Міністерство освіти і науки України
Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Національний університет «Львівська політехніка»

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
V Всеукраїнської науково-практичної конференції
молодих учених, студентів і курсантів

26 листопада 2021 року

Львів – 2021

ББК 32.81+78.362

*Інформаційна безпека та інформаційні технології: з*бірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 26 листопада 2021 року. Львів, ЛДУ БЖД, 2021, 225 с.

За точність наведених фактів, самостійність наукового аналізу та нормативність стилістики викладу, а також за використання відомостей, що не рекомендовані до відкритої публікації відповідальність несуть автори опублікованих матеріалів.

Секція 1
КІБЕРБЕЗПЕКА

УДК 004.056

РІВНІ ТА СМИСЛОВА ОРГАНІЗАЦІЯ ЛОГ-ФАЙЛІВ

Башкіров М., Навитка М.
Львівський державний університет безпеки життєдіяльності

Використання незахищених веб-додатків в рази збільшує ризики несанкціонованого доступу до корпоративних ресурсів і призводить до порушення працездатності веб-сайтів

В даній статті проведено аналіз рівнів та організації лог-файлів. Сформульовано і наведено типи лог-файлів та рівні логування.

Ключові слова: *ПЗ, інформаційне середовище, лог-файли.*

The use of unprotected web applications increases the risk of unauthorized access to corporate resources and leads to disruption of websites

This article analyzes the levels and organization of log files. The types of log files and levels of logging are formulated and given.

Keywords: *software, information environment, log files.*

Забезпечення безпеки інформаційного середовища - завдання складне і відповідальне. Дослідження вмісту файлу реєстрації помилок після виникнення неполадок часто дозволяє зрозуміти їх причини. Основні функції лог-файлів дуже часто розширюються виробниками ПЗ під свої конкретні потреби. Розробляються нові формати зберігання даних, нові методи і стандарти представлення даних. Покращують продуктивність і універсальність систем логування.

Рівні логування виглядають так:

– рівень trace виводить все підряд. У ньому корисно відзначати виклики різноманітних блокуючих і асинхронних операцій.

– рівень debug виводить журнал роботи моментів виклику «великих» операцій. Старт/Стоп потоку, запит користувача і т. п.

– рівень info виводить разові операції, які повторюються вкрай не часто, але не регулярно. (Завантаження налаштувань, додатків, запуск резервування даних).

– рівень warning виводить несподівані параметри виклику, дивний формат запиту, використання стандартних значень на заміну не коректних. Взагалі все, що може свідчити про не штатне використання.

– рівень error виводить підставу для уваги розробників. Тут розглядається конкретне місце помилки.

– рівень fatal – виводить все найкритичніше.

За смисловою організацією лог-файлів слід розділяти на три групи.

1) Група інформування, з відповідним рівнем для всіх джерел. Це інформація для адміністратора. Тут можуть бути такі дані: час старту додатку, чи правильно вичитані налаштування, чи доступні необхідні сервіси, і т. д. Його основна властивість тому, що файл змінює розмір тільки при

перезавантаженні додатка. В процесі роботи, файл рости не повинен. Це допоможе забезпечити автоматизований зовнішній контроль успішності запуску додатка. Досить перевірити відсутність у файлі ключових слів Error і Fatal. Перевірка завжди буде займати невеликий проміжок часу.

2) Група застережень. Це теж інформація для адміністратора. Цей файл при нормальній роботі повинен бути відсутнім або бути порожнім. Відповідно моніторинг його стану відразу вкаже на збої в роботі. Гнучко налаштувавши фільтри за різними джерелами, можна підібрати досить точний критерій, коли взагалі слід звернути увагу на сервіс.

3) Група Спостереження. Як правило в ході впровадження виділяються деякі проблемні модулі. Інформація від них в деталізації Debug якраз і прямує сюди.

Сеанс автоматично завершується, якщо користувач у програмі не запитав або не оновив сторінку протягом певного періоду часу. За промовчанням цей період становить 20 хвилин. Зменшуючи вказаний за умовчанням час очікування сеансу, можна одночасно встановити властивість Timeout (очікування) для об'єкта Session (сеанс).

Отже, все залежить від того, як налаштований додаток. Для читання таких додатків найчастіше використовується спеціальне програмне забезпечення, так як лог-запис, в якому кожна подія розтягнуто на кілька рядків, а ще й самі події залежать один від одного, досить важко інтерпретувати.

Втім, деякі виробники попереджають про можливі проблеми незалежно від конфігурації. Хоч, зазвичай, є можливість підібрати конфігурацію системи аудиту, яка буде не надто обтяжливою. Також використання бази даних для логування інформації, що стосується транзакцій і безпеки, не скасовує того, що інші послуги, що входять в СУБД, можуть мати лог-файли.

Література

1. Сайт Microsoft присвячений вивченню і розробці програмного забезпечення [Електронний ресурс] – Режим доступу: https://msdn.microsoft.com.

2. Бегун А. В. Web-програмування : навч. посіб. / А. В. Бегун, О. Є. Камінський. К. : КНЕУ, 2011. – 324 с.

6. Захист WEB-додатків. Чому це актуально? URL: https://blog.liga.net/user/vberegovoy/article/33552.

7. НД ТЗІ 2.5-010-03. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.

8. НД ТЗІ 3.6-001-2000. Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження і модернізації засобів технічного захисту інформації від несанкціонованого доступу.

УДК 004.65

ОСОБЛИВОСТІ ЗАХИСТУ МЕРЕЖІ WI-FI З ПРОТОКОЛОМ ШИФРУВАННЯ WPA3

Богданов О., Бурак Н.
Львівський державний університет безпеки життєдіяльності, м. Львів

Проведено дослідження особливостей захисту мережевого трафіку у безпровідникових мережа з використання протоколу WPA, зокрема оновленої версії 3. Висвітлено переваги та недоліки у порівнянні з попередніми версіями.
Ключові слова: WPA3, безпека, шифрування, мережа

A study of the features of network traffic protection in wireless networks using the WPA protocol, in particular the updated version 3. Highlights the advantages and disadvantages compared to previous versions.
Keywords: WPA3, security, encryption, network.

До недавнього часу для надійного захисту мережі Wi-Fi зазвичай було достатньо використовувати WPA2 і досить довге і складне ключове слово. І хоча WPA2 пропонує безліч покращень у плані безпеки в порівнянні з WPA, він все ще страждає від використання слабких паролів. Алгоритм вразливий для атак методом перебору, які можуть бути успішними, коли користувач використовує прості паролі.

Коли клієнт підключається до бездротового пристрою (WiFi-маршрутизатора, точки доступу і т.д.), пароль, який потрібно для підключення, зазвичай передається за допомогою алгоритму WPA2. У 2018 році Wi-Fi Alliance представив WPA3, що відкриває можливості щодо його реалізації для виробників бездротового обладнання зв'язку. WPA і WPA2 з'явилися (перший у 1999 році, а інший – у 2004 році), щоб подолати серйозні недоліки, яким був схильний старий алгоритм WEP.

Крім того, завжди рекомендується не використовувати поширений SSID (ідентифікатор мережі WiFi), оскільки зловмисники можуть використовувати попередньо створені райдужні таблиці для прискорення атаки. Атаки, які використовують PIN-код WPS на маршрутизаторі Wi-Fi для отримання несанкціонованого доступу до мережі Wi-Fi, дуже поширені.

Дослідження Меті Ванхофа вказують на можливість відкриття вмісту пакетів даних, які проходять між захищеними WPA/WPA2 WiFi-маршрутизаторами/точками доступу та клієнтськими пристроями, навіть не зламавши пароль для захисту бездротової мережі інших користувачів. Після оголошення про виявлення вразливості виробники WiFi-пристроїв одразу випустили оновлення програмного забезпечення для виправлення вразливості.

Однак проблема стосується самого стандарту, і оновлення системи безпеки випущені не для всіх пристроїв, що знаходяться в обігу. Тому перехід на нову та безпечнішу версію WPA стає необхідністю, а WPA3, як зазначається у дослідження, забезпечить вирішення усіх недоліків попередньої версії протоколу.

Розробником протоколу шифрування WPA3 є некомерційна асоціація Wi-Fi Alliance, утворена основними «великими» компаніями у галузі IT – Apple, Samsung, Sony, LG, Intel, Dell, Broadcom, Cisco, Qualcomm, Motorola, Microsoft та Texas Instruments).

Усі пристрої Wi-Fi, для яких виробник хоче відобразити логотип Wi-Fi CERTIFIED WPA2 або Wi-Fi CERTIFIED WPA3, повинні суворо відповідати специфікаціям, опублікованим альянсом.

Сьогодні, час при використанні громадських мереж Wi-Fi (наприклад, в аеропортах, готелях, барах та ресторанах, житлових приміщеннях, громадських місцях) їхня безпека залишається «під знаком питання».

Мережний трафік, що генерується пристроєм (за винятком зашифрованого трафіку, наприклад, що передається по HTTPS), після підключення до загальнодоступної мережі Wi-Fi фактично може бути прочитаний третіми особами, підключеними до того ж маршрутизатору або точці доступу. Тому завжди рекомендується використовувати VPN у таких ситуаціях, що забезпечує найкращі гарантії при використанні загальнодоступного Wi-Fi, керованого третіми особами.

Якщо у є VPN-сервер у домашній або офісній мережі (найповніші та універсальні маршрутизатори підтримують OpenVPN), можливо встановити віддалене зашифроване з'єднання або використовувати службу VPN.

WPA3 дозволяє подолати ці проблеми, активуючи індивідуальне шифрування даних: щоразу, коли абонемент підключається до загальнодоступного Wi-Fi, весь трафік, що передається між окремим пристроєм і точкою доступу, буде зашифрований, навіть якщо пароль не вимагався.

Щоразу, коли пристрій підключається до точки доступу Wi-Fi, запускається процедура, яка називається рукостисканням, яка дозволяє перевірити правильність введеного пароля та продовжити узгодження з'єднання.

Процедура рукостискання виявилася вразливою для атак методом перебору, хоча виправлення, випущені різними виробниками обладнання, дозволяють мінімізувати ризики.

WPA3 встановлює новий спосіб виконання рукостискання, надійний та виключає використання методу «грубою сили». Рішення WPA3 настільки надійне, що робить мережу Wi-Fi захищеною, навіть якщо користувач встановить простий пароль.

За останні кілька років світ сильно змінився, і тепер все частіше трапляються пристрої з інтерфейсом Wi-Fi, які не мають дисплея. Це насамперед пристрої, що належать світові Інтернету речей (IoT).

Для підключення цих пристроїв до мережі Wi-Fi зазвичай потрібно встановити програму або підключитися до локального веб-сервера, встановленого на цих пристроях, за допомогою іншого терміналу, підключеного до тієї ж локальної мережі.

WPA3 включає функцію, яка покликана спростити процес налаштування кожного пристрою Wi-Fi без дисплея.

Високий рівень безпеки для промислових програм. WPA3 включає 192-бітовий пакет безпеки, який зробить використання нового протоколу придатним для всіх додатків, де важлива конфіденційність даних. Такі специфікації дозволять активувати захист військового рівня, який також може використовуватись державними органами та компаніями для промислового застосування.

Слід зазначити, що для кожного WiFi-маршрутизатора WPA3 повинні використовуватися бездротові клієнти, сумісні з WPA3. В іншому випадку нові функції WPA3 не можуть бути використані. З метою легкого переходу клієнтів на новий стандарт, WPA3-сумісні маршрутизатори також зможуть приймати з'єднання WPA2. Крім того, навіть коли WPA3 буде досить поширеним, слід очікувати досить тривалого перехідного періоду, протягом якого деякі пристрої будуть підключатися до маршрутизатора через WPA3, а інші – через WPA2.

Таким чином, на основі проведеного аналізу особливостей реалізації нового протоколу WPA3, можна зробити висновок про необхідність його терміново впровадження в усіх сферах використання безпровідникових мереж різного призначення. Інтеграційні процеси не передбачають одночасної заміни всіх мережевих інтерфейсів та їх програмного забезпечення. Впровадження можливе поступово, оскільки у стандарті WPA3 залишиться підтримки попереднього стандарту WPA2.

Література

1. Що таке WPA3 і як він робить мережі Wi-Fi більш безпечніши-ми. [Електронний ресурс] – режим доступу до ресурсу - https://windows-school.ru/blog/chto_takoe_wpa3/2020-05-24-641.

2. Протокол WPA3: нове покоління чи планова модернізація WiFi? [Електронний ресурс] – режим доступу до ресурсу - https://wifi-solutions.ru/protokol-wpa3-novoe-pokolenie-ili-planovaya-modernizaciya-wifi/

3. Безпека WPA3 [Електронний ресурс] – режим доступу до ресурсу - https://spy-soft.net/wpa3

4. WPA3 – новий рівень безпеки WiFi 802.11. [Електронний ресурс] – режим доступу до ресурсу -https://www.atraining.ru/wpa3-802-11-2018/

УДК 004.6

ВИЯВЛЕННЯ НЕБЕЗПЕЧНИХ ВХОДЖЕНЬ У КОМП'ЮТЕРНУ МЕРЕЖУ ЗА ДОПОМОГОЮ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Боднар О., Лагун А., Ткачук Р.
Львівський державний університет безпеки життєдіяльнсті, м. Львів

В роботі розглядаються вимоги до систем виявлення та запобігання вторгнень, а також описаний вибір методів та критеріїв досліджень IDPS. Проведено аналіз сучасних IDPS-систем, досліджено особливості їх роботи.
***Ключові слова**: IDS/IPS системи, інформаційна безпека, Snort, Suricata.*

The paper considers the requirements for intrusion detection and prevention systems, as well as describes the choice of methods and criteria for IDPS research. The analysis of modern IDPS-systems is carried out, features of their work are investigated.
***Key words:** IDS/IPS systems, information security, Snort, Suricata.*

Найважливішим атрибутом нашого часу є глобальна інформаційна інтеграція, заснована на побудові комп'ютерних мереж масштабу підприємства і їх об'єднання за допомогою Інтернету.

Складність логічної і фізичної організації сучасних мереж призводить до об'єктивних труднощів при вирішенні питань управління та захисту мереж. В процесі експлуатації комп'ютерних мереж адміністраторам доводиться вирішувати дві головні завдання [5]:

– діагностувати роботу мережі і підключених до неї серверів, робочих станцій і відповідного програмного забезпечення;

– захищати інформаційні ресурси мережі від несанкціонованої діяльності хакерів, впливів вірусів, мережевих черв'яків і тп. ті. забезпечувати їх конфіденційність, цілісність і доступність.

При вирішенні завдань, пов'язаних з діагностикою та захистом мережевих ресурсів, центральним питанням є оперативне виявлення станів мережі, що призводять до втрати повної або часткової її працездатності, знищення, перекручення чи витоку інформації, що є наслідком відмов, збоїв випадкового характеру або результатом отримання зловмисником несанкціонованого доступу до мережевих ресурсів, проникнення мережевих черв'яків, вірусів і інших загроз інформаційної безпеки. Раннє виявлення таких станів дозволить своєчасно усунути їх причину, а також попередить можливі катастрофічні наслідки.

Для їх виявлення використовується великий спектр спеціалізованих систем. Так, при вирішенні проблем діагностики мереж застосовуються засоби систем управління, аналізатори мережевих протоколів, системи тестування навантаження, системи моніторингу мережі. Проблеми захисту

інформаційних ресурсів мереж вирішуються за допомогою міжмережевих екранів (firewall), антивірусів, систем виявлення атак (вторгнень) (СВВ) (Intrusion Detection System, IDS), систем контролю цілісності, криптографічних засобів захисту [3, 4].

Характерними особливостями використання цих систем є або їх періодичне і короткочасне застосування для вирішення певної проблеми, або постійне використання, але зі статичними настройками. В результаті методи аналізу, що використовуються в сучасних системах, спрямовані на виявлення відомих і конкретніше згаданих типів впливів, але можуть виявитися не в змозі виявити їх модифікації або нові типи, що робить їх використання малоефективним.

Таким чином, на сьогоднішній день дуже актуальним завданням є пошук більш ефективних методів виявлення неприпустимих подій (аномалій) в роботі мережі, які є наслідком технічних збоїв або несанкціонованих дій. Основною вимогою до цих методів є можливість виявлення довільних типів аномалій, в тому числі нових, а також впливів, розподілених у часі.

Цей напрямок наукових досліджень є дуже молодим. Перші роботи, присвячені даній проблемі, були опубліковані в 90-х роках минулого століття.

На даний момент дослідження в цій області ведуться великими закордонними комерційними компаніями. Загальний підхід, який лежить в основі цих досліджень, полягає в пошуку методів аналізу, що дозволяють виявляти аномальні стани інформаційних ресурсів у вигляді відхилень від звичайного («нормального») стану. Ці відхилення можуть бути результатами збоїв в роботі апаратного і програмного забезпечення, а також причинами мережевих атак хакерів. Такий підхід теоретично дозволить виявляти як відомі, так і нові типи проблем. Від ефективності і точності апарату, що визначає «нормальний» стан і фіксує відхилення, залежить в цілому ефективність рішення питань діагностики та захисту мережевих ресурсів. Особливу важливість на поточний момент становить проблема виявлення аномальних станів в роботі мережі, що мають розподілений у часі характер. Вони можуть бути наслідками спеціально маскуючих мережевих атак зловмисників, прихованих апаратно-програмних збоїв, нових вірусів і т. п.

Системи виявлення та запобігання вторгнень (IDPS) в основному зосереджені на виявленні можливих інцидентів, реєстрації інформації про них, спробі їх зупинити і повідомленні про них адміністраторам безпеки. Існує багато типів технологій IDPS, які диференціюються насамперед за типами подій, які вони можуть розпізнати, та методологіями, які вони використовують для виявлення можливих інцидентів [1, 2].

Типи технологій IDPS:

– Network-Based;
– Host-Based;
– Wireless;

– Application-Protocol-Based;
– Protocol-Based;
– Network Behavior Analysis;
– Hybrid.

Більшість IDPS використовують кілька методологій виявлення, як окремих, так і інтегрованих, для забезпечення більш широкого і точного виявлення. Основними класами методологій виявлення є наступні:

– виявлення на основі підписів;
– виявлення на основі аномалій.

Перш ніж обирати продукцію IDPS, організації повинні спочатку визначити загальні вимоги, яким повинна відповідати продукція. Функції, що надаються продуктами IDPS, та методології, які вони використовують, значно різняться, тому продукт, який найкраще відповідає вимогам однієї організації, може не відповідати вимогам іншої організації. Спочатку оцінювачі повинні зрозуміти характеристики системного та мережевого середовища організації та плани на короткострокові зміни, щоб можна було обрати IDPS, який буде сумісним з ними та матиме змогу контролювати події, що цікавлять системи та / або мережі. Ці знання також необхідні для розробки рішення IDPS. Отримавши розуміння існуючої системи та мережевого середовища, оцінювачі повинні сформулювати цілі та завдання, які вони хочуть досягти, використовуючи IDPS. Оцінювачі також повинні переглянути свої існуючі правила безпеки та інші IT-політики перед вибором продуктів. Ці правила слугують специфікацією для багатьох функцій, які повинні надавати продукти IDPS. Крім того, оцінювачі повинні розуміти, чи підлягає організація нагляду чи перегляду іншою організацією чи ні. Якщо так, вони повинні визначити, чи вимагає цей орган нагляду IDPS або інші конкретні ресурси системи безпеки. Обмежувачі ресурсів також повинні враховуватися оцінювачами. На додаток до визначення загальних вимог, оцінювачі також повинні визначити більш спеціалізовані набори вимог [4, 5]:

– захисні можливості, включаючи збір інформації, реєстрацію, виявлення та запобігання;

– ефективність, включаючи максимальну потужність та характеристики продуктивності;

– управління, включаючи проектування та впровадження, експлуатацію та технічне обслуговування та навчання, документація та технічна підтримка;

– витрати життєвого циклу, як початкові, так і витрати на обслуговування.

Отже, ми можемо зробити висновок, що системи виявлення вторгнень та запобігання вторгнень проводять моніторинг подій, що відбуваються в комп'ютерній системі або мережі, і аналізують їх на наявність ознак мож-

ливих інцидентів, які є порушеннями або неминучими загрозами порушення політик комп'ютерної безпеки, політик допустимого використання або стандартних методів забезпечення безпеки та здійснюють спроби зупинки виявлених можливих інцидентів. Деякі організації використовують IDPS для інших цілей, таких як виявлення проблем з політиками безпеки, документування існуючих загроз і утримання окремих осіб від порушення політик безпеки. IDPS стали необхідним доповненням до інфраструктури безпеки майже кожної організації.

IDPS не можуть забезпечити повністю точне виявлення; всі вони генерують false positivse (невірне визначення доброякісної активності як шкідливої) і false negativse (нездатність ідентифікувати шкідливу активність).

Вибір правильної системи з точки зору компанії залежить від ряду факторів:

– необхідного рівня захисту мережі;
– сфери діяльності компанії;
– підготовки фахівців;
– бюджету організації.

Література

1. Офіційний сайт фірми Snort [Електронний ресурс] // Snort IDPS – 2021 - Режим доступу до ресурсу: https://www.snort.org/.

2. Офіційний сайт фірми Suricata [Електронний ресурс] // Suricata Open Source IDS / IPS / NSM engine – 2021 – Режим доступу до ресурсу: https://suricata-ids.org/.

3. Офіційний сайт фірми OSSEC [Електронний ресурс] // OSSEC HIDS – 2021 – Режим доступу до ресурсу: https://www.ossec.net/.

4. Система обнаружения вторжений на базе IDS Snort [Електронний ресурс] // OpenNET – 2007 – Режим доступу до ресурсу: https://www.opennet.ru/base/sec/snort_ids.txt.html.

5. Системы обнаружения вторжений. Разворачиваем Snort и пишем правила [Електронний ресурс] // Эксплойт – 2018 – Режим доступу до ресурсу: https://telegra.ph/Sistemy-obnaruzheniya-vtorzhenij-Razvorachivaem-Snort-i-pishem-pravila-11-25.

УДК 004.056

ПАРСИНГ ДАНИХ З ВЕБ СТОРІНОК

Брітвін А., Ткачук Р.
Національний університет "Львівська політехніка", м .Львів
Львівський державний університет безпеки життєдіяльності, м .Львів

В роботі описано основні ключові фактори розробки автоматизованої системи парсингу інформації з веб сторінок. Ключовим фактором дослідження є усвідомлення необхідності оптимізації алгоритму, створення безперебійної системи з автоматичним відновленням стану, та мінімізацією шансу втрати даних.

Ключові слова: *аналіз веб-сторінки, великі дані, модель клієнт-сервер, побудова системи.*

The paper describes the main key factors in the development of an automated system for parsing information from web pages. A key factor in the study is the awareness of the need to optimize the algorithm, create a seamless system with automatic recovery, and minimize the chance of data loss.

Keywords: *web page analysis, big data, client-server model, system construction.*

З моменту впровадження великих обсягів даних у наші сучасні бізнес моделі потреба у вилученні, аналізі та обробці даних стає все більш важливою для компаній у всіх галузях промисловості. Зі збільшенням збору даних зростає потреба їх читати та розуміти [1].

Парсинг даних – це процес взяття даних в одному форматі та перетворення їх в інший формат. Цей процес є дуже важливий у сучасному світі, оскільки сьогоднішнє життя переходить на цифровий рівень.

Парсинг даних включає у себе лексичний і синтаксичний аналіз. Загалом його можна охарактеризувати як процес аналізу рядка символів у мові, що відповідає правилам формальної граматики. Аналіз з точки зору дослідження даних розширює це визначення у двоетапний процес, в якому синтаксичний аналізатор програмовано вказує, які дані читати, аналізувати або перетворювати. Результатом зазвичай є більш структурований формат.

Важливим аспектом придатності даних для цілей є структура, в якій вони знаходяться. Часто сама структура не підходить для потреб даних [2].

Веб парсинг – це метод отримання великого обсягу загальнодоступних даних з веб -сайтів. Він автоматизує збір даних і перетворює зібрані дані у формати на ваш вибір, такі як HTML, CSV, Excel, JSON, txt [3]. Цей просес насамперед складається з 3 частин:

– аналіз HTML сторінки;

– видобуток даних;

– зберігання даних.

Найважливіше у парсингу даних – це програмування. Через це багатьом компаніям потрібно наймати досвідчених розробників для сканування

веб-сайтів. Тоді як для тих, хто не має великого бюджету та не володіє навичками кодування, стануть у нагоді інструменти для скребку в Інтернеті. І парсингові мови програмування, і використання інструментів веб-парсингу мають деякі спільні переваги. Серед основних переваг парсингу даних можна виділити:

– видобуток даних автоматизований;
– висока швидкість;
– зібрана інформація є набагато точнішою ніж зібранна в ручну;
– отримання чистих та структурованих даних.

Після збору даних зазвичай відбувається їх очищення та реорганізація, оскільки зібрані дані не є структурованими та готовими до використання. Інструменти веб-скребку перетворюють неструктуровані та напівструктуровані дані у структуровані, а інформація веб-сторінки реорганізовується у презентабельні формати [3, 4].

Для того щоб створити сценарії парсингу даних з веб сторінок, нам необхідно зробити декілька кроків з налаштування нашого проекту. Першим кроком необхідно додати в проект бібліотеку selenium webdriver. Далі створимо екземпляр Chrome із шляхом до драйвера, який завантажили через веб-сайти відповідного браузера. Далі використовуючи метод .get () драйвера для завантаження веб-сайту. Ми також можемо завантажити локальний сайт розробки, оскільки цей процес еквівалентний відкриттю вікна Chrome на локальній машині, введенню URL-адреси та натисканню Enter. Метод .get () не тільки починає завантаження веб-сайту, але і чекає його повного візуалізації, перш ніж перейти до наступного кроку. Після успішного завантаження сторінки можна скористатися атрибутом .title для доступу до текстового заголовка веб-сторінки.

Тобто, для того щоб пропарсити дані з веб-сторінки нам необхідно створити драйвер браузера, який буде імітувати звичайний веб-браузер. Далі необхідно задати адресу потрібного нам сайту, та користуючись командами даної бібліотеки отримати необхідні елементи сторінки.

Література

1. Viktor Mayer-Schönberger. Big Data: A Revolution That Will Transform How We Live, Work /, Kenneth Cukier., 2014. – 280 с. – (3). – (2).

2. Cathy O'Neil, Rachel Schutt. Doing Data Science: Straight Talk from the Frontline / Cathy O'Neil, Rachel Schutt., 2013. – 510 с. – (O'Reilly Media, Inc.).

3. Selenium is an umbrella project for a range of tools and libraries that enable and support the automation of web browsers. [Електронний ресурс] // Selenium. – 2021. – Режим доступу до ресурсу: https://github.com/SeleniumHQ.

4. HTML [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://developer.mozilla.org/ru/docs/Web/HTML.

УДК 004.056

АЛГОРИТМ ВИЯВЛЕННЯ MITM-АТАКИ ПІД ЧАС ARP-POISONING

Бурнашов С., Ящук В.
Львівський державний університет безпеки життєдіяльності, м. Львів

Розглянуто методи та способи деструктивного програмного впливу на інформаційні системи. Запропоновано алгоритм виявлення MITM (Man in the middle) атаки під час ARP-poisoning, який зчитує ARP таблицю та перевіряє чи є два або більше ідентичних MAC-адрес. У разі виявлення однакових MAC-адрес алгоритм інформує, від'єднує від мережі або блокує ті хости які мають однакову адресу в залежності де працює алгоритм на маршрутизаторі чи персональному комп'ютері.

Ключові слова: *MITM, Man in the middle, ARP-poisoning, ARP, MAC-адреса.*

The algorithm for detecting MITM (Man in the middle) an attack is considered, namely during ARP-poisoning. The algorithm reads the ARP table and checks if there is two or more identical MAC addresses. If identical MAC addresses are detected, the algorithm informs, disconnects from the network or blocks those hosts that have the same address, depending on where the algorithm works on the router or a personal computer.

Key words: *MITM, Man in the middle, ARP-poisoning, ARP, MAC- address.*

Сьогодні прискорення виробничих процесів, підвищення мобільності та оперативності доступу до інформації та послуг, можливість віддаленого управління банківськими рахунками, замовлення й оплати товарів і послуг – це низка очевидних переваг, що зумовлює значне зростання вартості інформації, що циркулює в комп'ютерних мережах. Забезпечення працездатності мереж, а також працездатності інформаційних систем, залежить не тільки від надійності використовуваної апаратури, але і від здатності мережі протистояти цілеспрямованим діям, які спрямовані на порушення її роботи.

Слід зазначити, що атаки на інформаційні системи з кожним роком стають усе досконалішими, масштабнішими та інтенсивнішими. Тому актуальною є проблема розроблення та вдосконалення систем виявлення вторгнень, головним завданням яких є саме виявлення мережевих атак, спроб несанкціонованого доступу та використання ресурсів мережі. Постійний стрімкий розвиток методів та способів деструктивного програмного впливу на інформаційні системи зумовлює необхідність виявлення атак та запобігання вторгненням з метою визначення найбільш ефективних механізмів захисту інформації.

Розглянемо метод компрометації каналу зв'язку, при якому зловмисник, приєднавшись до каналу між контрагентами, здійснює втручання в протокол

передачі, видаляючи або змінюючи інформацію. Такий вид атак має назву атака «людина посередині», MITM-атака (англ. Man in the middle).

Атака зазвичай починається з прослуховування каналу зв'язку та закінчується тим, що зловмисник намагається підмінити перехоплене повідомлення, витягти з нього корисну інформацію, перенаправити його на який-небудь зовнішній ресурс. Атаки «людина посередині» становлять загрозу для систем, що здійснюють фінансові операції через інтернет — наприклад, електронний бізнес, інтернет-банкінг, платіжний шлюз. Застосовуючи цей вид атаки, зловмисник може отримати доступ до облікового запису користувача та здійснювати різні фінансові махінації.

На рис. 1 наведено мережу для проведення MITM атаки та її виявлення, де ПК1 та ПК3 це користувачі, а ПК2 це комп'ютер зловмисника.

Маршрутизатор має IP-адресу 192.168.1.1 та MAC-адресу 00-00-00-00-00-AA

ПК1 має IP-адресу 192.168.1.2 та MAC-адресу 00-00-00-00-00-BB

ПК2 має IP-адресу 192.168.1.3 та MAC-адресу 00-00-00-00-00-CC

ПК3 має IP-адресу 192.168.1.4 та MAC-адресу 00-00-00-00-00-DD

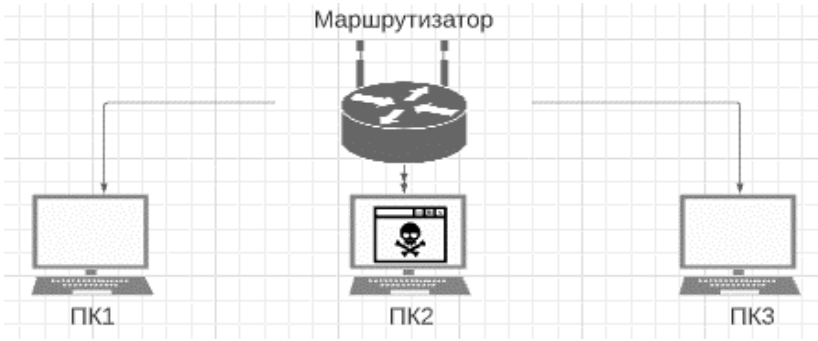


Рис. 1. Мережа для проведення MITM атаки та її виявлення

Якщо зловмисник на ПК2 здійснить атаку на всі хости то ми побачимо змінену ARP-таблицю з MAC-адресою ПК2, а саме 00-00-00-00-00-CC. Наприклад користувач ПК1 бачитиме таку таблицю:

Interface: 192.168.1.2 – 0x8

192.168.1.1 00-00-00-00-00-CC

192.168.1.3 00-00-00-00-00-CC

192.168.1.4 00-00-00-00-00-CC

Якщо зловмисник на ПК2 здійснить атаку на ПК1 та маршрутизатор то MAC-адреси, для ПК1 матимуть вигляд:

Interface: 192.168.1.2 – 0x8

192.168.1.1 00-00-00-00-00-CC (змінена на MAC-адресу ПК2 зловмисника)

192.168.1.3 00-00-00-00-00-CC (MAC-адреса ПК2)

192.168.1.4 00-00-00-00-00-DD (не змінена)

MAC-адреси для ПК3 матимуть вигляд:

Interface: 192.168.1.4 – 0x8

192.168.1.1 00-00-00-00-00-CC(змінена на MAC-адресу ПК2 зловмисника)

192.168.1.2 00-00-00-00-00-CC(змінена на MAC-адресу ПК2 зловмисника)

192.168.1.3 00-00-00-00-00-CC(MAC-адреса ПК2)

Отже, під час ARP-poisoning атаки маємо 1 або більше збігів з MAC-адресою ПК2 зловмисника. Тому за допомогою методу перебору всіх MAC-адрес та порівняння їх між собою можемо визначити наявність MITM атаки, якщо під час перебору та порівняння маємо збіг 2 або більше MAC-адрес то атака існує.

Цей алгоритм можемо виконати будь-якою мовою програмування за такої послідовності: отримуємо ARP-таблицю; відфільтровуємо данні, та отримуємо тільки два параметри IP та MAC-адреса ПК в мережі; перебираємо та порівнюємо список ПК за їх MAC-адресою; якщо маємо збіг MAC-адрес, виводимо повідомлення з IP та MAC-адресою всіх ПК на які здійснена атака; сповіщаємо користувача, або передаємо IP-адресу для блокування на певний час у фаєрвол.

Література

1. Атака «людина посередині» [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/%D0%90%D1%82%D0%B0%D0%BA%D0%B0_%C2%AB%D0%BB%D1%8E%D0%B4%D0%B8%D0%BD%D0%B0_%D0%BF%D0%BE%D1%81%D0%B5%D1%80%D0%B5%D0%B4%D0%B8%D0%BD%D1%96%C2%BB

2. ARP [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/ARP

3. ARP spoofing [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/ARP_spoofing

УДК 004.056

ПРОФІЛАКТИЧНІ ЗАХОДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМП'ЮТЕРНИХ МЕРЕЖ

Власенко В.
ДВНЗ «Київський національний економічний університет ім. Вадима Гетьмана», м. Київ

Анотація: *В роботі описується важливість безпеки комп'ютерної мережі та методи ефективних контрзаходів.*

Ключові слова: *комп'ютерна мережа, Інтернет, інформація та безпека*

Abstract: *The paper describes the importance of computer network security and methods of effective countermeasures.*

Keywords: *computer network, Internet, information and security*

Вступ. Комп'ютерна мережа відіграє важливу роль у всіх сферах життя, а також є одним із важливих проявів глобалізації. Комп'ютер тісно пов'язаний з нашим життям і роботою, тому багато важливих документів і матеріалів зберігаються у вигляді електронних файлів. Однак комп'ютери не є абсолютно безпечними, час від часу трапляються випадки крадіжки інформації. Для вирішення цих проблем існує багато рівнів технологій, таких як технологія криптографії, технологія мережевої безпеки тощо. У нашій країні також проведено чимало досліджень щодо захисту безпеки комп'ютерних мережевих технологій, і ці результати досліджень також досягли певних результатів у реальній побудові комп'ютерної мережі.

Виклад основного матеріалу. Із збільшенням розміру мережі, все більше і більше небезпечних факторів, таких як мережева атака, є серйозною загрозою для інформаційної безпеки. Безпека комп'ютерної мережі стала глобальною проблемою. Технологія захисту комп'ютерних мереж та інформації є основним питанням ефективного захисту комп'ютерних і мережевих систем. Витік, підробка та підробка інформації в Інтернеті, поширення вірусів і поширення поганої інформації створюють дуже згубну загрозу для мережі. Безпека комп'ютерної мережі, вживаючи різноманітні технічні та управлінські заходи, забезпечують нормальну роботу мережевої системи, забезпечуючи доступність, цілісність і конфіденційність мережевих даних.

Будь-яка мережева послуга спричиняє загрозу безпеці, а отже, постає питання в тому, як мінімізувати ризик. Наведемо декілька контрзаходів захисту мережі:

1. Дуже важливо створити безпечне мережеве середовище, включаючи моніторинг користувачів, встановлення дозволів користувача, використання контролю доступу, ідентифікацію, моніторинг маршрутизаторів тощо.

2. Профілактика комп'ютерних вірусів. Комп'ютерні віруси створюються штучно, використовуючи лазівки в комп'ютерному програмному забезпеченні. Завдяки швидкому розвитку комп'ютера та появі нових вірусів швидкість передачі стає все швидшою. Крім того, шкода стає все

більш серйозною. Найпоширенішим засобом профілактики комп'ютерних вірусів є встановлення антивірусного програмного забезпечення для перевірки та знищення файлів, заражених вірусом.

3. Технологія брандмауера. Брандмауер – це система, яка використовується для захисту мережевої безпеки різних хостів, користувачів або підмереж. Основною функцією брандмауера є впровадження та застосування політики безпечного доступу між різними підмережами. Брандмауер розділяє мережу користувача на різні підмережі відповідно до функцій і рівня безпеки, а також здійснює контроль доступу через брандмауер.

Інтранет – це мережа довіри. Він може отримати доступ до зовнішніх мереж, таких як Інтернет, через брандмауери. Він також може отримати доступ до мережі, яка надає послуги через брандмауер, тобто до спільної підмережі безпеки. Видно, що через брандмауер ми можемо контролювати доступ між підмережами різних рівнів безпеки та запобігати зловмисному чи несанкціонованому доступу.

4. Шифрування даних. Оскільки мережеві хакери можуть вторгнутися в систему, викрасти дані або підслуховувати дані в мережі. Шифрування даних може призвести до того, що вкрадені дані не будуть просто відкриті, тим самим трохи зменшивши втрати. На даний момент технологія шифрування є відносно зрілою, і зазвичай використовуються два типи технологій шифрування: технологія шифрування симетричного ключа та технологія шифрування з відкритим ключем.

5. Цифровий підпис. Це метод аутентифікації цифрової інформації, заснований на технології шифрування з відкритим ключем. Це може ефективно гарантувати безпеку мережевої інформації та електронної пошти. Якщо немає ключа користувача, він не зможе прочитати інформацію. Крім того, він може ідентифікувати та перевіряти електронні документи, таким чином ефективно захищаючи конфіденційність та цілісність електронної пошти. Шифрування файлів відноситься до шифрування мережевої інформації та даних, щоб запобігти їх крадіжці, щоб сприяти підвищенню конфіденційності.

Висновок. Люди все більше уваги приділяють безпеці комп'ютерної мережі. В умовах стрімкого розвитку індустрії мережевої безпеки та прискорення інформаційного процесу продовжуватимуть застосовуватися різноманітні нові технології. Безпека потребує посилення застосування керування обліковими записами, антивірусного програмного забезпечення, системи ідентифікації електронної пошти, цифрового підпису та шифрування документів. Тому, дослідження, як краще захистити безпеку комп'ютерних мереж, відіграють важливу роль у захисті інформаційної безпеки та інтересів користувачів мережі.

Література

1. Xinzhou He. Research on Computer Network Security Problems and Countermeasures – 2021. – Режим доступу до ресурсу: https://iopscience.iop.org/article/10.1088/1742-6596/1992/3/032069/pdf

2. Ajala Funmilola. Review of Computer Network Security System – 2015. – Режим доступу до ресурсу: https://core.ac.uk/download/pdf/234686636.pdf

УДК 514.18:004.056

ІНФОРМАЦІЙНИЙ ЗАХИСТ КРЕСЛЯРСЬКОЇ ДОКУМЕНТАЦІЇ

Гумен О., Селіна І., Абрамова А.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського», м. Київ

Інформаційні технології глибоко увійшли в наше життя. Інформація є величезною цінністю в цифрову епоху, тому і необхідно її збирати, захищати і правильно зберігати. Багато спеціалістів працюють над захистом інформації, технологій, креслеників, інших документів, тобто над захистом конфіденційної інформації. Необхідність в інженерно-технічному захисті викликана активним розвитком засобів видобутку інформації. Системний підхід до його забезпечення і контроль дозволять здійснювати та будуть запорукою успішного захисту інформаційних ресурсів.

Ключові слова: *конфіденційна інформація, інженерно-технічний захист, кресленики.*

Information technologies are deeply ingrained in our lives. Information is of great value in the digital age, so it is necessary to collect, protect and properly store it. Many specialists work on the protection of information, technologies, drawings and other documents, that is on the protection of confidential information. The need for engineering protection is caused by the active development of information mining. A systematic approach to its provision and control will allow and will be the key to successful protection of information resources.

Keywords: *confidential information, engineering and technical protection, drawings.*

Сучасний світ неможливо уявити без комп'ютерних і інформаційних технологій. Сюди входять розробки нових проектів, креслеників, винаходи і різні ноу-хау. Інформація є величезною цінністю в цифрову епоху, тому і необхідно її збирати, захищати і правильно зберігати, а інакше будь-яке порушення цієї системи може призвести до зупинки виробництва, припинення функціонування логістики компанії та інших вкрай негативних для бізнеса наслідків [1]. У даному випадку відбуваються такі процеси як порушення конфіденційності, що добре для конкурентів, далі – порушення цілісності інформації, а також порушення доступності інформації [2].

Досить багато спеціалістів працюють над захистом інформації, технологій, креслеників, інших документів, тобто над захистом конфіденційної інформації [3-5]. Принципи захисту, над якими працюють спеціалісти, полягають в детальному аналізі векторних зображень. У випадку спроби порушення цілісності інформації – і навіть фрагмента кресленика – спеціалісти створюють систему, що визначає приналежність кресленика чи його фрагмента до конкретного еталонного документа, і оповіщають службу інформаційної безпеки про витік даних. Для цього використовують інженерно-технічний захист, що є сукупністю технічних засобів і заходів, націлених на запобігання витоку даних, розголошення інформації і несанкціо-

нованого доступу до мережевих ресурсів [6]. Програми проводять автоматичний аудит файлової системи, маркують секретні кресленики і навіть фрагменти креслеників.

Необхідність в інженерно-технічному захисті викликана активним розвитком засобів видобутку інформації, і для цього застосовують наступні методи захисту інженерно-технічної інформації: фізичні – це спостереження за територією та приміщеннями; апаратні – це виявлення каналів витоку інформації; програмні – захист даних, проектів, креслеників; криптографічні – математичні моделі кодування повідомлень.

Що стосується програмного захисту, то повноцінний програмний захист вимагає як захисту даних, так і захисту програм, який оснований на безлічі паралельних і найчастіше тих, що перетинаються, алгоритмів. Але це може мати внутрішні конфлікти в системі, тому застосовують комплексні захисні системи, тобто системи для захисту даних, захисту програм, самозахисту від вторгнення, копіювання, модифікації і знищення.

Можемо зробити основні висновки про способи і заходи захисту:

1. Найбільшого ефекту досягаємо у випадку об’єднання всіх методів в єдиний і цілісний механізм захисту інформації.
2. Потрібне поєднання обробки і захисту даних.
3. Існує необхідність здійснювати постійний контроль функціонування механізмів захисту.

Отже, системний підхід і контроль дозволять здійснювати та будуть запорукою успішного захисту інформаційних ресурсів.

