслуговування.

Етап контролю умовно поділяється на моніторинг та аналіз. На етапі моніторингу збирають початкові дані про роботу мережі

На етапі аналізу дані осмислюються і досліджуються на предмет виявлення помилок у роботі, і причин можливого сповільнення роботи.

Основним пунктом в оптимізації мережі є постійний контроль за роботою локальної мережі, що становить основу будь-якої корпоративної мережі, це необхідно для підтримки системи постійно працездатною. Контроль - це обов'язковий етап, який повинен виконуватися при управлінні мережею. Взявши до уваги необхідність цієї функції її часто відокремлюють від інших функцій систем управління і реалізують спеціальними засобами. Такий поділ функцій контролю і управління зазвичай необхідне для невеликих і середніх мереж, для яких установка системи управління просто недоцільна. Використання автономних засобів контролю допомагає адміністратору мережі виявляти несправні ділянки і устаткування мережі, а їх відключення або реконфігурацію він може виконувати в цьому випадку вручну.

Процес контролю роботи мережі зазвичай ділять на два етапи – моніторинг і аналіз

На етапі моніторингу виконується більш проста процедура - процедура збору первинних даних про роботу мережі: статистики про кількість циркулюючих в мережі кадрів і пакетів різних протоколів, стан портів концентраторів, комутаторів і маршрутизаторів і т. п.

Далі виконується етап аналізу, під яким розуміється складніший і інтелектуальний процес осмислення зібраної на етапі моніторингу інформації, зіставлення її з даними, отриманими раніше, і вироблення припущень про можливі причини сповільненої або ненадійної роботи мережі.

Також для оптимізації систем можна використовувати метод моделювання.

Моделювання є потужним методом наукового пізнання, при використанні якого досліджуваний об'єкт замінюється більш простим об'єктом, який називається моделлю. При фізичному моделюванні досліджувана система замінюється відповідної їй іншої матеріальної системою, яка відтворює властивості досліджуваної системи зі збереженням її фізичної природи. Прикладом такого виду моделювання може служити пілотна мережа, за допомогою якої вивчається принципова можливість побудови мережі на основі тих чи інших комп'ютерів, комунікаційних пристроїв, операційних систем та програм.

Список використаних джерел:

1. Уилсон Эд. Мониторинг и анализ сетей. Методы выявления неисправностей : моногр. М.: Лори, 2002. 368 с.
2. Кулаков Ю. А., Омелянский С. В. Компьютерные сети. Выбор, установка, использование и администрирование. Киев : Юниор, 2010. 544 с.