Світ інформаційних технологій (фото з мережі Інтернет)

Література

1. Защита информационных активов компании. https://confident.org.ua.
2. Защита конфиденциальных данных. https://my-itspecialist.com.
3. Новости и экспертиза в области серверных технологий, стандартов и практических решений. https://servernews.ru.
4. Google sites. https://sites.google.com.
5. Технические средства защиты информации. https://confident.org.ua.
6. Защита от утечек конфиденциальной информации. https://infowatch.ru.

УДК 35:004.56

ТРІАДА БЕЗПЕКИ ЗБЕРІГАННЯ ДАНИХ У ХМАРНИХ СХОВИЩАХ ДЛЯ СИСТЕМИ АВІАЦІЙНОГО ПОШУКУ І РЯТУВАННЯ

Гурник А., Литовченко А., Ядченко Д.
***Інститут державного управління та наукових досліджень з цивільного захи**сту*, м. Київ

***Анотація**. В роботі запропоновано провести аналіз фізичної і мережевої безпеки інформаційно-аналітичних рішень й комплексне вивчення стану гарантій збереження даних у хмарних сховищах системи авіаційного пошуку і рятування. У зв'язку з вищевикладеним виділені найголовніші складові для захисту інформації у хмарних сховищах з дотримання вимог стандартів безпеки, затверджених юридичними органами, і яке є обов'язковим в інтересах автоматизованої системи управління авіаційним пошуком і рятуванням.*

***Ключові слова:** система авіаційного пошуку і рятування, інформаційно-аналітична діяльність, безпека збереження даних, хмарні сховища.*

***Summary.** The paper proposes to analyze the physical and network security of information and analytical solutions and a comprehensive study of the state of data storage guarantees in cloud storage of aviation search and rescue systems. In connection with the above, the most important components for the protection of information in cloud storage on compliance with safety standards approved by legal authorities. It is mandatory in the interests of the automated management system for aviation **search** and rescue.*

***Keywords:** aviation search and rescue system, information and analytical activities, data storage security, cloud storage.*

Розгортання державотворчих процесів на всіх рівнях організації цивільного захисту, стрімкий розвиток науково-технологічної сфери життєзабезпечення населення в умовах надзвичайних ситуацій викликають різке зростання вимог до рівня інформатизації та безпеки інформаційно-аналітичного забезпечення оперативної діяльності в системі авіаційного пошуку і рятування (АПР) [1].

Основною функцією інформаційно-аналітичних рішень в системі АПР є підвищення ефективності пошуково-рятувальних робіт в умовах ризику чи невизначеності [2].

Сьогодні використовується апарат різних існуючих інформаційно-аналітичних підходів і методів для застосування в управлінській практиці, де інформаційна безпека відіграє ключову роль в контексті оповіщення взаємодіючих органів управління системи АПР, обґрунтування раціонального складу пошуково-рятувальних сил, розрахунку району пошуку та способів його здійснення, а також організації й координації заходів реагування при проведені операції з АПР.

Оскільки інформаційна безпека (безпека даних) передбачає набір методів, спрямованих на захист даних від несанкціонованого доступу чи змін, як при їх зберіганні, так і при передачі між пристроями, зусилля щодо захисту інформації в автоматизованій системі управління авіаційним пошуком і рятуванням (АСУ-АПР) набувають все більшого значення.

Основні складові інформаційної безпеки в АСУ-АПР найчастіше підсумовуються так званою тріадою принципів: конфіденційність, цілісність та доступність. Конфіденційність є тим елементом тріади, який спадає на думку про інформаційну безпеку. Для забезпечення конфіденційності призначені такі методи як: паролі, шифрування, автентифікація та захист від атак проникнення. Більшість методів, що забезпечують конфіденційність, також захищають цілісність даних. Але можуть застосовуватися інші інструменти, які допомагають більш глибоко захистити цілісність: програмне забезпечення для контролю версій та шифрування даних; періодичні резервні копії для відновлення даних до правильного стану; застосування контрольних сум для перевірки даних на цілісність. Дзеркальним відображенням конфіденційності є доступність даних. Забезпечення доступності даних передбачає відповідність мережевих та обчислювальних ресурсів обсягу доступу до очікуваних даних, і впровадження належної політики резервного копіювання з метою відновлення після аварій.
Засоби, за допомогою яких ці принципи застосовуються до системи АПР, мають форму політики безпеки. Це не апаратне або програмне забезпечення безпеки; а документ, який, наприклад Головний авіаційний координаційний центр пошуку і рятування складає, виходячи зі своїх власних специфічних потреб і завдань та функцій, щоб встановити, які дані потрібно захищати та якими способами. Ця політика спрямовує рішення щодо закупівлі засобів кібербезпеки, а також передбачає поведінку та відповідальність персоналу.

Важливим поштовхом для реалізації безпеки даних в АСУ-АПР є перехід до використання приватних хмарних ресурсів, а також таких найбільших провайдерів на ринку як: AWS, Microsoft Azure, Google Cloud та інші. Однак, незважаючи на це, згідно з даними компанії Microsoft, понад 50 відсотків організацій вважають хмарне сховище найризикованішою категорією програм [3].

Хмарні обчислення програм [4] є важливою опорою цифрової трансформації, а також є фундаментальною передумовою для з'єднання цифрового з фізичним світом. Це дає можливість використовувати такі ресурси, як інфраструктура, програми та дані, які надаються зовнішнім постачальником послуг за допомогою різних моделей, що відрізняється головним чином групою користувачів (приватна / спільнота / громадська / гібридна хмара).

Найголовнішими аспектами для захисту інформації у хмарних сховищах, які притаманні усім сучасним провайдерам, можна виділити такі методи як: автентифікації та ідентифікації, контролю доступу, шифрування, безпечного видалення, відновлення даних.

Дотримання вимог стандартів безпеки в інтересах системи АПР, затверджених юридичними органами, є обов'язковими. Основне завдання стандарту безпеки – надати доступ до даних лише тим, хто отримав дозвіл на виконання певного завдання.

Стандарти управління інформаційною безпекою, такі як ISO/IEC 27002 та ISO/IEC 27017 описують засоби управління для провайдерів. Належним підходом до захисту даних є підхід до управління даними АСУ-АПР. Вибір підходу до управління даними допомагає керувати, захищати та використовувати інформацію в системі АПР, що, у свою чергу, допомагає завоювати впевненість персоналу у прийнятті оптимальних рішень та підходах до них.

При виборі безпеки даних враховуються стандарти: серія ISO/IEC 27000, ISO/IEC 27002, ISO/IEC 27040: 2015, HTTPS, SFTP. Додатки встановлюються на всіх рівнях хмар. Якщо програму скомпрометовано, це не тільки знижує репутацію цієї хмарної платформи, а й компрометує велику кількість даних. Політика, пов'язана з безпекою програм на цьому етапі, надає велику допомогу у забезпеченні безпеки, пов'язаної з розгортанням та наданням програми. Політика застосування допомагає у розгортанні, шифруванні та вимогах до цілісності. Існують різні методи, які слід розглядати в хмарних додатках: Брандмауери, VPN, Відмова у наданні послуг публічно розкритим кінцевим точкам.

Підсумовуючи, слід додати, що існуючі хмарні рішення для системи АПР не є досконалими у питанні безпеки інформації АСУ-АПР й потребують аналізування. За дотриманням юридичного аспекту доцільно створювати низку правил чи своєчасно вносити до них відповідні зміни, які повинні бути обов'язковими для виконання та підтримання всіма хмарними провайдерами, а стійкість самих хмарних систем повинна удосконалюватися безперервно, як самими користувачами так і штучним інтелектом АСУ-АПР.

Література

1. Наказ Міністерства внутрішніх справ України від 16.03.2015 № 279 «Про затвердження Правил авіаційного пошуку і рятування в Україні». [Електронний ресурс.] – Режим доступу: http://zakon4.rada.gov.ua/laws/show/z0364-15

2. Аналіз функціонування системи авіаційного пошуку і рятування в Україні та визначення шляхів підвищення її ефективності / ІДУЦЗ, НДР «Авіапошук – ефективність», К. –2013. – 229 с.

3. Офіційний сайт Microsoft [Електронний ресурс] – Режим доступу до ресурсу: https://www.microsoft.com/uk-ua/microsoft-365/growthcenter/resources/6-security-red-flags-when-identifying-the-perfect-cloud-storage-solution?.

4. Віблий В.М. Безпека інформації у хмарних сховищах / В.М. Віблий, О.О. Смотр // зб. тез доповідей ІІІ Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів "Захист інформації в інформаційно-комунікаційних системах". Львів, ЛДУ БЖД, 2019, – с.88-90.

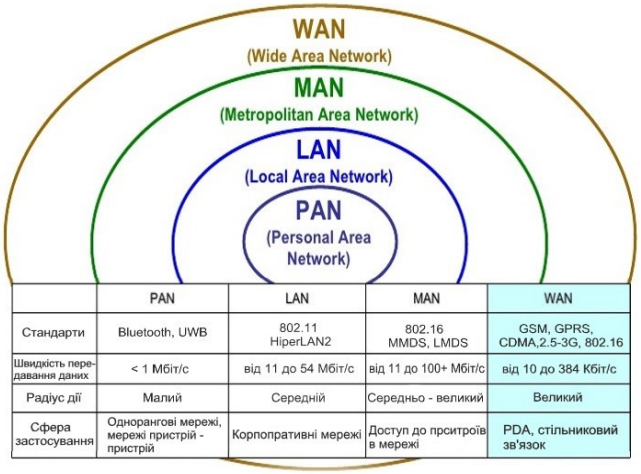
УДК 004.056:061.68

ШИФРУВАННЯ ПОВІДОМЛЕНЬ В БЕЗПРОВІДНИХ МЕРЕЖАХ НА ОСНОВІ АЛГОРИТМУ “КАЛИНА”

Дудикевич В., Микитин Г., Кутень Р., Галунець М..
Національний університет “Львівська політехніка”, Львів

Вступ. Тривають процеси інтелектуалізації суспільства у просторі Концепції Індустрії 4.0, які взаємозв’язані з Стратегією кібербезпеки України і цілісно спрямовані на протидію внутрішніх і зовнішнім загрозам у кіберпросторі, розвиток та функціонування безпечних технологій інфраструктури суспільства, насамперед об'єктів критичної інформаційної інфраструктури. Безпровідні мережі (БМ) зв’язку є одним з головних сегментів інтелектуалізації предметних сфер згідно універсальної функціональної платформи “відбір/збір інформації – обмін інформацією – аналіз/обробка – управління”. Відповідно актуальним є завданням забезпечення основних профілів безпеки обміну повідомленнями в БМ – конфіденційності, цілісності, доступності.

Криптографічний алгоритм шифрування повідомлень Калина. Блокові шифри є найбільш поширеними в криптозахисті комунікаційного середовища інтелектуальних технологій (ІТ), зокрема БМ, класифікація яких та характеристики показані на рис. 1.



	PAN	LAN	MAN	WAN
Стандарти	Bluetooth, UWB	802.11 HiperLAN2	802.16 MMDS, LMDS	GSM, GPRS, CDMA,2.5-3G, 802.16
Швидкість передавання даних	< 1 Мбіт/с	від 11 до 54 Мбіт/с	від 11 до 100+ Мбіт/с	від 10 до 384 Кбіт/с
Радіус дії	Малий	Середній	Середньо - великий	Великий
Сфера застосування	Одноранговi мережі, мережі пристрій - пристрій	Корпопративні мережі	Доступ до прситроїв в мережі	PDA, стільниковий зв'язок

Рис. 1. Класифікація і характеристики безпровідних мереж

Блоковий алгоритм шифрування “Калина” [1] забезпечує високий рівень безпеки і високу продуктивність програмної реалізації на 64-бітових процесорах загального призначення та підтримує характеристики, що наведені в табл. 1. Схема формування ключів використовує односпрямований генератор псевдовипадкових послідовностей.

Таблиця 1 – Характеристики блокового алгоритму шифрування “Калина”

Розмір блоку (l)	Довжина ключа (k)	Кількість раундів (t)	Кількість рядків матриці стану (c)
128	128	10	2
	256	14	
256	256	14	4
	512	18	
512	512	18	8

Ще однією важливою характеристикою алгоритму шифрування “Калина” є швидкодія, порівняння якої представлено на рис. 2.

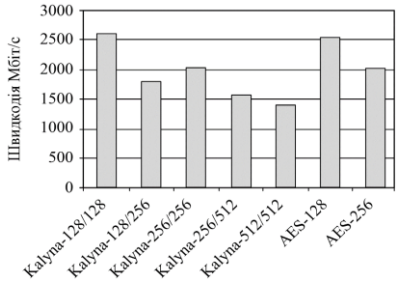
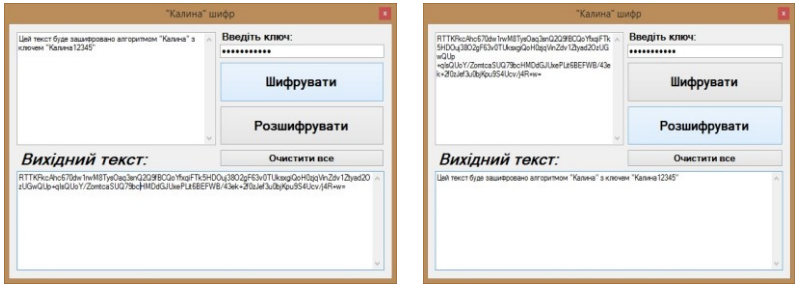


Рис. 2. Порівняння швидкості блокових алгоритмів шифрування даних

Особливості алгоритму блокового шифрування “Калина”, зокрема висока криптостійкість та швидкодія уможливлюють його ефективне застосування для криптографічного захисту повідомлень в БМ. З метою його ефективної реалізації використано об’єктно-орієнтовану мову програмування C#, яка забезпечує надійність та кросплатформовість алгоритму. На рис. 3 наведено скріншоти програмної реалізації шифрування/ дешифрування повідомлень на базі ключа довжиною 128 біт.



а) б)

Рис. 3. Програмна реалізація алгоритму “Калина”: а) шифрування; б) дешифрування

Висновок

Проаналізовано класифікацію БМ у просторі безпеки ІТ Індустрії 4.0, розгорнуто переваги блокового алгоритму “Калина”, програмно реалізовано шифрування/дешифрування даних засобами C#, що забезпечить високий рівень криптографічного захисту БМ.

Література

1. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення: ДСТУ 7624: 2014. – [Чинний від 2015-07-01]. – К: Держспоживстандарт, 2016. – 117 с.

УДК 004.056

ХАРАКТЕРИСТИКИ ЗАХИСТУ ІНФОРМАЦІЇ У ПРОТОКОЛАХ ДОСТУПУ ДО ОБ’ЄКТІВ

Довганик Д., Марти І., Навитка М.
Львівський державний університет безпеки життєдіяльності

Принципи забезпечення інформаційної безпеки містять: законність, баланс інтересів особи, суспільства і держави; комплексність; системність; інтеграція з міжнародними системами безпеки; економічна ефективність

В даній статті проведено аналіз технологій, які часто використовують веб-інтерфейси Web 2.0. Наведено характеристики та відмінності між технологіями SOAP та REST

Ключові слова: *прикладний програмний протокол, веб-ресурси*

The principles of information security include: legality, balance of interests of the individual, society and the state; complexity; systematicity; integration with international security systems; economic efficiency

This article analyzes the technologies that often use Web 2.0 web interfaces. The characteristics and differences between SOAP and REST technologies are given

Keywords: *application program protocol, web resources*

Веб-інтерфейси Web 2.0 часто використовують взаємодії на основі таких технологій як REST та SOAP. У той час як прикладний програмний інтерфейс у Web історично був практично синонімом для веб-служби, останнім часом тенденція змінилась (так званий Web 2.0) на відхід від Simple Object Access Protocol (SOAP) на основі веб-сервісів і сервіс-орієнтованої архітектури (SOA) до більш прямих передач репрезентативного стану (REST) стилів веб-ресурсів та ресурсно-орієнтованої архітектури (ROA).

SOAP — протокол обміну структурованими повідомленнями в розподілених обчислювальних системах, базується на форматі XML.

Спочатку SOAP призначався, в основному, для реалізації віддаленого виклику процедур (RPC), а назва була абревіатурою: Simple Object Access Protocol — простий протокол доступу до об'єктів. Зараз протокол використовується для обміну повідомленнями в форматі XML, а не тільки для виклику процедур. SOAP є розширенням мови XML-RPC.

SOAP можна використовувати з будь-яким протоколом прикладного рівня: SMTP, FTP, HTTP та інші. Проте його взаємодія з кожним із цих протоколів має свої особливості, які потрібно відзначити окремо. Найчастіше SOAP використовується разом з HTTP. SOAP є одним зі стандартів, на яких ґрунтується технологія веб-сервісів.

REST — підхід до архітектури мережевих протоколів, які надають доступ до інформаційних ресурсів. В основі REST закладено принципи функціонування Всесвітньої павутини і, зокрема, можливості HTTP. Розроблено REST паралельно з HTTP 1.1 базуючись на попередньому протоколі HTTP 1.0.

Дані повинні передаватися у вигляді невеликої кількості стандартних форматів (наприклад, HTML, XML, JSON). Будь-який REST протокол (HTTP в тому числі) повинен підтримувати кешування, не повинен залежати від мережевого прошарку, не повинен зберігати інформації про стан між парами «запит-відповідь». Такий підхід забезпечує масштабовність системи і дозволяє їй еволюціонувати з новими вимогами.

Підхід RPC дозволяє використовувати невелику кількість мережевих ресурсів з великою кількістю методів і складним протоколом. При підході REST кількість методів і складність протоколу суворо обмежені, що призводить до того, що кількість окремих ресурсів має бути великою. REST — це архітектурний стиль для розподілених гіпертекстових систем.

Різниця між SOAP і REST

• SOAP – це протокол обміну повідомленнями на основі XML, а REST - архітектурний стиль.

• SOAP призначений для обробки розподілених обчислень, тоді як REST передбачає зв'язок від точки до точки, де посередник не відіграє значної ролі.

• REST не вимагає нічого, крім HTTP. SOAP вимагає повного набору інструментів і підтримки проміжного програмного забезпечення.

• У REST є вбудований обробник помилок. Такого обробника немає в SOAP.

Неможливо створити систему, захист якої не можна буде зламати, основним принципом може бути створення такого механізму захисту, вартість злому якого буде дорожчою за інформацію, яку можна отримати. Тому необхідним є впровадження програмних засобів безпеки, які вмонтовані до складу програмного забезпечення системи і є потрібними для виконання функцій захисту.

Літертура

1. Стандарт SOAP – http://www.w3.org/TR/soap

2. Технології та засоби консолідації інформації: Навчальний посібник. Дерев'янко О.С., Солощук М.М. – Харків: НТУ "ХПІ", 2008. – 432 с.

3. Херрон Девід. Node.js Розробка серверних веб-додатків на javascript. - ДМК Прес, 2012. – 146 с.

4. Шеллі Пауерс, Вивчаємо Node.js – Санкт-Петербург: "Пітер", 2014. – 402 с.

УДК 004.056.53

ОСНОВНІ ПІДХОДИ ДО ПОБУДОВИ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Драб Ю., Ящук В.
Львівський державний університет безпеки життєдіяльності, Львів

Розглянуто методи проведення атак на системи захисту інформації, проаналізовано дії реального порушника контурів захисту інформації, наведено етапи створення систем захисту інформації. Запропоновано підходи до побудови системи управління інформаційною безпекою відповідно до стандарту ISO 2700, що надає підприємству конкурентну перевагу, демонструючи здатність керувати інформаційними ризиками, та збільшує капіталізація компанії.
Ключові слова: *захист інформації, системи управління інформаційною безпекою, система захисту інформації, несанкціонований доступ.*

The methods of carrying out attacks on information protection systems are considered, the actions of the real violator of information protection circuits are analyzed, the stages of creation of information protection systems are given. Approaches to building an information security management system in accordance with the ISO 2700 standard are proposed, which gives the company a competitive advantage, demonstrating the ability to manage information risks and increase the company's capitalization.
Key words: *information protection, information security management systems, information protection system, unauthorized access.*

Розвиток інформаційно-комунікаційних систем відіграє важливу роль у життєвому циклі більшості підприємств. Проблеми захисту та оцінки даних інформаційних систем в умовах пандемії набувають особливої актуальності. У сучасному світі інформація є найціннішим ресурсом. Для забезпечення необхідного рівня безпеки інформації необхідно регулярно проводити аудит безпеки інформаційних систем.

Головна мета захисту інформації полягає у тому, щоб виключити можливість їх несанкціонованого використання або втрат у відповідному середовищі. Важливим напрямом протидії таким ситуаціям є проведення періодичних перевірок захищеності системи шляхом тестувань на проникнення. Такий метод ґрунтується на реалізації різних способів проникнення до інформаційно-комунікаційної мережі, що імітують дії реального порушника. Це дозволить отримувати фактичні результати з питань дослідження рівня та стану інформаційної безпеки.

Інвестиції в сферу забезпечення інформаційної безпеки підвищать конкурентоспроможність підприємства на ринку. Нездатність належним чином захистити свої ресурси може призвести до непоправних збитків, а в деяких випадках – до банкрутства. Аналіз сьогоднішнього ландшафту

кіберзагроз дає зрозуміти, що недостатньо інвестувати тільки в захист. Підприємства повинні покращувати загальну стратегію безпеки, а це означає, що інвестиції в захист, виявлення і реагування повинні бути узгоджені.

Сучасна практика з питань інформаційної та кібербезпеки розрізняє та виділяє декілька основних методів проведення атак на системи захисту інформації, серед яких вирізняються як суто технічні методи (апаратне та програмне забезпечення), так і методи, що пов'язані із використанням психологічних та соціологічних прийомів впливу на людей, маніпуляцією людським фактором.

Однією з прогалин у системі захисту інформації є відсутність уніфікованої моделі захисту інформації. Більша частина дослідників згодна між собою в загальній концепції щодо етапів формування системи захисту інформації, що була запропонована в стандарті НД ТЗІ 3.7-003-05 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційнотелекомунікаційній системі" [3]. Дана загальна концепція визначає наступні основні етапи створення систем захисту інформації в різних суб'єктах господарювання (рис. 1).

Рис.1. Етапи створення комплексної системи захисту інформації (розроблено авторами на основі [3])

Відсутність уніфікованої моделі захисту інформації актуалізує процес розроблення системи управління інформаційною безпекою (Information Security Management System, ISMS), як частини загальної системи управління, що базується на аналізі ризиків і призначена для проектування, ре-

алізації, контролю, супроводження та вдосконалення заходів у галузі інформаційної безпеки. Цю систему складають організаційні структури, політика, дії з планування, обов'язки, процедури, процеси і ресурси.

Побудова СУІБ дозволяє чітко визначити, як взаємопов'язані процеси та підсистеми ІБ, хто за них відповідає, які фінансові та трудові ресурси необхідні для їх ефективного функціонування тощо. Одним із ключових чинників успішності системи управління інформаційною безпекою підприємства є побудова її на базі міжнародних стандартів ISO/IEC 27001. Міжнародний стандарт ISO 27001 надає інструмент для розробки, впровадження, супроводу, моніторингу, підтримки та вдосконалення добре документованої системи управління інформаційною безпекою в контексті розгляду бізнес ризиків.

СУІБ і сертифікація на відповідність стандарту ISO 27001 дає підприємству такі переваги, як управління інформаційною безпекою в межах єдиної корпоративної політики, управління ризиками та їх своєчасне виявлення, зниження ризиків від зовнішніх і внутрішніх загроз, систематизація процесів забезпечення ІБ, встановлення пріоритетів підприємства в області ІБ. У свою чергу це забезпечує підприємству конкурентну перевагу, демонструючи здатність керувати інформаційними ризиками, при цьому також збільшується капіталізація компанії.

Таким чином, в процесі проведеного дослідження визначено роль процесу захисту інформації в інформаційно-комунікаційних системах та мережах, класифіковано методи захисту, визначено порядок формування систем захисту інформації, їх використання, окреслено стандарти, що стосуються захисту інформації.

Література

1. Oriyano Sean-Philip. Penetration Testing Essentials. Sybex, a Wiley brand, 2017, 363 p.

2. Baloch Rafay. Ethical hacking and penetration testing guide. Auerbach Publications, 2017, 523 p.

3. Нормативні документи з питань захисту інформації ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі [Електронний ресурс]. – Режим доступу: http://surl.li/gnbi.

4. ISO 27001:2005 «Інформаційні технології – Методи забезпечення безпеки – Системи управління інформаційною безпекою – Вимоги».

УДК 004.621.3

РАЦІОНАЛЬНИЙ ВАРІАНТ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА (УСТАНОВИ, ОРГАНІЗАЦІЇ) В ЗАЛЕЖНОСТІ ВІД НАЯВНИХ РЕСУРСІВ

Дзюба Т.
Державний університет телекомунікацій, м. Київ

В доповіді висвітлюються питання вибору раціонального способу забезпечення інформаційної безпеки підприємства (установи, організації) в залежності від наявних ресурсів. Розглядаються варіанти самостійної організації власної системи інформаційної безпеки, повного або часткового аутсорсингу послуг інформаційної безпеки, розміщення основних інформаційних активів в захищених зовнішніх центрах даних та операційних центрах безпеки.

Ключові слова: *ресурсне забезпечення інформаційної безпеки, аутсорсинг послуг інформаційної безпеки, зовнішні центри даних, операційні центри безпеки.*

The report covers the choice of a rational way to ensure the information security of the enterprise (institution, organization) depending on available resources. Options for independent organization of own information security system, full or partial outsourcing of information security services, placement of major information assets in secure external data centers and operational security centers are considered.

Keywords: *information security resources, information security services outsourcing, external data centers, operational security centers.*

Одним з основних завдань менеджменту інформаційної безпеки підприємства (установи, організації) є визначення доцільного способу використання ресурсів на створення та експлуатацію системи заходів інформаційної безпеки, яка б, з одного боку, гарантувала необхідний рівень захищеності інформаційних процесів та активів, з іншого, потребувала залучення мінімально необхідної кількості ресурсів:

людських (фахівців за різними напрямами забезпечення інформаційної безпеки);

фінансових (необхідних для створення системи заходів інформаційної безпеки, її утримання, оплати праці персоналу, відповідних операційних витрат);

часових (час, потрібний для створення системи заходів інформаційної безпеки, час впровадження, термін дії).

Окремими ресурсами, необхідними для забезпечення інформаційної безпеки підприємства (установи, організації) можуть розглядатися необхідні технології, інакше – стандартизовані рішення щодо організації та здійснення відповідної системи заходів, апаратні та програмні засоби захисту тощо. В сучасних умовах їх достатність та ефективність може визначатись шляхом порівняння їх характеристик з характеристиками актуальних кіберзагроз, зокрема загроз «нульового дня».

Ефективне використання ресурсів для забезпечення інформаційної безпеки означає, що ризики інформаційній безпеці зменшені до величини,

яка дозволяє їх зберегти (прийняти) і, при цьому, використовується мінімально необхідна кількість ресурсів.

Сьогодні в Україні існує достатня кількість різних підходів до забезпечення інформаційної безпеки.

Так, кожне підприємство (установа, організація) може організувати всю систему заходів власними силами; може придбати готові технології (рішення) інформаційної безпеки та відповідне програмне і апаратне забезпечення (варіант: з навчанням персоналу та супроводженням в процесі експлуатації); використати можливості аутсорсингу (передачі функцій забезпечення інформаційної безпеки: повністю або частково, зовнішнім організаціям); розмістити свої цінні інформаційні активи в захищених зовнішніх центрах даних (датацентрах, центрах зберігання та обробки даних) або використовувати можливості зовнішніх операційних центрів безпеки (SOC) як послуги (SOCaaS).

Сучасний ринок послуг інформаційної безпеки (зовнішніх відносно підприємства) пропонує 24-годинний моніторинг подій безпеки, аналіз поточних подій безпеки, активну сигналізацію про події, підготовку звітів про ситуацію та аналіз безпеки; захист від DDoS-атак, використання безпекових рішень для SIEM, IDS/IPS, виявлення та усування прогалин у безпеці, послуги IT-криміналістики, управління мережевими екранами, управління профілями користувачів інформаційних систем, безпеку застосунків, використання електронної пошти та користування комп'ютерними мережами.

Порівняльний аналіз різних підходів до забезпечення власної інформаційної безпеки показує, що використання аутсорсингу є більш дешевим за рахунок оптимального розподілу ресурсів між декількома замовниками без капітальних затрат; має чітко регламентовані терміни: від декількох днів до 1 – 2 місяців після підписання договору; характеризується відсутністю кадрових проблем за рахунок взаємозамінності та чисельності фахівців, можливості залучати додаткових фахівців; реалізує перехресне інформування всіх клієнтів про релевантні (для їхніх інформаційних інфраструктур) загрози кібербезпеці; співробітнитцво з правоохоронними органами, національними та міжнародними партнерами щодо обміну інформацією про інциденти, діяльність хакерів, підозрілі IP-адреси тощо.

Водночас, зовнішні послуги інформаційної безпеки характеризуються складністю гарантованого надання послуг в рамках підписаного договору, стягнення штрафних санкцій та відшкодування збитків у разі невиконання договору; поверхневим (тільки в рамках підписаного договору) контролем інформаційних процесів; повною залежністю підприємства (установи, організації) від компанії-аутсорсера, яка надає послуги інформаційної безпеки.

За таких обставин задача менеджера інформаційної безпеки полягає в оцінці всіх можливих підходів і вибору найбільш раціонального з них.

В якості критерію ефективності такого вибору можна визначити максимальне значення зниження остаточних ризиків інформаційної безпеки при мінімальних сумарних затратах підприємства (установи, організації) на придбання (розробку), впровадження та використання цього рішення.

УДК 004.45

АНАЛІЗ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОБ'ЄКТУ ТИПУ "РОЗУМНИЙ ДІМ"

Дацків Н., Полотай О.
Львівський державний університет безпеки життєдіяльності, м. Львів

В роботі розглядаються вимоги до систем аналізу загроз інформаційної безпеки об'єкту типу "розумний дім". Проведено аналіз сучасних систем, досліджено особливості їх роботи.

***Ключові слова**: Інформаційна безпека, захист даних, розумний дім.*

The paper considers the requirements for information security threat analysis of a "smart home" object. The analysis of modern systems is carried out, features of their work are investigated.

***Key words:** Information security, data protection, smart home.*

Система «розумний будинок», побудована з централізованого способу, складається з елемента управління, центрального контролера і керованого устаткування, об'єднаних в єдину телекомунікаційну мережу для прийому і передачі сигналів або команд управління.

На відміну від централізованого підходу, в децентралізованому підході відсутній центральний контролер. В цьому випадку система складається з датчиків, сенсорів і активаторів.

Ефективна і багатофункціональна система «розумного будинку» включає в себе різноманітні датчики, які реєструють і передають параметри середовища, і іншу важливу інформацію. Датчики автоматизації представляють собою конструктивно автономний самостійний пристрій, що змінює свій сигнал відповідно відстежувальних параметрів.

Уразливості проявляються в зв'язку з впливом наступних факторів:

- електромагнітного випромінювання;
- електричного шуму;
- акустичні перешкоди;
- перепади освітленості;
- пошкодження даних;
- наявність в повітрі хімічних речовин;
- несанкціоновані зміни;
- екранування поля, випромінюваного активними датчиками і об'єктами в зоні виявлення.

Базовими загрозами інформаційній безпеці «розумного будинку» є:

- порушення конфіденційності;
- порушення цілісності;
- порушення доступності інформації (всі разом КЦД).

У контексті аналізу «розумного будинку» під конфіденційністю мається на увазі такий стан ІТ-системи управління «розумним будинком», при якому відсутня можливість витоку інформації через підсистеми. Приклад реалізації загрози – витік персональної інформації або витік інформації про конфігурацію ІТ-систем «розумного будинку».

Цілісність інформації – це достовірність і повнота інформації отримується системою від різних датчиків і пристроїв, встановлених в системі, наприклад, при отримання невірної інформації системою про наявність в приміщенні людини може привести до помилкового спрацьовування системи контролю доступу.

Доступність інформації стосовно «розумному будинку» – це стан інформації або ресурсів ІТ-системи, при якому суб'єкти або сама система, що мають права доступу, можуть реалізувати різні дії відповідно до сценарію роботи (вимикати / включати датчики, відкривати замки). Приклад реалізації даної загрози – виведення з ладу комунікаційного обладнання системи.

Загрози інформаційної безпеки за своєю природою виникнення можна розділити на 2 групи: загрози, зумовлені людським фактором і загрози середовища (природні).

Зокрема, загрози першої групи розрізняються за способом здійснення: цілеспрямовані (навмисні) і випадкові (ненавмисні). Деякі приклади таких загроз наведені в табл. 1, варто відзначити, що загрози другої групи (загрози середовища), не піддаються прогнозуванню, і як правило, під ними мають на увазі природні катаклізми.

Таблиця 1

Класифікація загроз безпеки інформації ІТ-системи «розумного будинку»

Загрози, обумовлені людським фактором		Загрози середовища
Цілеспрямовані	Випадкові	
Модифікація інформації	Помилки ПЗ	Пожежа
Перехоплення інформації	Помилки користувача	Затоплення
Викрадення обладнання	Помилки при обслуговуванні	Блискавка
Хакерська атака	Апаратні відмови	Землетрус
Шкідливе програмне забезпечення (ПЗ)	Помилки маршрутизації	Екстремальні величини температури і вологості

Іншим суттєвим фактором для визначення загроз інформаційної безпеки є ідентифікація можливих джерел загроз в залежності від їх розташування: внутрішні і зовнішні. До внутрішніх загроз відносяться загрози, розташовані всередині контрольованої зони, до зовнішніх – зовні (табл. 2). Більш повний список загроз можна подивитися на сайті бази даних загроз безпеки інформації.

Таблиця 2

Приклади внутрішніх і зовнішніх загроз інформації ІТ-системи «розумного будинку»

Внутрішні загрози	Зовнішні загрози
Загроза застосування коду або даних	Загроза відключення (екранування) контрольних датчиків
Загроза використання механізмів розробника	Загроза спотворення вводиться і виводиться на периферійні пристрої інформації
Загроза підміни програмного забезпечення	Загроза несанкціонованого віддаленого позаполосного доступу до апаратних засобів
Загроза доступу / перехоплення / зміни HTTP-cookies	Загроза подолання фізичного захисту
Загроза доступу до локальних файлів сервера за допомогою URL	Загроза міжсайтового підроблення запиту

Література

1. Viktor Mayer-Schönberger. Big Data: A Revolution That Will Transform How We Live, Work /, Kenneth Cukier., 2014. – 280 с. – (3). – (2).

2. Cathy O'Neil, Rachel Schutt. Doing Data Science: Straight Talk from the Frontline / Cathy O'Neil, Rachel Schutt., 2013. – 510 с. – (O'Reilly Media, Inc.).

3. Selenium is an umbrella project for a range of tools and libraries that enable and support the automation of web browsers. [Електронний ресурс] // Selenium. – 2021. – Режим доступу до ресурсу: https://github.com/SeleniumHQ.

4. HTML [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://developer.mozilla.org/ru/docs/Web/HTML.

УДК 334

БЕЗПЕКА МАЙБУТНЬОГО: ЧОМУ НЕОБХІДНО ПЕРЕХОДИТИ НА ХМАРНІ СЕРВІСИ

Дулова О.
Відокремлений структурний підрозділ «Ірпінський фаховий коледж Національного університету біоресурсів і природокористування України»,м.Ірпінь

Анотація: *Хмарні обчислення та рішення для зберігання даних надають користувачам і підприємствам різні можливості для зберігання і обробки їх даних у центрах обробки даних сторонніх виробників. Є ряд питань які пов'язані з безпекою хмарних обчислень, але ці питання діляться на дві великі категорії: питання безпеки, з якими стикаються під час використання хмарних послуг і питання безпеки, з якими стикаються їх клієнтів.*
Ключові слова: *хмара, рішення, безпека, обчислення, користувачі, дані, обробка.*

Abstract: *Cloud computing and storage solutions provide users and businesses with a variety of options for storing and processing their data in third-party data centers. There are a number of issues that are related to the security of cloud computing, but these issues fall into two broad categories: security issues that are encountered when using cloud services and security issues that are faced by their customers.*
Keywords: *cloud, solution, security, computation, users, data, processing.*

Зберігання файлів, розробка проектів, робота з базами даних — усе це активно використовується сьогодні. Разом із тим, компанії змушені також займатися самостійною підтримкою інфраструктури, у разі коли інформація зберігається в локальних системах компанії. Хмарні сервіси стали популярними не тільки у кінцевих користувачів для зберігання особистих файлів. У масштабах бізнесу можна так само віддалено створити віртуальну IT-інфраструктуру, розгорнути резервне сховище даних, запустити і обслуговувати власні програми та багато іншого.

Згідно дослідження від Gartner, зростання популярності хмарних технологій та IaaS (інфраструктури як послуги) у цьому році буде тривати. За прогнозами цей сегмент зросте майже на 27%.

І все ж деякі компанії скептично налаштовані до переходу на хмарні сховища, вбачаючи в цьому потенційну загрозу для конфіденційності інформації. Однак провідні хмарні служби забезпечують набагато більшу захищеність файлів, ніж «аналогові» сховища. Більш того, провайдери використовують власні системи захисту від кіберзагроз, а саме моніторинг атак і антивірусні програми.

Міграція в хмару допоможе значно скоротити кількість проблем, які зазвичай пов’язані з керуванням IT-інфраструктурою. Робота з додатками, налаштування та обслуговування бізнес-процесів помітно полегшиться, як

і власне процес оновлень. Хмара робить бізнес гнучкіше в багатьох питаннях: від аналітики і роботи з соціальними мережами до управління всіма ключовими бізнес-процесами.

Перейшовши в хмару, компанія може забути про необхідність постійно модернізувати свою ІТ-інфраструктуру. Як показує досвід, у середньому вже через 3 роки фізичне обладнання застаріває і на нього закінчується сервісна гарантія від виробника. Саме тому компанії вважають за краще залучитися ІТ-підтримкою хмарного провайдера. З цього моменту турбота про оновлення фізичного обладнання, встановлення патчів по функціоналу і безпеки, і до решти стає клопотом хмарного провайдера.

Хочемо ми цього чи ні, але весь наш бізнес все одно опиниться в хмарі. Навіть немає сумнівів у тому, що в міру розвитку продуктів або сервісів наші бізнес-процеси також будуть ставати складнішими. І саме тут на допомогу компаніям приходять хмарні технології.

Чомусь звично думати, що міграція в хмару є дорогим і досить тривалим процесом. Насправді ж, усе набагато швидше, ніж ми думаємо. Співпраця із хмарним провайдером робить процес переходу максимально простим та мінімізує наше залучення.

Усі документи із нашої системи стануть доступні на будь-якому пристрої. Погодьтеся, що це значно прискорить роботу та покращить рівень продуктивності співробітників. А у найближчому майбутньому — заощадить вашому бізнесу час і гроші.

Перевага використання хмарних сервісів:

1. Обслуговування. Розвиток та обслуговування ІТ-інфраструктури, її безпека, надійність і дієздатність стануть завданнями хмарного провайдера. При самостійному розгортанні хмари будуть потрібні вагомі ресурси — регулярні бекапи, відстеження фізичного стану серверів, актуалізація їх ПО і таке інше.

2. Скорочення витрат. Провайдери пропонують різноманітні пакети послуг і обсяги віртуального простору. Компанія зможе оплачувати лише використаний обсяг ресурсів, який в майбутньому можна збільшувати або зменшувати. Вартість утримання і обслуговування власного сервісу значно перевищує його хмарний аналог. Особливо це стосується резервного копіювання.

3. Безпека. Часто під час розміщення фізичного сервера в офісі виникає ризик, що інформація про бізнес опиниться під загрозою. Фізичні сервери можуть вилучити або вкрасти, отримавши доступ до даних. Теж саме стосується і надзвичайних ситуацій. Сучасні хмарні провайдери використовують принцип територіального розподілу центрів обробки даних. Це дозволяє уникнути проблем із роботою хмари під час надзвичайних ситуацій.

Типи хмарних сервісів для бізнесу.

Віртуальний сервер. Забезпечує доступ до обчислювальних ресурсів, дискового простору та операційної системи. Компанія реально скорочує

витрати на покупку й обслуговування фізичних серверів. А головною перевагою є швидке масштабування. Бо якщо потрібно збільшити обчислювальні потужності, робиться це за кілька хвилин.

Середовище для розробки. Підтримка безлічі користувачів і масштабування сервісів-платформ підвищує ефективність розробки. Крім того, при використанні не буде виникати проблем із ліцензіями на необхідне програмне забезпечення.

Додатки в хмарі. Це повноцінне програмне забезпечення, створене для спільної роботи без прив'язки до місця і конкретного комп'ютера. Користувачі підключаються до них через Інтернет, як правило, за допомогою браузера. Уся інфраструктура знаходиться в центрі обробки даних провайдера.

Найважливішим при виборі провайдера хмарного сервісу є чітке розуміння, навіщо це потрібно, які файли в ньому будуть зберігатися і як буде здійснюватися доступ співробітників до інформації. Саме це дозволить підібрати сервіс, що максимально задовольняє потребам компанії.

Література

1. Gartner: Seven cloud-computing security risks. Електронний ресурс. Режим доступу: [https://www.infoworld.com/article/2652198/gartner--seven-cloud-computing-security-risks.html]

2. Cloud Access Security Brokers (CASBs). Електронний ресурс. Режим доступу: [https://www.gartner.com/en/information-technology/glossary/cloud-access-security-brokers-casbs]

3. Multi-Cloud Management: Tools, Challenges and Best Practices. Електронний ресурс. Режим доступу:[https://www.simform.com/blog/multi-cloud-management/]

УДК 004.056

ПРОБЛЕМА ФІШИНГУ ДЛЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ. ОРГАНІЗАЦІЙНІ СПОСОБИ ПРОТИДІЇ

Запорожченко М.
Державний університет телекомунікацій, м. Київ

Анотація. *Захист інформації від фішингових атак може бути досягнуто шляхом впровадження комплексу організаційних та технічних заходів. В тезах наведено основні організаційні заходи, яких слід дотримуватись підприємствам для захисту від порушення інформаційної безпеки внаслідок цільових фішингових атак.*
Ключові слова*: інформаційна безпека, фішинг, соціальна інженерія*

Abstract. *Protection of information from phishing attacks can be achieved by implementing a set of organizational and technical measures. The abstracts present basic organizational measures that enterprises should follow to protect against information security breaches due to targeted phishing attacks.*
Keywords*: information security, phishing, social engineering*

Впродовж останніх років зі збільшенням кількості користувачів цифрових сервісів, зокрема, внаслідок вимушеного переходу роботи в цифрове середовище через пандемію, спостерігається стрімке зростання випадків застосування зловмисниками прийомів соціальної інженерії стосовно співробітників організацій та звичайних користувачів (рис. 1). Застосовуючи методи соціальної інженерії, злочинці можуть завантажувати шкідливий код, зламувати корпоративну інфраструктуру й отримувати облікові дані користувачів, що надає їм нові можливості для розвитку подальших атак [1].

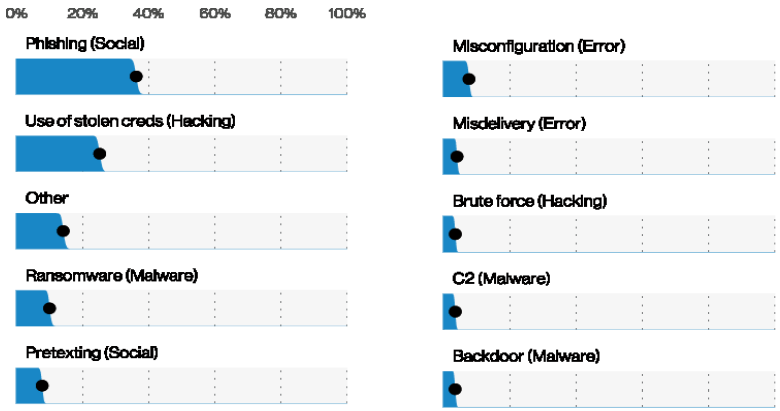


Рис. 1. Рейтинг атак, що стали причиною витоку даних у 2020 р. (фрагмент)

Одним з різновидів соціальної інженерії є цільовий фішинг. Його відмінність від звичайного фішингу полягає в тому, що атака планується та реалізується з урахуванням знань зловмисника про цільову компанію, конкретного її співробітника або ж звичайного користувача, на яких спрямована фішингова атака. Найпопулярніший спосіб реалізації такої атаки – створення та відправлення жертві фішингового електронного листа, який нерідко за рахунок застосування зловмисником знань з психології та соціології написано таким чином, щоб викликати в жертви необхідність перейти за посиланням в листі, яке веде на веб-ресурс зловмисника, або завантажити та відкрити прикріплений шкідливий файл для можливості завантаження зловмисником спеціального ПЗ. Крім того, що цільові фішингові атаки спрямовані на користувача, який зазвичай є найменш захищеної ланкою в інформаційній системі компанії, фішингові листи не завжди можуть бути виявлені засобами автоматизованого аналізу. До того ж, використання окремих технологій захисту не надасть належний рівень захисту від цільового фішингу. Його може забезпечити лише комплекс з програмно-технічних засобів та організаційних заходів [2].

Першочергово з організаційної точки зору для протидії фішинговим атакам доцільно буде зрозуміти, яку інформацію про компанію і її співробітників може отримати зловмисник. Зловмисника можуть зацікавити дані про інфраструктуру компанії та інформація про її співробітників, наприклад, їх контактні дані, інтереси, друзі, колеги тощо. Якщо зловмисник володіє такою інформацією, для нього буде легше провести вдалу фішингову атаку, оскільки він зможе створити правдоподібний фішинговий лист, наприклад, звіт за минулий тиждень від колеги з прикріпленим файлом, завантаження або відкриття якого дозволить зловмиснику завантажити своє ПЗ на комп'ютер жертви. Для того, щоб знайти інформацію про свою компанію, можна застосувати інструменти Kali Linux TheHarvester та recon-ng, які проводять пошук по відкритим джерелам.

Наступним важливим кроком є навчання працівників і підвищення рівня обізнаності. Необхідно навчити співробітників, навіть тих, які не мають відношення до ІБ, звертати увагу на фішингові листи шляхом ознайомлення з їх основними ознаками та проведення регулярних фішингових симуляцій (наприклад, за допомогою фреймворку Gophish). Також необхідно забезпечити, щоб персонал перенаправляв всі підозрілі листи, які пропустила система захисту, до служби ІБ.

Оскільки фішинг часто передбачає створення копії веб-ресурсу для несанкціонованого отримання облікових даних користувача або завантаження шкідливого ПЗ, доцільно буде розробити регламент роботи зі зверненнями клієнтів щодо виявлення ними доменів-клонів або ж доменів, які за написанням дуже схожі на доменне ім'я компанії або інших відомих сайтів – тайпсквоттингових доменів. Така практика реєстрації схожих до-

менів поширена серед кіберзлочинців, які розраховують на неуважність користувачів, коли ті переходять за посиланням, яке також може бути прикріплено до фішингового листа. Таким чином, користувач може не помітити помилку в назві веб-ресурсу та передати зловмисникові свої облікові дані. Щодо таких доменів слід також розробити регламент їх моніторингу та реагування.

Необхідно розробити регламент моніторингу та реагування на фішингові атаки. Це дозволить зменшити кількість успішних атак та відповідно зменшити витрати на нейтралізацію наслідків, додатково за рахунок оперативного реагування. На основі комплексу наявних технічних та організаційних заходів та засобів рекомендується розробити систему показників ефективності захисту від фішингових атак. Також доцільним рішенням буде розробка політики використання e-mail в компанії.

З огляду на те, що фішинг є доволі простим та ефективним способом порушення інформаційної безпеки компанії, захисту від нього слід приділяти значну увагу. Зловмисникові не потрібно зламувати систему захисту всього підприємства ззовні, він з високою ймовірністю зможе отримати доступ до інформаційної системи за допомогою самих працівників, які вже знаходяться всередині. Саме тому необхідно проводити теоретичне та практичне навчання персоналу, щоб зменшити відсоток нерозпізнаних фішингових атак з його боку, слідкувати за розміщенням даних про компанію та її працівників у відкритому доступі, особливо у соціальних мережах, та розроблювати регламенти та політики у контексті захисту від фішингових атак.

Література

1. 2021 DBIR Master's Guide. Verizon Business. URL: https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/

2. Zhurin S. I., Komarkov D. E. Protection of external information perimeter of organization from spear phishing. Bezopasnost informacionnyh tehnology. 2018. Vol. 25, no. 4. P. 96–108. URL: https://doi.org/10.26583/bit.2018.4.09

УДК 004.056.53

ТЕСТУВАННЯ БЕЗПЕКИ ПРОГРАМНОГО КОДУ

Казмірчук Є., Ткачук Р.
Львівський державний університет безпеки життєдіяльності, м .Львів

В роботі проведено аналіз існуючих методик розробки програмного забезпечення, методів тестування безпеки програмного коду а також здійснено аналіз платформи Kubernetes та Kubernetes операторів, як засобу автоматизації роботи додатків.

Ключові слова: *безпека програмного забезпечення, програмний код, тестування, вразливість.*

The paper analyzes the existing methods of software development, methods of testing the security of software code, as well as the analysis of the platform Kubernetes and Kubernetes operators as a means of automating applications.

Keywords: *software security, software code, testing, vulnerability.*

Сьогодні сфера розробки програмного забезпечення розвивається дуже швидко. Щодня з'являються нові розробники та компанії, готові запропонувати послуги з розробки програмного забезпечення. З іншого боку, у світі також активно розвивається сфера кіберзлочинності, тому вкрай важливо забезпечити надійний рівень безпеки програм, що розробляються.

Інструменти, що використовуються для підвищення безпеки програмного забезпечення, зазвичай включають пошук, виправлення, попередження та запобігання вразливостям безпеки. Як правило, інструменти та методи використовуються для виявлення слабких місць у життєвому циклі програмного забезпечення, таких як планування, проектування, розробка, розгортання, модифікація та обслуговування. Передбачається, що тести безпеки будуть виконуватися протягом усього життя програми, щоб уразливості були належним чином усунені.

Кіберзлочинці все частіше націлені на веб-додатки, тому організаціям потрібно відавати пріоритет питанням безпеки в SDLC. Це особливо актуально, коли програмне забезпечення є критичним.

Використання сканера безпеки веб-додатків та виконання інших форм тестування безпеки веб-додатків на початку процесу допоможе зменшити ризик, вирішити проблеми, що виникають, і знизити витрати [1].

SDLC є ефективним методом проектування та створення програмного забезпечення

Безпека програмного продукту включає аналіз архітектури під час проектування, перегляд коду під час кодування та конструювання, а також тестування на проникнення перед випуском [2]. Основні переваги безпечного підходу SDLC:

– програмне забезпечення безпечніше, оскільки безпека є постійною складовою при розробці;

– всі причетні до інформаційного продукту обізнані з міркуваннями безпеки;

– недоліки конструкції виявляються до їх кодування;

– економія коштів за рахунок раннього виявлення та усунення дефектів;

– зниження загальних внутрішніх бізнес-ризиків для організації.

Захищений SDLC передбачає інтеграцію тестування безпеки та інших заходів у існуючий процес розробки. Реалізація безпеки SDLC впливає на кожну фазу процесу розробки програмного забезпечення.

Існує багато типів автоматизованих інструментів для виявлення вразливостей програмного забезпечення. Поширені технології для виявлення вразливостей програмного забезпечення включають:

– статичний тест безпеки (SAST);

– динамічна перевірка безпеки (DAST);

– інтерактивне тестування безпеки додатків (IAST).

Автоматизація в кожній галузі дає переваги підвищення продуктивності та зниження витрат. Завдяки гнучкій розробці програмного забезпечення автоматизація стала настільки невід'ємною частиною гнучкого тестування, що одне без іншого важко уявити.

Тестування безпеки розвивається швидше, ніж будь-який інший ринок безпеки, оскільки рішення AST адаптуються до нових методів розробки та збільшують складність додатків.

Таким чином, автоматизовані тести інтегруються в цикл тестування, а модель DevOps залишається в центрі уваги. Це породило широкий спектр інструментів і технологій, які можна використовувати для проведення тестування безпеки з точки зору DevOps. Безперервне тестування та розгортання є основою моделі DevSecOps і роблять процес тестування та розробки спільним [2].

Kubernetes - це портативна, розширювана платформа з відкритим кодом для керування робочими навантаженнями та контейнерними службами, яка полегшує як декларативну конфігурацію, так і автоматизацію. Має велику, швидко зростаючу екосистему. Служби, підтримка та інструменти Kubernetes широко доступні.

Kubernetes забезпечує основу для сталого впровадження розподілених систем. Він дбає про масштабування та відновлення після відмови програми, надає схеми розгортання тощо.

Kubernetes визначає набір будівельних блоків, які разом забезпечують механізми для розгортання, керування та масштабування програм на основі процесора, пам'яті або метричних показників користувача. Kubernetes є вільно з'єднаним і розширюваним, щоб забезпечувати різні навантаження.

Ця розширюваність значною мірою забезпечується Kubernetes API, який використовується внутрішніми компонентами, а також розширеннями та контейнерами, що працюють на Kubernetes [3]. Платформа контролює обчислювальні ресурси та ресурси зберігання та визначає ресурси як об'єкти, якими потім можна керувати.

Додаток на Kubernetes – це програма, яка розгорнута на самому Kubernetes і керується за допомогою Kubernetes API та інструментів kubectl.

Щоб отримати максимальну віддачу від Kubernetes, потрібен доступ до повного набору API, які можна розширити, щоб підтримувати та керувати своєю програмою на основі Kubernetes. У цьому випадку оператори діють як середовище виконання для керування цим типом додатків у Kubernetes.

Оператори Kubernetes можуть виконувати різноманітні операційні завдання, від базової функціональності до логіки. Більш просунуті оператори можуть автоматично реагувати на помилки та виконувати оновлення. Оператори можуть бути адаптовані до потреб конкретної організації, і вони можуть бути повторно використані в різних програмах [4]. Щоб створити власних операторів, ви можете використовувати Operator Framework, який надає інструменти, необхідні для створення, керування та моніторингу ефективності оператора.

Література

1. OWASP Testing Guide 4.0 [Електронний ресурс] – Режим доступу: https://owasp.org/www-pdf-archive/OTGv4.pdf

2. OWASP Software Assurance Maturity Model [Електронний ресурс]: Режим доступу: https://owaspsamm.org

3. Офіційний сайт платформи Kubernetes [Електронний ресурс]: Режим доступу: https://kubernetes.io/docs/home/

4. Офіційна документація Kubernetes Operators [Електронний ресурс]: Режим доступу: https://kubernetes.io/docs/concepts/extend-kubernetes/operator/

УДК: 316.101

ПОНЯТТЯ ІНФОРМАЦІЙНОЇ ВІЙНИ СУЧАСНОСТІ

Катула М.
Відокремлений структурний підрозділ
«Ірпінський фаховий коледж Національного університету біоресурсів і природокористування України», місто Ірпінь

Анотація: *Інформаційна вразливість людей у час інтернету грає надто важливу роль. Будь яка інформація, як позитивна, так і негативна осідає у головах молоді так як вони ще не встигли сформувати власну точку зору. І що б захистити їх від цього впливу, нам потрібно знати що таке Інформаційна війна.*

Ключові слова: *точка зору, громадська думка, світогляд, інформація, інформаційна вразливість, інформаційна гігієна, засоби масової інформації, інформаційний агресор, інформаційні потоки, інформаційні ресурсів, дезінформація.*

Annotation: *People's information vulnerabilities on the Internet play a very important role. Any information, both positive and negative, settles in the minds of young people because they have not yet formed their own point of view. And to protect them from this influence, we need to know what Information Warfare is.*

Keywords: *point of view, public opinion, worldview, information, information vulnerability, information hygiene, mass media, information aggressor, information flows, information resources, misinformation.*

Сьогодні інформаційна війна стала одним з найнебезпечніших видів зброї. Користуватися компроматами, виливанням бруду, підкиданням неправдивої інформації, намагання за допомогою інформації ввести в оману стало для багатьох сенсом життя. Інформація має вплив на маси, тобто за умови вдалого маніпулювання свідомістю мас можна досягти практично будь-якої мети.

Інформаційна війна — викладення інформації у спосіб, який формує у суспільстві чи групі людей потрібну точку зору, громадську думку, хід взаємодоповнюючих логічних думок, вичерпну систему поглядів щодо окремих питань на користь організатора інформаційної пропаганди. Розвиток людини влаштований так, що людина завжди шукає відповіді про питання, які її турбують, що є невід'ємною рисою безперервних процесів пізнання.

У молодому віці, у мало освічених прошарках суспільства, у вигляді м'якої несформованої свідомості та прогалин у знаннях, завданням інформаційної війни є їх закриття потрібною, надзвичайно легкою для засвоєння та логічною на перший погляд інформацією. Відповідно, із зростанням обізнаності зменшується вразливість, у такому випадку, інформаційна війна потребує більш складного підходу для породження сумнівів, використовує численні техніки перекручування інформації, наприклад, подання неправди з логічними доказами правдивості цих фактів, фальсифікованими дослідженнями та доказами у які жертва гіпотетично має повірити і прийняти їх як свої переконання.

Інформаційна війна можлива через природну потребу навіть дорослого організму у новій інформації (для закриття прогалин у знаннях, спростуванні чи підтвердженні породжених сумнівів, перевірці та детальному вивченні нових суперечливих фактів), тому, інформаційна вразливість притаманна всім суспільним прошаркам, освіченість суспільства лише визначає, наскільки вичерпною та розгорнутою має бути подана альтернативна інформація щоб здаватись правдивою. Для мінімізації критичного ставлення до нових фактів обов'язковою умовою для початку інформаційної війни є встановлення довіри до альтернативного джерела інформації, подача його як авторитетного, науково підтвердженого тощо.

Антидотом у інформаційній війні є комплекс заходів під спільною узагальнюючою назвою інформаційна гігієна, який розкриває механізми боротьби з інформаційною війною, пояснює механізми інформаційної війни, розробляє протидію — від створення швидкого легкозасвоюваного «інформаційного цукру» на випередження, де простими словами пояснюється суть явища, до пояснення складних механізмів перевірки джерел інформації, виявлення фальшивих новин, загальноосвітня діяльність з акцентуванням уваги на можливе перекручування окремих фактів супротивником.

Відомо, що великомасштабні інформаційні технології, які дістали назву «інформаційних воєн», мають тисячолітню історію.

Інформаційна війна дозволяє управляти людьми, але тільки якщо суспільство піддається впливу цієї інформації. Варто розглянути динаміку прогресу в свідомості суспільства. Багато країн відстежують і тестують своє населення за допомогою різних опитувань і зустрічей з політичними діячами, з'ясовують переконання різних груп населення. Вся зібрана інформація дозволяє в подальшому вносити корективи в пропаганду і налаштовувати людей на певну хвилю. Прикладів інформаційного впливу на моральну, духовну стійкість супротивника можна знайти чимало і у древньому Римі, і в епоху феодалізму (боротьба з «єрессю», за «істинну віру» тощо), і в пізніші часи.

Особливого значення інформаційні війни набули у XX столітті, коли газети, радіо, а потім і телебачення стали справді засобами масової інформації, а поширювана через них інформація — справді масовою. Уже у 20-х роках США вели радіопередачі на регіони своїх «традиційних інтересів» — країни Латинської Америки, Велика Британія — на свої колонії. Німеччина, яка домагалася перегляду умов Версальського миру — на німців Померанії і Верхньої Сілезії у Польщі, Судетів — у Чехії. Тоді ж, у 30-х роках, інформаційні війни перестають бути додатком до збройних і перетворюються у самостійне явище — як от: німецько-австрійська радіовійна 1933-34 рр. з приводу приєднання Австрії до рейху. Саме тоді з'явилося і набуло поширення поняття «інформаційний агресор».

За умов трансформації інформаційної війни будуть змінюватися також її форми. Так, для інформаційної боротьби першого покоління це:

- ведення радіоелектронної боротьби;
- одержання розвідувальної інформації шляхом перехоплення й розшифровки інформаційних потоків;
- здійснення несанкціонованого доступу до інформаційних ресурсів з наступною їх фальсифікацією чи викраденням;
- масове подання в інформаційних каналах супротивника чи глобальних мережах дезінформації для впливу на особи, які приймають рішення;
- одержання інформації від перехоплення відкритих джерел інформації.

Інформаційна боротьба другого покоління передбачає:

- маніпулювання суспільною свідомістю соціальних груп населення країни з метою створення політичної напруженості та хаосу;
- дестабілізація політичних відносин між партіями, об'єднаннями й рухами з метою провокації конфліктів, розпалення недовіри, підозрілості, загострення політичної боротьби, провокування репресій проти опозиції і навіть громадянської війни;
- зниження рівня інформаційного забезпечення органів влади й управління, інспірація помилкових управлінських рішень;
- підрив міжнародного авторитету держави, його співробітництва з іншими країнами;

З інформаційною війною можна і потрібно боротися. Наприклад, американські фахівці рекомендують організувати інформаційне протиборство: створити центр по інформаційній боротьбі поруч з президентом, щоб в разі загрози відразу узгодити дії з міністерствами, а також оцінити слабкі місця в інфраструктурі, коригувати рівень безпеки і прогнозувати можливі критичні ситуації.

Література

1. Політологічний енциклопедичний словник / уклад.: Л. М. Герасіна, В. Л. Погрібна, І. О. Поліщук та ін. За ред. М. П. Требіна. — Х . :Право, 2015

2. Почепцов Г. Г. «Сучасні інформаційні війни». Видавничий дім «Києво-Могилянська Академія» - 2015. Про книгу Почепцова.

3. Ландэ Д. В., Додонов В. А., Коваленко Т. В. Информационные операции в компьютерных сетях: моделирование, выявление, анализ // МОДЕЛИРОВАНИЕ-2016: материалы пятой Международной конференции МОДЕЛИРОВАНИЕ-2016, Киев, 25-27 мая 2016 г. / ИПМЕ НАН Украины, 2016. — С. 198—201

УДК 658.52; 681.3

ЗАГРОЗИ БЕЗПЕКИ WI-FI МЕРЕЖ ТА ОСНОВНІ ПРОТОКОЛИ ЗАХИСТУ

Кичма А., Полотай О.
Національний університет «Львівська політехніка», м. Львів
Львівський державний університет безпеки життєдіяльності, м. Львів

Розглядаються основні загрози безпеки бездротових мереж та основні протоколи захисту Wi-Fi мереж
Ключові слова: *безпека Wi-Fi, WEP, WPA, WPA2, WPA3, атаки, сніфінг, несанкціонований доступ, експлойти вразливості.*

The main security threats to wireless networks and the main protocols for protecting Wi-Fi networks are considered
Keywords: *Wi-Fi security, WEP, WPA, WPA2, WPA3, attacks, sniffing, unauthorized access, vulnerability exploits.*

Протоколи безпеки бездротового зв'язку, такі як Wired Equivalent Privacy (WEP) і Wi-Fi Protected Access (WPA) – це протоколи безпеки аутентифікації, створені Wireless Alliance, які використовуються для забезпечення безпеки бездротового зв'язку. Наразі доступні чотири бездротових протоколи безпеки: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access Wi-Fi (WPA), Protected Access Wi-Fi 2 (WPA2), Protected Access Wi-Fi 3 (WPA 3).

Wired Equivalent Privacy (WEP) — це перший протокол безпеки, який був запроваджений на практиці. WEP використовує схему шифрування даних, яка заснована на комбінації значень ключів, створених користувачем і системою. Однак відомо, що WEP є найменш безпечним типом мережі, оскільки хакери розробили тактику зворотного інжинірингу та зламу системи шифрування.

Wi-Fi Protected Access (WPA) був розроблений для усунення недоліків, які були виявлені в протоколі WEP. WPA пропонує такі функції, як протокол часової цілісності ключа (TKIP), що був динамічним 128-бітним ключем, який було важче зламати, ніж статичний, незмінний ключ WEP. Він також представив перевірку цілісності повідомлень, яка сканує на наявність будь-яких змінених пакетів, надісланих хакерами, протокол цілісності тимчасового ключа (TKIP) і попередньо спільний ключ (PSK).

Згодом WPA2 вніс значні зміни та додаткові функції в бездротовий гамбіт безпеки. WPA2 замінив TKIP протоколом аутентифікації коду шифрування в режимі лічильника (CCMP), який є набагато кращим інструментом шифрування.

WP3 запровадив перші серйозні зміни в бездротовій безпеці. Деякими помітними доповненнями до протоколу безпеки стали: більший захист паролів, індивідуальне шифрування для особистих і відкритих мереж, більше безпеки для корпоративних мереж.

Оскільки Інтернет стає все більш доступним, безпека даних стає головною проблемою. Порушення даних і збої в безпеці можуть коштувати особам і підприємствам тисячі доларів. Важливо знати, які загрози є найбільш поширеними, щоб мати можливість застосовувати належні заходи безпеки. У 2021 році найпоширенішими загрозами для мереж WiFi, за даними Агентства кібербезпеки та безпеки інфраструктури США (CISA) є: Piggybacking and wardriving; Wireless sniffing; несанкціонований доступ та Vulnerability exploits.

Якщо бездротова мережа незахищена, хтось із бездротовим пристроєм може просто шукати відкриті бездротові з'єднання та відразу включатися. Контейнерство (Piggybacking) є злочином через близькість. Хтось перебуває в тому ж місці, що й ваша мережа, і використовує ваше з'єднання. Wardriving – це спільні зусилля, коли люди їздять навколо, шукаючи відкритих зв'язків для проникнення. Як зазначає CISA, ці непрохані користувачі «можуть здійснювати незаконну діяльність, контролювати та захоплювати веб-трафік або красти особисті файли». Для виправлення даних вразливостей необхідна система керування, яка блокує доступ і дозволяє лише перевіреним користувачам і гостям доступ до мережі.

Іноді злочинців більше цікавлять дані, які надходять і виходять, ніж отримання самих даних. Зрештою, якщо вони можуть перехопити незахищений трафік, коли він покине мережу, менше шансів, що їх спіймають. Інструменти сніфінгу (sniffing) є звичайними та простими у використанні, тому важливо переконатися, що весь трафік, що виходить із мережі Wi-Fi, надійно зашифрований.

Незважаючи на те, що люди повертаються на робочі місця, є багато співробітників, які все ще працюють віддалено. Це означає, що їхні незахищені мережі можуть діяти як відкриті двері в сервери та дані системи. Щоб уникнути будь-яких ризиків, потрібно зробити кілька кроків. По-перше, потрібно переконатися, що співробітники використовують пристрої, захищені надійним, часто змінюваним паролем. По-друге, переконатися, що співробітники можуть обмінюватися файлами або папками лише в корпоративних мережах або коли в цьому є реальна потреба. Обмін файлами ніколи не повинен залишатися відкритим і незахищеним.

Кіберзлочинці постійно шукають шляхи до мережі. Часто це відбувається у вигляді відомої вразливості або невиправленого програмного забезпечення чи сервера. Тому потрібно постійно виконувати регулярне сканування уразливостей, використовувати двофакторну автентифікацію та вмикати автентифікацію на рівні мережі.

Отже, якщо ви хочете захистити свої дані, вдома чи віддалено, необхідно мати протоколи безпеки для бездротових мереж та використовувати необхідні заходи захисту для передачі даних у мережі. Даний перелік роботи з кібербезпеки може здатися складним і трудомістким. Але наявність хмарної платформи Wi-Fi, яка постійно самооновлюється, щоб виправлення та вразливості завчасно вирішувалися, полегшує роботу. І ще краще, якщо ця платформа також включала безпеку корпоративного рівня на основі штучного інтелекту, щоб блокувати розширені загрози та поміщати в карантин проблемні пристрої з окремими зонами для користувачів.

Література

1. The Top Four Security WiFi Risks of 2021. – [Електронний ресурс]. – Режим доступу: https://www.plume.com/workpass/blog/the-top-four-security-wifi-risks-of-2021

2. A Complete Guide To Wireless (Wi-Fi) Security. – [Електронний ресурс]. – Режим доступу: https://www.securew2.com/blog/complete-guide-wi-fi-security

3. WHAT ARE THE DIFFERENT SECURITY PROTOCOLS FOR WIRELESS NETWORKS? – [Електронний ресурс]. – Режим доступу: https://blog.rsisecurity.com/what-are-the-different-security-protocols-for-wireless-networks/

4. IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. (2016 revision). IEEE-SA. 14 December 2016. doi:10.1109/IEEESTD.2016. 7786995. ISBN 978-1-5044-3645-8.

5. What Is Wi-Fi Security? – [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/products/wireless/what-is-wi-fi-security.html

УДК 004.056.53

ОСОБЛИВОСТІ ПОБУДОВИ ЗАХИЩЕНОЇ МЕРЕЖІ ПІДПРИЄМСТВА

Кленик О., Ткачук Р.
Львівський державний університет безпеки життєдіяльності, м .Львів

В роботі прорведено дослідження із організації захисту корпоративної мережі. Описані особливості вистановлення контролю периметру корпоративної мережі, організація безпеки всередині самої мережі. А також розглянуто заходи із підвищення захищеності систем в аспекті зменшення поверхні можливої атаки на мережу.
Ключові слова: *локальна мережа, безпека, захист, контроль.*

The research on the organization of corporate network protection is carried out in the work. Features of establishment of control of perimeter of a corporate network, the organization of safety within the network are described. Also, measures to increase the security of systems in terms of reducing the surface of a possible attack on the network are considered.
Keywords: *local network, security, protection, control.*

Зі збільшенням обсягу даних, які використовуються користувачами інформаційної системи, збільшуються труднощі у веденні успішного бізнесу. Одним з найважливіших завдань для успішного функціонування інформаційної системи компанії є забезпечення збереження даних у мережі.

Для того, щоб зберегти конфіденційність даних всередині компанії, необхідно налаштувати систему інформаційної безпеки. Однак при її побудові потрібно зберегти принципи конфіденційності, цілісності та доступності. Але без виявлення та оцінки ризиків налагодити систему інформаційної безпеки неможливо. Хоча міжнародний стандарт ISO 27000 не визначає, який метод слід використовувати для оцінки ризиків, це завдання зазвичай покладається на керівників або відповідальних за створення системи захисту інформації в компанії.

Контроль периметру корпоративної мережі

Для того, щоб створити безпечну мережу, контроль спочатку вводиться на периметр мережі компанії. Для контролю трафіку використовуються мережеві екрани з функціями керування на рівні програми та системи контролю вторгнень (ips) – next generation firewal (NGFW). Публічні сервіси встановлюють в окремих нейтральних зонах і налаштовують правила доступу для контролю потоків даних і відмови від використання загальних сутностей, таких як «any», «all» [1].

Також для захисту периметра необхідно використовувати проксі-сервер для контролю доступу в Інтернет користувачів. Також необхідно

заблокувати доступ до ресурсів із забороненою тематикою, поганою репутацією, високим ризиком та фішинговими ресурсами. Антивірусне сканування та фільтрація завантаження вмісту є обов'язковими. Зокрема, потрібно заблокувати завантаження виконуваних файлів для звичайних користувачів. Також необхідно налаштувати повне сканування SSL для виявлення загроз у зашифрованому трафіку. Відповідно, необхідно організувати заборону на використання безумовних білих списків для доступу до зовнішніх ресурсів та організувати білі списки внутрішніх систем в обхід правил тематичного огляду [3, 4].

Зокрема, щоб створити безпечний периметр, потрібно використовувати електронний шлюз для захисту корпоративної електронної пошти від спаму та зовнішніх загроз. Передача інформації між підрозділами компанії та з віддаленим доступом користувачів через Інтернет-канали має відбуватися тільки через VPN з відповідним рівнем шифрування (aes-256 і вище) та з обов'язковим моніторингом і фіксацією вжитих заходів. Все це стосується як зовнішніх партнерів, так і підрядників компанії.

Безпека локальної мережі

Однак недостатньо лише створити захищений периметр мережі необхідно організувати належний рівень безпеки в самій мережі.

Спочатку потрібно сегментувати локальну мережу за функціональним призначенням, тобто розділити сервіси на відповідні сегменти сервера. Крім того, необхідно заборонити створення сегментів у великій кількості систем, оскільки технологія VLAN дозволяє створити сегмент із 4096 пристроями. Для особливо критичних систем і сервісів необхідно мікросегментувати мережу, в ідеалі за принципом один сегмент - одна система.

Також потрібно ізолювати порти на комутаторах доступу користувачів, щоб уникнути прямої взаємодії між системами користувача. Технології захисту від атак, такі як ARP-спуфінг і DHCP-серверів, також повинні бути налаштовані, щоб запобігти перехопленню трафіку даних [3].

Також необхідно заблокувати пряму мережеву взаємодію між Інтернет-сервісами та корпоративною мережею. Зв'язок між сегментами має відбуватися тільки через проксі-сервери, які розташовані в нейтральних зонах на вузлі мереж. Крім того, трафік між нейтральною зоною та ресурсами Інтернету, а також між нейтральною зоною та корпоративною мережею повинен контролюватися брандмауерами.

Захищеність корпоративних систем

Наступним кроком буде підвищення безпеки систем, що експлуатуються в організації (мережевих пристроїв, серверних і користувацьких систем) з метою зменшення можливої зони атаки на мережу [4].

Необхідно видалити та деактивувати зайві компоненти та служби, які не використовуються або не потрібні в робочому процесі. Також слід уни-

кати використання застарілих протоколів, таких як NTML, SMBv1 тощо. Слід вжити механізмів та заходів для протидії передачі паролів з пам'яті та системних процесів.

Також потрібно заборонити створення локальних облікових записів або змінювати їхні паролі, оскільки інформація про обліковий запис і пароль доступна всім користувачам мережі. Регулярні оновлення системного та прикладного програмного забезпечення також повинні дозволяти блокувати механізм автоматичного виявлення проксі-серверів WPAD.

Необхідно постійно перевіряти, що на сервері та системі організації встановлено новітнє антивірусне програмне забезпечення, і регулярно оновлювати його. Крім того, організувати наявність в системах організації встановленого рішення Host IPS з увімкненим функціоналом [2]:

– брандмауер з налаштованими мінімальними дозволами, необхідними для роботи;

– захист сигнатур від атак як на рівні мережі, так і всередині самої системи;

– блокування невідомих процесів в робочій і системній пам'яті;

– поведінковий аналіз дій програмних процесів і блокування у разі підозрілої діяльності;

– блокування підлеглих процесів, які створюють документи Office.

І нарешті, потрібне рішення для контролю підключення периферійних пристроїв і знімних носіїв до робочих станцій організації. Крім того, слід налаштувати правила для підключення до корпоративної мережі лише перевірених корпоративних носіїв.

Література

1. Методи захисту мереж [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: https://studopedia.su/6_4733_metodi-zashchiti-setey.html.

2. Росляков О. О. Віртуальні приватні мережі. Основи побудови та застосування / О. О. Росляков, С. В. Попов. – Київ: Еко-трендз, 2006. – 301 с. Snader J. J. VPNs illustrated: Tunnels, VPN's and IPsec / John Junior Snader., 2006. – 445 с.

3. Захист мережі: комплексний підхід [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://goo.su/16VM.

4. Концепції захисту IT-інфраструктури від сучасних загроз [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: http://netwave.ua/ru/kontseptsy-ya-zashhy-ty-y-t-y-nfrastruktury-ot-sovremenny-h-ugroz.

УДК 004.9

СИСТЕМИ АВТОМАТИЧНОГО КЕРУВАННЯ ПРОГРАМНИМ ЗАБЕЗПЕЧЕННЯМ

Колядич І., Ткачук Р.
Національний університет "Львівська політехніка", м .Львів
Львівський державний університет безпеки життєдіяльності, м .Львів

В роботі проведено аналіз існуючих рішень та технологій для побудови систем автоматичного керування програмним забезпеченням. Спираючись на дослідження надані рекомендації для проектування власної системи керування програмним забезпеченням, обґрунтовано вибір технологій та методів для усунення недоліків в уже існуючих системах.

Ключові слова: *програмне забезпечення, керування, встановлення, адміністрування, автоматизація, технології.*

The analysis of existing solutions and technologies for the construction of automatic software control systems is carried out in the work. Based on the research, recommendations for designing your own software management system are provided, the choice of technologies and methods for eliminating shortcomings in existing systems is substantiated.

Keywords: *software, management, installation, administration, automation, technology.*

З кожним роком, як в приватному, так і в державному секторі, зростає інтенсивність використання в практичній діяльності різноманітних програмних продуктів, також їхня кількість зростає і з розвитком самих компаній. Завдання, встановлення, видалення та підтримка в актуальному стані ПЗ потребує багато як людських так і апаратних ресурсів. Для уникнення такої рутинної роботи застосовують інструменти розгортання програмного забезпечення. Ці інструменти автоматизують існуючі послуги та завдання розгортання, відстежують користувачів та активність програм а також покращують інформаційну безпеку. Розгортання програмного забезпечення – складний процес. Компанії мають налаштувати, перевірити та відстежувати функціонування інструменту розгортання програмного забезпечення.

Вирішення питання централізованого встановлення, видалення та оновлення програмного забезпечення на комп'ютерах підприємства можливе декількома шляхами [1]:

Перший, найпростіший, шлях полягає у встановленні ПЗ на комп'ютери-абоненти вручну адміністратором.

Другий варіант вирішення проблеми полягає у створенні хмарного сховища, у якому адміністратор розміщує стиснуті дані необхідних для інсталяції програм та їх компонентів.

Третій варіант полягає у використанні автоматизованої системи мережевої інсталяції – спеціальної програми, яка у режимі прямого підключення до клієнтів по локальній мережі буде проводити встановлення необхідного програмного забезпечення незалежно від наявності чи відсутності контролю з боку адміністратора. Така методика поєднує переваги першого та другого методів – компетенція адміністратора може забезпечувати інсталяцію, але у той же час вона економить робочий час системи як при застосуванні хмарного середовища.

Така система повинна забезпечувати стійку роботу з усіма абонентами локальної мережі, допускаючи можливість працювати як з окремими комп'ютерами так і з цілими виділеними робочими групами комп'ютерів. По-друге, гіпотетична система інсталяції повинна мати можливість доступу до встановлених на клієнтських комп'ютерах програмних додатків щоб уникнути повторної інсталяції та, як її наслідок, нераціонального використання пам'яті комп'ютерів-абонентів, у випадку якщо необхідний софт вже встановлений.

Наразі існує кілька методів та програм з керування програмним забезпеченням, що відповідають цим вимогам, найпопулярніші із них це встановлення програм за допомогою групових політик, відповідно, до яких відбувається налаштування робочого середовища Windows в каталозі Active Directory. Встановлення програм за допомогою менеджера пакетів для Windows під назвою Chocolatey який працює по аналогії з системами встановлення програм в операційних системах на основі ядра Linux, використання спеціального програмного забезпечення – такого як Total Software Deployment яке дозволяє в локальній мережі встановлювати або видаляти програмне забезпечення [2, 3].

Оскільки система має бути простою для розуміння системними адміністраторами слід використовувати ті технології з якими вони можуть бути потенційно знайомі. В середовищі систем Windows є достатньо технологій що полегшують виконання адміністративних задач, навіть встановлення ПЗ, однак інтерфейс їх використання не завжди зрозумілий і без додаткових модулів та методів керування як правило не придатний. Для вирішення поставленої проблеми можна використати наявний інформаційний продукт: WMI(Windows Management Instrumentation), об'єкти групової політики що входять до елементів каталогу Active Directory, інструмент psexec, утиліти для роботи з реєстром(reg), а також необхідні будуть технології тихого встановлення ПЗ які пропонують самі розробники ПЗ або які присутні у програмах для інсталяції даного ПЗ.

Ці технології є корисними в певних задачах вони можуть вирішити проблему централізованого оновлення чи встановлення певного ПЗ однак об'єднати їх в комплексну систему можна тільки за допомогою відповідної мови програмування. Найбільше для вирішення цієї задачі підходить мова програмування Python. Він простий, потужний і підтримує спеціальні пакети, які підвищують його ефективність. Завдяки лаконічності мови Python можна швидко прочитати код і знайти слабкі місця [4].

Таким чином вказані технології можна об'єднати в цілісну програму і побудувати навколо них зручний та зрозумілий інтерфейс програми за допомогою мови Python. Це дозволить користуватися всіма перевагами даних технологій і змінювати та реалізовувати потрібні функції програми без залучення додаткового, стороннього ПО, що значно спростить її використання. До того ж дані технології широко використовуються у сфері адміністрування і є зрозумілими для потенційних користувачів.

Література

1. Manukhina D., Potapov A., Solomatina L., Badmayev A., Nilova A., Fedotov D. Analysis of modern technologies for deployment of applications and software tools for creating installation packages // Visnyk of TSU. Natural and technical sciences series. – 2014. – T. 19, № 6. – S. 1841 – 1844

2. Svidergol B., Meloski V., Wright B., Martinez S., Bassett D., Mastering Windows Server 2016 / Svidergol B., Meloski V., Wright B., Martinez S., Bassett D., John Wiley & Sons, 2018, 608 p.

3. Russinovich M., Margosis A.., Troubleshooting with the Windows Sysinternals Tools/ Russinovich M., Margosis A., Microsoft Press, 2016, 648 p.

4. Hughes J. M., Real World Instrumentation with Python: Automated Data Acquisition and Control Systems/ Hughes J. M., "O'Reilly Media, Inc.", 2010, 622p.

УДК 004.9

ХМАРНІ СХОВИЩА ТА ЇХ ПРАВИЛА БЕЗПЕКИ

Кравченко В.
ДВНЗ «Київський національний економічний університет ім. Вадима Гетьмана», м. Київ

***Анотація**: Національний інститут стандартів і технологій (NIST) визначив хмарні обчислення як модель для забезпечення зручного мережевого доступу за вимогою до спільного пулу настроюваних обчислювальних ресурсів, які можна швидко надати та випустити з мінімальними зусиллями керування або взаємодії з провайдером хмари. Хмарні обчислення мають потенціал змінити те, як організації керують інформаційними технологіями, і одночасно трансформувати економіку обладнання та програмного забезпечення. Основною метою цієї статті є виявлення проблем конфіденційності та безпеки в розподіленому середовищі та занепокоєння учасників і користувачів хмарних обчислень.*

***Ключові слова:** хмарні обчислення, безпека та конфіденційність, інформаційні технології, IT, програмне забезпечення, інформаційні технології, сервер, хмарне сховище.*

***Abstract:** The National Institute of Standards and Technology (NIST) defined cloud computing as a model for enabling convenient, ondemand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or cloud provider interaction. Cloud computing has the potential to change how organizations manage information technology and transform the economics of hardware and software at the same time. A principal goal of this paper is to identify privacy and security issues in the distributed environment and concern to cloud computing participants and users .*

***Keywords:** cloud computing, security and privacy, information technology, IT, software, information technology, server, cloud storage service.*

Вступ. Зберігати документи, фотографії, відео та звіти на жорсткому диску комп'ютера? Це стає майже дивним. Сьогодні люди все частіше зберігають свої файли в хмарі, сховищі не на їхніх комп'ютерах чи пристроях, а на серверах, розміщених сторонніми провайдерами. Але якщо дані потрапляють в зовнішню хмару, то складно сказати наскільки вони захищені і чи не будуть з часом викрадені і/або змінені за бажання конкурентів або зловмисниками, які промишляють проникненням в чужі сховища постійно. За даними Cloud Security Alliance, хмарні служби за своєю захищеністю не поступаються локальним сховищам, а подекуди й переважають їх, але міркування безпеки залишаються основною перешкодою на шляху до впровадження хмарної інфраструктури. Саме через це захист хмарних служб – пріоритетний напрямок для інвестицій постачальників послуг.

Виклад основного матеріалу. Ви коли-небудь писали есе, яке ви зберегли в Google Docs? Тоді ви використали хмару. Ви коли-небудь дивилися фільм на Netflix, зберігали зображення в Dropbox або надсилали повідомлення електронною поштою через Yahoo Mail? Це все хмарні сервіси. В основному, хмара відноситься до будь-якого типу програмного забезпечення або служби, які не розташовані на вашому персональному комп'ютері чи пристроях, а працюють в Інтернеті.

Серед популярних постачальників хмарних послуг – Google Cloud Platform, Amazon Web Services і Microsoft Azure. Все, від Hulu і Dropbox до Gmail і Office 365, розміщується в хмарі, а не на вашому персональному комп'ютері чи телефоні.

Все більше організацій усвідомлюють численні переваги для бізнесу від перенесення своїх систем у хмару. Хмарні обчислення дозволяють організаціям працювати в масштабі, знижувати витрати на технології та використовувати гнучкі системи, які дають їм конкурентну перевагу. Однак дуже важливо, щоб організації були повністю впевнені в безпеці своїх хмарних обчислень і щоб усі дані, системи та програми були захищені від крадіжки, витоку, пошкодження та видалення даних.

Хмарна безпека, також відома як безпека хмарних обчислень, складається з набору політик, засобів керування, процедур і технологій, які працюють разом для захисту хмарних систем, даних та інфраструктури від кіберзагроз та атак. Надійна хмарна кібербезпека має важливе значення для запобігання втрати даних та допомоги організації у дотриманні правил щодо конфіденційності даних. Якщо хмарні дані будуть скомпрометовані, компанії ризикують втратити на кількох рівнях. Йдеться про втрату доходу, репутації та безперервності бізнесу.

Спосіб забезпечення хмарної безпеки буде залежати від окремого постачальника хмари або наявних рішень хмарної безпеки. Однак впровадження процесів хмарної безпеки має бути спільною відповідальністю між власником бізнесу та постачальником рішень.

Ось деякі із заходів безпеки, які постачальники хмарних послуг часто використовують для захисту ваших даних:

1. *Послідовні оновлення безпеки.* Ваш постачальник хмарних послуг регулярно оновлюватиме свої заходи безпеки.
2. *Інструменти штучного інтелекту та автоматичне виправлення.* Ці програми покладаються на вбудовані алгоритми для пошуку та виявлення можливих вразливостей у заходах безпеки.
3. *Вбудовані брандмауери*. Це ускладнює для хакерів можливість пропустити зловмисне програмне забезпечення або віруси за межі заходів безпеки, які використовує ваш постачальник хмарних послуг.
4. *Надлишковість*. Більшість найбільших хмарних провайдерів практикують резервування. Це означає, що вони копіюють ваші дані кілька разів і зберігають їх у багатьох різних центрах обробки даних. Таким чином, якщо один сервер вийде з ладу, ви зможете отримати доступ до своїх файлів із резервного сервера.
5. *Тестування безпеки сторонніми розробниками.* Ваш постачальник хмарних послуг також повинен наймати сторонні компанії безпеки для регулярного тестування своїх серверів і програмного забезпечення, щоб переконатися, що вони захищені від хакерів, кіберзлочинців та найновіших шкідливих програм і вірусів.

Які заходи безпеки ви можете вжити, щоб підвищити безпеку в хмарі? [2]

1. *Аудит і перевірка ваших файлів та загальних папок.* Будьте пильні до тих, кому поширюєте файли та папки, додавайте паролі доступу і терміни закінчення їх дії у свої загальні ресурси, якщо ці функції доступні.
2. *Використовуйте Менеджер паролів.*
3. *Використовуйте двофакторну аутентифікацію.*
4. *Впровадити шифрування в хмарі.*
5. *Керуйте доступом для сторонніх програм.* Деякі програми запитують дозвіл на маніпулювання або навіть видалення ваших даних, коли їм це не потрібно. Як компанія, ви повинні уважно ознайомитися з положеннями та умовами, щоб оцінити рівень ризику, на який ви потенційно можете поставити свій бізнес.
6. *Резервне копіювання хмарних даних.*
7. *Увімкніть сповіщення та повідомлення про дії в акаунті*. Більшість хмарних сервісів зберігання даних можуть відправляти вам сповіщення про різні події в обліковому записі, такі як нові входи, зміни в файлах та доступі до них.

Висновок. Хмарні обчислення є артефактом високотехнологічних досліджень віртуалізації, розподілених обчислень із використанням програмного забезпечення та пов'язаних з ним послуг,

а також мереж. Це повністю відкриває новий передовий і захищений світ можливостей для бізнесу, але в поєднанні з пропозиціями та високим рівнем проблем безпеки, які необхідно враховувати, коли суспільство використовує передові концепції хмарних обчислень.

Література:

1. Чмир П. Особливості використання хмарних серверів зберігання інформації / Чмир П., Бурак Н.: збірник тез доповідей II Міжвузівської науково-практичної конференції студентів і курсантів. – Львів: ЛДУ БЖД, 2017. С.61 – 62.

2. Безпека хмарних сховищ і технологій. Основні правила. [Електронний ресурс] – Режим доступу до ресурсу: https://datami.ua/bezpeka-hmarnih-shovishh-i-tehnologij-osnovni-pravila/

УДК 004

БЕЗПЕКА ХМАРНИХ СХОВИЩ

Легомінова С.В., Рабчун Д.І.
Державний університет телекомунікацій, м.Київ

Визначено основні проблемні питання використання хмарних технологій споживачами, а саме виокремлено дисбаланс інтересів провайдерів IT-ланшафтів та споживачів, запропоновано доопрацювання методів захисту інформації для знаходження балансу інтересів.

Ключові слова: *інформаційна безпека,хмарні технології, провайдери, споживачі.*

The main problematic issues of the use of cloud technologies by consumers are identified, namely, the imbalance of interests of providers of IT-landscapes and consumers is highlighted, the refinement of information protection methods to find a balance of interests is proposed.

Key words: *information security, cloud technologies, providers, consumers.*

Хмарні технології (Cloud Computing). – це підхід, який дозволяє знизити складність комп'ютерних систем за рахунок використання ефективних інформаційних технологій, які доступні в рамках віртуальної інфраструктури для самостійного керування чи надаються в якості сервісів [1].

Проблемним питанням бізнесу та державних організацій є використання оптимальних інфраструктур дата-центру, або декількох дата-центрів, що дозволило би побудувати будь-які складні та повністю зарезервовані IT-ландшафти, але важливою вимогою є інформаційна безпека у хмарі, яка має бути підтверджена сертифікацією.

Надання послуг щодо використання хмарних технології супроводжується акцентуванням на перевагах застосування хмари, а саме: всеосяжна доступність до даних з будь–якого пристрою, що має доступ до інтернету; використання сучасних обчислюваних ресурсів; можливість організації роботи з даними зацікавленими ком'юніті; надання гарантій щодо забезпечення збереження цілісності даних при ймовірних збоях; забезпечення цілісності даних споживача за рахунок якісного виконання своїх обов'язків провайдера хмари, що включає придбання, обслуговування, підтримку IT-ланшафту задля збереження даних споживача: персональних даних, публічних репозиторіїв, документації підприємств та організацій, а також надання послуг обчислення.

Однак, нагальною проблемою залишається захист інформації від несанкціонованого доступу, безпека використання хмарних технологій, а також передбачення ймовірних ризиків, які мають виникати в процесі використання хмарних сховищ. В першу чергу, це довіра провайдерові, надання йому права доступу до інформації, що можна охарактеризувати, як втрату контролю над власними даними споживача, що формує ризик втрати інформації при певних умовах. В той же час провайдери в ліцензійних угодах намагаються обмежити свою відповідальність щодо збереження інформаційних даних споживача. Провайдер прописує , що дані можуть підвергатися пошкодженню, спотворенню або втраті й в цьому випадку він не гарантує цілісність інформації, також в разі втрат бізнесом, провайдер обмежує свою відповідальність тільки абонентською платою використання сервісів.

Тому на часі є розробка та впровадження нових методів захисту інформації у хмарі.

Найбільш ефективними способами збереження даних у хмарі на сьогодні є : шифрування, захист даних при передаванні, аутентифікація та ізоляція користувачів.

Знаходження балансу між вимогами споживача та провайдера хмарних послуг є запорукою продуктивного розвитку та ефективного використання технологічних досягнень.

Література

1. Ялова К.М., Яшина К.В., Веремейченко М.О. Безпека і ризики хмарного збереження даних. *International scientific journal «Grail of Science».2021.* № 2-3. 320-323.

2. Соснин, В.В. Облачные вычисления в образовании. Москва: ИНТУИТ, 2016. 96 с.

УДК 004.056

ЗАХИСТ ВЕБ-РЕСУРСІВ НА ПРИКЛАДІ ЛОГУВАННЯ ДІЙ КОРИСТУВАЧІВ

Лесик Ю., Навитка М.
Львівський державний університет безпеки життєдіяльності

Найважливішим завданням, яке доводиться вирішувати при створенні веб-додатків, є збереження відомостей, що відносяться до користувача, за весь сеанс його роботи, в той час як сам користувач може вільно переміщатися між сторінками програми.

В даній статті проведено аналіз особливості стану захисту веб-ресурсів на прикладі логування дій користувачів. Сформульовано якісний підхід до інформаційної безпеки.

Ключові слова: *веб-ресурси, логування, лог-файли.*

The most important task to solve when creating web applications is to save information related to the user for the entire session of his work, while the user can move freely between the pages of the program.

This article analyzes the peculiarities of the state of protection of web resources on the example of logging user actions. A qualitative approach to information security is formulated.

Keywords: *web resources, logging, log files.*

Постійний розвиток сучасних технологій провокує зловмисників на безперервне ускладнення різних загроз. Грамотний захист завжди будується на розумінні слабкостей ПЗ, яке необхідно захистити. Це дозволяє відсіяти неактуальні спроби атак і виділити тільки ті, які стосуються реальних вразливостей, які знаходяться в системі.

Логування дій користувачів у веб-ресурсах, де синонімом логування можна вважати ведення протоколу (або протоколювання) у хронологічному порядку з різним ступенем деталізації відомостей, що відбуваються в системі (помилки, попередження, повідомлення) та запису його зазвичай в файл. В абсолютній більшості сучасних програм використовуються текстові файли протоколів (одна подія – один рядок), вони легко генеруються програмою і аналізуються людиною. Як виняток, в інтерактивних утиліти (командного рядка) повідомлення про події виводяться прямо на екран користувачеві, однак і цей висновок при необхідності можна перенаправити в файл.

Лог-файли (log-files) – представляють собою спеціальні текстові файли, в яких записуються певні дії користувача або самої програми. Їх використовують для виявлення і усунення несправностей в місцях, де їх складно або неможливо виявити вручну.

Найпростіший і тому найпоширеніший спосіб – це логування в текстовий файл. Спосіб, при якому окрема подія є окремий рядок. З точки зору реалізації – досить легко налагодити таке логування в коді більшості мов програмування, – так і з боку використання – читати такий лог-файлів можна будь-яким текстовим редактором.) Найпростіший і тому найпоширеніший спосіб – це логування в текстовий файл. Спосіб, при якому окрема подія є окремий рядок. З точки зору реалізації – досить легко налагодити таке логування в коді більшості мов програмування, – так і з боку використання – читати такий лог-файлів можна будь-яким текстовим редактором.

Найчастіше логування – процес непомітний. Система пише логзаписи, використовуючи конфігурацію, яка передбачена виробником. Зазвичай конфігурація логування підбирається так, щоб це не викликало якоїсь проблеми у користувача. Проблеми можуть бути найрізноманітніші: від зниження продуктивності через постійний запис інформації в лог-файли (на жорсткий диск) до проблем з вільним місцем на жорсткому диску.

Проаналізувавши лог-файли, можна отримати зведені дані про несправності в роботі програми або інформацію про активність користувачів для вивчення закономірності поведінки груп користувачів і оцінити ефективність рекламної кампанії. Часто використовувані дані можуть записуватися відразу в базу даних, а не тільки в лог-файл.

Отже, найважливішим завданням, яке доводиться вирішувати при створенні веб-додатків, є збереження відомостей, що відносяться до користувача, за весь сеанс його роботи, в той час як сам користувач може вільно переміщатися між сторінками програми. Кожен HTTP запит для сторінки обробляється веб-сервером незалежно. Таким чином, сервер не зберігає відомостей про попередні запити незалежно від того, наскільки малі проміжки часу між ними. Ця особливість ускладнює створення деяких програм, наприклад інтерактивного каталогу, де необхідно зберігати відомості про вибрані користувачем елементи каталогу при його переміщенні між сторінками каталогу. Потрібно мати всі необхідні інструменти й дані для швидкого вирішення проблем, і логи — невіддільна частина цього процесу.

Література

1. Онищенко С. В. WEB-технології : навч.-метод. комплекс. Бердянськ : «БДПУ», 2016. 500 с.

2. Бондаренко О., Ушкаленко І. Безпека web-додатків: актуальні проблеми та їх аналіз. Формування ринкової економіки в Україні. Львів, 2017. С. 28-36. URL: http://repository.vsau.org/getfile.php/17100.PDF

3. Василенко І. В. Універсальній метод захисту веб-додатків. Системи обробки інформації. 2016. Вип. 1. С. 122-124.URL: http://nbuv.gov.ua/UJRN/soi_2016_1_27.

ІНФОРМАЦІЙНА ВІЙНА ЯК СЬОГОДЕННА РЕАЛЬНІСТЬ

Малець Б.І., Малець І.О.
Львівський національний університет ім. Івана Франка,
Львівський державний університет безпеки життєдіяльності

Анотація: *Розглянута проблема інформаційних війн та наслідки інформаційних війн, як впливають на суспільство і чим це загрожує. Розглянуто способи захисту населення від неправдивої інформації*

Ключові слова: *мережа "інтернет", інформаційна війна, соціальні мережі, медіа-простір, захист населення.*

Сьогодні люди мають можливість переглядати безліч інформації проте дуже часто її не перевіряють на істинність. За останні 30 років відбувся неймовірний розвиток галузі інформації що дало змогу людству розвиватися значно швидше, проте це спричинило також і свої наслідки якими є інформаційне сміття, це можуть бути як і чутки так і розповсюдження недостовірної інформації, також цей розвиток прийшов до того що з'явилось нове поле бою між країнами яке називається Інформаційною війною.

Інформація на даний момент є однією з найбільш важливих стратегічних одиниць для будь якої країни. Чим більш ерудоване населення, чим більше воно звертає увагу на інформацію яке отримує і перевіряє її тим краще становище буде в державі оскільки люди будуть розуміти в якому ми зараз стані і що відбувається насправді. На даний момент є 4 ключові теми в інформаційній війні з Росією які вона пробує просунути максимально як це дозволяє на даний момент мережа інтернет. Звіт від українського кризисного центру показує що найчастіше інформаційна війна була направлена на такі теми:

- вакцинацією від COVID-19;
- ескалацією на фронті;
- Днем пам'яті і примирення та історичною дезінформацією;
- відносинами з західними партнерами.

На сьогодні ключовою проблемою України є дезінформація населення, що призводить до багатьох проблем які випливають на життя населення а також на здоров'я населення. Як показує практика варто забезпечити людей вмінням розрізняти інформацію і все буде простіше. Так наприклад в Україні є ресурси які дають змогу проаналізувати чи це є фейк новина чи це є правдива інформація. Один з таких ресурсів є StopFake.org який дає змогу перевірити чи ця інформація надійшла від перевіреного джерела, чи від джерела яке часто розповсюджувало фейкові новини.

Також ми можемо відчути наслідки інформаційної війни від 2013 року в яких зіграли важливу роль люди які були мало освідченні і не задумувалися над тим що справді відбувалося і вбирали інформацію як губки воду без її аналізу. Розглянемо ключові точки які просувало РФ в період інформаційної війни

2014–2015 рр.:
- поляризація суспільства через інструменталізацію міфу про загрозу російськомовному населенню;
- дискредитація військово-політичного керівництва України;
- рух за «третій Майдан» з метою спровокувати контрольований Кремлем хаос;
- популяризація ідей «Русского мира».

2016–2018 рр.:
- продовження руху за «третій Майдан»;
- політизація будь-яких тем – від питань мови та релігії до проблем освіти;
- операції на підрив двосторонніх відносин між Україною та партнерами, зокрема з Польщею.

2018–2020 рр.:
- маргіналізація українського уряду та фокус на Україні як «недодержави» для посилення суспільного невдоволення;
- операції, спрямовані на поширення та закріплення анти-західної риторики;
- дискредитація громадянського суспільства;
- операції на підрив двосторонніх відносин між Україною та партнерами, зокрема з Угорщиною;
- інформаційні операції, пов'язані з пандемією COVID-19.

Дуже велика кількість мало освіченого населення було обмануте неправдивою інформацією. Що привело до того, що люди стали відноситися агресивно до різних частин країни, сприймаючи неправдиву інформацію за правду. Це призвело до ескалації конфлікту на тимчасово окупованих територіях, підтримку проросійських сил які тоді почали активно діяти. Також важливу роль відіграли кремле-боти які тоді активно мусолили ці теми в інтернеті, що також мало свій вплив на цю ситуацію, і на людей які проживали на цих територіях.

Отже робимо висновок що інформаційна війна це нове поле бою яке може бути використано проти всіх неосвічених людей які свято вірять тому що написано десь там в інтернеті або десь там сказано якщо людина усвідомлює і фільтрує інформацію то вона з легкістю зможе розібратися де правда де не правда.

Література

1. Огляд основних операцій російського інформаційного впливу в Україні за перше півріччя 2021 року https://drive.google.com/file/d/1iGc0ltCf-Yp23vN_8WukS7pZp5dSRAYv/view.

УДК 004.056.2

ВИКОРИСТАННЯ SPLUNK ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ В ОРГАНІЗАЦІЯХ

Малькевич Р., Балацька В.
Львівський державний університет безпеки життєдіяльності, Львів

***Анотація**: Сучасне функціонування організацій будь яких форм власності практично неможливо без використання співробітниками різних серверів для роботи з даними, це безпосередньо впливає на рівень інформаційної безпеки. У роботі розглянуто використання інструменту Splunk, який функціонує на збиранні логів та виявлення в них подій.*

***Ключові слова**: Splunk, MapReduce, forwarder, big data, Splunk Enterprise Security.*

***Summary**: The modern functioning of organizations of any form of ownership is almost impossible without the use of employees of different servers to work with data, it directly affects the level of information security. The paper considers the use of the Splunk tool, which works on collecting logs and detecting events in them.*

***Keywords**: Splunk, MapReduce, forwarder, big data, Splunk Enterprise Security.*

Безпека та конфіденційність даних завжди були важливими, але враховуючи значні порушення, які відбулися протягом останніх двох років, вони стають все більш важливими з кожним днем. Для підвищення безпеки підприємств, організацій та захисту інформації у них, пропонується почати з більш ефективного використання даних, які система вже реєструє. Також для кращого захисту важливої інформації необхідно зібрати більше даних, щоб краще розуміти систему і легше помітити будь-які підозрілі події. У будь-якому випадку необхідно використовувати інструмент, який спеціалізується на роботі з даними журналів, щоб не доводилося читати неструктуровані дані з багатьох різних джерел. Ось тут на допомогу приходить Splunk.

Splunk – це система зберігання та аналізу логів [1]. Її принцип роботи можна описати так: є сервер Splunk, який зберігає, індексує та дозволяє аналізувати логи, і є робочі машини (сервери), які ці логи створюють і передають на сервер Splunk. Сервер Splunk в свою чергу може бути кластером з декількох фізичних машин, між якими розподіляється зберігання інформації і які використовуються для її обробки за технологією MapReduce. Способів передавати логи з робочих машин дуже багато: через спеціальну програму forwarder, яка вміє швидко і ефективно відсилати зміни логів на сервер, через технології типу NFS/SMB, або SNMP, можна самостійно відсилати дані в Splunk по TCP/IP (наприклад, замість того, щоб писати в файл). Під Windows Splunk вміє брати дані з Windows Events, Performance Counters або Реєстру.

Платформа Splunk фіксує та аналізує масивні шматки неструктурованих машинних даних. Запущений інструмент має можливість показати змістовне представлення даних, створених людиною [2]. DATA - нескінченна річ, у яку люди роблять свій внесок щодня. Розглянемо статистичні дані, які дадуть чітке уявлення про світ Big Data. Кількість користувачів мобільних мереж з кожним роком зростає, за останні 4-6 років кількість користувачів зросла на 1 мільярд. Мобільні телефони є основним джерелом більш ніж половини веб-трафіку у всьому світі. Одна з найпопулярніших пошукових систем є Googl обробляє більше 40 000 пошукових запитів щосекунди. І це лише Google, але окрім нього також існують інші пошукові системи, які теж оброблять величезну кількість запитів та інформації.

Як саме працює Splunk? [3]. Splunk має три основні фази роботи. У першій фазі, він ідентифікує дані за допомогою рішення. У другій фазі, ці машинні дані він перетворює в результати. І нарешті, у третій фазі, є змога конвертувати ці результати у звіти, діаграми або графіки для широкого використання візуальної інформації. Важливим компонентом є машинні дані, вони створюються та насичуються за допомогою нових технологій та систем, які люди використовують щодня. Одні з популярних сервісів є: AWS, APM, медичний простір, веб-сервери, системні журнали. Інформацію, яку поглинають дані сервіси, мають широке застосування та сприяють величезній кількості випадків використання у будь-якій з цих організацій. Самі дані є складними для розуміння масивами, що відображаються у різних форматах. Багато із традиційних інструментів або платформ не в змозі допомогти користувачам розібратись з цими даними і саме тут Splunk може голосно про себе заявити.

Splunk служить виявленням зловмисних дій співробітників та інших внутрішніх загроз до того, як станеться крадіжка конфіденційних даних, їх пошкодження чи зловживання повноваженнями [4]. За допомогою Splunk можна визначити неправильне використання дозволів, аномальну поведінку навіть у разі використання законних облікових записів, рівнів доступу або джерел. Наприклад, надмірно тривалі сеанси, нестандартний час або вхід. А дані, що накопичуються, про різні дії користувача дозволяють засновувати дослідження на історичних даних. У платформі можлива інтеграція з Active Directory або базами даних HR для отримання інформації про співробітників. Splunk дозволяє аналізувати інциденти для визначення обставин та масштабів інциденту. Це досягається за допомогою пошуку та знаходження кореляцій за ключовими словами, термінами або значеннями для різних мережевих пристроїв, хостів, зчитувачів і т.д. Для аналітиків безпеки це дає широкий контекст інциденту, що допомагає швидше та краще оцінювати рівень загрози, визначати причини та наслідки.

Також архітектури безпеки зазвичай включають різні рівні інструментів і продуктів. Як правило, вони не призначені для спільної роботи та

містять прогалини у питаннях роботи фахівців з безпеки щодо встановлення зв'язків між різними доменами. Splunk усуває ці прогалини, забезпечуючи єдиний інтерфейс для автоматичного вилучення даних, що дозволяє будувати комплексну аналітику та реагувати на погрози серед продуктів різних постачальників.

Основним прикладом готових рішень є Splunk Enterprise Security (ES) [5] — система управління інформаційною безпекою та подіями (англ. Security and information event management, SIEM), яка формує докладну картину машинних даних, що створюються різними технологіями безпеки (мережа, кінцеві точки, доступ, шкідливі програми, вразливість). Завдяки Splunk Enterprise Security фахівці з безпеки можуть швидко виявляти внутрішні та зовнішні атаки та вживати заходів у відповідь. Це дозволяє спростити операції із захисту від загроз, мінімізувати ризик та забезпечити безпеку бізнесу. Splunk Enterprise Security оптимізує всі аспекти захисту та підходить для організацій будь-якого масштабу та професійного рівня. Організації по всьому світу використовують Splunk Enterprise Security (ES) як SIEM для моніторингу безпеки, розширеного виявлення загроз, реагування на інциденти та використання широкого спектру аналітичних програм для аналізу безпеки.

Висновок: незалежно від того, у якій галузі функціонує підприємство, воно створює величезну кількість даних , що генеруються веб-сайтами, додатками, серверами, мережевими та мобільними пристроями. Це одна з найбільш швидко зростаючих і складних частин великих даних. Програмне забезпечення Splunk перетворює зібрану інформацію у цінні дані в режимі реального часу. Ці відомості поглиблюють розуміння клієнта, покращують рівень обслуговування, знижують експлуатаційні витрати та зменшують ризики кібербезпеки.

Література

1. Splunk для аналізу логів [Електронний ресурс] – Режим доступу: https://www.mogroup.com.ua/?p=205, вільний;

2. Splunk [Електронний ресурс] – Режим доступу: https://techexpert.ua/it-products/splunk-platform/, вільний;

3. What's new at Splunk [Електронний ресурс] – Режим доступу: https://www.splunk.com/, вільний;

4. Splunk® [Електронний ресурс] – Режим доступу: https://auditagency.com.ua/splunk/, вільний;

5. Security Information and Event Management (SIEM) with Splunk [Електронний ресурс] – Режим доступу: https://www.cprime.com/resources/blog/security-information-and-event-management-siem-splunk/, вільний.

УДК 004.056.2

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ ПІДПРИЄМСТВА В УМОВАХ ПАНДЕМІЇ

Малькевич Р., Ящук В.
Львівський державний університет безпеки життєдіяльності, Львів

Розглянуто актуальні проблеми забезпечення безпеки інформації підприємства в умовах пандемії, проаналізовано основні тенденції процесу збору, оброблення, перетворення та зберігання конфіденційної інформації. Наведено опис сучасних концепцій віддаленого доступу та Bring your Own Device, та найслабших ланок у ланцюзі безпеки. Запропоновано у межах програми управління інформаційною безпекою проведення моніторингу безпеки, який захищає від порушень даних, зменшуючи витрати на аудит та сприяючи дотриманню внутрішніх і зовнішніх стандартів безпеки та конфіденційності.

Ключові слова: *інформаційна безпека, конфіденційна інформація, моніторинг безпеки, ландшафт кіберзагроз.*

The current problems of information security of the enterprise in a pandemic are considered, the main trends in the process of collecting, processing, converting and storing confidential information are analyzed. Describes modern concepts of remote access and Bring your Own Device, and the weakest links in the security chain. It is proposed within the information security management program to conduct security monitoring, which protects against data breaches, reducing audit costs and promoting compliance with internal and external standards of security and confidentiality.

Key words*: information security, confidential information, security monitoring, cyber threat landscape.*

Сьогодні сучасні підприємства створюють, об'єднують і зберігають великі обсяги інформації про своїх клієнтів, включаючи поведінкову аналітику, дані про використання, особисту інформацію, дані про кредитні картки та платежі, інформацію про медичне обслуговування та багато іншого. Збільшення обсягів збору корпоративних даних за останнє десятиліття разом із зростанням загрози кібератак і злому даних призвело до значних змін у сфері управління інформаційною безпекою для IT-організацій.

Управління інформаційною безпекою описує набір політик і процедурних засобів контролю, які впроваджують в IT та бізнесі для захисту своїх інформаційних активів від загроз та вразливостей. Відповідальність за інформаційну безпеку може бути покладена на начальника відділу безпеки, головного технічного директора або менеджера з IT-операцій, до команди якого входять IT-оператори та аналітики безпеки. Більшість організацій розробляють офіційний документований процес для управління InfoSec, який називають системою управління інформаційною безпекою або СУІБ.

У випадку, коли підприємство не збирає ідентифікаційну або особисту інформацію від клієнтів, виникає питанням, чи потрібно приймати процеси управління інформаційною безпекою для захисту даних. Всі організації володіють інформацією, яку вони не хотіли б поширювати або оприлюднювати. Незалежно від того, чи зберігаються ці дані в цифровому чи фізичному форматі. Управління інформаційною безпекою має вирішальне значення для захисту даних від несанкціонованого доступу або крадіжки.

Інформаційна безпека на організаційному рівні зосереджена навколо тріади ЦРУ: конфіденційність, цілісність та доступність. Для забезпечення конфіденційності, цілісності та доступності захищеної інформації введені засоби контролю інформаційної безпеки. Фахівці InfoSec та команди SecOps повинні розуміти кожен нещодавно впроваджений контроль з точки зору того, як він сприяє тріаді CIA для захищеного класу даних [1,2].

Збереження конфіденційності інформації означає забезпечення того, що лише уповноважені особи можуть отримати доступ до даних або змінити їх. Щоб дані вважалися захищеними, IT-організація повинна переконатися, що вони належним чином зберігаються і не можуть бути змінені чи видалені без відповідних дозволів. Процеси і процедури, які забезпечують доступність важливої інформації авторизованим користувачам у разі потреби.

Для деяких підприємств управління інформаційною безпекою є більш ніж вимогою захисту конфіденційних внутрішніх документів та інформації про клієнтів. Залежно від галузі управління інформаційною безпекою існують юридичні вимоги для захисту конфіденційної інформації, яка надходить від клієнтів.

Підприємства, які збирають персоналізовані медичні записи або записи про медичне обслуговування, зобов'язані дотримуватися вказівок щодо конфіденційності та безпеки даних щодо перенесення та підзвітність медичного страхування. Організації, які обробляють платежі кредитними картками, несуть відповідальність за відповідність стандарту безпеки даних індустрії платіжних карток. Організації, які збирають персоналізовану інформацію від клієнтів, підпадають під загальний регламент про захист даних і можуть отримати тисячі або мільйони доларів штрафу за їх недотримання.

У період пандемії число віддалених працівників зростає в геометричній прогресії. Аналізуючи ландшафт кіберзагроз, виникає питання впливу домашніх пристроїв користувачів на загальну безпеку. В такій ситуації актуальними є два сценарія, таких як віддалений доступ і Bring your Own Device (BYOD). За даними Gallup [4], 43% зайнятих американців вже працюють віддалено, а це означає, що вони використовують свою власну інфраструктуру для доступу до ресурсів компаній. Посилює цю проблему зростання числа компаній, які дозволяють концепцію BYOD на робочому місці. Хоча існують способи безпечного впровадження BYOD, але біль-

шість збоїв в сценарії BYOD зазвичай відбувається через погане планування і мережну архітектуру, які призводять до небезпечної реалізації.

Спільного між усіма технологіями, згаданими вище є те, що керувати ними, потрібен користувач, і він як і раніше є головною метою для атаки. Люди - найслабша ланка в ланцюзі безпеки. З цієї причини старі загрози, такі як фішингові електронні листи, продовжують рости в обсязі, оскільки вони зачіпають психологічні аспекти користувача, спонукаючи його клікнути що-небудь, наприклад, додаток файлу або шкідливе посилання. Зазвичай, коли користувач виконує одну з цих дій, його пристрій заражається шкідливим ПЗ або до нього віддалено отримує доступ хакер.

Головним напрямом у процесі забезпечення інформаційної безпеки підприємства являється дотримання у таємниці комерційної інформації, що дозволяє підприємству успішно залишатися конкурентоспроможним на ринку товарів та послуг. Наслідком недотримання цих вимог стають проблеми у ділових справах; зриви переговорів з конкурентами, втрата вигідних контрактів; невиконання договірних зобов'язань тощо.

Для розв’язання проблем інформаційної безпеки підприємства необхідно створити підрозділ інформаційної безпеки, який входить до складу служби економічної безпеки підприємства. Цей підрозділ повинен підпорядковуватись вищому керівництву.

Отже, ефективний моніторинг безпеки та реагування є важливими аспектами програми управління інформаційною безпекою. Платформа хмарної аналітики дозволяє IT-організаціям легко збирати найновіші дані про загрози, налаштовувати сповіщення про загрози в реальному часі та автоматизувати реагування на інциденти у гібридних середовищах із розрізненими даними. Також моніторинг безпеки захищає від порушень даних, одночасно зменшуючи витрати на аудит і сприяючи дотриманню внутрішніх і зовнішніх стандартів безпеки та конфіденційності.

Література

1. Управління інформаційною безпекою [Електронний ресурс] – Режим доступу: https://studfile.net/preview/9650065/.

2. Система управління інформаційною безпекою як ключовий чинник успішності організації [Електронний ресурс] – Режим доступу: https://ua.ikmj.com/isms/.

3. Управління інформаційною безпекою підприємства для утримання конкурентних позицій на ринку [Електронний ресурс] – Режим доступу: https://valtek.com.ua/ua/system-integration/security-control-system/integrated-security-systems/information-security-system-review.

4. Система Управління інформаційною безпекою [Електронний ресурс] – Режим доступу: https://core.ac.uk/download/pdf/48401951.pdf.

УДК 004.056

АНАЛІЗ ЗАХИЩЕНОСТІ ВЕБ-РЕСУРСІВ. ПРИНЦИПИ АУДИТУ ТА СТАНДАРТИ У СФЕРІ ІБ

Малькевич Р., Нагірняк Д., Навитка М.
Львівський державний університет безпеки життєдіяльності

Значний внесок у комплексну безпеку Web-проекту вносять такі складові забезпечення інформаційної безпеки, як захищеність інформаційного середовища Web-сервера і засоби захисту комп'ютерів, що входять до складу КІС компанії, що управляє сайтом.

В даній статті проведено аналіз захищеності веб-ресурсів, принципи аудиту та стандартів у сфері ІБ. Представлено доцільність архітектури безпечного Web-додатку, яку використовують сучасні компанії:

Ключові слова: *web-додатки, web-сервери, web-проекти, захист, CMS-системи, аудит, ІБ.*

Significant contribution to the overall security of the Web-project is made by such components of information security as security of the information environment of the Web-server and means of protection of computers, which are part of the CIS of the company that manages the site.

This article analyzes the security of web resources, audit principles and standards in the field of IS. The expediency of the architecture of a secure Web-application used by modern companies is presented:

Keywords: *web-applications, web-servers, web-projects, protection, CMS-systems, audit, IS.*

Принципи проведення аудиту є передумовою результативної і надійної підтримки політики керівництва та контролю. Вони забезпечують менеджмент організації інформацією, на основі якої реалізуються цілі, спрямовані на удосконалення характеристик бізнес-діяльності, а також є основою для об'єктивних висновків аудиту. Необхідність проведення регулярного аудиту інформаційної безпеки полягає в оцінці реального стану захищеності ресурсів ІТС та її змозі протистояти зовнішнім і внутрішнім загрозам інформаційної безпеки, які постійно змінюються та адаптуються.

Аудит інформаційної безпеки – це системний процес одержання об’єктивних якісних і кількісних оцінок поточного стану безпеки інформаційної системи, комплексна оцінка рівня інформаційної безпеки клієнта з урахуванням трьох основних факторів: персоналу, процесів і технологій. До принципів проведення аудиту відносять:

а) етичність поведінки – основа професіоналізму.

б) неупередженість – зобов'язання надавати правдиві і точні звіти.

в) професійна обережність – старанність і вміння приймати правильні рішення при проведенні аудиту.

г) незалежність – основа неупередженості та об'єктивності висновків аудиту.

д) підхід, заснований на свідченнях, фактах, даних – це основа для досягнення надійних і відтворювальних висновків аудиту.

Дані аудиту є вибірковими, оскільки аудит здійснюється в обмежений період часу і обмеженими ресурсами. Відповідно використання вибірок тісно пов'язане з довірою, з якою ставляться до висновків, отриманими за результатами аудиту. Під даними аудиту розуміють записи, виклад фактів або іншу інформацію, які стосуються критеріїв аудиту і можуть бути перевірені.

У зв'язку з тим, що існує безліч стандартів у сфері ІБ, організації нерідко стикаються з проблемою вибору найбільш для них придатного. Розглянемо деякі з відомих стандартів:

- CobiT є стандартом корпоративного управління IT, розроблений ISACA. Він адресований фахівцям в області IT, керівництву та аудиторам.

- ITIL – інструмент, який може застосовуватися для удосконалення системи ІБ, є бібліотека інфраструктури інформаційних технологій (англ. Information Technology Infrastructure Library, ITIL).

- ISO/IEC 15408 - ще одним широко обговорюваним стандартом у галузі безпеки є стандарт ISO/IEC 15408 (Загальні критерії). Цей стандарт технічний і іноді важкий для сприйняття бізнесом. Він корисний для постачальників і покупців продукції ІБ.

Отже, перед виконанням роботи по перевірці безпеки не варто переживати, що необхідно буде виконувати додаткові дії, наприклад, відредагувати конфігурації сервера, передати доступи або первинні коди. Головна мета – визначити реальний рівень захисту сторінки. Забезпечення належного рівня інформаційної безпеки ресурсу можливо за умови проведення регулярних аудитів. Документування проведених перевірок, що є невід'ємною частиною будь-якого аудиту, бо це не тільки підтвердження факту виконання аудиту, а й можливість удосконалити систему управління інформаційною безпекою в цілому.

Література

1. Засоби і методи захисту інформації [Електронний ресурс]. – Режим доступу: http://kiev-security.org.ua

2. Чубарук Т. Проблеми законодавчого забезпечення інформаційної безпеки в Україні//Право України. — 2007. — № 9 – С. 67 — 69

3. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: навчальний посібник. Рекомендовано МОН України для вищих юридичних навчальних закладів. – К.: Кондор, 2004. – 384 с.

УДК 004.738

БЕЗПЕКА БЕЗДРОТОВИХ МЕРЕЖ РОЗУМНОГО БУДИНКУ

Махно Ю., Пташник В.
Львівський національний аграрний університет, Львів

Анотація. Проведено огляд загроз інформаційній безпеці розумного будинку. В роботі також проаналізовано основні протоколи зв'язку і рівні їх надійності. Основну увагу сконцентровано на самих протоколах, зокрема: Z-Wave, ZigBee, Wi-Fi, Thread. Проведений аналіз цих протоколів та порівняння їх надійності, безпеки та вибір кращого варіанту на даний момент.

Ключові слова: *розумний будинок, Z-Wave, ZigBee, Wi-Fi, Thread.*

Summary. A review of threats to the information security of a smart home has been performed. The main protection protocols and their levels of reliability were also analyzed. Most of the attention was focused on the protection protocols themselves, such as: Z-Wave, ZigBee, Wi-Fi, Thread, Bluetooth. The analysis of these protocols and comparison of their reliability, security and selection of the best option at the moment.

Key words: *"smart home", Z-Wave, ZigBee, Wi-Fi, Thread.*

Уперше термін «розумний будинок» було використано Американською асоціацією забудовників (American Association of House Builders) у 1984 році, яка відзначила, що таке помешкання відмінне від звичайного здатністю забезпечувати продуктивне та ефективне використання робочого та житлового простору. Розумні технології спрощують обслуговування будинку, зменшують видатки на його утримання, значно підвищують комфорт та безпеку житла. Окремої уваги заслуговують технології розумного будинку зосереджені на безпеці, наприклад, інтегрована система розумного спостереження, пожежна сигналізація і навіть аквасторож. Однак підвищуючи безпеку багатьох побутових процесів розумний будинок, як і інші автоматизовані інформаційні системи, потребує надійного захисту від несанкціонованого зовнішнього втручання.

Невід'ємним етапом аналізу інформаційної безпеки розумного будинку є вивчення характеристик та вибір протоколів зв'язку. Бездротові рішення можуть використовуватись для організації бездротового зв'язку за допомогою призначених для користувача протоколів передавання даних, або для реалізації рішень, що використовують стандартні мережеві стеки комунікації на основі специфікації IEEE 802.15.4 або рішень фірм-виробників компонентів для бездротових систем. Стандарт IEEE8 02.15.4 є основою для таких додатків, як ZigBee RF4CE, що підтримують профіль дистанційного керування (ZRC) або профіль пристроїв введення (ZID). Широке поширення отримали ZigBee PRO-сумісні бездротові мережі, такі як мережі автоматизації приміщень (ZHA), автоматизації будівель (ZBA), управління освітленням (ZLL) або інтелектуального розподілу електроенергії (ZSE). Стандарт IEEE 802.15.4 ZigBee погано захищений від перешкод великої та середньої потужності створених іншими пристроями. Одноканальна структура ZigBee далеко

не завжди може ефективно боротися з завадами, які часто зустрічаються в перевантаженій смузі 2,4 ГГц, яка спільно використовується протоколом з такими технологіями як Wi-Fi або Bluetooth. Протокол Bluetooth також використовує частотний діапазон 2,4 ГГц. На відміну від ZigBee Bluetooth підтримує певний інструментарій для протидії завадам, однак його ефективність значно залежить від інтенсивності перешкод та кількості під'єднаних пристроїв. Ще одним недоліком використання неліцензованого частотного діапазону у 2,4 ГГц є значне поглинання сигналу.

В результаті аналізу технологій побудови розумного будинку обґрунтовано доцільність використання безпровідних технологій та встановлено, що для обміну даними в таких системах надаються неліцензовані радіочастотні діапазони, які можуть використовуватися без оформлення спеціального дозволу і абсолютно безкоштовно за умови дотримання вимог щодо ширини смуги та випромінюваної потужності. Обґрунтовано важливість вибору частоти передавання даних при проектуванні системи розумного будинку та актуальність розробки адаптивного методу вибору каналів зв'язку з метою формування переліку пріоритетних вільних частот для обміну інформацією між модулями розумного будинку.

УДК 331.108.2:65.012.8

ЗАСТОСУВАННЯ КАДРОВИХ ТЕХНОЛОГІЙ У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Мужанова Т., Мосійчук В.
Державний університет телекомунікацій, м. Київ

Анотація. *Розглянуто сутність поняття «кадрові технології» та представлено перелік найбільш поширених видів зазначених технологій. Встановлено, що застосування технологій управління персоналом у сфері інформаційної безпеки має свої особливості. На основі вивчення традиційних підходів до управління персоналом та врахування його специфіки у сфері інформаційної безпеки запропоновано схему застосування кадрових технологій для мінімізації та/або нейтралізації ризиків інформаційній безпеці, пов'язаних з персоналом.*

Ключові слова: *забезпечення інформаційної безпеки підприємства, управління персоналом, кадрові технології у забезпеченні інформаційної безпеки підприємства.*

Abstract. *The essence of the concept of «personnel technologies» is considered and the list of the most widespread types of the specified technologies is presented. It is established that the application of personnel management technologies in the field of information security has its own peculiarities. Based on the study of traditional approaches to personnel management and taking into account its specifics in the field of information security, a scheme of application of personnel technologies to minimize and / or neutralize information security risks associated with personnel is proposed.*

Keywords: *information security of the enterprise, personnel management, personnel technologies in ensuring the enterprise information security.*

Статистика інцидентів інформаційної безпеки свідчить про потужний вплив «людського» чинника на стан захищеності інформаційного середовища підприємства. Сьогодні саме персонал найчастіше є джерелом порушень інформаційної безпеки, які є наслідком непрофесійності, халатності або навмисних злих намірів безвідповідальних або невдоволених працівників. З огляду на зростання числа внутрішніх загроз інформаційній безпеці сучасне підприємство має приділяти велику увагу роботі з персоналом шляхом використання різноманітних управлінських технологій.

Під кадровою технологією (технологією управління персоналом) розумітимемо набір операцій і процедур впливу на персонал підприємства, які дозволяють забезпечити укомплектування необхідною кількістю працівників з очікуваними професійними й особистісними характеристиками, досягти оптимальної продуктивності праці і, в кінцевому рахунку, гарантувати ефективне функціонування бізнесу.

Відповідно до положень теорії управління персоналом [1, 2] можна виділити такі види кадрових технологій:

– визначення потреби в кадрах, формування їх кількісного та якісного складу;

– розробка кадрової політики;

– забезпечення адаптації працівників;

– оплата і стимулювання праці, формування матеріальної та моральної зацікавленості працівників;

– сприяння розвитку кадрів (підготовка та перепідготовка, планування кар'єри);

– створення системи загального та професійного навчання персоналу;

– оцінка діяльності та атестація кадрів, орієнтація на заохочення та просування працівників за результатами праці та цінності працівника для підприємства;

– забезпечення сприятливих умов для гармонійних міжособистісних відносин між працівниками, адміністрацією та громадськістю підприємства.

Зазначений перелік не є вичерпним і представлений у науковій літературі в різних варіантах.

Однак, застосування технологій управління персоналом у сфері інформаційної безпеки має свої особливості. З огляду на високу ціну пошкодження, втрати чи витоку конфіденційної інформації управління персоналом має допомагати у виконанні переліку таких важливих завдань із забезпечення інформаційної безпеки. Для зменшення ризиків нанесення шкоди інформаційним активам підприємства з боку персоналу особливого зна-

чення набувають: формування стабільного трудового колективу і подолання плинності кадрів; посилений контроль і ускладнена процедура оцінювання персоналу перед працевлаштуванням та під час роботи; встановлення персональної відповідальності й чіткий розподіл обов'язків із захисту інформації; нормативне закріплення вимог та обмежень щодо нерозголошення інформації; формування ефективної системи мотивування персоналу, формування лояльного, відданого колективу тощо [3, 4].

На основі вивчення традиційних підходів до управління персоналом та врахування його специфіки у сфері інформаційної безпеки запропоновано схему застосування кадрових технологій для мінімізації та/або нейтралізації ризиків інформаційній безпеці, пов’язаних з персоналом (Рис.1).

Рис.1. Схема застосування кадрових технологій у забезпеченні інформаційної безпеки

Таким чином, основні технології управління персоналом, які використовують як засоби забезпечення інформаційної безпеки підприємства, можна умовно поділити на два блоки: перший блок включає кадрові технології, які забезпечують формування кваліфікованого і відповідального персоналу через переважно (але не виключно) використання адміністративних засобів впливу; другий – технології формування лояльного і надійного персоналу, реалізація яких частіше здійснюється економічними та психологічними методами.

Література

1. Богатырева О.Н., Бармина Е.Ю. Кадровые технологии в системе управления персоналом: учебное пособие. СПбГТУРП. СПб., 2013. 46 с.
2. Управління персоналом : навч. посібник / Ожиганова М.І. та ін. В. : ВНТУ, 2014. 188 с.
3. Маркіна І.А., Дячков Д.В. Основи формування системи менеджменту інформаційної безпеки підприємства. Проблеми і перспективи розвитку підприємництва : зб. наук. пр. ХНАДУ. Харків : ХНАДУ, 2016. № 3 (14), Т. 1. С. 80-88.
4. I.Chernysh, V.Makhovka, L.Lobach. Управління інформаційною безпекою підприємства в умовах динамічного бізнес-середовища. Економіка і регіон. Полтава: ПНТУ, 2020. Т. (1(76). С. 106-112.

УДК 659.3

ІНФОРМАЦІЙНІ ВІЙНИ 21 СТОЛІТТЯ

Охват М.
Відокремлений структурний підрозділ «Ірпінський фаховий коледж Національного університету біоресурсів і природокористування України», Ірпінь

***Анотація**: У 21 столітті форма ведення війни, в якій фізична шкода завдається військовим силам та інфраструктурі противника, є лише однією з форм нападу. Натомість держави все частіше проводять нелетальні атаки на інформаційні системи супротивника – це і є зростання інформаційної війни.*

***Ключові слова:** інформаційні війни, інтернет, інформація, електронна війні, кібератаки, психологічні операції.*

***Annotation**: In the 21st century, the form of warfare, in which physical damage is inflicted on the enemy's military forces and infrastructure, is only one form of attack. Instead, states are increasingly carrying out non-lethal attacks on enemy information systems – this is the growth of information warfare.*

***Keywords:** information wars, internet, information, electronic warfare, cyberattacks, psychological operations.*

Західні лідери інвестують мільярди у розвиток можливостей, які можна порівняти з можливостями Китаю та Росії, створюючи військові команди для атак, захисту та використання вразливостей мереж електронних комунікацій. Інформаційна війна поєднує в собі електронну війну, кібервійни та псі-OPS (психологічні операції) в єдину бойову організацію, і це матиме ключове значення для всієї війни у майбутньому.

Сьогодні зв'язок значною мірою спирається на Інтернет або через зв'язок з використанням різних частин електромагнітного спектру (наприклад, радіо або мікрохвиль) через наземні мережі зв'язку або супутникові мережі в космосі. Ми живемо у світі, де все взаємопов'язане, але не потрібно багато часу, щоб поринути у нестабільність чи навіть хаос.

Електронна війна використовується для порушення або нейтралізації цих електромагнітних передач. Це можуть бути засоби електронної протидії та радіоперешкоди, які використовуються для виходу з ладу військового зв'язку або систем наведення зброї. Або він може включати використання в цивільних цілях, наприклад, систему керування повітряним рухом ADS-B, використовувану повітряними суднами для запобігання зіткнень у польоті, або нещодавно прийняту Європейську систему керування залізничним рухом (ERTMS), яка замінює сигналізацію на залізничних коліях та забезпечує повний контроль над поїздами. Заклинювання чи погіршення будь-якого з них викличе хаос.

Ми дізналися про кібератаки, які проводяться через Інтернет проти цифрових мереж, які можуть унеможливити роботу підприємств. Як, видно, з атак на Sony Pictures і TalkTalk, після цього можуть виникнути колосальні збитки за вартістю та репутацією. Обвалення фондової біржі може призвести до величезних фінансових втрат. Кібератаки також можуть бути спрямовані на системи управління виробництвом, що використовуються на виробничих підприємствах або в електроенергетиці, водопостачання та газопостачання. Маючи можливість впливати на таке широке коло об'єктів національної інфраструктури, життя буде поставлене під загрозу.

Психологічні операції спрямовані більше на зниження морального духу та благополуччя громадян країни. Це може включати поширення хибної інформації, чуток і побоювань через соціальні мережі та агенції новин. Високий рівень взаємопов'язаності, який існує сьогодні у населення, є його сильною стороною, але миттєвий взаємозв'язок означає, що дезінформація та страх також можуть швидко поширюватися, що призводить до паніки.

Інформаційна війна, таким чином, є інтеграцією радіоелектронної боротьби, кібервійни та психологічних операцій як для нападу, так і для захисту.

Література

1. Інформаційна війна – зброя масового знищення!. Електронний ресурс. Режим доступу: [https://www.pravda.com.ua/rus/articles/2006/04/20/4399050/]

2. Інформаційні війни: тенденції та шляхи розвитку Георгій Почепцов / Електронний ресурс. Режим доступу: [https://ms.detector.media/manipulyatsii/post/6479/2012-08-12-informatsiyni-viyny-tendentsii-ta-shlyakhy-rozvytku/]

3. Я. Малик. ІНФОРМАЦІЙНА ВІЙНА І УКРАЇНА.

УДК 004.056

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ВИКОРИСТННЯ ХМАРНИХ СХОВИЩ ДЛЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Ориник С., Ящук В.
Львівський державний університет безпеки життєдіяльності, м. Львів

Проаналізовано переваги та розглянуто основні тенденції розвитку та впровадження хмарних сховищ. Окреслено характерні ознаки розвитку технології «хмарних обчислень» та визначено головні переваги та недоліки «хмарних» рішень для українських підприємств. Описано принципи та основні вимоги до хмарних сховищ, як сервісу для зберігання та оброблення інформації користувачів. Запропоновано основні правила щодо забезпечення безпеки користування хмарними технологіями.

Ключові слова: *хмарні технології, хмарні сервіси, забезпечення безпеки, інтернет-технології.*

The advantages are analyzed and the main tendencies of development and introduction of cloud storage are considered. The characteristic features of the development of "cloud computing" technology are outlined and the main advantages and disadvantages of "cloud" solutions for Ukrainian enterprises are identified. The principles and basic requirements for cloud storage as a service for storing and processing user information are described. The basic rules for ensuring the safety of using cloud technologies are proposed.

Keywords: *cloud technologies, cloud services, security, Internet technologies.*

Створення нового покоління центрів обробки даних, в яких архітектурна концепція дозволяє зменшити витрати на обчислювальні потужності, ресурси зберігання даних і мережеві ресурси можливо досягнути, використавши концепцію «хмарних обчислень». Сьогодні найпопулярнішими хмарними сховищами є Dropbox, Google Drive (Google Диск), Microsoft OneDrive та ICloud для користувачів технікою Apple. Існують також інші, маловідомі, хмарні сховища даних, та технологія роботи у них приблизно однакова. Важливим питанням є захищеність даних Dropbox, Google Диска чи Microsoft OneDrive, а доступ до них простий та зрозумілий.

Хмарні сховища сьогодні - це зручний сервіс для зберігання та оброблення будь-якої інформації користувачів, що тісно інтегровані в настільні ПК і мобільні операційні системи на смартфонах. На сьогоднішній день активно використовуються захищені браузери для підключення до хмарних технологій. Щодня здійснюється синхронізація з хмарою і зберігається в ній велика кількість фотографій, відео, документів, музики та навіть паролі, збережені в інших сервісах. Розвиток інтернет-технологій позбавив необхідності використання зовнішніх носіїв для збереження великого обсягу даних або обміну файлами. Тепер ці функції делеговані хмарним сховищам.

Принцип роботи будь-якого «хмарного» сховища такий: на персональний комп'ютер або ноутбук ставиться програма-клієнт «хмарного» сховища, прописується шлях до папок розташованим на жорсткому диску, які планується помістити в «хмару». 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.

При зміні файла, що зберігається в «хмарі», програма внесе правки в копії файлів на комп'ютері. Такий підхід дозволяє мати актуальний набір файлів на будь-якому з пристроїв (смартфоні, комп'ютері, планшеті тощо). Єдина умова, яку потрібно забезпечити для безперебійної роботи сховища з файлами комп'ютера - повна синхронізація. При включенні ПК потрібно дочекатися, поки пройде синхронізація даних. Швидкість здійснення даного процесу багато в чому залежить від швидкості з'єднання з інтернетом. Якщо вимкнути пристрій передчасно, можлива помилка синхронізації даних хмарного сховища.

Володіти доступом до усіх даних з будь-якої точки планети та з будь-якого доступного пристрою є великою перевагою. Але це також відкриває великі можливості для тих, хто так само може отримати файли — для кіберзлочинців.

Наведемо основні правила щодо забезпечення безпеки користування хмарними технологіями:

1. Слід використовувати надійні паролі та двофакторну (чи багатофакторну) аутентифікацію. Обирати довгі й унікальні паролі, які важко відгадати та користуватись менеджером (генерація, зберігання і управління).

2. Перевірка файлів та загальних папок. Сервіси хмарного зберігання підходять для обміну файлами з іншими людьми — від членів сім'ї до колег по роботі, але вони можуть залишити дані відкритими для несанкціонованого доступу. Якщо хтось знайде ці посилання, то зможе отримати доступ до облікового запису людини, з якою ви поділились цими файлами.

3. Необхідно очистити "вже видалені" файли. Багато хмарних сервісів зберігання використовують так звану корзину, зберігаючи протягом певного часу видалені файли на випадок, якщо виникне потреба їх відновити. Необхідно впевнитися, що важливі конфіденційні файли будуть цілком знищені та ніхто більше не зможе їх відновити.

4. Перевіряйте підключені додатки та облікові записи. Навіть, якщо хакери не зможуть увійти у облікові записи звичними способами, вони можуть спробувати отримати доступ "через бокове вікно з двору" — наприклад, з допомогою іншого облікового запису, що підключений до вашого поточного хмарного сховища.

5. Увімкніть сповіщення та повідомлення про дії в акаунті. Більшість хмарних сервісів зберігання даних можуть відправляти вам сповіщення про різні події в обліковому записі, такі як нові входи, зміни в файлах та доступі до них. Тому важливо переконатися, що ці сповіщення увімкнені.

6. Необхідно деактивувати старі пристрої, на яких все ще є доступ до акаунту. Більшість хмарних сервісів зберігання дозволяють синхронізувати файли з декількома пристроями, тому, якщо оновлюєте (або купуєте новий) телефон чи користуєтесь новим ноутбуком, важливо правильно вимкнути та деактивувати старі пристрої.

7. Виходити з облікових записів, якщо не працюєте в них. Для зручності ми не виходимо з облікових записів хмарного сховища навіть коли не працюємо в них. Проте, коли ми закінчуємо в них працювати, важливо вийти з системи, щоб ніхто інший не отримав доступу до ваших файлів.

8. Захистити свої пристрої так добре, як і акаунти. Фізична безпека також важлива. Тримайте телефони, ноутбуки та інші пристрої, на яких користуєтеся обліковими записами хмарних сховищ, захищеними від стороннього доступу.

Хмарне сховище даних - це віртуальний носій інформації, який зберігає і обробляє дані на численних серверах, розкиданих у всесвітній павутині. Причин для розміщення даних в хмарі може бути досить багато, і для різних користувачів вони можуть мати різний пріоритет. Наприклад, для приватних осіб важливіша буде можливість доступу до даних з різних місць інтернету і з різних пристроїв, а для корпоративних користувачів більш істотними можуть виявитися надійність і вартість зберігання.

Література

1. Безпека хмарних сховищ і технологій. Основні правила. 25 August 2020 [Електронний ресурс] – Режим доступу:https: //datami.ua/bezpeka-hmarnih-shovishh-i-tehnologij-osnovni-pravila/https://datami.ua/bezpeka-hmarnih-shovishh-i-tehnologij-osnovni-pravila/.

2. Як забезпечити захист інформації та інформаційну безпеку конфіденційних даних, використовуючи хмарні технології [Електронний ресурс] – Режим доступу: http://www.dut.edu.ua/ua/news-1-569-9733-yak-zabezpechiti-zahist-informacii-ta-informaciynu-bezpeku-konfidenciynih-danih-vikoristovuyuchi-hmarni-tehnologii_kafedra-cistem-tehnichnogo-zahistu-informacii

3. Ящук В. І. Тренди використання технології «хмарних обчислень» в ІТ-сфері України / В. І. Ящук // Торгівля, комерція, підприємництво : збірник наукових праць / [редакц. кол.: Апопій В. В., Дайновський Ю. А., Скибінський С. В. та ін.]. – Львів : Львівська комерційна академія, 2012. – Вип. 14. – С. 104-108.

4. Що таке хмарні сховища та як вони працюють 10 Вересня, 2021 [Електронний ресурс] – Режим доступу:https: https://info.nic.ua/uk/blog-uk/cloudstorage-2/

5. Хмарні сховища [Електронний ресурс] – Режим доступу: https://sites.google.com/site/karnasiyk1course/home/hmarni-shovisa.

6. Хмарне зберігання даних. 7 квітня 2020 [Електронний ресурс] – Режим доступу: https://compbest.com.ua/ua/oblachnoe-khranenie-dannykh/.

УДК 004.056

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ IT – ПРОЕКТІВ З ВИКОРИСТАННЯМ МЕТОДИКИ DEVSECOPS

Смик Д., Ящук В.
Львівський державний університет безпеки життєдіяльності, Львів

Розглянуто методологію систематизації існуючих засобів захисту програмного забезпечення, що забезпечують взаємодію команди розробників та фахівців із захисту інформації в межах одного життєвого циклу розробки. Проведено класифікаціюпідходів до побудови процесів DevSecOps, проаналізовано необхідні складники для побудови DevSecOps процесів. Проведений аналіз дозволяє класифікувати процес розробленнята захисту програмного забезпечення за допомогою методології DevSecOps.

Ключові слова: *IT – проект, інформаційна безпека, DevOps, DevSecOps.*

The methodology of systematization of the existing means of protection of the software providing interaction of a team of developers and experts on protection of the information within one life cycle of development is considered. The classification of approaches to building DevSecOps processes is carried out, the necessary components for building DevSecOps processes are analyzed. The analysis allows us to classify the process of software development and protection using the DevSecOps methodology.Key words: IT project, information security, DevOps, DevSecOps.

Методологія розробленнята захисту програмного забезпечення в межах DevSecOps змінила підхід до забезпечення безпеки з реактивного на проактивний, а також підкреслює важливість забезпечення безпеки на всіх рівнях організації. DevSecOps означає забезпечення безпеки в розробленні додатків від ранніх етапів до самого завершення, а також включає в себе автоматизацію деяких шлюзів безпеки, щоб запобігти уповільненню робочого процесу DevOps. Необхідно підтримувати короткі і часто повторювані цикли розробки програмного продукту, а також інтегрувати заходи безпеки. Вибір правильних інструментів для безперервної інтеграції безпеки може допомогти в досягненні цих цілей.

Сучасні інструменти автоматизації допомогли підприємствам впровадити більш гнучкі методи розробки, а також відіграли важливу роль у розробленні нових заходів безпеки. Для ефективного захисту DevOps потрібні не тільки нові інструменти, а й зміни на підприємстві процесів DevOps, дляпришвидшення інтегрування роботи груп фахівців з безпеки з іншими спеціалістами, що призведе до покращення якості продукту.

DevSecOps – одна з найважливіших тенденцій DevOps. Це підхід до безпеки операцій, що дозволяє використовувати принципи і кращі практики DevOps для забезпечення кращої, швидкості більш безпечної доставки програмного забезпечення. По суті, це означає, що всі вимоги безпеки з самого початку кодифіковані, а контроль безпеки і розробка здійснюються паралельно, причому безпеку намагаються впровадити в кожну частину процесу agile-розробки. Завдяки цьому DevSecOps може знизити витрати пов'язані з виправленням недоліків безпеки [1].

DevSecOps – це вбудована безпека, а не безпека, яка функціонує як периметр навколо програм та даних. Якщо безпека залишається в кінці конвеєра розробки, організації, що застосовують DevOps, можуть повернутися до довгих циклів розробки, яких вони намагалися уникати в першу чергу.

Зазвичай, методики для оптимізації процесів розроблення програмного забезпечення націлені виключно на підвищення ефективності всередині команди, але в DevSecOps мова йде про застосування автоматизованих інструментів для гарантування комплексного захисту. Варто зазначити, що кожна з доступних методик стрімко прискорює роботу, жертвуючи при цьому безпекою інфраструктури. Більшість компаній може бути не готова до такого стрибка підвищення вимог якості в даній сфері. Саме тому, подальший розвиток DevOps порушив питання інформаційної безпеки. Прискорення роботи команд-розробників створило безперервний потік оновлюваних функцій, а також постійний потік даних з боку сервісів, користувачів та інших додатків [2]. Розгортання коду має відбуватися частіше і завершуватися за менший час. Коротший час циклу є ознакою оптимізованих процесів, в той час як більш тривалий час може бути ознакою того, що необхідно переглянути свої кращі практики або інструменти кодування.

Стратегією DevSecOps є визначення толерантності до ризиків та проведення аналізу ризику. Автоматизація повторюваних завдань є ключовим чинником DevSecOps, оскільки запуск ручних перевірок безпеки в конвеєрі може вимагати багато часу.

DevSecOps дозволяє організації застосовувати попереджуючий підхід до безпеки. Це спонукає розробників програмного забезпечення інтегрувати безпеку в свої повсякденні зусилля. У той же час групи безпеки можуть працювати з розробниками програмного забезпечення, щоб допомогти організації виявити і усунути вразливості безпеки, перш ніж вони вийдуть зпід контролю. DevSecOps змінює безпеку з реактивної на проактивну, а також підкреслює важливість безпеки на всіх рівнях організації, і уповноважує співробітників служби безпеки приймати рішення, які мають позитивний вплив на їхній бізнес.

Таким чином, DevSecOps, як концепція і практика, весь час розвивається, зі збільшенням кількості організацій, які впроваджують DevSecOps як рішення для їх проблеми безпеки [1]. Попит на DevSecOps збільшиться в організаціях всіх розмірів і у всіх галузях. У міру того, як все більше організацій шукають способи виявлення та виправлення проблем безпеки на ранніх етапах процесу розробки програмного забезпечення, попит на інструменти для підтримки DevSecOps відповідно збільшуватиметься.

Підприємство, яке впроваджує інструменти DevSecOps отримує стійку конкурентну перевагу. Надаючи розробникам програмного забезпечення і командам безпеки зручні та ефективні інструменти DevSecOps, підприємство розвиває культуру співпраці, спілкування, прозорості та відкритості. В результаті організація створює середовище, в якій розробники та групи безпеки постійно удосконалюються.

Переваги, які DevSecOps приносить компаніям це – зниження витрат, збільшення швидкості доставки, швидкості відновлення, відповідність в масштабі і пошуку загроз. Сукупний ефект цих переваг – це підвищення ділової репутації та більш плавна бізнес-модель. DevSecOps успішно видалить бар'єри між DevOpsi Security, яка заважають їм працювати як єдине ціле. DevSecOps матиме можливість знаходити і виправляти проблеми безпеки на початку процесу розробки, тим самим значно скорочуючи витрати, пов'язані з їх виявленням і виправленням. Важливо включити гарантування безпеки в життєвий цикл розробки Agile. Завдяки DevSecOps розробники можуть краще зрозуміти критичність уразливостей, які існують у їхньому коді, і виправити ці вразливості, надаючи швидкі, але безпечніші продукти або рішення. Оскільки підхід DevSecOps автоматизований, тому команді розробників більше не потрібно записувати правила безпеки у свій код. DevSecOps знижує ризик перенапруження даних, оптимально застосовуючи ресурси.

Література

1. IT - безпека [Електронний ресурс] Режим доступу до ресурсу: https://astwellsoft.com/uk/blog/software-security.html.

2. Чим займається DevOps – інженер [Електронний ресурс] // Режим доступу до ресурсу: https://vc.ru/hr/51144-kto-takoy-devops-inzhener-i-chem-on-zanimaetsya.

3. Що таке DevSecOps [Електронний ресурс] // Режим доступу до ресурсу: https://itfb.com.ua/chto-takoe-devsecops/.

4. Ящук В. І. Тренди використання технології «хмарних обчислень» в ІТ-сфері України / В. І. Ящук // Торгівля, комерція, підприємництво : збірник наукових праць / [редакц. кол.: Апопій В. В., Дайновський Ю. А., Скибінський С. В. тощо.]. – Львів : Львівська комерційна академія, 2012. – Вип. 14. – С. 104-108.

УДК 004.6

ДОСЛІДЖЕННЯ ОСНОВНИХ ПРОБЛЕМ ПРИ ПОБУДОВІ МОДЕЛЕЙ ЗАХИСТУ ІНФОРМАЦІЇ В КОМП'ЮТЕРНІЙ МЕРЕЖІ ЗАХИЩЕНОЇ ЛАБОРАТОРІЇ

Фарбітник В., Лагун А.
Львівський державний університет безпеки життєдіяльнсті, м. Львів

В роботі розглядаються питання причин захисту інформації, цілей та методів, також розглядаються основні моделі захисту інформації, звертається увага на основні проблеми при побудові моделей на прикладі комп'ютерної мережі захищеної лабораторії.
***Ключові слова**: захист інформації, моделі захисту інформації , основні проблеми при побудові моделей.*

The paper considers the reasons for information security, goals and methods, as well as the main models of information security, draws attention to the main problems in building models on the example of a computer network of a secure laboratory.
***Keywords:** information protection, information protection models, main problems in model building.*

Безпека в Інтернеті та локальних мережах зараз є на першому плані серед проблем, пов'язаних із комп'ютерними мережами [1]. Завдяки еволюції мереж та Інтернету, загрози інформації та мережам різко зросли. Багато з цих загроз дозволяють здійснювати атаки, що спричиняють шкоду або мають наслідком крадіжку. Інформаційні технології продовжують зростати в геометричній прогресії. Особисті, державні та бізнес-критичні програми стають все більш поширеними в Інтернеті. Ці мережеві додатки та послуги можуть становити загрозу безпеці як для приватних осіб, так і для інформаційних ресурсів компаній, різних лабораторій та уряду. У багатьох випадках поспіх з підключенням відбувається за рахунок належної безпеки мережі.

Інформація – це актив, який необхідно захищати [2]. Без належного захисту або мережевої безпеки багато людей, підприємств та урядів ризикують втратити цей актив. Мережева безпека – це процес захисту цифрових інформаційних активів, цілями безпеки є захист конфіденційності, підтримка цілісності та забезпечення доступності.

З огляду на це, актуальність обраної теми дослідження обумовлюється надзвичайною важливістю захисту мережі від загроз та вразливостей, щоб різні підприємства могло реалізувати свій повний потенціал.

Як правило, ці загрози постійні через вразливості, які можуть виникнути через неправильно налаштоване обладнання або програмне забезпечення, погану архітектуру мережі, властиві слабкі сторони технології або

необережність кінцевого користувача. Захищену лабораторію можна вважати малою чи середньою організацією, бо в середньому зазвичай там працює до 500 працівників, незважаючи приватна лабораторія чи державна. За даними «Фінансовий пульс» кількість підприємств малого та середнього бізнесу станом на 01.01.2017 складала 99,9% від загальної кількості підприємств та приносила 55% ВВП. Тому так важливо підвищити обізнаність про обов'язки інформаційної безпеки підприємств цього рівня щодо захисту цінних системних та інформаційних ресурсів для нації.

В умовах глобального розповсюдження комп'ютеризованих інформаційних систем малі організації, подібні до великих, використовують інформаційні системи для автоматизації своїх завдань та розповсюдження своєї продукції та послуг. Цей рух до взаємопов'язаного інформаційного світу підкреслює важливість проведення досліджень інформаційної безпеки та впровадження стратегій безпеки, щоб захистити ці організації від кібератак. Для малих та середніх підприємств надзвичайно важливо захищати усі конфіденційні дані. Крім того, кожен повинен захищати свою інтелектуальну власність, маркетингові дані та цінну інформацію, як-от стратегічні плани, фінансову інформацію та маркетингові звіти, щоб зберегти свою репутацію та зберегти конкурентоспроможність.

Великі організації інвестують в ресурси захисту інформації, включаючи технології, людей, процеси та бюджети, щоб покращити безпеку цінної та конфіденційної інформації. З іншого боку, малі та середні організації не мають таких рівнозначних ресурсів для побудови надійної системи захисту інформації. Тому хакери та кіберзлочинці нещодавно зосередили свої напади на малому та середньому бізнесі, коли виявили, що великі організації важко атакувати та те, що вони мають добре захищену інфраструктуру.

Отже, ми можемо зробити висновок, що Застосування інформаційних технологій (ІТ) вимагає підвищеної уваги до питань інформаційної безпеки. Руйнування інформаційного ресурсу, його тимчасова недоступність або несанкціоноване використання можуть завдати значних матеріальних збитків. Без належної ступеня захисту інформації впровадження ІТ може виявитися економічно невигідним в результаті значних втрат конфіденційних даних, що зберігаються і обробляються в комп'ютерних мережах.

Реалізація рішень, що забезпечують безпеку інформаційних ресурсів, істотно підвищує ефективність всього процесу інформатизації в організації, забезпечуючи цілісність, справжність і конфіденційність дорогої інформації, що циркулює в локальних і глобальної інформаційних середовищах.

Таким чином, лабораторія має на увазі комплексну безперервну систему захисту даних. Відповідно, при розробці та побудові комплексної системи захисту інформації необхідно дотримуватися певних методологічних принципів проведення досліджень, проектування, виробництва, експлуатації та розвитку захищаються ресурсів. Вибір методів захисту – це досить

складна оптимізаційна задача, і при її вирішенні необхідно прораховувати ймовірність виникнення загроз безпеці інформації, вартість реалізації тих чи інших способів захисту та ін. Крім того, система захисту повинна постійно вдосконалюватися разом з розвитком обчислювальної інфраструктури. Проте, основною вразливістю системи захисту лабораторії є люди.

Проблема побудові моделі захисту інформації в комп'ютерній мережі захищеної лабораторії буде вирішена, тільки якщо створена і безвідмовно функціонує комплексна система захисту інформації, що охоплює весь життєвий цикл обчислювальної інфраструктури, починаючи від розробки і до її знищення, а також весь технологічний ланцюжок збору, зберігання і обробки інформації, що захищається.

Література

1. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу // НД ТЗІ 1.1–002–99, ДСТСЗІ СБ України, Київ, 1999.

2. Мирошник М.А. Диагностические эксперименты в системах защиты информации на сетях клеточных автоматов. / М.А. Мирошник, Я.Ю.Королева // Інформаційно-керуючі системи на залізничному транспорті. – 2009. – №4. – С. 142–145.

3. Мирошник М.А. Методы эффективного кодирования внутренних состояний микропрограммных автоматов. / М.А. Мирошник, Я.Ю.Королева, // Технология приборостроения. – 2011. – №1. – С. 12–16.

4. Miroshnik M. Uses of programmable logic integrated circuits for implementations of data encryption standard and its experimental linear cryptanalysis. /Miroshnik M., Kovalenko M. // Інформаційно-керуючі системи на залізничному транспорті. – 2013. – №6, с.36-45.

5. Мирошник М.А. Методы защиты цифровой информации в распределенных компьютерных сетях. Інформаційно-керуючі системи на залізничному транспорті. – 2014. – №5. – с. 66-70.

УДК 004.056.5

INFORMATION SECURITY OF UKRAINE IN THE CONTEXT OF NATIONAL SECURITY

Чубаєвська М., Запотічна Р.
Львівський державний університет внутрішніх справ, Львів

Анотація. *Досліджено проблему інформаційної безпеки України та захисту національного інформаційного простору від негативних пропагандистсько-маніпулятивних інформаційних впливів. Проаналізовано теоретичні підходи до визначення сутності поняття інформаційна безпека. Розглянуто дії щодо вдосконалення державної інформаційної політики та створення ефективної системи інформаційної безпеки України.*

Ключові слова: *інформаційна безпека, інформаційні загрози, інформаційний простір, кіберзлочинність, кіберпростір.*

Abstract. *The problem of information security of Ukraine and protection of the national information space from negative propaganda and manipulative information influences is investigated. Theoretical approaches to defining the essence of the concept of information security are analyzed. Actions to improve the state information policy and creation of an effective information security system of Ukraine are considered.*

Key words: *information security, information threats, information space, cybercrime, cyberspace.*

The paper is aimed at analyzing different requirements to handle information threats, as well as exploring important security measures related to providing information security of Ukraine.

In today's global and regional information confrontation, destructive communicative influences, multi-vector collisions, national information interests, dissemination information expansion and aggression, protection of the national information space and guarantee information security is becoming a priority strategic task of modern states in the system of global information relations. Preservation information sovereignty, the formation of an effective security system in the information field is an urgent problem for Ukraine, which is often the case for external information expansion, manipulative propaganda technology and destructive information invasion [3].

In terms of the Russian-Ukrainian conflict protecting the national information space from negative information-psychological influences, operations and wars, guaranteeing information security and information sovereignty are of particular importance and become a factor in preserving Ukraine's national identity and operating it as a sovereign and an independent state.

There are two aspects of interpreting information security in the context of national security. On the other hand, information security is regarded as an inde-

pendent element of national security of any country, and on the other hand, an integrated component of any other security: military, economic, political, etc. [1, p. 23].

The most complete is the following definition: informational security is a state of vitality interests of the individual, society and the state in which minimizes the risk of damage through incomplete, untimely and unreliable information, negative information impact, negative consequences of information technology functioning [5]. This definition is optimal and reflects all aspects of interaction among subjects of information relations.

Ukraine's information sovereignty means Ukraine's exclusive power under the Constitution of Ukraine, Ukrainian legislation and the rules of international law to individually and independently identify and implement national and geopolitical information interests, domestic and foreign information policy, dispose own information resources, build an infrastructure of the national information space, pave the way for integrating it into a global information space and ensure the national information security.

Information infrastructure means organizational structures and systems in their entirety providing for the functioning and development of the information space, means of information exchange and user access to information resources. Provision of information security means the activity aimed at prevention, timely identification, removal or neutralization of real and potential threats to Ukraine's information security.

Cyber security means security of vital interests of an individual, citizen, society and the state in the cyberspace. Cyberspace means the environment, which emerges due to information (automated), telecommunication and information and telecommunication systems operating based on the unified principles and common rules.

Cybercrime means an act in the cyberspace, which is socially dangerous and punishable under applicable criminal laws of Ukraine [2, p. 45]. The level of information security of the state is largely determined by the level of its information security infrastructure. Unfortunately, as V. Petryk points out, low overall level of information infrastructure of Ukraine contributes to expansion of information services market by foreign companies, which creates favorable conditions for the redistribution of airtime in favor of foreign programs, some of which clog up the Ukrainian information space with their own vision of events, promote lifestyle and traditions, thus destructively affecting society and the state, destroying the moral and ethical fundamentals of the gene pool of the Ukrainian nation.

Insufficient professional, intellectual and creative level domestic producer of information product and services, its uncompetitiveness not only on the world market, but also in Ukraine, leads to the situation, when the Ukrainian audience naturally prefers foreign information programs.

Therefore, the national information space unfortunately, Ukraine is facing significant threats, challenges, which endanger the functioning of the state, its political and economic development, integration into the European and Euro-Atlantic structures. Threats to the national security of Ukraine in information sphere is a set of conditions and factors that threaten the vital interests of the state, society and the individual through possibility of negative information influence on awareness and behavior of citizens as well as on information resources and information technology infrastructure [4].

The National Cybersecurity Strategy is a document that defines strategic objectives and high-level action plans for ensuring the cybersecurity of Ukraine. The main goal of the Strategy is to establish the conditions necessary for ensuring the safe use of cyberspace by individuals, society and the government. To achieve that goal, Ukraine should establish a robust national system of cybersecurity, enhance capabilities across public security and defence sectors and ensure the cybersecurity of the state government information resources and critical information infrastructure.

To conclude, in today's globalized information a society where cyberspace is turning into a field the fight against major threats to information security states (and Ukraine, in particular) are cybercrime, cyberterrorism, cyberwarfare, which imply confronting national interests in Internet usage, computer and Internet technologies to harm the enemy. Most often cyber warfare, cyberterrorism technologies are focused on the sphere of state security and defense and pose a real threat to sovereignty of the state. Further development of the scientific, theoretical, legal and organizational foundations of cybersecurity is one of the most important tasks of Ukrainian science, especially in the context of the path towards Euro-Atlantic integration of Ukraine.

Література

1. Bondarenko V. 2011. Information security of the modern states: conceptual reflections [Electronic resource]. - Access mode: http://www.crime-research.iatp.org.ua/library/strateg.htm

2. Doktryna informatsiinoi bezpeky Ukrainy [Electronic resource]. - Access mode: http://www. zakon3.rada.gov.ua/laws/show/514/2009

3. Zakhyst informatsiinoi bezpeky yak funktsiia derzhavy [Electronic resource]. – Access mode: http://www.mego.info/material/23-zakhystinformatsiinoi-bezpeky-iakfunktsiia-derzhavy

4. Kontseptsiia natsionalnoi bezpeky Ukrainy [Electronic resource]. - Access mode: http://www.w1.c1. rada.gov.ua/pls/zweb2/webproc4_1

5. Kormych B. 2017. Orhanizatsiino-pravovi zasady polityky informatsiinoi bezpeky Ukrainy [Tekst]: monohrafiia. Yurydychna literatura. – 471 s.

УДК 004.6

АНАЛІЗ ЗАГРОЗ ІРОЗРОБЛЕННЯ ЗАХОДІВ ЗАХИСТУ ПОТОКІВ ІНФОРМАЦІЇ У СЕРВЕРНОМУ ЦЕНТРІ

Шевчук В.-Ю., Брич Т.
Львівський державний університет безпеки життєдіяльнсті, м. Львів

В роботі розглядаються вимоги до серверних центрів та протидія можливим атакам на них. Проведено опис структури серверних центрів та їх аналіз загроз.
***Ключові слова**: інформаційна безпека, захист даних,серверні центри.*

The paper considers the requirements for server centers and counteracts possible attacks on them. A description of the structure of server centers and their threat analysis.
***Key words:** information security, data protection, server center.*

Серверний центр – цефізичний об'єкт, який організації використовують для розміщення своїх програм таданих. Дизайн дата центру базується на мережі ресурсів обчислювальних та зберігання даних, які забезпечують доставку спільних програм та даних. Ключові компоненти центру включають в себе маршрутизатори, комутатори, брандмауери, системи зберігання, сервери та контролери доставки додатків.

Сучасні центри обробки даних сильно відрізняються від тих що були нещодавно. Інфраструктура перейшла від традиційних фізичних серверів до віртуальних мереж, які підтримують додатки та робочі навантаження.

У світі ІТ, в основному, дата центри спроектовані для підтримки бізнесдодатків та дій, які включають в себе таке:

– обмін файлами та електронною поштою;

– продуктивність розвитку додактів;

– управління відносинами з клієнтами (CRM – Customer relationship management);

– планування корпоративних ресурсів (ERP – Enterprise resource planning) табазданих;

– підримка bigdata, artificia lintelligence (штучний інтелект) та machine learning

Серверний центр включає в себе маршрутизатори, комутатори, брандмауери, системи зберігання даних, сервери та контролери доставки додатків. Оскільки ці компоненти зберігають та керують критично важливими для бізнесу даними та програмами, безпека центру обробки даних має вирішальне значення при проектуванні дата центру.

Разом вони забезпечують:

Мережеву інфраструктуру. Це пов'язує сервери (фізичні та віртуалізовані), послуги центрів обробки даних, сховище та зовнішнє підключення до місцеположень кінцевих користувачів.

Інфраструктура зберігання. Дані є паливом сучасного центру обробки даних. Системи зберігання використовуються для зберігання важливої інформації.

Обчислювальні ресурси. Додатки – це двигуни центру обробки даних. Ці сервери забезпечують обробку, пам'ять, локальне сховище та мережеві зв'язки, що керують програмами.

Серверний центр – це набагато більше, ніж просто склад для серверів. Сучасний дата центр – це складне мережеве середовище передачі даних, яке пропонує величезні можливості своїм клієнтам, надаючи їм можливість будувати інфраструктуру, необхідну для просування їх бізнесу вперед. Оцінюючи можливості центру обробки даних, важливо виміряти їх за рядом ключових стандартів проектування дата центру, які мають прямий вплив на продуктивність.

Дата центри також мають свої особливості, наприклад:

– велике енергоспоживання;

– охолодження;

– надмірний термін служби серверів;

– безпека.

Оскільки всі засоби масової інформації зосереджені на кібербезпеці, легко забути, що заходи фізичної безпеки настільки ж важливі, коли йдеться про захист ціннихданих та програмних активів. Провідні стандарти проектування центрів обробки даних забезпечують найкращий можливий захист від фізичних порушень даних за допомогою безлічірівнів захисту, щовключають як фізичні, такілогічнізаходи. Відпростихфункційбезпеки, таких як огородження периметра за допомогою камер та датчиків руху, до більшскладнихінструментів, таких як біометричнісканери, добре продуманий дата центр данихможегарантувати, що доступ до активівклієнтівможеотримати лише уповноважений персонал.

Мета цієї роботи полягала в аналізі загроз на серверні центри і представлення їх функцій і можливостей та розроблення методів захисту інформації в серверному центрі та протидія атакам.

Література

1. Центр обробки даних [Електронний ресурс] // Режим доступу до ресурсу: https://www.fortinet.com/ru/solutions/enterprise-midsize-business/data-center-firewall

2. Центр обробки даних [Електронний ресурс] // Режим доступу до ресурсу: https://www.vxchnge.com/blog/data-center-design-standards

3. Кібербезпека [Електронний ресурс] // Режим доступу до ресурсу https://cybericus.com/

УДК 004.056.5

АНАЛІЗ ЗАГРОЗ ПРИ ПРОВЕДЕННІ КІБЕРСПОРТИВНИХ ЗМАГАНЬ

Якименко Ю., Поляков Д.
Державний університет телекомунікацій,

Анотація: *Питання безпекової складової у змаганнях з комп'ютерних ігор ще недостатньо розкрито в науковій літературі. Критично важливим стає питання захисту даних гравців та забезпечення кібербезпеки під час проведення турнірів, вивчення тактики кіберзлочинців. Пропонується створювати інтегровану систему безпеки, яка включає системи: відеоспостереження, контролю і управління доступом, охорони периметра, захисту інформації, інформаційної безпеки.*

Ключові слова*:загрози, кіберспортивні змагання, забезпечення безпеки, інформація, гравці, DDoS-атака.*

Annotation. *The issue of security in computer game competitions is still poorly understood in the scientific literature. The issue of protecting players' data and ensuring cybersecurity during tournaments and studying cybercrime tactics is becoming critical. It is proposed to create an integrated security system, which includes systems: video surveillance, access control and management, perimeter security, information security, information security.*

Key words: *threats, e-sports competitions, security, information, players, DDoS-attack.*

У комплексному забезпеченні інформаційної безпеки при проведенні кіберспортивних змагань значна увага приділяється організаційній роботі з аналізу внутрішніх і зовнішніх загроз конфіденційної інформації та виробленню заходів щодо забезпечення її захисту. У кожному конкретному випадку ці організаційні заходи в роботі при проведенні кіберспортивних змагань носять специфічну форму і зміст, спрямовані на забезпечення безпеки інформації в конкретних умовах.

Кіберспорт є формою змагальної діяльності, в основі якої лежить використання комп'ютерних ігор. Питання безпекової складової у змаганнях з комп'ютерних ігор ще недостатньо розкрито в науковій літературі, що визначає актуальність в проведенні дослідження. Змагання проводяться в спеціальних місцях, де публіка може спостерігати за гравцями, що сидять за комп'ютерами, а хід змагань відстежувати на своїх ноутбуках або великому електронному екрані, де транслюється саме ігровий процес. Змагання можуть також проводитись в комп'ютерних або кіберспортивних клубах, а хід його – наживо транслюватись через Інтернет і інші медіаресурси (аналоги телебачення). Велика кількість електронних пристроїв, які фіксують, обробляють, зберігають та надають до широкого доступу цифрову, друковану та відео інформацію про хід змагань, команди, гравців, тренерів, суддів та ін, змушує звертати увагу на забезпечення безпеки їх функціонування. Масове використання комп'ютерних засобів та інструментів комунікації у кіберспортивних змаганнях завжди буде пов'язано також з наявністю можливих кіберзагроз і виникненням інцидентів інформаційною безпе-

ки. Саме це буде визначати економічні можливості і тенденції успішного розвитку кіберспорту, підіймати його престиж на сучасному етапі.

Автори [1] наводять результати аналізу загроз, спрямованих у вигляді атак на професійних гравців, розробників ігор та організаторів змагань, а також глядачів та відвідувачів кіберспортивних турнірів; даються прогнози щодо подальшого розвитку загроз, націлених на кіберспорт та кіберспортсменів. У зв'язку з цим критично важливим стає питання захисту даних гравців та забезпечення кібербезпеки під час проведення турнірів, вивчення тактики кіберзлочинців та способів організації їм протидії. Основними видами загроз є: блокування профілів за допомогою шифрувальників-здирників з вимогою викупу, крадіжка та перепродаж ігрових облікових записів на кіберзлочинних форумах. В результаті фішингових дій можуть бути захоплені сервери, викрадені облікові записи елітних гравців, а сама гра — скомпрометована або використана для нелегальних угод. Ігрові турніри та власники ігрових сервісів стають мішенню для DDoS-атак, створюючи проблеми організаторам в інфраструктурі кібертурніру. DDoS-атаки можуть викликати серйозні проблеми із запізненням передачі даних, що є критичною проблемою у змаганнях, де за мілісекунди можна визначити виграші та програші. DDoS-атака може завдати репутаційної шкоди проведенню самого турніру. Вона також може бути використана для здирства, коли злочинці вимагають грошей з турнірів, щоб зупинити їх проведення.

На більшості великих кіберспортивних заходів також має місце така загроза, як крадіжка особистих даних гравців, тренерів, суддів. Якщо зловмисник використовує мережеві вразливості комп'ютерної системи для досягнення своїх цілей і коли на заході є тільки одна точка доступу до комп'ютерної мережі, то це ставить під удар проведення кіберспортивного змагання в цілому та його безпеку. Тому важливим аспектом цих замагань є захист від проникнення в систему і забезпечення цілосності інформації, як при підготовці до змагання, так і під час його проведення.

Відповідно до Правил [2,п.15)] створення умов для безпеки під час проведення спортивних змагань з кіберспорту повинно здійснюватися відповідно до законодавства України.

Для комплексного забезпечення інформаційної безпеки при проведенні кіберспортивних змагань пропонується створювати інтегровану систему безпеки, яка включає системи: відеоспостереження, контролю і управління доступом, охорони периметра, захисту інформації, інформаційної безпеки. Склад кожної конкретної системи може змінюватися - доповнюватися новими підсистемами. Це залежить від конкретних завдань, визначених на етапі проектування системи.

Література

1. Trend Micro исследовала угрозы в киберспорте и игровой индустрии. URL: https://www.pcweek.ua/themes/detail.php?ID=159809&sphrase_id=88456.

2. ПРАВИЛА спортивних змагань з кіберспорту (електронного спорту) . URL: https://sport.gov.ua/storage/app/sites/16/Sport/Pravyla_zmagan/2020/pravila-kibersport.pdf.

Секція 2
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 338.47

ПЕСПЕКТИВИ 3D ДРУКУ ДЛЯ РОЗВИТКУ ЛОГІСТИКИ

Базюк В.,Товарянський В.
Львівський державний університет безпеки життєдіяльності, Львів

Окреслено поняття 3D друку та зазначено його актуальність в умовах сьогодення. Наведено приклади застосування тривимірних технологій в галузях промисловості, зокрема в машинобудуванні, архітектурі, легкій промисловості. Відзначено тенденції впровадження 3D технологій для логістики та вантажних перевезень. Відзначено, що особливої уваги заслуговують процеси складування продукції, оптимізувати які можливо з використанням промислових 3D принтерів. Ключові слова: 3D друк, 3D принтер, логістика, сировина, виробництво.

The concept of 3D printing is outlined and its relevance in today's conditions is noted. Examples of the application of three-dimensional technologies in industries, in particular, in mechanical engineering, architecture, and light industry are given. The trends in the introduction of 3D technologies for logistics and freight transportation are noted. It was noted that special attention should be paid to product storage processes, which can be optimized using industrial 3D printers. Key words: 3D printing, 3D printer, logistics, raw materials, production.

Сьогодні актуальним є поняття «3D друк». Такий друк реалізується шляхом використання тривимірних пристроїв. 3D принтер − це спеціальний пристрій для формування тривимірних даних. Цей принтер забезпечує створення певних фізичних об'єктів цифрової 3D моделі. В основі технології 3D друку закладено принцип пошарового створення моделі [1]. 3D принтери застосовуються для швидкого виготовлення прототипів об'єктів і використовуються в різних галузях. Створення моделей дозволяє оцінити функціональність, ергономіку виробу, а також запобігти появі помилок перед початком його серійного або масового виробництва. 3D друк сьогодні застосовується в машинобудуванні, в тому числі – автомобілебудуванні; в архітектурі – для створення макетів будівель чи власне самих будівель; в дизайні та виробництві текстилю.

Сьогодні з'являються гіпотези, що бурхливий розвиток 3D друку і поширення цих технологій в промисловому виробництві, може негативно вплинути на такі галузі, як логістика і транспорт, оскільки в перспективі тривимірні принтери можуть стати доступними для всіх бажаючих. А оскільки продукцію можна буде виробляти чи не в домашніх умовах, відбудеться скорочення обсягів вантажних перевезень для різних видів транспорту. Проте, окресленим думкам передує спростування, яке пояснюється тим, що продукцію все одно доведеться доставляти, а логістичні ланцюги постачання надалі функціонуватимуть.

Якщо охарактеризувати матеріальний потік з огляду виробництва певної продукції, то зазвичай це рух сировини до місць виготовлення цієї продук-

ції. Потім продукція відправляється на великі розподільні центри до споживачів. Отримана на таких центрах продукція розподіляється різними каналами збуту до споживача безпосередньо, чи через магазини і проміжні склади, де може накопичуватися, довго зберігатися і перетворитися на неліквідну. Проте, з врахуванням вище зазначених технологій, можливість виробляти продукт в момент виникнення потреби звільнить від необхідності планування та розвантажить склади [2], на яких скорочуватимуться запаси. І це лише одна з перспектив застосування 3D принтера в складській логістиці. Пору з цим перспективи логістики майбутнього з використанням 3D друку зокрема такі: розвиток технології промислових 3D принтерів дозволить зменшити частку традиційного виробництва і оптимізувати матеріальні потоки; виготовлення виробів зміститься у бік споживача, скорочуючи традиційний ланцюг постачання та розвиваючи логістику сировини; виробництво у визначений момент потреби дозволить не створювати надлишкових запасів; розвиток технології дозволить враховувати індивідуальні особливості споживача. Тому, 3D друк може отримати подальший розвиток в логістиці, проте за умов належної експлуатації промислових 3D принтерів, із врахуванням їх обслуговування.

Література

1. Manners-Bell, J., & Lyon, K. (2012). The implications of 3D printing for the global logistics industry. *Transport Intelligence*, 1−5.

2. Decyk, K., & Wieczorek, A. (2018). Technologia druku 3D jako innowacyjne rozwiązanie w branży transportowej. *Przedsiębiorczość i Zarządzanie*, *19* (5, cz. 3 Zarządzanie logistyczne-wyzwania przyszłości), 389−401.

УДК 004

3D АНІМАЦІЯ У СОЦІАЛЬНІЙ РЕКЛАМІ

Вальчук О.І., Воронцова Д.В.
Національний технічний університет «Харківський політехнічний інститут», Харків

В роботі розглядаються переваги методу 3D моделювання при розробці відео соціальної реклами, як прогрессивного методу привернення уваги до певної проблематики. Реклама не просто закликає до певних дій, а малює ідеальну картинку, в якій ці дії показуються, виступають прикладом для наслідування або, навпаки, засуджуються. Зважаючи на вище сказане, засобами полігонального моделювання розроблено 3D моделі головних персонажів соціального ролику. Отримані 3Доб'єкти та їх концепт планується застосувати у повній 3D сцені майбутнього відео.

The paper considers the advantages of the 3D modeling method in the development of social advertising video as a progressive method of attracting attention to certain issues. Advertising not only calls for certain actions, but paints a perfect picture in which these actions are shown, set an example to follow or, conversely, condemned. Taking into account the above, 3D models of the main characters of the social video have been developed by polygonal modeling. The resulting 3D objects and their concept are planned to be used in the full 3D scene of the future video.

Ключові слова: *мультимедійні технології, 3D моделювання, соціальна реклама, тривимірна графіка, тривимірна мультиплікація.*

Все більшу популярність сьогодні набирає соціальна реклама [3], що має на меті привернути увагу громадськості до певної соціальної проблеми. Реклама не просто закликає до певних дій, а малює ідеальну картинку, в якій ці дії показуються, виступають прикладом для наслідування або, навпаки, засуджуються. Згідно з дослідженням Facebook, анімаційна графіка зазвичай триває від 30 секунд до 3 хвилин, і навіть 10 секунд перегляду реклами в соціальних мережах з анімованою графікою достатньо для підвищення залучення та усвідомлення того, що відбувається. Один з розповсюджених на сьогодні жанрів анімаційних сцен є 3D [1]. 3D моделювання – це безмежні можливості. 3D візуалізація - неймовірно ефективний інструмент для реалізації сцен, які ніколи не були зняті на відео з технічних або етичних причин. Існують два основні способи створення 3D-моделей: створення моделі у програмі для 3D-моделювання та використання об'єкту з реального світу для створення його цифрової моделі за допомогою 3D-сканера [2]. Однією з ключових ланок створення 3D анімації є розробка 3D моделей для анімаційного ролика, розробка для кожного з них анімації, визначення фону, ефектів та ін. Від цього залежить сприйняття анімаційних роликів.

Майбутній відео ролик соціальної реклами присвячено темі «Доброта врятує Світ». У сюжеті здійснюється взаємодія двох персонажів. Засобами полігонального моделювання були розроблені моделі, що приведені на рисунках 1, 2.

Рисунок 1 – Головний персонаж

Рисунок 2 – Додатковий персонаж

Література

1. Голованов, Н.М. Геометричне моделювання/Н.М. Голованів. – К.: 2002. – 630 с.

2. Прахов, А. Blender. 3D-моделювання та анімація. Керівництво для початківців / А. Прахов. – М: БХВ-Петербург, 2009. - 272 с.

3. Миколайшвілі Г.Г. Соціальна реклама: Теорія та практика // М., Аспект Прес, 2008 – 191 с.

УДК 004.421

ДОСЛІДЖЕННЯ РОБОТИ ДВИГУНА З ВИКОРИСТАННЯМ ПЛАТИ ARDUINO

Варениця А., Лясковська С.
Національний університет «Львівська політехніка»

Автоматизація розмаїтих виробничих процесів у теперішньому прогресивному індустріалізованому світі набирає все більших розмахів. Для більшості виробництв використовують високотехнологічні автоматизовані лінії, котрі характеризуються багатозадачністю модуля керування. Такі системи керування є складними у виготовленні та обслуговуванні висококваліфікованими спеціалістами. Тому щораз частіше використовують спрощені схеми управління, котрими можна керувати навіть з телефона. Одними з таких є плати Arduino, які належать до обчислювальних платформ простого (навчального) конструювання [1]. Для формування моделі автоматизації певного обладнання чи руху робочого органу деталі машини нами складений такий план:

- аналіз принципу роботи верстата та його кінематичної схеми;
- вибір схеми (плати) Arduino;
- проектування або модернізація виконавчого органу;
- програмування плати для контролю обладнання.

Нами обраний свердлильний верстат 2М112 для проведення досліджень можливості автоматизації руху його робочого органу тобто патрона (рис.1). Така модернізація здійснюється для того, аби була можливість виконувати не стандартні роботи, наприклад, нарізання різі чи свердління високоякісних отворів. Обертовий рух передається до патрона 1 верстата від двигуна 2 через набір шківів за допомогою клинопасової передачі 3. Робочим органом у верстаті є патрон 1, який знаходиться на шпинделі. Він приводиться в дію двигуном 2 для обертового руху. А повздовжній рух шпинделя приводиться в дію рукояткою. Для модернізації роботи свердлильного верстата 2М112 нами запропоновано встановити крокoвий двигун 4 та допоміжну шестерню 5. Вони у свою чергу автоматизують повздовжній рух шпинделя верстата, на якому розташований патрон із закріпленим у ньому інструментом.

Наступним етапом досліджень є вибір плати Arduino. Нами проведений аналіз таких видів плат Arduino: Arduino ADK, Arduino BT (Bluetooth), Arduino Diecimila, Arduino Due, Arduino Duemilanove, Arduino Ethernet, Arduino Fio, Arduino Leonardo, Arduino LilyPad, Arduino Mega, Arduino Mega2560, Arduino Nano, Arduino Pro Mini, Arduino Uno, Arduino MK-duino. Для проведення дослідження обрано плату Arduino BT (Bluetooth). Така плата має наступі переваги: можливість керування з телефона через Bluetooth, доступна вартість, простота використання, малі розміри.

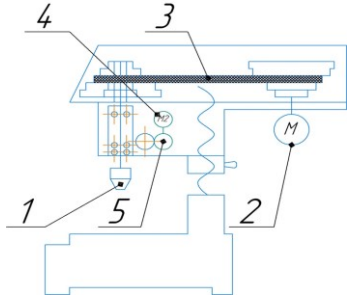


Рис.1. Кінематична схема свердлильного верстата 2М112.

Для точного позиціонування або переміщення об’єкта на задане число обертів вала використаний крокoвий двигун **Stepper motor**. Обрана плата **Arduino** може управляти двигуном за допомогою драйвера і бібліотеки **stepper.h.** На рис.2 подано програмну частину програмного забезпечення ПЗ для контролю роботи крокового двигуна верстата.

```
#include <Stepper.h>

const int stepsPerRevolution = 200;  // change this to fit the number of steps per revolution
// for your motor

// initialize the stepper library on pins 8 through 11:
Stepper myStepper(stepsPerRevolution, 8, 9, 10, 11);

void setup() {
  // set the speed at 60 rpm:
  myStepper.setSpeed(60);
  // initialize the serial port:
  Serial.begin(9600);
}

void loop() {
  // step one revolution  in one direction:
  Serial.println("clockwise");
  myStepper.step(stepsPerRevolution);
  delay(500);

  // step one revolution in the other direction:
  Serial.println("counterclockwise");
  myStepper.step(-stepsPerRevolution);
  delay(500);
}
```

Рис.2. Програмна частина ПЗ для контролю роботи крокового двигуна верстата 2М112

Керування кроковим двигуном здійснюється через плату **Arduino** шляхом подачі імпульсів на обмотки двигуна в певній послідовності. Обертання вала двигуна здійснюється за допомогою сигналу, який керує магнітним полем котушки в статорі двигуна. Сигнал генерує драйвер крокового двигуна. Магнітне поле, яке з'являється при проходженні електричного струму в обмотках статора, заставляє обертатися вал, на якому встановлені магніти. Число обертів вала двигуна **Stepper motor** задається в програмі з використанням бібліотеки **Arduino IDE**.

Література

1. https://www.arduino.cc

.

УДК 004.7

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЇ В ОСВІТІ

Василюк В., Малець І.
Львівський державний університет безпеки життєдіяльності

Анотація :у роботі розглянуто впровадження інформаційних технологій у світі та Україні, їх розвиток та майбутнє. Особливості дистанційного навчання та його перспективи.

Ключові слова:*процес навчання, інформаційні технологій, запровадження концепції, дистанційне навчання.*

Abstract: introduction of information technologies in the world and Ukraine, their development and future. Features of distance learning and its prospects.

Key words: *learning process, information technologies, implementation of the concept, distance learning.*

Процес навчання в освіті – це постійний симбіоз вчителя і учня, що постійно удосконалюється, у ході якої вирішуються проблеми освіти, виховання та загального розвитку студентів. Особливо помітний вплив культури, науки, економіки, політики і техніки в процесі розвитку, які проявляють себе у вигляді певних тенденцій. Використання сучасних інформаційних технологій впливає на процес сприйняття навчального матеріалу та, врешті-решт, впливає на успішність навчального процесу.

Взагалі, що таке інформаційні технології?

Інформаційна технологія – процес, що використовує сукупність засобів і методів збору, обробки, зберігання та передачі даних для отримання інформації кращої якості про станоб'єкту, процесу або явища.Розвиток технологій, якікористуються великим попитом у людей, призводить до покращення змісту навчального процесу.

Етапи розвитку інформаційних технологій:

Ручний етап – розпочався з винаходу першого письма.

Механічний етап – розпочався з винаходу книг.

Електричний етап – розпочався з винаходу електричних пристроїв.

Комп'ютерний етап – розпочався з винаходу електронної обчислювальної машини.

З початком розвитку інформаційних технологій підвищується їх роль та використання у освітній сфері. Світовою перевагою у сфері освіти стають загальнодоступні онлайн-курси MOOCs і медіа-освіта. Засновники наголошуютьна тому, що запровадження нових технологій навчання та оволодіння ними вимагають тотальну налаштованість як викладачів, так і студентів до серйозних змін, що відповідають договорамнеперервного та швидкого інформаційного суспільства .

На початку 2010 року в Україні запровадили концепцію медіаосвіти України, що має ціль розбудови в Україні дієвої системи медіа-освіти для за-

безпечення підготовки молодого покоління до безпечної та ефективної взаємодії із сучасними системами медіа, розвитку обізнаності у сфері медіа, грамотності і компетентності згідно до їхніх вікових та персональних особливостей.

Онлайн-курси в наші дні стали невід'ємним засобом навчання. Така форма навчання дає змогу спілкування студентів та викладачів між собою, а також прийому сесії в дистанційному форматі. Це одна із найновіших форм дистанційного навчанняв усьому світі, зокрема і в Україні. Використання в освітній практиці технологій, пов'язаних з Інтернетом, дозволяє реалізувати принцип безперервної та безконтактної освіти – «навчання впродовж усього навчального року», яка не вимагає присутності студентів у навчальних закладах освіти.

Звичайно таке онлайн навчання має як плюси так і звичайно мінуси. До плюсів ми відносимо:

− доступ до бази найуспішніших університетів і викладачів;

− сучасна інформація, технології;

− можливість вибору і навчання будь-де і будь-коли.

Однак є і мінуси:

− сучасний студент зіштовхується і з проблемами недостатньої мотивації;

− нестача практичних вмінь та навичок;

−недостатній розвиток комунікабельності;

− складність оцінити знання чи їх відсутність.

У країні не має відповідних програм загальнодержавного та регіонального рівнів. Невисокий рівень комп'ютеризації суспільства та системи освіти зокрема, несформованість національного освітнього простору в Web-середовищі та ін. не дають змоги в даний час реалізувати значні потенційні можливості дистанційного навчання. Ми на стадії розвитку, однак у зв'язку із теперішньою ситуацією у країні, пов'язаною з пандемією, нас очікують масштабні зміни на краще. Дистанційне навчання має великі перспективи, тому що виправдовує себе і є дійсно зручним.

Оновлення підходів до процесу здобуття освіти з використанням передових інформаційних технологій дозволяє активізувати цікавість здобувачів до освіти та досягнути високої якості підготовки в сучасних умова, викликаних пандемією COVID-19, що на даний час є досить важливим аргументом, у порівнянні із традиційними підходами.

Література

1. Биков В.Ю. Наукове забезпечення дистанційної професійної освіти: проблеми та напрямки досліджень// Професійна освіта: педагогіка і психологія. За ред.: І.Зязюна, Н.Ничкало, Т.Левовицького, І.Вільш. Україно-польський журнал. Видання II.. Видавництво: ЗАТ "ВІПОЛ", Київ-Ченстохова. – 2000.https://www.dli.donetsk.ua/news/2020-06-04-3

2. Інформаційне суспільство. Шлях України // Бібліотека інформаційного суспільства. – К.: "Відродження" та ПРООН, 2004. – 309 с.

УДК 004

ПРОГНОЗУВАННЯ РУХУ ЦІН АКЦІЙ ЗА ДОПОМОГОЮ МЕТОДІВ МАШИННОГО НАВЧАННЯ

Васьків А., Пастущак О.
Львівський національний університет імені Івана Франка, Львів

Анотація. *Робота присвячена вивченню можливостей прогнозування руху цін акцій за допомогою методів машинного навчання, а саме методу опорних векторів та багатошарового перцептрона.*

Ключові слова: *машинне навчання, прогнозування фондового ринку, таксономія, штучні нейронні мережі, метод опорних векторів, інвестиційні рішення.*

Abstract. *The work is devoted to the study of the possibilities of forecasting the movement of stock prices using the methods of machine learning, namely the support vector machines method and multilayer perceptron.*

Keywords: *machine learning, stock market prediction, artificial neural network, support vector machine, investment decision.*

Передбачення руху цін акцій є складною проблемою, однією з тих, що широко вивчаються і привертають увагу дослідників з багатьох галузей, включаючи економіку, історію, фінанси, математику та комп'ютерні науки [1]. Фінансові установи та біржові маклери створили і далі створюють багато різних власних моделей, які намагаються обійти ринок з вигодою для себе чи своїх клієнтів, але мало хто зміг таким чином досягнути постійно високих доходів [2]. Тим не менше, проблема прогнозування цін акцій є надалі привабливою, оскільки покращення прогнозів лише на кілька відсотків може збільшити прибутки на мільйони доларів цим установам. Тому отримання точних методів прогнозування зміни цін на фондовому ринку надалі залишатиметься великою метою як фінансової, так і технологічної спільноти. Через нестабільний характер фондового ринку застосування простих часових рядів або технік регресій не дає бажаних результатів [3].

У цій роботі ми зосередилися на порівнянні двох моделей: SVM з ядром RBF та моделі MLP для прогнозування руху ціни акцій. І порівнюємо їх у різні періоди: 2007-2014 роки – період світової фінансово-економічної кризи, та період 2012-2019 – період відновлення та стабільного зростання світових економік.

Під час нашого дослідження ми зосередились на технологічному секторі. Робота з цим сектором, на відміну від загального ринку, дозволила нам протестувати моделі на компаніях, схожих між собою, роблячи наші результати відносно стандартизованими.

Ми використовували індекс NASDAQ-100 (^NDXT) як загальний індекс сектору технологій. Індекс складається з технологічних гігантів, таких як Microsoft та Apple, а також менш відомих компаній, таких як ANSYS Inc. та Workday Inc.

У цьому дослідженні ми використали чотири характеристики для прогнозування напряму руху цін акцій – волатильність ціни, імпульс ціни, волатильність сектору та імпульс сектору. Кожна з цих чотирьох ознак обчислюється шляхом усереднення деякої статистики за останні n днів. Ми провели наше дослідження, варіюючи цей параметр n, щоб побачити, як саме тенденції волатильності та імпульсу ціни як окремої акції, так і цілого сектору впливають на прогнозування зміну ціни.

Нехай n1 – к-сть днів для усереднення статистики цілого сектору, а n2 – к-сть днів усереднення статистики для окремої акції, $n1,n2 \in \{5,10,20,90,270\}$. Ці параметри відповідно представляють усереднення за один тиждень, за два тижні, за один місяць, за один квартал і за один рік. У кожній ітерації ми взяли деяку комбінацію n1, n2 і використали ці параметри для обчислення нашої множини векторів характеристик. Потім ми тренували наші моделі на цих даних і прогнозували на них, та перевірили точність результатів. Загалом було проведено 25 ітерацій, по одній для кожної комбінації n1, n2.

Аналіз результатів продемонстрував, що обидві моделі SVM та MLP показують схожу ефективність, однак модель SVM у період 2007-2012 показала більшу точність, ніж MLP (в середньому на 1-2%). Проте ми спостерігаємо протилежну картину на даних періоду 2012-2019.

Якщо збільшувати параметр m (к-сть днів для прогнозування), ми помітили, що середнє та медіанна точності передбачення збільшуються, коли m = 5, 10, 20, але потім незначно зменшуються, коли m = 90 та m = 270.

Також було спостережено, що при малому m, зміна n1 та n2 мало впливає на загальну точність. Наприклад, коли m = 1, середня точність знаходиться в межах 49,5% і 50,53% для кожної комбінації n1, n2. Варто відзначити, що для прогнозування, коли m = 1, найефективніші дуже малі або дуже великі значення n1, n2. Загальне середнє та медіана точності найвищі, коли принаймні одне з двох дорівнює 5, або коли обидва дорівнюють 90 або 270. Це означає, що дуже короткострокові або довгострокові тенденції найкраще підходять для прогнозування цінового напрямку на наступний день. Однак тенденції на два тижні або місяць менш ефективніші, ніж просте випадкове вгадування в такому випадку. Це твердження справедливе для обох періодів.

Параметри n1 та n2 починають ставати більш важливими, коли ми збільшуємо m. Коли m = 10, середня точність прогнозування коливається між 53,3% і 56,8%, набагато більший діапазон, ніж при m = 1. Це твердження перебільшене, коли m = 90, тобто коли ми намагаємося передбачи-

ти зміну ціни протягом наступного кварталу. Деякі комбінації n1, n2, такі як n1 = 10, n2 = 90, насправді призводять до точності менше 50%, що означає, що краще було б підкинути монету, тоді як інші комбінації мають дуже високу точність. Наприклад, n1 = 270, n2 = 5 , що призводить до 61,5% точності прогнозування.

Інша помітна тенденція полягає в тому, що загалом n1 = 270 забезпечує найвищу точність прогнозування для всіх m у період 2007-2012. Тобто загальні історичні дані сектору за минулий рік, як правило, допомагають прогнозувати ціновий напрямок у будь-який момент у майбутньому. Це більш корисно, оскільки ми намагаємось передбачати подальше майбутнє, але навіть у короткостроковій перспективі, схоже, річна тенденція сектору є кращим прогнозистом, ніж короткострокова тенденція сектора. Але в період з 2012-2012 n1=5 є кращим параметром, проте не настільки сильно як в попередньому випадку.

Література

1. Narasimhan Jegadeesh S. T. / Returns to buying winners and selling losers: Implications for stock market. – S. T. Narasimhan Jegadeesh. – “The Journal of Finance”, 1993.

2. Zvi Bodie A. M. / Investments. – A. M. Zvi Bodie, Alex Kane. – “McGraw-Hil”, 2014.

3. Bontempi G. / Machine Learning Strategiesfor Time Series Forecasting. – G. Bontempi, S. B. Taieb. – режим доступу до ресурсу: https://www.researchgate.net/publication/236941795_Machine_Learning_Strategies_for_Time_Series_Forecasting

УДК 004

ДОСЛІДЖЕННЯ ТА АНАЛІЗ ТЕХНОЛОГІЙ ДОПОВНЕНОЇ РЕАЛЬНОСТІ

Власенко В., Воронцова Д.
Національний технічний університет «Харківський політехнічний інститут», Харків

Робота присвячена дослідженню технологій доповненої реальності, які застосовуються у додатках мобільних телефонів. В роботі приведено аналіз та результати тестування різних інструментів та методів щодо реалізації функції AR. Виявленні переваги та недоліки існуючих рішень представлені у вигляді порівняльної таблиці. В роботі пропонуються рекомендації щодо покращення функції доповненої реальності у мобільних додатках.

The work is devoted to the study of augmented reality technologies used in mobile phone applications. The paper presents the analysis and testing results of various tools and methods for implementing the AR function. Identifying the advantages and disadvantages of existing solutions are presented in the form of a comparative table. The paper offers recommendations for improving the AR function in mobile applications.

Ключові слова: *доповнена реальність, AR, сучасні технології, мобільний додаток.*

На сьогоднішній день, технологія доповненої реальності є найпопулярнішою серед розробників мобільних додатків. З її допомогою, можна познайомитись із різними об'єктами, коли немає фізичної можливості зробити це наживо. Технологію доповненої реальності дуже часто використовують для освітніх цілей як у загальних шкільних, так і в університетських закладах освіти.

Система доповненої реальності є посередником між реальністю і людиною, а значить, на виході вона повинна створювати сигнал для одного з відповідних органів [1]. За типом подання інформації можна виділити наступні системи: візуальні системи, аудіо системи, аудіовізуальні системи, геопозиційні системи, оптичні, автономні, інтерактивні системи. Якщо говорити про сферу освіти, то саме інтерактивні системи зручні та дієві в процесі навчання. Розглянемо саме їх у даній роботі.

Розробка функції доповненої реальності інтерактивного типу передбачає вирішення двох основних задач:

1. Створення віртуального контенту і методів взаємодії з ним.
2. Визначення положення цифрових об'єктів на зображенні.

Для вирішення першого завдання існують програми, які дозволяють «оживити» статичні об'єкти. Графічний двигун повинен плавно об'єднувати сцени доповненої реальності з реальним середовищем. Unity 3D – популярний кросплатформенний конструктор для створення деталізованого AR-контенту; ці ж функції виконує програма Blender. Пакет інструментів RealityKit від Apple, що прийшов на зміну SceneKit, дозволяє моделювати складну 3D-графіку на iOS. А за допомогою SceneForm від Google розробники можуть створювати реалістичні тривимірні візуалізації для браузерів або додатків доповненої реальності на Android [2].

Друге завдання пов'язане з комп'ютерним зором: необхідно проаналізувати реальний світ і задати координати створених об'єктів через розпізнавання спеціального маркера – як правило, 2D-зображення, визначити його положення в просторі і побудувати щодо нього віртуальний об'єкт. Для цього знадобляться спеціальні засоби для розробки доповненої реальності. Будучи основним технологічним двигуном, SDK доповненої реальності (Software Development Kit) забезпечує весь процес розробки AR, включаючи рендеринг контенту і накладення віртуальних об'єктів і цифрової інформації на реальний світ. Далі приведені найбільш популярні платформи для роботи з AR [3]: Vuforia, Wikitude SDK, ARKit, ARKit 4, ARCore, MaxST AR SDK. Проаналізувавши вище зазначені платформи прийшли до висновку, що технологія доповненої реальності ARCore підходить найбільше для розробки функції доповненої реальності інтерактивного типу у освітньому мобільному додатку. тому Цій інструмент дозволяє налаштувати камеру смартфона для визначення площини в просторі учня та розмістити в ньому об'єкт дослідження. Було проаналізовано відповідну кількість мобільних додатків, що використовують подібну технологію (табл. 1). Кожен з таких додатків має свої переваги, але усі вони мають один суттєвий недолік, розмір моделі, що додається у середовище користувача чітко заданий. Його можна змінювати, але одразу при додаванні об'єкту він буде стандартний.

Таблиця 1

Назва мобільного додатку	Призначення	Базові маніпуляції з моделями	Розмір моделі, в залежності від простору
Froggipedia	Дослідження життєвого циклу жаби	+	-
BBC Civilisations AR	Вивчення різноманітних історичних артефактів	+	-
Mondly	Вивчення іноземної мови	-	-
Pokémon Go	Гра, мета якої збирати покемонів у реальному світі	-	-
Ink Hunter	Додаток для нанесення ескізів тату	+	-
Star Walk 2	Спостереження за зірковим небом, додаток дозволяє дізнатись де саме знаходиться потрібне сузір'я, планета тощо	-	-

Планується в подальшій роботі вирішити вище зазначену проблему додаванням чотирьох опорних точок, знаходити площу отриманого чотирикутника, а потім, в залежності від цієї площі генерувати відповідний масштаб об'єкту.

Література

1. Lee, Kangdon Augmented Reality in Education and Training. // TechTrends. – 56 (2): 13–21 – 7 February 2012.
2. Бойченко І.В., Лежанкін А.В. Доповнена реальність: стан, проблеми та шляхи рішення. – Доповіді ТУСУРу, № 1 (21), частина 2. – 2010. Доповнена реальність [Електронний ресурс] // woxapp.com – Режим доступу: https://woxapp
3. Інструменти для створення доповненої реальності [Електронний ресурс] // сайт evergreens.com.ua – Режим доступу: https://evergreens.com.ua/ru/articles/web-ar-tools-overview.html

УДК 614.8

АНАЛІЗ ІСНУЮЧИХ ПРОГРАМНИХ ПРОДУКТІВ, ЩО ВИКОРИСТОВУЮТЬСЯ ДЛЯ ПРОГНОЗУВАННЯ ВИНИКНЕННЯ НАДЗВИЧАЙНИХ СИТУАЦІЙ

Гаврись А., Пекарська О.
Львівський державний університет безпеки життєдіяльності, м.Львів

Важливо не тільки вміти швидко та якісно реагувати на катастрофи, але також вміти їх передбачати. Ці заходи допоможуть завчасно дізнатися можливу зону ураження, оцінити приблизні збитки,або забезпечити якісну евакуацію людей. Тому для прогнозування виникнення природних катастроф передові країни використовують безліч допоміжних програм.

Ключові слова: *цивільний захист, картографія, програмне забезпечення, прогнозування.*

It is important not only to be able to respond quickly and efficiently to disasters, but also to be able to predict them. These measures will help to know in advance the possible area of danger, estimate the approximate damage, or ensure a quality evacuation of people. Therefore, advanced countries use many support programs to predict the occurrence of natural disasters.

Key words: *civil protection, cartography, software, forecasting.*

За 2020 рік на території України виникло біля 64 подій природного характеру. Серед них найбільш спустошливою природною небезпекою стало утворення пожеж. Так, за даними офіційної сторінки сайту ДСНС України [1] вагомі пожежі виникли на території Луганської області, Житомирської та Харківської. Основною спільною проблемою виникнення катастроф стали погодні умови, а саме: сильний поривчастий вітер (до 25 м/с) та висока температура повітря. Як наслідок, всього було пошкоджено 383 будинки, з яких 35 – було повністю знищено; евакуйовано – 252 людини, 18 – постраждало, а 10 – загинуло. Кількість природних катастроф, які виникають на території України залишаються незмінним, так само, як і їх збитки, яких вони завдають. До прикладу, лише в одній Харківській області на період 6-го жовтня 2021 року біля 16 людей загинуло тільки від пожеж [1]. Тож стає зрозумілим, що хоч наша держава і не є центром

утворення багатьох стихійних лих, проте завчасна підготовка до виникнення можливих природних небезпек врятувала б життя не одній людині.

Метою даної роботи було проаналізувати програмне забезпечення прогнозування природних катастроф, яке використовують у світі та в Україні. Знайти їхні переваги і, недоліки.

Україна – це держава з великим потенціалом та амбіціями, але із застарілим підходом та методами в рятуванні людей. Це стосується і впровадження новітніх технологій та програмного забезпечення (далі - ПЗ) у державні підрозділи, що займаються прогнозуванням надзвичайних ситуацій.

Danube HIS – це інформаційна система, яка діє в рамках проєкту DAR EFFORT. ЇЇ метою є надати в реальному часі дані стосовно підняття рівня води в річці Дунай, усім 12-тьом країнам-партнерам, щоб запобігти витоку річки за межі її берегів. Наразі даний проєкт триває, тому більш детальних даних про цю інформаційну систему немає [2]. Недоліком даної ПЗ є те, що проєкт перебуває у стадії розробки, тому реальних результатів ще не видає.

WRF-Україна – оперативна система, яка є розробкою Інституту проблем математичних машин і систем (ІПММС) НАН України з ліквідації наслідків Чорнобильської катастрофи, використовується у прогнозуванні розповсюдження радіаційних частинок у разі виникнення аварії на АЕС. Крім того, прогнозує стихійні гідрометеорологічні явища на Закарпатті [3]. Працює на основі ГІС-технологій. Недоліком даної системи є виключно комерційне використання, тобто системи не має у вільному доступі.

Країни Європи та північна Америка активно використовують допоміжні програми у своїй діяльності: на мобільних пристроях, які доступні для багатьох людей, комп'ютерні програми з більш професійним набором інструментів, які є у вільному доступі, а також ліцензійні програми, які використовуються лише за призначенням. Нижче буде розглянуто деякі з них.

Wildfire Analyst – програмне забезпечення, яке забезпечує аналіз поведінки лісових пожеж у реальному часі та моделює поширення лісових пожеж. Воно відбувається за декілька секунд, надаючи результати, які дозволять вчасно прийняти рішення [4].

FiResponse – програма для підприємства, яка надає змогу відслідковувати пожежі в дикій місцевості. Також вона автоматично відправляє і відстежує сили і засоби, на ліквідацію детектованої пожежі [5]. Недоліком використання цих програм в Україні є їх комерційна основа.

Sahana Disaster Management Software — передає точну інформацію, що забезпечує готовність до надзвичайних ситуацій, реагування на них. Також вона є доступною для всіх, оскільки є безкоштовною. В ній зберігаються такі дані: організаційний довідник, управління людськими ресурсами; оповіщення та планування інцидентів; інформація про медичні заклади та відстеження захворювань та пацієнтів, управління активами, логістика; демографічні дані, ризики, інструменти оцінки; інструменти для спільної роботи, включаючи картографування, обмін повідомленнями та обробку документів [6].

InaSAFE – використовується в Азії для передбачення катастроф. Програма створює реалістичні сценарії впливу природних небезпек, що

забезпечує краще планування, готовність та реагування. Перевагою є те, що програма цілком безкоштовна, але недоліком – що вона надає інформацію лише для території Індонезії та Австралії [7].

Crisis Mappers використовує мобільні та веб-додатки, карти спільного використання та дані про події з медіа, аерофотознімки та супутникові знімки, геопросторові платформи, розширену візуалізацію, симуляцію в реальному часі та обчислювальні та статистичні моделі для ефективного раннього попередження для швидкого реагування на складні гуманітарні надзвичайні ситуації. Ця група включає 9 600+ членів у більш ніж 160 країнах, які пов'язані з більш ніж 3 000 різних установ, включаючи понад 400 університетів, 50 установ та проєктів Організації Об'єднаних Націй [8].

Global Disaster Alert and Coordination System (GDACS) — це співпраця між Організацією Об'єднаних Націй, Європейською Комісією та рятувальниками у всьому світі для покращення оповіщень, обміну інформацією та координації на першому етапі після великих раптових катастроф. Перевагою цієї програми є те, що вона відображає масштабні події усього світу он-лайн [9].

Дуже важливо рухатися з часом і використовувати новітні технології у боротьбі з непередбаченим стихійним лихом [10]. Важливо прораховувати всі можливі варіанти розвитку подій, щоб ліквідувати катастрофу якомога швидше і щоб встигнути врятувати не одне людське життя. Саме тому варто використовувати вже існуючі програми, довершити їх, або ж створити власні, відповідно до українських реалій.

Література

1. Офіційний сайт ДСНС України. Режим допуску: https://www.dsns.gov.ua/ua/Dovidka-za-kvartal/119288.html
2. Офіційний сайт Українського гідрометеорологічного центру. Режим допуску: https://meteo.gov.ua/ua/33312/dareffort/dareffort_about
3. Офіційний сайт Національної академії наук України. Режим допуску: https://www.nas.gov.ua/EN/Messages/Pages/View.aspx?MessageID=2419
4. Офіційний сайт проєкту Wildfire Analyst. Режим доступу: https://www.wildfireanalyst.com/
5. Офіційний сайт проєкту Technosylva Inc. Режим доступу: https://technosylva.com/firesponse/
6. Офіційний сайт United Nations ESCAP. Режим доступу: https://drrgateway.net/e-resilience/tool/sahana-disaster-management-software
7. Офіційний сайт програми InaSAFE. Режим доступу: http://www.inasafe.org/
8. Офіційний сайт програми CrisisMappers. Режим доступу: http://crisismapping.ning.com/
9. Офіційний сайт системи GDACS. Режим доступу: https://www.gdacs.org/default.aspx
10. Гаврись А.П., Моренюк Р.Я., Гарасимюк І.М. Метод просторового розміщення пожежонебезпечних ділянок на підставі даних дистанційного зондування Землі. Збірник наукових праць «Науковий вісник НЛТУ». – Львів. – 2019. – №29(8). – с. 36-42.

УДК 614.8

СТВОРЕННЯ КАРТ РИЗИКІВ ВИНИКНЕННЯ НАДЗВИЧАЙНИХ СИТУАЦІЙ, ЯК ЕФЕКТИВНИЙ СПОСІБ ІНФОРМУВАННЯ НАСЕЛЕННЯ ПРО ЗАГРОЗИ

Гаврись А., Шинкаренко М.
Львівський державний університет безпеки життєдіяльності, м.Львів

Зі збільшенням кількості різноманітних природних та техногенних катастроф, постає питання про можливість попередження виникнення надзвичайних ситуацій, ліквідацію ризику їх виникнення і зменшення потенційної небезпеки. Для ефективного інформування населення про потенційну небезпеку пропонується широко використовувати карти ризиків виникнення надзвичайних ситуацій, що знаходитимуться у вільному доступі на он-лайн платформах.

Ключові слова: *ризик, картографія, моделювання, візуалізація, затоплення, прогнозування.*

With the increase in the number of various natural and man-made disasters, the question arises about the possibility of preventing emergencies, eliminating the risk of their occurrence and reducing the potential danger. In order to effectively inform the population about the potential danger, it is proposed to widely use the risk maps of emergencies, which will be freely available on online platforms.

Key words: *risk, cartography, modeling, visualization, flooding, forecasting.*

Мабуть, не є новиною, що в кожному суспільстві існує ризик виникнення надзвичайних ситуацій (НС), які останнім часом показують в новинах майже кожного дня. Велика їх частина відбувається у віддалених місцях, і вони швидко забуваються. Інші привертають увагу світових засобів масової інформації на більш тривалий період. Події, які отримують максимальну увагу з боку засобів масової інформації, є такими, які відбуваються миттєво і викликають значні збитки і людські жертви, наприклад: землетрус, цунамі, урагани, повені і т.д.. Ці процеси і явища можуть викликати місцеві, регіональні і глобальні впливи в довгостроковій перспективі.

Оскільки ризик виникнення тої чи іншої надзвичайної ситуацій на певній території може бути не очевидним для простого населення, уряд країн, міжнародні організації та громадські об'єднання створюють карти ризиків територій і завантажують їх в он-лайн платформи з вільним доступом.

Одним з найважливіших просторових атрибутів одиниць картографування для інвентаризації елементів ризику є використання землі. Використання землі визначає в значній мірі тип будівель, що можуть постраждати від НС, види економічної діяльності, які здійснюються в досліджуваних територіях, щільність населення в різні періоди дня і т.п. Карти покриву землі та використання землі складаються шляхом класифікації зображень в невеликих масштабах або, за допомогою візуальної інтерпретації в великих масштабах. Інформація про елементи ризику збирається з великої кількості джерел. Існує також багато районів у світі, для яких щодо елементів ризику не існує ніяких докладних цифрових даних. У

таких ситуаціях, дані повинні переводитися в цифрову форму з аналогових карт, або в разі, якщо їх також не існує, вони повинні картографувати на місці, наприклад, з використанням мобільних ГІС. Використовуючи мобільний ГІС, стає можливим безпосередньо збирати просторову інформацію на основі зображення з високою роздільною здатністю, який може бути завантажено в кишеньковий комп'ютер або смартфон, і з'єднати його з атрибутивними даними, які збираються на місці. Деякими з найбільш використовуваних засобів для мобільного ГІС при картографуванні елементів ризику є ArcMap [1].

Для прикладу розглянемо карти ризиків затоплення територій.

Карта ризиків затоплення – це візуальний засіб відображення утворення ризику затоплення на певній території. За допомогою карти ризиків затоплення можна визначити глибину, площу затоплення та подібну інформацію. Карти, при відповідному наповненні, часто відображають розмір можливих збитків, що використовується як додатковий інструмент при прийняті управлінських рішень [2]. Особливу роль карти затоплення відіграють при плануванні дій в надзвичайних ситуаціях, при плануванні містобудівної, архітектурної, землевпорядної документації та при розробці заходів цивільного захисту територій.

Карти ризиків затоплення зазвичай доступні для громадян у країнах, де ведуться спостереження за надзвичайними ситуаціями природного і техногенного характеру, проте можливості поширення таких карт зазвичай відрізняються в різних країнах. У деяких країнах такі карти випускають у паперовому вигляді, вони доступні пересічним громадянам за місцем проживання або робочих місцях. Найчастіше карти ризиків затоплення знаходяться на вільних он-лайн платформах. де кожен бажаючий може знайти необхідну йому інформацію. Прикладом застосування інформаційних технологій в моделюванні підтоплень може слугувати служба IFIS «Iowa Flood Information Systems», яка створює карти такого типу для штату Айова, США.

Карти ризиків виникнення надзвичайних ситуацій вже показали свою ефективність при інформуванні населення про потенційні небезпеки регіонів у більшості країн світу. Тому, розроблення та використання таких карт є не невід'ємною частиною вдосконалення механізму цивільного захисту по інформуванню населення про загрози в Україні.

Література

1. Стародуб Ю.П. Побудова моделі вивчення екогеофізичного стану території з використанням GIS технології [Текст] / Стародуб Ю.П., Гаврись А.П. // Матеріали VI Всеукраїнської заочної науково-практичної конференції «Проблеми цивільного захисту населення та безпеки життєдіяльності: Сучасні реалії України». – Київ. – 2020. – с. 146-147.

2. Starodub Y. Flood risk assessment of Chervonograd mining-industrial district [Text] / Y. Starodub, V. Karabyn, A. Havrys, I. Shainogal, A.Samberg // Proc. SPIE 10783, Remote Sensing for Agriculture, Ecosystems, and Hydrology XX, 107830P (10 October 2018); doi: 10.1117/12.2501928.

3. Офіційний сайт IFIS. Режим допуску: https://ifis.iowafloodcenter.org/ifis/

004.65

ТЕНДЕНЦІЇ РОЗВИТКУ БАЗ ДАНИХ

Гелешко І., Карабин О.
Львівський державний університет безпеки життєдіяльності, Львів

Розглянуто основні типи організації баз даних та систем управління ними, перелічено основні клієнтські програми для серверів баз даних, перелічено найбільш розповсюджені засоби для розробки додатків базах даних.

***Ключові слова**: бази даних, системи управління базами даних, архітектура баз даних, клієнт, сервер.*

The main types of database organization and management systems are considered, the main client programs for database servers are listed, the most common tools for database application development are listed.

***Keywords:** database, database management systems, database architecture, client, server.*

В сучасному суспільстві, перенасиченому інформацією, її організація і систематизація, є надзвичайно актуальною задачею в усіх сферах економічного, господарського та суспільного життя. Організовану структуру, призначену для зберігання, зміни та обробки взаємозалежної інформації переважно великих обсягів, називають базою даних. Системою управління базами даних називають комплекс мовних і програмних засобів, призначених для створення, ведення і спільного використання базами даних багатьма користувачами. Розрізняють такі основні типи організації (архітектури) баз даних: автономні (локальні), файл-серверні, клієнт-серверні, багаторівневі, розподілені, об'єктно-орієнтовані. Розглянемо коротко особливості кожної з цих архітектур.

Автономні (локальні) бази даних є найбільш простим типом організації баз даних. Вони розміщуються на одному комп'ютері і з ними має змогу працювати тільки один користувач, оскільки мережа в такому випадку не використовується. Автономні бази даних широко застосовуються на невеликих підприємствах для бухгалтерського і кадрового обліку, а також окремими користувачами для збереження й обробки власних даних.

Поняття файл-серверних і клієнт-серверних технологій увійшло в ужиток у 80-ті роки XX ст., коли було розроблено локальні обчислювальні мережі та з'явилися настільні робочі станції, які потребували організації колективного використовування інформаційних ресурсів. Тому коли йдеться про клієнт-серверну технологію оброблення інформації, то це означає, що прикладні програми (додатки) будуть мати розподілений характер. Іншими словами, частину функцій прикладної програми буде реалізовано в програмі-клієнтові, іншу — у програмі-сервері, при цьому для їх взаємодії буде використовуватись відповідний протокол.

Багаторівневі системи баз даних пропонують один підхід до безпеки, який передбачає наявність різних рівнів безпеки даних в базі. Метою таких систем є обмін даними, що мають різні рівні безпеки, і запобігання несанкціонованому доступу до них.

Розподілені бази даних - це множини логічно взаємозалежних баз даних, розподілених у комп'ютерній мережі. Розподілені бази даних складають ще один напрям в просторі досліджень і розробок систем керування базами даних. У цих системах доводиться вирішувати всі завдання, властиві централізованим системам керування базами даних, але, як правило, в більш складних постановках. В даний час більшість розподілених систем керування базами даних базується на реляційній моделі даних і розрахована на використання в локальних обчислювальних мережах.

Об'єктно-орієнтовані бази даних зазвичай рекомендовані для тих випадків, коли потрібна високопродуктивна обробка даних, що мають складну структуру.

У світі в даний час розроблені і застосовуються сотні різних систем управління базами даних, які можна класифікувати по виду використовуваної програми, характеру і моделі даних. Найбільш розповсюдженими з них є повнофункціональні та багатокористувальницькі.

Повнофункціональні системи управління базами даних, що підтримують локальні і загальні бази даних з архітектурою «файл-сервер», що мають інтерфейс, який дозволяє створювати, модифікувати структури таблиць, уводити дані, формувати запити, розробляти звіти, виводити їх на друк: Visual FoxPro, dBASE, Paradox, Access і ін.

Богатокористувальницькі багатофункціональні системи управління базами даних включають у себе як можливості сервера баз даних, так і клієнтів: Oracle, Informix, SyBase і ін.

Сервери баз даних призначені для організації центрів обробки даних в архітектурі «клієнт-сервер». Обмін із клієнтськими програмами здійснюється за допомогою операторів SQL. Прикладами є програми: MS SQL Server (MicroSoft), InterBase (Embarcadero), MySQL (Oracle), IBM DB2, Oracle Database, Cache (Inter Systems).

Клієнтськими програмами для серверів баз даних можуть бути повнофункціональні системи управління базами даних (Access, FoxPro), електронні таблиці (Excel), текстові процесори (Word), програми електронної пошти. Взаємодія користувача із системою управління базами даних відбувається через інтерфейс за допомогою спеціально розробленого додатка, що дозволяє вводити дані, формувати запити до баз даних і зображати результати пошуку інформації.

В існуючих системах управління базами даних для розробки додатків використовують ручне кодування програм (Access, IBM DB2, MS SQL Server Oracle, Cache); створення текстів додатків за допомогою генераторів

(Application Express Oracle); автоматичну генерацію готового додатка за допомогою програм візуального програмування(форми Access, Oracle, Cache).

Найбільш розповсюдженими засобами для розробки додатків базах даних є Delphi, C#, C++ Builder, Visual Basic, Java.

Основні напрями та тенденції розвитку сучасного програмного забезпечення для проектування та супроводження баз даних наступні:

- пошук сучасних моделей зберігання інформації, впровадження нових типів даних в базах;
- розробка нових архітектур системами управління базами даних, що забезпечує можливість зберігати і обробляти дані обсягів до петабайт;
- розширення областей застосування баз даних: опрацювання надвеликих обсягів інформації.

УДК 514.18

ГРАФІЧНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У СФЕРІ ЦИВІЛЬНОГО ЗАХИСТУ

Гончаренко М.О., Мартин Є. В.
Львівський державний університет безпеки життєдіяльності

У сфері цивільного захисту використовуються засоби створення і оброблення документації, зокрема, графічної із залученням можливостей інженерної, інженерної комп'ютерної, наукової, ілюстративної та ділової графіки.

Наприклад, в інженерній графіці застосовуються графічні засоби для побудови генерального плану будівлі чи споруди. Розглянувши план, можна встановити, де сталася пожежа, як швидко її можна ліквідувати. Генеральний план, а саме його графічні засоби, надають можливість встановити причини виникнення пожежі. Наприклад, інженерна, включаючи комп'ютерну, графіка є основним інструментом у сфері цивільного захисту в частині створення генеральних планів та план-графіку щодо спеціалізації інспекції. Дані норми призначені для застосування органами державної виконавчої влади, місцевого самоврядування, юридичними та фізичними особами – учасниками інвестиційного процесу незалежно від форм власності та господарювання [1]. Генеральний план повинен відповідати вимогам законів України, указів Президента України та постанов Кабінету Міністрів України, санітарного законодавства, державних нормативних документів, що регламентують будівельні, екологічні та інші аспекти містобудування, зокрема:

- правил, норм та стандартів безпеки та організації дорожнього руху;
- уповноважених на це законодавством органів державної виконавчої влади щодо врахування державних інтересів при плануванні територій;
- щодо узгодження приватних, громадських та державних інтересів;
- щодо забезпечення сталого розвитку населеного пункту;
- щодо охорони навколишнього середовища та ефективного ресурсокористування;
- щодо збереження історико-культурної спадщини.

На рис.1 приведений генеральний план будівлі, на якій сталася пожежа, а на рис.2 показаний план виробництва, де запобігли виникненню НС.

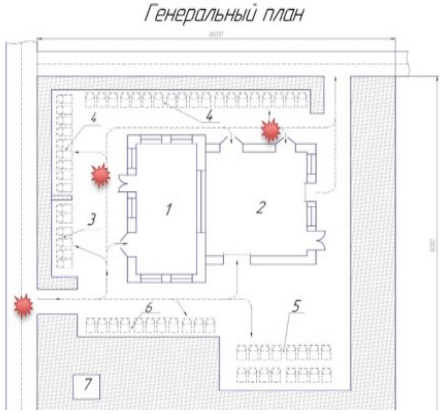


Рис. 1 Генеральний план виробництва, де сталася пожежа

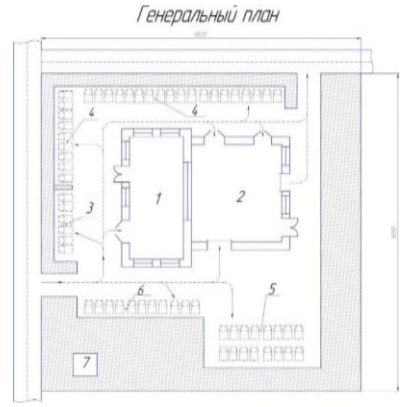


Рис. 2 Генеральний план виробництва, де запобігли виникненню НС

Планові перевірки суб'єктів господарювання здійснюються відповідно до створених засобами ділової графіки квартальних планів-графіків. Вони затверджуються керівником відповідного органу Держтехногенбезпеки України до двадцятого числа останнього місяця кварталу, що передує плановому. Прикладом може слугувати таблиця 1 із залученням створеної нами графіки (рис.3). Побудувавши цей графік, бачимо як застосовується найчастіше ділова графіка в сфері цивільного захисту.

Табл.1 Аналіз діяльності суб’єктів господарювання

№	Суб’єкт господарювання	Планова к-сть	Позапланова к-сть
1.	АЗС	1	2
2.	ТОВ «ЗОС»	3	1
3.	ХІМДЕКОР, ПП	5	10
4.	NEW BETON	10	4
5.	ІНТЕР БІР ТРЕЙД	4	2

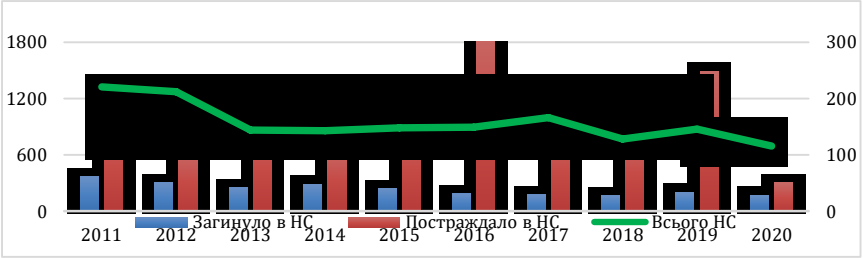


Рис.3. Динаміка виникнення НС та їх наслідків

З побудованих нами графічних залежностей, приведених на рис. 3, можна зробити висновок, що, враховуючи збереження рівня наслідків від НС, рівень ризиків виникнення НС природного та техногенного характеру та ризиків збитків від них залишаються практично незмінними та досить високими для більшості регіонів України. Це підтверджується рекордною сумою завданих надзвичайними ситуаціями збитків у 2020 році. Бачимо, що ділова графіка підвищує результативність роботи в сфері цивільного захисту, тому оброблення інформації широко застосовується в інспекції, наприклад, для формування плану-графіка [2].

Література:

1. Мураховський В. І. Комп'ютерна графіка Популярна енциклопедія. АСТ «ПРЕСС». 2012. С. 20.

2. Пічугін М.Ф. Комп'ютерна графіка. Навчальний посібник — К.: Центр учбової літератури, 2013. 346 с.

УДК 004.42: 699.8

СИСТЕМА ЗБОРУ ТА ОБРОБКИ ДАНИХ ДЛЯ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ПІД ЧАС ЛІКВІДАЦІЇ ПОЖЕЖ В ЖИТЛОВИХ БУДИНКАХ

Гулковський М.,' Дзень В., Придатко О.
Львівський державний університет безпеки життєдіяльності, Львів

У роботі описано концепцію програмного забезпечення для збору та обробки даних про багатоповерхові житлові будівлі. Система призначена для обробки первинної інформації, що орієнтована на підтримку прийняття рішень при проведенні рятувальних дій, евакуації мешканців та ліквідації пожежі в багатоповерхових житлових будівлях.

Ключові слова: *програмне забезпечення, мобільний застосунок, облік даних, житловий будинок*

The paper describes the concept of software for data collection and processing of multi-storey residential buildings. The system is designed to process primary information, which is focused on supporting decision-making during rescue operations, evacuation of residents and fire fighting in multi-storey residential buildings.

Keywords: *software*, mobile application, data accounting, residential building

В організації роботи рятувальних підрозділів з метою підтримки прийняття ефективних рішень в процесі гасіння пожеж важливу роль відіграють плани та картки пожежогасіння. Це затверджені документи, що містять інформацію про об'єкт, яка може бути корисною для керівника гасіння пожежі в процесі прийняття управлінських рішень. Проте означені документи ведуться та обліковуються здебільшого до промислових об'єктів, об'єктів з масовим перебуванням людей, навчальних закладів тощо. Поза увагою подібного роду документації є багатоквартирні житлові будинки (окрім висотних). А як показує статистика, частка пожеж у житловому секторі складає близько 60% від загальної кількості пожеж. Зважаючи на це виникає потреба ведення обліку інформації про об'єкти житлового сектора, що може бути корисною під час гасіння пожеж та ліквідації інших надзвичайних ситуацій.

Звичайно інформація про місця відключення інженерних мереж, чи кількість людей в будинку можливо отримати під час проведення розвідки, проте час витрачений на отримання інформації від жителів у подібний спосіб може відігравати важливу роль у порятунку життя людей. Слід зважати, що отримані дані в ході ліквідації пожежі можуть бути не достовірними, що може мати фатальні наслідки як для людей так і рятувальників. Саме тому в роботі запропонована концепція збору та обробки даних для підтримки прийняття рішень під час ліквідації пожеж в житлових будинках.

Вирішення поставленого завдання розділено на декілька етапів. Перший етап – це формування переліку даних про об'єкт, які потрібні рятувальникам для успішного проведення рятувальних робіт. За консультаційної допомоги відповідних фахівців сформовано перелік даних, якими бажано володіти в холі ліквідації пожежі або інших надзвичайних ситуацій в багатоквартирному житловому будинку:

- кількість жителів під'їзду (будинку);
- кількість та місце знаходження людей, які не здатні самостійно покинути будівлю;
- місце розташування первинних засобів пожежогасіння;
- місце знеструмлення будівлі;
- місце перекриття газопостачання (або інших інженерних мереж);
- план евакуації з будівлі (поверховий план);
- наявність сухотрубів;
- місце розташування найближчих джерел протипожежного водопостачання.

Для обліку, зберігання та швидкого доступу до даних виникає потреба розробки відповідної системи. Концепція системи передбачає її реалізацію за клієнт-серверною архітектурою. Клієнтська частина буде реалізована у вигляді мобільного застосунку із вбудованою функцією сканування QR-коду. Відповідні QR-коди пропонується розміщувати на вхідних дверях до під'їзду. При прибутті рятувальних підрозділів на місце виклику, доступ до необхідних даних можливо буде здійснювати за допомогою пропонованого мобільного застосунку. Отримана з бази даних інформація у відповідності до пошукового запиту міститиме усі перелічені вище дані та дозволятиме рятувальним підрозділамх швидко та ефективно проводити невідкладні роботи.

Наповнення бази даними пропонується здійснювати відповідальними особами рятувальних підрозділів в районі обслуговування яких перебуває об'єкт. Дані надаватимуться представниками об'єднання співвласників багатоквартирних будинків або управляючих компаній (комунальних підприємств). Для реалізації цього задуму передбачено створення CRM-підсистеми із WEB-інтерфейсом, основне призначення якої націлено на створення об'єкту в базі даних та наповнення необхідною інформацією в ручному режимі.

Із програмної сторони це буде виглядати наступним чином. Android застосунок із передбаченим функціоналом сканування QR-коду здійснює запит до бази даних за ID відповідного об'єкту. Серверна частина опрацювавши запит надсилає на клієнтську сторону упорядковану інформацію, яка відображатиметься на інтерфейсі мобільного пристрою. Для реалізації системи буде використано кросплатформену технологію Java та PostgreSQL.

На рисунку 1 зображено відношення акторів та системи між собою.

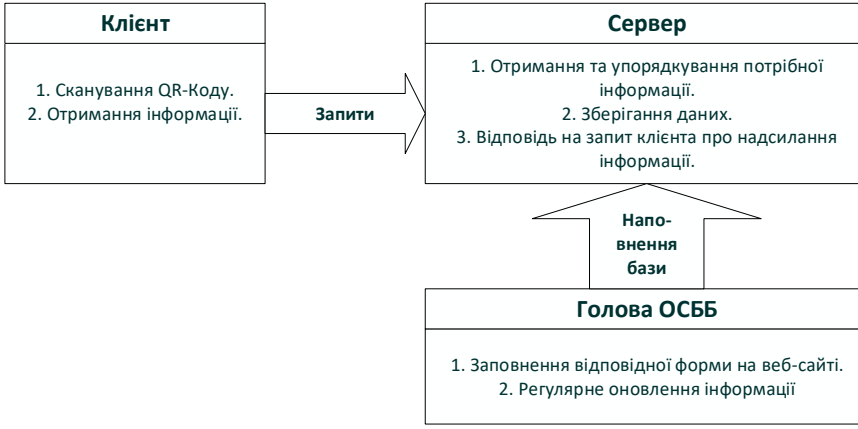


Рис. 1 Схема взаємозв'язків та відношень в системі

Після реалізації буде проведено тестування системи та усунення всіх недоліків, які будуть виявлені під час роботи.

Останньою частиною стане впровадження системи в структурні підрозділи ДСНС України.

Для кращого розуміння процесом користування системи необхідно приділити достатньо уваги естетичності та максимальної простоти інтерфейсу. Також буде розроблено презентацію із покроковою інструкцією-поясненням щодо використання додатку, з метою його успішного запуску та використання в територіальних управліннях Державної служби України з надзвичайних ситуацій.

Література

1. Гріффітс Девід, Гріффітс Дон Г58 Head First. Програмування для Android. 2-ге вид. – СПб.: Пітер, 2018. – 912 с.: іл. – (Серія "Head First O'Reilly").

2. The Busy Coder's Guide to Android Development by Mark L. Murphy

3. Android. Програмування для професіоналів 3-тє вид. – СПб.: Пітер, 2017. – 688 с.: іл. – (Серія «Для професіоналів»).

УДК [004.42+005.6]:378.1

ДОСВІД РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНО-ДОВІДКОВОЇ СИСТЕМИ "UNIBELL" В РАМКАХ РЕАЛІЗАЦІЇ СТУДЕНТСЬКИХ R&D ПРОЄКТІВ

Дзень В., Гулковський М., Придатко О.
Львівський державний університет безпеки життєдіяльності, Львів

Анотація. *У роботі описано функціональну частину та особливості застсоування розробленої інформаційно-довідкової системи віддаленого доступу до навчального розкладу. Описано особливості інтеграції додатку до існуючої системи управління навчальним закладом.*
Ключові слова. *Розклад, мобільний додаток, клієнт-серверний застосунок*

Abstract. *The paper describes the functional part and features of the application of the developed information and reference system of remote access to the training schedule. Features of integration of the application into the existing management system of the educational institution are described.*
Keywords. *Schedule, mobile application, client-server application*

В рамках реалізації студентських R&D проєктів у Львівському державному університеті безпеки життєдіяльності реалізується низка сервісів та інформаційних систем [1, 2]. Зокрема, в організацію освітнього процесу успішно інтегрована адаптивна інформаційно-довідкова система «Unibell» [3]. Система розроблена за клієнт-серверною архітектурою [4] та призначена для автоматичного надсилання і обробки запитів щодо навчального розкладу при вході в систему. Запити формуються системою автоматично залежно від способу реєстрації. Процес реєстрації передбачає вхід в систему науково-педагогічним працівникам та здобувачам освіти. В залежності від аутентифікованої особи, запити щодо навчального розкладу формуються автоматично для відповідної категорії користувачів та миттєво відображаються клієнтською частиною застосунку.

Крім автоматичного формування пошукових розпоряджень для авторизованого користувача, інформаційно-пошукова система «UniBell» наділена опцією персоналізованого пошуку, яка також працює на рівні «клієнт-сервер». За умови використання цього інструменту будь якому користувачеві стає доступний пошук інформації щодо розкладу занять за прізвищем викладача, навчальною групою або аудиторією. Ця процедура вимагає ручного формування пошукового запиту: викладач → прізвище → дата; група → шифр → дата; аудиторія → номер → дата. Особливістю меню пошуку є можливість вибору діапазону дат для аналізу шуканої інформації у певному часовому проміжку. За описаної процедури кожне пошукове розпорядження формується та обробляється як індивідуальний запит.

Розроблена система також передбачає формування пошукових запитів за допомогою сканера QR-коду. Кожній аудиторії закладу освіти присвоєно індивідуальний QR-код, який можливо відсканувати за допомогою інтегрованої функції сканування. Запит порівнюється із пошуковим образом у базі даних в режимі реального часу та повертає до клієнтської частини дані щодо заняття, навчальної групи та викладача в аудиторії.

Серверна частина призначена для зберігання, пошуку та обробки інформації щодо навчального розкладу закладу освіти. Додатковий функціонал серверної частини передбачає підтримку працездатності системи через реалізовану CRM-підсистему. Ця підсистема надає віддалений доступ до бази даних навчального розкладу із можливістю коригування даних та внесення змін.

Важливим компонентом розробленого додатку є його інтеграція до системи обліку навчального навантаження та управління роботою закладу освіти «Політек-софт» [5]. Дві системи адаптовані таким чином, що оновлення бази даних розкладу проводиться автоматичного раз на добу. За потреби періодичність синхронізації може змінюватись. За необхідності проведення змін в навчальному розкладі, який відображається системою «Unibell», передбачено механізм внесення правок до вже існуючого розкладу навчальних занять за допомогою CRM-підсистеми (рис.2).

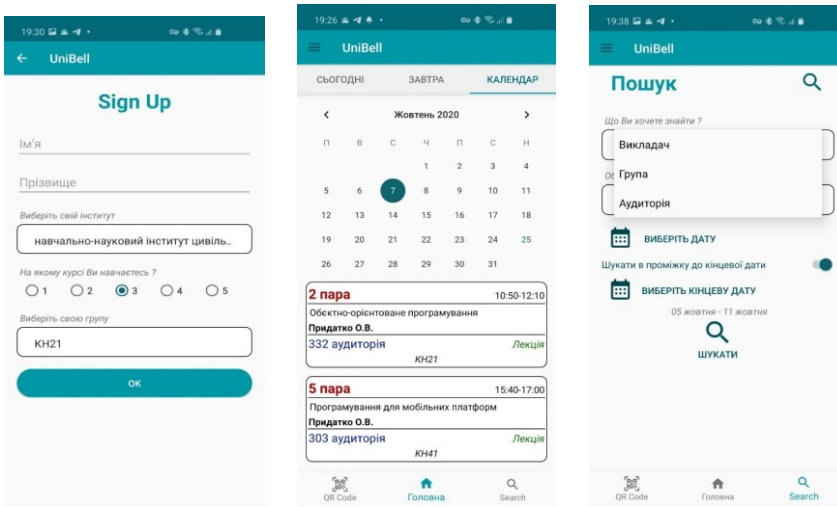


Рис. 1. Клієнтська частина системи «Unibell»

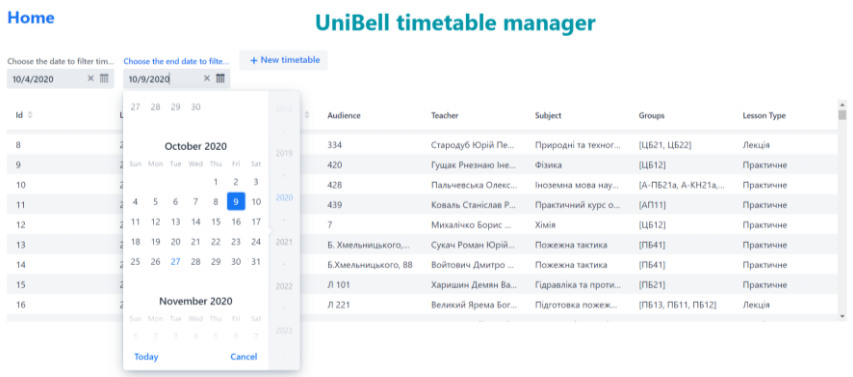


Рис. 2. CRM підсистема «Unibell»

Висновки. На основі розроблених архітектурних рішень програмної системи та з використанням технологій Java і мови структурованих запитів SQL розроблено систему віддаленого доступу до бази даних навчального розкладу Львівського державного університету безпеки життєдіяльності, що відповідає концепції діджиталізації закладу освіти.

Література

1. Malets, I., Popovych, V., Prydatko, O., Dominik, A. (2018). Interactive Computer Simulators in Rescuer Training and Research of their Optimal Use Indicator. 2018 IEEE Second International Conference on Data Stream Mining & Processing (DSMP), 2, 558-562. https://doi.org/10.1109/DSMP.2018.8478486

2. Prydatko, O., Prydatko, V., Borzov, Yu., & Dzen V. (2018). Integration of the new method of mobile education in educational projects of programmer training. Bulletin of Lviv State University of Life Safety, 18, 71-80. https://doi.org/0.32447/20784643.18.2018.07

3. Придатко О. В., Бурак Н. Є., Дзень В. Є., Кунинець М. С. Адаптивна інформаційно-довідкова система "UniBell" як складова частина проєкту "Smart-університет". Науковий вісник НЛТУ України. 2020, т. 30, № 5. С. 105–113. https://doi.org/10.36930/40300518

4. Дзень В. Архітектура інформаційно-довідкової системи "UNIBELL" / В. Дзень, М. Кунинець, О. Придатко // Інформайна безпека та інформаційні технології : збірних тез доповідей IV Всеукраїнської науково-практичної конференції молодих вчених, курсантів та студентів 27 листопада 2020 року. – Львів, ЛДУ БЖД, 2020. – С.167-169.

5. Програмне забезпечення для вищих навчальних закладів України «Політек-Софт» [Електронний ресурс] – режим доступу: http://www.politek-soft.kiev.ua/

УДК 004.932

ЗАСТОСУВАННЯ ДОВГОТРИВАЛОЇ КОРОТКОЧАСНОЇ ПАМ'ЯТІ В НЕЙРОМЕРЕЖНИХ МЕТОДАХ РОЗБЛЮРЕННЯ ЗОБРАЖЕНЬ

Дунаєв Р., Павлюк О.
Національний університет «Львівська політехніка», Львів

Науково-технічний прогрес не спадає і з кожним роком можна побачити мобільні телефони з все більшою і більшою пам'яттю та знімками з більшою роздільною здатністю. Та не завжди вдається зняти весь матеріал, від початку і до кінця, використовуючи штатив чи інші кріплення. На зйомку впливають різноманітні природні фактори: вітер, тремор рук, шуми, так і не природні – стиснення файлів. Використання графічних редакторів все сильніше інтегрується в повсякденне використання. Щоб отримати з спотвореного зображення очікуване застосовують машинне навчання.

За допомогою бібліотеки TensorFlow створені чотири нейронні мережі. Перша мережа натренована на кольорових зображеннях, друга - на чорнобілих. Третя і четверта мережа використовує послідовність кольорових та відповідно чорнобілих кадрів зображень з відеопотоку та комірки довго короткотривалої пам'яті. Датасет зображень поділений на 5 груп. Для кожної мережі визначено функції втрат. Навчальна вибірка для кожної мережі складає 50% усіх зображень. По результатах дослідження доведено зв'язок між включенням в нейромережу комірок довго короткотривалої пам'яті та часу навчання мережі.

Ключові слова:*довга короткочасна пам'ять; розблюрення; розфокусування; Tensorflow; PHM.*

Scientific and technological progress is not slowing down and every year we can see mobile phones with more and more memory and pictures with higher resolution. But, it is not always possible to take a video of all the material, from start to finish, using a tripod or other anchorage. The shooting is influenced by various natural factors: wind, hand tremors, noise, and non-natural - file compression. The use of graphic editors is increasingly integrated into everyday use. To get the distorted image expected use machine learning.

Four neural networks have been created using the TensorFlow library. The first network is trained on color images, the second - on grayscale photo. The third and fourth networks use a sequence of color and, respectively, grayscale frames of images from the video stream and enable long-term memory. Dataset of images divided into 5 groups. Loss functions are defined for each network. The training sample for each network is 50% of all images. According to the results of the research, the connection between the inclusion of long-term memory cells and the network training hours was proved.

Keywords: *long short-term memory; deblur; defocus; Tensorflow; RNN.*

В сучасному світі людина не може обійтися без смартфону. Це дозволило гаджетам тісно інтегруватися в різні сфери життя. Під час роботи, на презентаціях, зображують фотографії. Відпочиваючи – робимо "селфі". Та, незважаючи на розумні програми за інстальовані в смартфон, на якість фотографій впливають непередбачувані фактори. Найчастішими є відсутність стабілізації під час зйомки, спричинена різним факторами: струшу-

вання телефоном внаслідок тремтіння рук; рухами самого об'єкта який знімають, різкою зміною рівнем освітлення та інше. Не завжди є можливість перезнімати фото, та перетворювати процес зйомки в "міні фотосесію". Отже, необхідно усувати розмитість та розфокусовку (розблюреність) отриманих зображень [1].

Існують різні шляхи подолання блюру в зображеннях [2]. Найпопулярніші методи – це використання машинного навчання та послідовності фільтрів. Найбільш популярними є використання штучних нейронних мереж (ШНМ). Їх застосовують в усіх маніпуляціях з зображеннями - від розпізнавання емоцій до виділення областей об'єктів. Серед різновиду ШНМ, які найчастіше використовують для розв'язку поставленого завдання є нейронні мережі прямого поширення, де сигнали поширюються в одному напрямку. Більш потужнішими є рекурентні нейромережі (RNN).

Наявність зворотного зв'язку дозволяє передавати інформацію від одного кроку мережі до іншого. Рекурентні нейронні мережі використовують свою внутрішню пам'ять для обробки послідовностей які подаються на входи. На відміну від нейромережпрямого поширення де сигнали рухаються лише в один бік, від входу до виходу і не мають зворотного зв'язку [3]. У них вихід будь-якого прошарку не відповідає самому значенню шару. Така ШНМ дозволяє сигналам рухатися в обох напрямках.

Мережі зворотного зв'язку є потужними і динамічними. Вони можуть опрацьовувати складні дані, які нелінійно залежать від багатьох факторів. Її стани постійно змінюються, поки не досягнуть точки рівноваги. За останні кілька років рекурентні нейронні мережі з неймовірним успіхом застосували до цілого ряду завдань: розпізнавання мови, мовне моделювання, переклад [4].

Для покращення якості зображень використано динамічну мережу зворотного зв'язку. Вона здатна відтворити частини зображення які на неї подавали. Основною перевагою такого типу нейромереж є ітераційність та динамічність обробки даних, що позитивно впливає на навантаження обчислень. Тому, обрано для покращення якості розблюрених та нечітких зображень рекурентні нейронні мережі.

Розроблена модель нейромережі складається з 5 рівнів та використовує згорткову нейронну мережу. Згорткова нейронна мережа (convolutional neural network, CNN) – це нейронна мережа прямого поширення, яка застосовується до аналізу візуальних зображень, вимагає використання мінімального обсягу попередньої обробки, є просторово інваріантною.

Проаналізувавши значну кількість бібліотек [5] та програм для роботи з зображеннями [6] можна зробити такі висновки. Більшість з них є написані на мові програмування Python. Розробники тестуютьсвої програми на великих массивах даних, тому важливо оприділити обсяг даних, щоб отримати приблизні часові рамки для майбутнього навчання. Для полегшення майбутної перевірки програми і отримання навченої мережі зосередженої на більш окремий тип об'єктів на зображені, виділяють окремі категорії зображень.

Дані які отримані із загальнодоступних джерел використовувалися для навчання. Оскільки використано різні архіви зображень, то виникла необхідність у поділі на 5 категорій: ”будинки”- 10%, ”машини” – 10%, ”парки” – 25%, ”натов плюдей” – 35%, ”магазини” – 20%. Відсотки вираховують від кількості усіх зображень. Набір даних містить невеликий розмір і нестворює довготривалі затримки при завантаженні наступного блоку зображень. Тестова вибірка для навчання становила ½ усіх зображень, і є достатньою.

Результи функції втрат нейромережі при навчанні зображені на рис. 1. Графічне представлення реалізовано за допомогою пакету TensorBoard UI.

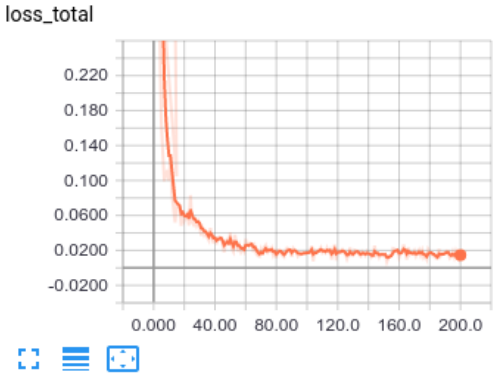


Рис. 1. Функція втрат нейромережі

Через використання довготривалої короткочасної пам’яті навчання мережі відбувалося 4 рази для: кольорових і чорнобілих зображень, та з і без включення довготривалої короткочасної пам’яті. Кількість ітерацій нейронної мережі для кольорових зображень без ви користування lstm203, та з використуваням lstm262, для чорнобілих без використання - 317 , та з lstm–436 ітерацій для однакового часу навчання 5 годин.

Проведено огляд проблеми використання інформаційних технологій для розблюрення зображень. Проаналізовано попередні дослідження, які показали, що використання додаткових методів в нейронній мережі може не тільки впливати на складність мережі, а й на такі параметри як якість і час навчання. Дослідження показали зв’язок між використанням довготривалої короткочасної пам’яті та мережі без неї вкількостях епох для навчанні мережі при досягненні однакових результатів. Цей вплив можна оцінити використовуючи бібліотеку TensorFlowUI. Отже, ефективність застосування інформаційних технологій для розблюрення фотографій була підтверджена.

Література

1. Wu, Y., Hong, C., Zhang, X., He, Y. Stack-based Scale-recurrent Network for Face Image Deblurring, Neural Processing Letters 53(6), pages 4419-4436, 2021.

2. Gampala, V., Kumar, M., Sushama, C., Sehar, E., Raj, F.I. Deep learning based image processing approaches for image deblurring, 2020, MaterTodayProc, pp. 601-609.

3. Abroyan, N. Convolutional and recurrent neural networks forreal-timed atac lassification, 7th International Conference on Innovative Computing Technology, INTECH 20178102422, pp. 42-45

4. G. Saon, Z. Tuske, K. Audhkhasi, and B. Kingsbury, "Sequence ¨ noise injected training for end-to-end speech recognition," in 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2019, pp. 6261–6265.

5. Martín Abadi, Ashish Agarwal, Paul Barham, Eugene Brevdo, Zhifeng Chen, Craig Citro, Greg S. Corrado, Andy Davis, Jeffrey Dean, Matthieu Devin, Sanjay Ghemawat, Ian Goodfellow, Andrew Harp, Geoffrey Irving, Michael Isard, YangqingJia, RafalJozefowicz, Lukasz Kaiser, ManjunathKudlur, Josh Levenberg, Dan Mané, RajatMonga, Sherry Moore, Derek Murray, Chris Olah, Mike Schuster, Jonathon Shlens, Benoit Steiner, Ilya Sutskever, Kunal-Talwar, Paul Tucker, Vincent Vanhoucke, Vijay Vasudevan, Fernanda Viégas, 10 Oriol Vinyals, Pete Warden, Martin Wattenberg, Martin Wicke, Yuan Yu, and Xiaoqiang Zheng.TensorFlow: Large-scale machine learning on heterogeneous systems, 2015.

6. Adam Paszke, Sam Gross, Francisco Massa, Adam Lerer, James Bradbury, Gregory Chanan, Trevor Killeen, Zeming Lin, Natalia Gimelshein, Luca Antiga, etal. Pytorch: Animperative style, high-performance deep learning library. In Advance sinneural information processing systems, pages 8026–8037, 2019

УДК 614.841

ОЦІНЮВАННЯ ТА ВІЗУАЛІЗАЦІЯ ІНДИВІДУАЛЬНИХ ПОЖЕЖНИХ РИЗИКІВ У ГОТЕЛЯХ

Ємельяненко С., Коваль Р., Безнос Н., Кушпа С.
Львівський державний університет безпеки життєдіяльності, м. Львів

Розкриваються питання використання методів та засобів оцінювання індивідуального пожежного ризику у готелях. За допомогою запропонованої шкали оцінювання індивідуального пожежного ризику можна будувати карту ризиків для візуалізації пожежних ризиків для готелів використовуючи геоінформаційні системи.

Ключові слова: *пожежний ризик, готель, матеріальні збитки, карта ризиків, геоінформаційні системи*

The issues of using methods and means of assessing individual fire risk in hotels are revealed. With the help of the proposed scale of individual fire risk assessment, you can build a risk map to visualize fire risks for hotels using geographic information systems.

Keywords: *fire risk, hotel, material damage, risk map, geographic information systems*

Зазвичай пожежі у готелях несуть значні матеріальні збитки, а останнім часом, як показує статистика, і людські втрати. В готельних господарствах важливе значення має забезпечення захисту будівлі, приміщень і людей від пожежі. Тому питання оцінювання індивідуальних пожежних ризиків на теперішній час є актуальним.

Готелі належать до об'єктів із масовим перебуванням людей, тому питання їх пожежної безпеки повинні стояти на першому місці. Це передбачає насамперед правильне проектування будівель, забезпечення їх надійним інженерним обладнанням, електропостачанням, системами зв'язку та сигналізації, шляхами евакуації тощо. Для оцінювання небезпек у готелях використано ризик-орієнтований підхід.

Ризик – це імовірнісна величина, яка дозволяє оцінити та усвідомити небажані події, що можуть виникнути. [2].

Метою роботи є оцінювання індивідуального пожежного ризику у готелях.

Об'єкт досліджень – індивідуальні пожежні ризикі у готелях.

Предмет дослідження – чинники впливу на пожежні ризики в готелях.

Методи дослідження: В роботі використано комплексний метод досліджень, який включає в себе: аналіз та узагальнення наукових досягнень в сфері пожежної безпеки, застосування та оброблення статистичних даних; застосування як аналітичних методів досліджень шляхом збору, узагальнення та аналізування чинних нормативних документів ДСНС України та статистичні, методи теорії ймовірностей, геопросторові, математичне моделювання, методи системного аналізу.

Оцінювання індивідуальних пожежних ризиків

Для оцінювання індивідуального пожежного ризику для готелів використано метод «Визначення рівня пожежної безпеки людей та індивідуального пожежного ризику» згідно ДСТУ 88.28:2019 «Пожежна безпека. Загальні положення».

Для оцінювання часу блокування евакуаційних шляхів використано програму PyroSim [4], яка дозволяє провести дослідження з урахуванням впливу небезпечних чинників пожежі та визначити час блокування евакуаційних шляхів. Ця програма містить користувацький графічний інтерфейс для моделювання динаміки развитку небезпечних чинників пожежі польовим методом на основі Fire Dynamics Simulator (FDS) [5].

Отримані розрахункові значення індивідуального пожежного ризику у готелі запропоновано оцінювати за загальноприйнятою шкалою Всесвітньої організації охорони здоров'я та основними кольоровими кодами і рівнями тяжкості, встановленими ДСТУ ISO 22324:2017 (ISO 22324:2015, IDT) «Соціальна безпека. Управління у надзвичайних ситуаціях. Методичні рекомендації щодо кольорового кодування попереджень про небезпеку» (табл. 1).

Таблиця 1

Шкала оцінювання індивідуального пожежного ризику для готелів

Колір [8]	Значення	Пропоновані дії	Рівень ризику [3, 6-8]
Червоний	Небезпека	Негайно прийняти заходи безпеки	Неприйнятний ризик $\geq 5 \cdot 10^{-4}$
Помаранчевий	Дуже обережно	Виконати відповідні дії з заходів безпеки	Високий ризик $5 \cdot 10^{-5} \div 5 \cdot 10^{-4}$
Жовтий	Обережно	Підготувати відповідні дії з заходів безпеки	Прийнятний ризик $10^{-6} \div 5 \cdot 10^{-5}$
Зелений	Безпека	Не вимагається ніяких дій	Незначний ризик $\leq 10^{-6}$

Висновки:

За допомогою шкали оцінювання індивідуального пожежного ризику можна будувати карту ризиків для візуалізації пожежних ризиків для готелів використовуючи геоінформаційні системи.

Особлива увага повинна приділятися питанням безпеки, удосконаленню систем запобігання пожежам та протипожежного захисту у готелях.

Відсутність належного нормативно-правового, фінансового, матеріально-технічного забезпечення призводить до відсутності належного рівня захисту.

Література

1. Концепція управління ризиками надзвичайних ситуацій техногенного і природного характеру [Електронний ресурс]. – Режим доступу: http://www.mns.gov.ua/content/education_kurns.html

2. Ковалевич О. М. К вопросу об определении "степени риска" / О. М. Ковалевич // Весник НТЦ ЯРБ Госатомнадзора России. – 2001. Вып. № 1. – С. 41-47.

3. Брушлинский Н. Н. Пожарные риски. Основные понятия / Н. Н. Брушлинский, Ю. М. Глуховенко, В. Б. Коробко. – М. : Бюлетень Национальной Академии Наук пожарной безопасности, 2004. – 47с.

4. Sitis Руководство пользователя [Електронний ресурс]. – Режим доступу : http://sitis.ru/media/documentation/PRS-RP-2012-1.pdf

5. Програма FDS (Fire Dynamics Simulator) [Електронний ресурс]. – Режим доступа : http://fds.sitis.ru/docs/FDS_5_User_Guide.pdf

6. Guidance Document for Incorporating Risk Concepts into NFPA Codes and Standards / prepared by: Susan Rose, Stephanie Flamberg, Fred Leverenz. – Massachusetts, 2007. – 125 p.

7. Jonkman S. N. An overview of quantitative risk measures for loss of life and economic damage / S. N. Jonkman, P.H.A.J.M. van Gelder, J. K. Vrijling // Journal of Hazardous Materials. – 2002. – A99. – P. 1-30.

8. ДСТУ ISO 22324:2017 (ISO 22324:2015, IDT) Соціальна безпека. Управління у надзвичайних ситуаціях. Методичні рекомендації щодо кольорового кодування попереджень про небезпеку [Електронний ресурс]. Закон від 28.06.1996 № 254к/96-ВР / Верховна Рада України. – Режим доступу : https://en.wikipedia.org/wiki/ISO_22324#cite_ref-2.

УДК 004.021

ЕТАПИ РОЗРОБКИ ПАРАЛЕЛЬНИХ АЛГОРИТМІВ

Жолубак Л.І., Бурак Н.Є.
Львівський державний університет безпеки життєдіяльності, м. Львів

У роботі розглянуто основні етапи розробки паралельних алгоритмів. Розв'язування задач за допомогою паралельних алгоритмів.
Ключові слова: *паралельна обробка даних, алгоритм, міжпроцесорний обмін, топологія.*

The main stages of development of parallel algorithms are considered in the work. Solve problems using parallel algorithms.
Keywords: *parallel data processing, algorithm, interprocessor exchange, multiprocessor system, topology.*

Поняття *паралельного алгоритму* (Parallel Algorithm) відноситься до фундаментальних в теорії обчислювальних систем. Це поняття, перш за все, асоціюється з обчислювальними системами з масовим паралелізмом. Паралельний алгоритм - це опис процесу обробки інформації, орієнтований на реалізацію в колективі обчислювачів. Такий алгоритм, на відміну від послідовного, передбачає одночасне виконання множини операцій в межах одного кроку обчислень і як послідовний алгоритм зберігає залежність подальших етапів від результатів попередніх.

Паралельний алгоритм рішення задачі складає основу паралельної програми. Паралельна програма у свою чергу, впливає на алгоритм функціонування колективу обчислювачів. Запис паралельного алгоритму на мові програмування, доступній колективу обчислювачів, називають паралельною програмою. Паралельні алгоритми і програми слід розробляти для складних або трудомістких завдань.

Вважатимемо, що відомо традиційний (послідовний) спосіб розв'язання деякої задачі і далі необхідно організувати її виконання з використанням паралельної обробки даних.

Загальна схема розробки паралельного алгоритму містить такі етапи:

– виконання декомпозиції задачі на складові частини одним із відомих способів;

– виявлення інформаційних залежностей;

– масштабування складових частин задачі;

– розподіл складових частин задачі між процесорами (ядрами).

Етап декомпозиції є першим етапом розробки паралельного алгоритму. Суть найвідоміших способів декомпозиції вже було детально розглянуто. Проблема може полягати у виборі того чи іншого способу.

Дуже часто вже наперед відома архітектура паралельної машини, де буде виконуватись задана обчислювальна задача. В цьому випадку архітектура машини визначатиме найоптимальніший варіант декомпозиції. Звичайно, можна використовувати одночасно декілька способів декомпозиції.

Після розбиття початкової задачі на складові частини виконується аналіз зв'язків між ними, тобто здійснюється ***етап виявлення інформаційних залежностей.*** При цьому необхідно розрізняти такі схеми взаємодії:

– локальні (на сусідніх процесорах) і глобальні (з участю всіх процесорів);

– структурні (відповідають типовим топологіям комунікацій згідно з вибраною на попередньому етапі архітектурою машини) і довільні;

– статичні (задаються на етапі проектування) та динамічні (визначаються під час роботи);

– синхронні (наступна операція виконується після закінчення попередньої всіма процесорами) і асинхронні (без очікування повного завершення всіх дій із передачі даних).

Дві підзадачі A та B вважаються інформаційно залежними, якщо результат виконання підзадачі A використовується як вхідні дані для підзадачі B або навпаки. Підзадачі A та B будуть також інформаційно залежними, якщо їх результати мають бути отримані одночасно для подальшого використання іншими підзадачами.

Етап масштабування складових частин задачі виконується в тому випадку, коли кількість наявних підзадач відрізняється від кількості наявних процесорів (ядер). Тут можливі два основних варіанти.

Якщо кількість k підзадач перевищує кількість n процесорів, то деякі підзадачі необхідно укрупнити, так щоб їх загальна кількість не перевищувала числа n.

Існує навіть спеціальний термін – «зернистість», – який характеризує рівень декомпозиції початкової задачі на окремі підзадачі. Дрібнозернистий паралелізм може оптимально завантажити всі наявні процесори, однак важко аналізувати паралельну програму. При цьому є межа складності підпрограм, коли загальний час виконання програм вже не буде зменшуватись внаслідок зростання числа допоміжних операцій зі створення нових процесів та потоків.

Таким чином, в багатьох випадках необхідний ще один етап розробки паралельних алгоритмів – ***етап розподілу підзадач між процесорами.***

Основний критерій успішності виконання цього етапу – ефективність використання процесорів, яка визначається як відносна частка часу, протягом якого процесори використовувались для обчислень, пов'язаних з виконанням поставленої задачі. Способи досягнення задовільних результатів в цьому напрямку базуються на таких самих принципах, як і в попер-

ніх етапах: рівномірний розподіл обчислювального навантаження процесорів та мінімізація обмінів даних між ними.

Варто відзначити, що вимога мінімізації міжпроцесних обмінів може суперечити умові рівномірного завантаження. Можна розмістити всі підзадачі на одному процесорі і тим самим повністю ліквідувати міжпроцесний обмін, але завантаження процесорів в цьому випадку буде неоптимальним.

Вирішення питань балансування обчислювального навантаження значно ускладнюється, якщо схема обчислень може змінюватись під час розв'язання задачі. Для динамічного керування розподілом обчислювального навантаження часто використовується схема «менеджер– виконавці». Відповідно до такої схеми виділяється окремий процесор (менеджер), якому доступна вся інформація про стан виконання всіх підзадач на інших процесорах (виконавцях). Процесор-менеджер отримує результати виконання підзадач від процесорів-виконавців, формує нові завдання та необхідні ресурси для їх виконання.

Завершення обчислень відбувається тоді, коли процесори-виконавці завершили виконання всіх переданих їм підзадач, а процесор-менеджер не має більше нових завдань.

Отже, паралельні алгоритми досить важливі з огляду на постійне вдосконалення багатопроцесорних систем і збільшення числа ядер у сучасних процесорах. Зазвичай простіше сконструювати комп'ютер з одним швидким процесором, ніж з багатьма повільними з тією ж продуктивністю. Однак збільшення продуктивності за рахунок вдосконалення одного процесора натрапляє на фізичні обмеження, такі як досягнення максимальної щільності елементів та тепловиділення. Зазначені обмеження можна подолати лише шляхом переходу до багатопроцесорної архітектури, що виявляється ефективним навіть у малих обчислювальних системах.

Література

1. Гаврилова Т.А. Онтологический подход к управлению знаниями при разработке корпоративных информационных систем // Новости искусственного интеллекта. – №2, 2003. – С. 24-30.

2. Дорошенко А.Е. Математические модели и методы организации высокопроизводительных вычислений, Киев: Наукова думка, 2000.

3. Немнюгин С.А., Стесик О.Л.Параллельное программирование для многопроцессорных систем. – СПБ. БХВ Петербург, 2002. – 400 с.

4. Цаленко М.Ш. Моделирование семантики в базах данных. – М.: Наука, 1989. –354с..

УДК: 004

ОГЛЯД ХАРАКТЕРИСТИК ОПЕРАЦІЙНИХ СИСТЕМ

Ільків Б., Борзов Ю.
Львівський державний університет безпеки життєдіяльності, м. Львів

У роботі розглянуто поняття операційної системи як базового комплексу програмного забезпечення, що виконує управління апаратним забезпеченням комп'ютера. Розглянуто її різновиди та стан на теперішній час.

Ключові слова: *Операційна система, програмне забезпечення, багатопроцесорні системи.*

This article considers the concept of the operating system as a basic software package that manages the computer hardware. Its varieties and current state are considered.

Key words: *Operating system, software, multiprocessor systems.*

Комп'ютерна система складається з внутрішніх і периферійних пристроїв та програм. Вони взаємодіють між собою і опрацьовують інформацію на комп’ютері. Для забезпечення ефективної взаємодії та функціонування призначена операційна система.

Операційна система – пр.ограми, що здійснюють функціонування комп'ютера і роботу користувача з ресурсами. Обчислювальними ресурсами називаються можливості, затребувані операційною системою, програмою і користувачем і які забезпечуються компонентами обчислювальної системи. ОС забезпечує виконання прикладних програм, розподіл ресурсів комп'ютерної системи, введення, виведення, збереження даних, керування даними, надає інтерфейс взаємодії з користувачем і іншими комп'ютерами та видає повідомлення. Ядро операційної системи, яке є її основною частиною, завантажується в оперативну пам'ять після включення комп'ютера на час роботи і управляє всією операційною системою, пам'яттю, виконанням прикладних програм, їх взаємодією з апаратурою, визначає порядок і час роботи різних програм з процесором. Інша частина операційної системи завантажується в пам'ять в міру необхідності і забезпечує інтерфейс користувача з прикладними програмами.

Функції операційної системи:

- забезпечення автоматичного завантаження ядра ОС в оперативну пам'ять з програмного коду в спеціальній області диска;
- організація файлової системи для зберігання даних на диску, забезпечення доступу до них і можливості обробки;
- завантаження програм в ОП і управління виконанням.

Сучасні ОС багатозадачні. Вони керують розподілом ресурсів комп'ютера між декількома додатками (прикладними програмами,

завданнями) такми чином, що кілька додатків можуть працювати одночасно, спільно використовуючи ресурси та обмінюватися даними між собою.

Коли відкриті кілька програм, то спрацьовує багатозадачний режим: система виділяє пам'ять, обчислювальний ресурс, виконує команди, посилає повідомлення кожному з додатків або користувачеві про стан та можливі помилки.

У багатопроцесорних системах або багатоядерному процесорі програми виконуються паралельно. Операційна система і програми можуть створювати в оперативній пам'яті буфер обміну, або просто буфер, - захищену область тимчасового зберігання даних для виконання копіювання і перенесення між вікнами документів, програм або між програмою і пристроєм вводу і виводу. При запуску кількох великих програм одночасно операційна система організовує на жорсткому диску додаткову віртуальну пам'ять великого обсягу. Для неї на диску створюється спеціальний файл підкачки тимчасового зберігання частини даних в очікуванні їх перекачування в фізичну оперативну пам'ять в міру затребування процесором. Дані, найближчим часом не затребувані, відправляються в файл підкачки.

За використанням операційні системи поділяють на серверні та користувацькі. Серверні операційні системи використовують для роботи серверів, оскільки набір їх можливостей з точки зору адміністрування є набагато ширшим ніж у звичайних користувацьких ОС. Призначенням серверної ОС є керування прикладними програмами та сервісами, що обслуговують користувачів локальної мережі та мережі Інтернет.

Отже, ключовим моментом при виборі операційної системи є апаратне забезпечення, архітектура комп'ютера та перелік функціональних задач, які мають виконуватись комп’ютером.

На персональних комп’ютерах, сумісних з IBM PC, запускаються ОС сімейства Microsoft Windows, Linux, BSD, iOS.

Mac OS — це пропрієтарна (власна, запатентована) операційна система, що розроблена спеціально для використання на комп’ютерах і ноутбуках компанії Apple (iMac, Mac Pro, MacBook та ін.).

Література

1. https://sites.google.com/site/sunlight3555/ponatta-operacijnoie-sistemi-ta-ieie-skladovi
2. Шеховцов В. А. Операційні системи К.; Видавнича група BHV.2005. 17с.
3. https://stud.com.ua/54407/informatika/operatsiyni_sistemi
4. https://uk.wikipedia.org/wiki/Операційна_система

УДК 004.9: 631.1

РОЗРОБКА БАЗИ ДАНИХ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПЛАНУВАННЯ ЗАГОТІВЛІ МОЛОКА

Коваль Н.[1], Киліль С.[2], Тригуба А.[1,2]
[1]Львівський держаний університет безпеки життєдіяльності, м. Львів
[2]Львівський національний аграрний університет, м. Дубляни

Виконаний аналіз наукових праць та предметної галузі. Обґрунтовано доцільність розроблення інформаційної системи планування заготівлі молока та обґрунтування структури бази даних. Запропонована структура бази даних інформаційної системи планування заготівлі молока. Означено зміст таблиць бази даних, які було створено для функціонування інформаційної системи.

Ключові слова: *база даних, інформаційна система, планування, заготівля, молоко.*

The analysis of scientific works and subject branch is executed. The expediency of developing an information system for planning milk procurement and substantiating the structure of the database is substantiated. The structure of the database of the information system of milk procurement planning is proposed. The content of database tables, which were created for the functioning of the information system, is determined.

Key words: *database, information system, planning, procurement, milk.*

У світі на даний час існує багато технологій заготівлі молока та побудови оперативних планів цієї заготівлі. Кожна з країн використовує різні методи реалізації варіантів якісної та регламентованої у часі заготівлі молока. В Україні на жаль поки не існує відповідних систем, або ж існуючі виконують функції, що відрізняються від вимог предметної галузі [1]. Станом на 2021 рік велика кількість громад потребує інформаційної системи, яка буде враховувати особливості їх виробничих умов, наявні ресурси та виконувати планування автоматизовано.

У даній роботі увага приділяється створенню такої інформаційної системи, яка буде допомагати господарствам та населенню у найшвидші терміни заготовити молоко-сировину. Також важливими критеріями були своєчасне отримання інформації про можливі обсяги заготівлі для її наступної обробки, отримувати та аналізувати статистику таких надходжень. Розробка бази даних у запропонованій інформаційній системі планування заготівлі молока є однією із головних задач її створення.

Для того, щоб інформаційна система функціонувала в повному масштабі, для неї необхідна структурована база даних, котра буде зберігати та надавати інформацію для працездатності інформаційної системи. Запропонована структура бази даних (рис.) включає в себе опис змісту, структури і обмежень цілісності, що використовуються для створення і підтримки бази даних.

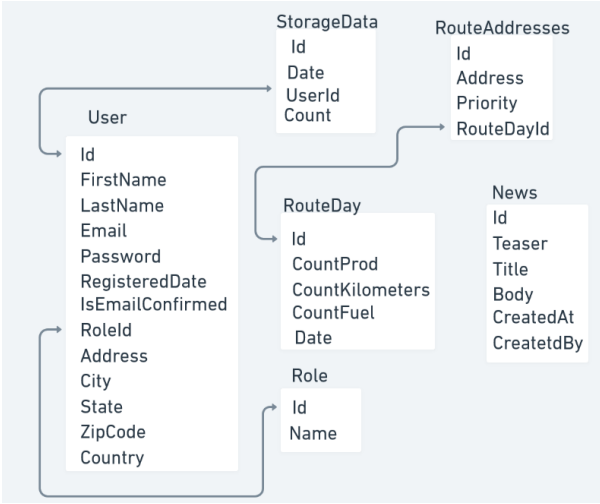


Рис. Структура бази даних інформаційної системи

Загальна структура бази даних інформаційної системи для формування оперативних планів заготівлі молока складається з 6 таблиць, характеристика яких подана нижче.

1. ***User*** – містить інформацію про зареєстрованих користувачів:

- ✓ *Id* – унікальний ідентифікатор об'єкту (первинний ключ);
- ✓ *FirstName* – ім'я користувача;
- ✓ *LastName* – прізвище користувача;
- ✓ *Email* – електронна скринька користувача (використовується для входу в систему);
- ✓ *Password* – хешований пароль користувача (використовується для входу в систему);
- ✓ *RegisterDate* – дата реєстрації користувача в системі;
- ✓ *IsEmailConfirmed* – чи підтверджено електронну скриньку (потрібно для активації аккаунту в системі);
- ✓ *RoleId* – роль користувача в системі (User or Admin, зовнішній ключ);
- ✓ *Address* – вулиця з номером будинку/квартири;
- ✓ *City* – місто\село користувача;
- ✓ *State* – область користувача;
- ✓ ZipCode – поштовий індекс користувача;
- ✓ *Country* – країна користувача.

2. ***Role*** – містить дані про ролі користувачів на сайті:
- ✓ *Id* – унікальний ідентифікатор об'єкту (первинний ключ);
- ✓ *Name* – назва ролі.

3. ***StorageData*** – містить дані про внесену кількість продукції користувачів:
- ✓ *Id* – унікальний ідентифікатор об'єкту (первинний ключ);
- ✓ *Date* – дата, коли було внесено дані;
- ✓ *Count* – кількість продукції, яку можу надати;
- ✓ *UserId* – ID коритсувача (зовнішній ключ).

4. ***RouteDay*** – містить інформацію про маршрути заготівлі:
- ✓ *Id* – унікальний ідентифікатор об'єкту (первинний ключ);
- ✓ *CountProd* – загальна кількість наданої продукції за цим маршрутом та днем;
- ✓ *CountKilometers* – загальна дальність маршруту для вибраного дня та маршруту;
- ✓ *Date* – дата, в який день було складено маршрут.

5. ***RoutesAddresses*** – адреси для шляхів:
- ✓ *Id* – унікальний ідентифікатор об'єкту (первинний ключ);
- ✓ *Address* – адреса, за якою буде здійснено забір продукції;
- ✓ *Priority* – номер адреси по порядку забору;
- ✓ *RouteDayId* – ID оперативного плану (зовнішній ключ).

6. ***News*** – новини від інформаційної системи та громади яка її використовує:
- ✓ *Id* – унікальний ідентифікатор об'єкту (первинний ключ);
- ✓ *Teaser* – картинка, тизер для новини;
- ✓ *Title* – титулка, назва новини;
- ✓ *Body* – тіло новини;
- ✓ *CreatedAt* – дата, коли створено новину;
- ✓ *CreatedBy* – ким створено новину.

Схематичне зображення таблиць бази даних, які було створено для функціонування інформаційної системи, зображено на рис.

Література

1. Тригуба А.М., Шелега О.В., Пукас В.Л., Михайлюк В.М. Узгодження конфігурацій інтегрованих проектів аграрного виробництва. *Вісник Національного технічного університету «ХПІ». Серія : Стратегічне управління, управління портфелями, програмами та проектами*. 2015. 2. С. 135-140. Режим доступу: http://nbuv.gov.ua/UJRN/vntux_ctr_2015_2_27. (Last accessed: 12.05.2021).

УДК 004.413

ОБҐРУНТУВАННЯ РОЗПОДІЛУ ПРІОРІТЕТІВ РОЗРОБКИ ПРОГРАМНОГО ПРОДУКТУ У ДИНАМІЧНОМУ ОТОЧЕННІ

Кордунова Ю., Придатко О., Смотр О.
Львівський державний університет безпеки життєдіяльності, м. Львів

У роботі описано основні фактори, які впливають на пріоритезацію завдань у беклозі Agile команди. Розв'язано задачу вибору пріоритету між завданнями, які мають великий ризик та велику цінність для створення програмного продукту. Зроблено відповідні висновки.

Ключові слова: *програмний продукт, беклог.*

The paper describes the main factors that affect the prioritization of tasks in the Agile backlog. The problem of choosing a priority between tasks that have a high risk and high value for creating a software product is solved. Relevant conclusions have been made.

Keywords: *software product, backlog.*

Відомо, що Беклог Продукту (Product Backlog) — це сформований і впорядкований список усього, що потрібно для того щоб створити та покращити продукт [2]. Іншими словами – це перелік завдань (користувацьких історій, функцій), які необхідно виконати команді розробників під час реалізації проєкту. Завдання у беклозі впорядковуються за пріоритетністю, а відповідальним за розподіл пріоритетів є власник продукту. На даному етапі важливо сформувати пріоритети виконання завдань «за цінністю для бізнесу». Для цього важливо врахувати наступні фактори:

- фінансова цінність впровадження завдання;
- витрати на розробку;
- обсяг і значущість засвоєння нових знань, створених унаслідок розробки завдання;
- обсяг ризику, що ліквідується завдяки розробці завдання.

Першим фактором під час пріоритезації завдань у беклозі є його фінансова цінність. Тобто, скільки грошей заробить чи заощадить замовник, якщо власник продукту включить це завдання у беклог. Для некомерційних проектів оцінити цінність можна за її бажаністю для нових та вже існуючих користувачів, тобто яке задоволення принесе розробка певного функціоналу для кінцевого користувача.

Проте, дуже багато функцій здаються чудовими, поки ми не дізнаємося їхню собівартість. Тому, дуже важливим фактором при визначенні пріоритету завдання є витрати на його розробку. Вони включають в себе як матеріальні, так і часові.

У великої кількості проєктів значна частина загальних зусиль витрачається на придбання нових знань. Даний фактор є важливим, оскільки в Agile-проєктах ми ніколи не знаємо усього, що нам потрібно знати для завершення проєкту. Ринок IT постійно змінюється та удосконалюється, тому учасникам проєкту важливо постійно навчатися і застосовувати ті знання на практиці. А це, в свою чергу, призводить до додаткових витрат та ризиків.

Практично всі Agile-проєкти містять в собі величезний обсяг ризику. В даному контексті під ризиком варто розуміти все, що може статися, поставивши під загрозу або обмеживши успішність продукту. Із проєктами пов'язана низка ризиків, серед яких є ризик зриву графіка, ризик збільшення витрат, ризик функціональності.

Під час розробки нового програмного продукту (ПП) завжди існує протистояння між розробкою функцій із високим ризиком та функцій із високою цінністю. Аби зробити вибір, варто проаналізувати переваги і недоліки кожного підходу.

Рішення полягає у тому, щоб не допустити ані домінування ризику, ані цінності під час визначення пріоритетів задач при розробці продукту. На рисунку 1 зображено координатну площину, яка допоможе нам визначити пріоритети розробки програмного продукту, зважаючи на високий ризик та високу цінність. У 1 четверті координатної площини містяться задачі із високим ризиком та високою цінністю. Ці функції є досить важливими для клієнта, але їх створення несе у собі значний ризик (наприклад – використання нових технологій, написання унікальних алгоритмів). У 4 четверті лежать також важливі для користувача функції, проте менш ризикові, у 3 – завдання, які не несуть високої цінності та і ризики мінімальні, а 2 четверть – це функції, які містять високі ризики, хоч і цінність у них низька.

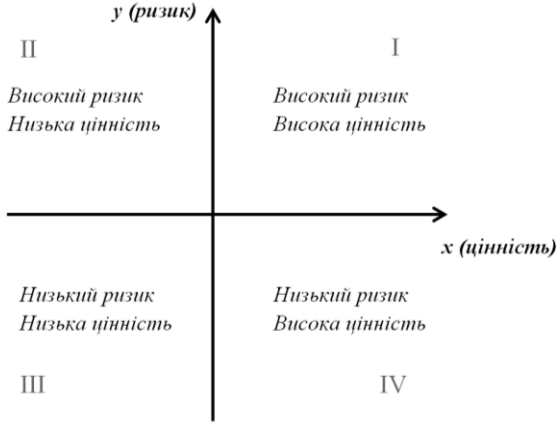


Рисунок 1 – Позначення цінності

Таким чином, логічно розподіляти пріоритети так, як показано на рисунку 2. Найперше потрібно розробляти функції, які лежать у 1 четверті. Ці функції приносять найбільший прибуток, а робота над ними паралельно усуває найбільші ризики. Наступні на черзі – функції з високою цінністю та низьким ризиком. Вони приносять такий же ж прибуток, як і попередні, проте вже з меншим ризиком. Далі йде розробка функцій із низькою цінністю та низьким ризиком. Ними займуться в останню чергу, оскільки вони менше за все впливають на сукупну вартість продукту. А функції із 2 четверті бажано взагалі уникати, оскільки високий ризик може призвести тільки до збільшення витрат на продукт.

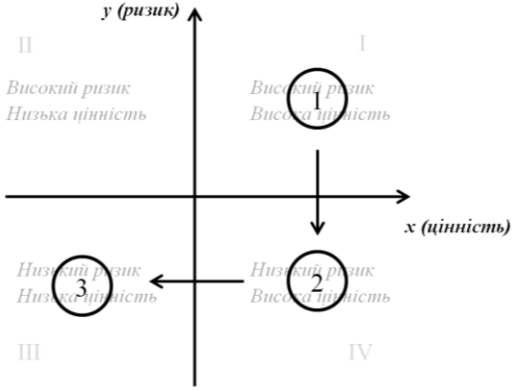


Рисунок 2 – Вирішення задачі, щодо вибору пріоритету

Таким чином, можна зробити висновок, що визначення пріоритетності завдань у беклозі Agile команди є дуже важливим і на нього впливає чимало факторів. Важливо ще перед початком роботи визначити цінність, витрати та ризики, які можуть суттєво повипливати на визначення пріоритету розробки програмного продукту.

Література

1. Agile-маніфест розробки програмного забезпечення [Електронний ресурс] – Режим доступу до ресурсу: https://agilemanifesto.org/iso/uk/manifesto.html.

2. The Scrum Guide [Електронний ресурс] – Режим доступу до ресурсу: https://scrumguides.org/docs/scrumguide/v2020/2020-Scrum-Guide-US.pdf

3. Cole R., Scotcher E. Brilliant Agile Project Management: A Practical Guide to Using Agile, Scrum and Kanban. Edinburg: Pearson, 2015. 187 p.

4. Кордунова Ю. С., Придатко О. В., Смотр О. О. Переваги використання Agile- методології під час розробки програмного забезпечення в умовах сучасного ринку. Інформаційна безпека та інформаційні технології : зб. наук. праць IV Всеукр. наук.-практ. конф. молодих учених, студентів і курсантів. м. Львів 27 листопада 2020 р. Львів, 2020. С. 206-207.

УДК: 681.518

ОГЛЯД ОСОБЛИВОСТЕЙ СУЧАСНОЇ CRM СИСТЕМИ SALESFORCE

Кошелєв М., Бурак Н.
Львівський державний університет безпеки життєдіяльності, Львів

У роботі здійснено огляд CRM системи Salesforce. Проведено аналіз системи управління взаємовідносинами з клієнтами та організація підприємства. Висвітлено основні можливості, переваги та недоліки CRM-системи та Salesforce.

Ключові слова: *CRM, Salesforce, взаємовідносини, бізнес-процеси, автоматизація, управління.*

The paper reviews CRM system of Salesforce. A brief analysis of customer relationship management system and organization of the enterprise.

Keywords: *CRM, Salesforce, relationship, business processes, automation, management.*

Високі темпи конкуренції, перенасичення ринку ідентичними товарами, зростаюча вимогливість споживачів диктують учасникам бізнесу нові умови у боротьбі за клієнтів. Тому в умовах інформаційного суспільства цілком закономірним є застосування сучасних інформаційних технологій, зокрема використання систем автоматизації відносин із клієнтами – CRM (Customer Relationship Management)– "управління взаємовідносинами з клієнтами". Основна мета CRM-системи – створення єдиної екосистеми по залученню нових та розвитку існуючих клієнтів.

Оскільки CRM-система забезпечує швидкий доступ до даних, користувачам стає набагато простіше співпрацювати між собою – як наслідок, підвищується продуктивність та ефективність деяких процесів. Ще один вагомий аргумент на користь CRM-системи полягає в тому, що ця система підходить для компаній будь-якого розміру та будь-якої галузі – банки, агентства нерухомості, транспортні компанії, телекомунікаційні компанії, медичні та державні установи та багатьох інших.

Серед основних можливостей CRM систем доцільно виділити наступні:

1. Управління інформацією про клієнтів. Клієнтська база консолідована, організація отримує повну інформацію про своїх клієнтів та їх вподобання і опираючись на ці дані, будує стратегію взаємодії.

2. Управління продажами. Система зберігає повну історію спілкування з клієнтами, що допомагає департаменту продажів аналізувати поведінку клієнтів, формувати для них відповідні пропозиції, завойовувати лояльність.

3. Автоматизація маркетингу в CRM програмах. CRM-система дозволяє оптимально організовувати управління маркетингом компанії,

проводити маркетингові заходи, управляти ресурсами та бюджетами на маркетинг, координувати маркетингові дії.

4. Автоматизація документообігу. Система передбачає всі необхідні інструменти для управління як зовнішнім, так і внутрішнім документообігом компанії. Ці інструменти надають засоби автоматичного формування документів по шаблону, підготовки друкованих форм документів, підтримки актуальної версії документів, швидкого пошуку документів в системі та багато іншого.

5. Управління бізнес процесами. Розкласти робочі процеси по поличках, формалізувати – нетривіальне завдання, яке вирішується бізнес-аналітиками. Зменшується кількість помилок, робота компанії прискорюється, а результати стають більш прогнозованими.

6. Аналітичні можливості CRM-системи. Система дозволяє компанії отримати статичну інформацію, провести складний аналіз даних, необхідний для прийняття стратегічно важливих бізнес процесів.

Salesforce – це платформа, яка повністю хоститься на серверах компанії Salesforce у хмарному середовищі. Дана система була заснована у 1999 році колишнім виконавчим директором компанії Oracle – Марком Беніоффом. Головна ідея створення – це побудова доступного програмного забезпечення і впровадження його повністю онлайн в якості сервісу. Salesforce уже не перший рік є світовим лідером серед CRM платформ (див. Рис.1.).

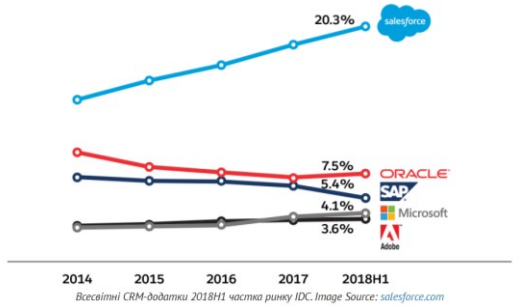


Рис. 1 – Статистика використання CRM систем відомих вендорів

Salesforce є багатокомпонентним рішенням. Окрім CRM-системи ця платформа також містить інструментарій, який дозволяє створювати та розгортати індивідуальні рішення, автоматизувати бізнес-процеси, інтегруватися із зовнішніми додатками. Більшість світових компаній є клієнтами Salesforce. Середи них : Adidas, AWS, Canon, Philips, Toyota, American Express, Cisco і багато інших.

Переваги роботи з Salesforce для розробників:

- Простий початок роботи. Не потрібно встановлювати жодних програм, немає ніяких вимог до обладнання. Розміщення в хмарному середовищі надає швидкий доступ до інформації. Для роботи з Salesforce потрібно мати лише доступ до інтернету.

• Платформа для багатьох користувачів. Усі користувачі мають спільну інфраструктуру та екземпляр програмного забезпечення. Це дає можливість автоматичного та одночасного оновлення для всіх користувачів на платформі.

• Організація навчання. Кожен має можливість створити безкоштовну організацію для навчання, практикування чи тестування. Це фактично повнофункціональне середовище для розробки.

• AppExchange. Salesforce дозволяє розробляти та продавати власні продукти або отримувати доступ до тисяч корисних, захищених та перевірених продуктів чи інтеграцій, створених іншими користувачами.

• Можливість інтеграції з сторонніми системами. Salesforce дає можливість для будь-якої інтеграції, також пропонує багато вбудованих інтеграцій – Heroku, Outlook, Gmail.

Salesforce має багато переваг, але разом з тим існує і низка недоліків:

• Salesforce має досить багато лімітів. До прикладу, за одну транзакцію можна зробити не більше 150 DM.

• Незручний механізм для дебагу коду. Для цього потрібно включити System.debug(‘message’). Тоді можна переглянути лог-файл.

• Статичні змінні «живуть» тільки в межах операції. Apex-змінна «живе» від початку до кінця реквесту, далі вона обнуляється

Отже, на основі проведеного огляду ринку сучасних рішень для ефективної організації бізнес моделей розвитку організацій, встановлено, що значну увагу приділяють використанню сучасних систем управління взаємовідносинами з клієнтами – CRM – системам. Значну популярність серед користувачів таких систем отримала CRM Salesforce, яка є комплексним рішення для якісної організації роботи, управління та контролю за діяльності компанії.

Література

1. Юрчук Н. П. CRM-системи: особливості функціонування та аналіз українського ринку / Н. П. Юрчук // Науковий вісник Ужгородського національного університету. Серія : Міжнародні економічні відносини та світове господарство. - 2019. - Вип. 23(2). - С. 141-147.

2. Що таке Salesforce і чим вона цікава для досвідчених розробників? [Електронний ресурс] – режим доступу до ресурсу - https://dou.ua/lenta/articles/what-salesforce-is/

3. Мозгова Г. В. Використання CRM-систем на українському ринку: особливості та перспективи / Г. В. Мозгова, А. О. Морозов, О. Д. Фомін // Проблеми системного підходу в економіці. - 2017. - Вип. 2. - С. 89-94. - Режим доступу: http://nbuv.gov.ua/UJRN/PSPE_print_2017_2_17

4. Можливості використання CRM-систем / Електронний ресурс. – Режим доступу: https://www.terrasoft.ua

УДК 614.842

КРИЗОВИЙ ЦЕНТР ЦИВІЛЬНОГО ЗАХИСТУ

Кузик А., Ємельяненко С., Безнос Н., Кушпа С.
Львівський державний університет безпеки життєдіяльності, м. Львів

Кризовий центр цивільного захисту створюється для підвищення рівня компетентностей та навиків курсантів, студентів, слухачів практичних працівників сфери цивільного захисту. Для набуття необхідних вмінь при прийнятті управлінських рішень, як у рятувальній справі, так і у планувальній діяльності міста. Для налагодження та відпрацювання взаємодії всіх органів держаної влади та оперативно-рятувальних підрозділів міста, та області у разі виникнення надзвичайної ситуації.

Ключові слова: *кризовий центр, надзвичайна ситуація, аварія, цивільний захист, взаємодія, навчання*

Crisis Center of Civil Protection is created to increase the level of competencies and skills of cadets and students as future specialists of civil defense workers. To acquire the necessary skills in making management decisions, both in rescue work and in the planning activities of the city. To establish and test the interaction of all public authorities and operational and rescue units of the city and region in case of emergency.

Key words: *crisis center, emergency, accident, civil protection, interaction, training*

На сьогоднішній день актуальним питанням стало прийняття управлінських рішень у разі виникнення чи попередження аварій, катастроф та інших НС природнього та техногенного характеру. Зосередження таких технологій потребує систем обробки інформації. Це стосується і менеджменту НС, який здійснюють працівники цивільного захисту. Таку базу даних може містити кризовий центр, тому у Львівському державному університеті безпеки життєдіяльності створюється Кризовий центр цивільного захисту, який може використовуватися для вирішення реальних завдань управління в НС.

Мета Кризового центру цивільного захисту – підвищення рівня компетентностей та навиків у відпрацюванні взаємодії всіх органів держаної влади та оперативно-рятувальних підрозділів міста та області у разі виникнення надзвичайної ситуації. Налагодження взаємодії та порядку залучення відповідних органів управління в умовах виникнення НС, зокрема з практичними працівниками, які безпосередньо входять до складу комісій ТЕБтаНС міста та області, штабу з ліквідації НС.

До основних завдань Кризового центру цивільного захисту належить:

– постійний моніторинг і комплексний аналіз наявних загроз для населення та територій;

- оцінювання ризиків виникнення та прогнозування надзвичайних ситуацій;
- координація дій відповідних відомств під час виникнення ситуацій, та ліквідації їх наслідків;
- вироблення рішень щодо попередження, подолання та мінімізації наслідків надзвичайних ситуацій.

Основні небезпеки, що має охоплювати Кризовий центр цивільного захисту (табл. 1).

Таблиця 1

Основні небезпеки, які охоплює Кризовий центр цивільного захисту

Природнього характеру	**Техногенного характеру**	**Соціального характеру**
Повені, селі	Пожежі, вибухи	Епідемії захворювань людей
Надмірні та швидкі атмосферні опади	Хімічні аварії та забруднення навколишнього середовища	Демонстрації, заворушення
Сильні вітри, урагани	Значні аварії в енергетиці, водопостачанні, газопостачанні та ін.	Тероризм
Епідемії захворювань чи нашестя паразитів, тварин та рослин	Значні аварії (на об'єктах інфраструктури) у телекомунікаційних мережах, зв`язку та ін.	Війна
Різка зміна температури	Значні порушення у роботі транспорту	Масові міграції
Посуха, пожежі	Смог, шум	Інші загрози та аварії…
Густі тумани	Загроза радіаційного випромінювання	
Землетруси, осідання землі, зсуви		

Вирішальне значення, під час масштабних аварій чи катастроф має застосування геоінформаційних технологій на базі геоінформаційних систем.

Проблеми готовності до дій у надзвичайних ситуаціях та реагування на них в основному стосуються оперативної взаємодії між відповідними відомствами управління підрозділами цивільного захисту. Незважаючи на багатогранність та широкий спектр аварій та катастроф, багато з яких становлять значну загрозу (пожежі, землетруси, урагани та ін.). Прийняття рішень в умовах КЦЦЗ, методи оцінки ризику, оцінки готовності та допомоги у реагуванні, мають багато спільного і можуть вирішуватися із застосуванням геоінформаційних систем.

Висновки. Наявність даного Кризового центру цивільного захисту, допоможе отримати необхідний досвід здобувачам вищої освіти та сформує у них необхідні практичні компетентності. Широкий спектр програмного забезпечення «Кризового центру» дозволить охопити більшість спеціальностей, яким навчаються студенти та курсанти. Допоможе краще розглянути проблемні питання міста і області, та виявити потенційно-небезпечні місця для попередження можливих надзвичайних ситуацій. У випадках настання загрози, даний Кризовий центр цивільного захисту може бути використаний для прийняття рішень, використовуючи геоінформаційні системи, методи оцінки ризиків, оцінки готовності підрозділів до виконання дій з локалізації та ліквідації НС.

Література

1. Кодекс цивільного захисту України (Відомості Верховної Ради, 2013, № 34-35, ст.458) (зі змінами від 19.02.2021№ 1259-IX). Електронний ресурс. Режим доступу: https://zakon.rada.gov.ua/laws/show/5403-17#Text

2. Постанова Кабінету Міністрів України від 24 березня 2004 р. № 368 «Про Порядок класифікації надзвичайних ситуацій техногенного та природного характеру за їх рівнями». Електронний ресурс. Режим доступу: https://www.kmu.gov.ua/npas/5390215

3. Наказ МВС України від 26.12.2014 № 1406 (Зареєстровано в Міністерстві

юстиції України від 16 січня 2015 р. № 47/26492) Про затвердження Положення про штаб з ліквідації наслідків надзвичайної ситуації та Видів оперативно-технічної і звітної документації штабу з ліквідації наслідків надзвичайної ситуації. Електронний ресурс. Режим доступу: https://zakon.rada.gov.ua/laws/show/z0047-15#n15

4. Постанова Кабінету Міністрів України від 9 січня 2014 р. № 11 «Про затвердження Положення про єдину державну систему цивільного захисту» Електронний ресурс. Режим доступу: https://zakon.rada.gov.ua/laws/show/11-2014-%D0%BF#n10

УДК 004.9

«ОНЛАЙН ПОЛІКЛІНІКА»: ПОПЕРЕДЖЕННЯ ХВОРОБ СЕРЦЯ З ТЕХНОЛОГІЄЮ МАШИННОГО НАВЧАННЯ

Лисишин В.
Львівський національний університет імені Івана Франка, м. Львів

Мета даної роботи – створити додатковий функціонал до сайту «Онлайн поліклініка», який буде обробляти дані пацієнтів і зможе попередити лікаря чи пацієнта про можливе серцево-судинне захворювання користувача.
Ключові слова: *веб-аплікація, машинне навчання, ASP.NET Core.*

The purpose of the work is to create additional functionality of site "Online Clinic", which will process patient data and will be able to warn a doctor or a patient about a possible cardiovascular disease of a user.
Keywords*: web application, machine learning, ASP.NET Core.*

У наш час важко уявити собі комп'ютерну техніку, локальні та глобальні мережі без основної частини – прикладного програмного забезпечення. Також враховуючи ситуацію сьогодення, яка склалась у світі, людям слід уникати громадських місць і намагатися якнайбільше проводити часу вдома. Тому минулого року, я розробив проєкт призначений для автоматизації роботи клієнт-серверної інформаційної системи «Онлайн поліклініка». Дана система являє собою веб-аплікацію реалізовану за допомогою ASP.NET Core MVC та Entity Framework Core.

Система «Онлайн поліклініка» містить наступні сутності:

- пацієнт (може записатися на прийом до лікаря, вести щоденник здоров'я, спілкування з лікарем за допомого чату, перевіритися на наявність серцевих захворювань тощо);
- лікар (може назначати запис для пацієнта, прикріплює PDF документ з результатами аналізів тощо);
- адміністратор (може переглядати статистику по сайту, додавати/редагувати/видаляти лікаря тощо).

Не беручи до уваги пандемію, в нашій державі серцево-судинні захворювання є головною причиною смертності населення [1]. Тому було вирішено допрацювати проєкт «Онлайн поліклініка» і створити новий функціонал, який зможе попередити пацієнта про хворобу. Машинне навчання виявляється ефективним у наданні допомоги у прийнятті рішень та прогнозів на основі великої кількості даних, отриманих у галузі охорони здоров'я [2]. У результаті було створено додатковий функціонал до сайту, який обробляє дані пацієнтів і, таким чином, зможе попередити лікаря/пацієнта про можливе серцево-судинне захворювання користувача. Для реалізації використано такі технології:

- бібліотеку ML.NET [3] – для аналізу серцевих захворювань;

- платформа ASP.NET Core – забезпечує відображення і користування базою даних;
- для зручного користування інформаційною системою інтерфейс сайту розроблено за допомогою MDB;
- спілкування пацієнта і лікаря реалізовано за допомогою SignalR.

Висновки. На мою думку, наявность в поліклініці власного офіційного веб-застосунку, який надаватиме послугу безкоштовної перевірки на загрозу захворювання, зможе запобігти великій кількості смертей. Отже, розробка офіційного сайту поліклініки з такою додатковою системою є актуальною і необхідною.

Література

1. Healthline : веб-сайт. URL: https://www.healthline.com/health/top-10-deadliest-diseases
2. The UCI Machine Learning Repository : веб-сайт. URL: https://archive.ics.uci.edu/ml/datasets/Heart+Disease
3. ML.NET : веб-сайт. URL: https://dotnet.microsoft.com/apps/machinelearning-ai/ml-dotnet

3D МОДЕЛЮВАННЯ ТА 3D ДРУК

Малецький С.
Відокремлений підрозділ Національного університету біоресурсів і природокористування України «Ірпінський фаховий коледж», м. Ірпінь

Анотація: *3D технології, які стімко розвиваються, надають змогу відкривати для конструкторів технічних систем різних галузей нові можливості та знання в розумінні процесів виробництва від технічного завдання до готової деталі, глибше зрозуміти деякі процеси навчання при використанні прототипів об'ємних моделей та розвиватися в актуальних на сьогоднішній час галузях таких як комп'ютерні технології.*

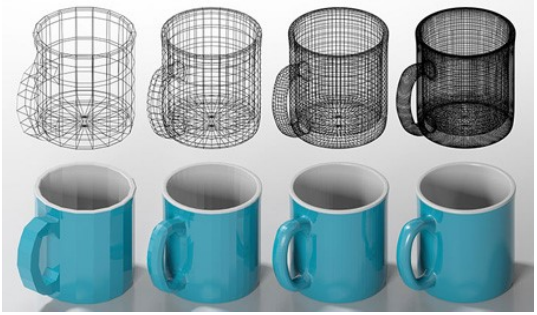
Ключові Слова: *комп'ютерна графіка, 3D-моделювання, 3D-модель, 3D-графіка, 3D-друк, 3D принтер, 3D технології.*

Anotation: *3D technologies, which are rapidly developing, make it possible to open up new opportunities and knowledge for designers of technical systems of various industries in understanding production processes from technical specifications to a finished part, to better understand some learning processes when using prototypes of volumetric models and to develop in today's topical industries such as computer technologies.*

Keywords: *computer graphics, 3D modeling, 3D model, 3D graphics, 3D printing, 3D printer, 3D technology.*

У комп'ютерній графіці 3D-моделювання — це процес розробки математичного представлення будь-якої тривимірної поверхні об'єкта за допомогою спеціалізованого ПЗ. Продуктом моделювання є 3D-модель. Вона може бути представлена у вигляді програмного коду або відображена у вюпорті чи вювері, як 3D-модель, а також за допомогою двовимірного зображення, що створюється за допомогою процесу рендерингу.

3D-моделі можуть створюватись вручну або автоматично. Виготовлення моделей вручну є подібним до створення скульптури в пластичному мистецтві. 3D-графіка призначена для імітації фотографування або відео зйомки тривимірних образів об’єктів, які попередньо створюються в пам’яті комп’ютера в такій послідовності: попередня підготовка, створення геометричної моделі сцени, настроювання освітлення і знімальних камер, підготовка і призначення матеріалів, візуалізація сцени. Таким чином створюється уявний світ, який часто називають віртуальним.



Попередня підготовка передбачає продумування складу сцени, розміщення об’єктів і їх деталей, які будуть видимими з передбачуваних напрямів спостереження.

На етапі створення геометричної моделі сцени за допомогою різноманітних інструментальних засобів будуються тривимірні геометричні моделі об’єктів сцени, після чого сцену можна розглядати і “фотографувати” з будь-якого потрібного ракурсу.

Правильний вибір джерел світла дозволяє виконувати імітацію фотографування сцени в будь-яких умовах освітленості, причому освітленість всіх об’єктів, тіні від них і бліки світла розраховуються автоматично. Моделі знімальних камер дають можливість розглядати тривимірну сцену і виконувати її знімання під будь-яким вибраним кутом зору.

На етапі підготовки і призначення матеріалів забезпечується надання сцені візуальної правдоподібності, що наближує якість зображення до реальної фотографії. Працюючи з матеріалами, можна настроювати такі їх якості, як сила блиску, прозорість, самосвічення, дзеркальність, рельєфність та інші. Реальні фотографії можна включати в склад матеріалів або використовувати для імітації фону.

Візуалізація сцени або рендерінг (rendering) полягає в проведенні програмою розрахунків і нанесення на зображення всіх тіней, бліків, взаємних відблисків об'єктів і т.п. і може тривати досить довго, що залежить від складності сцени і швидкодії комп'ютера.

В той же час, 3D-друк – це методика виготовлення об'ємних виробів на основі цифрових моделей. Незалежно від конкретної технології, суть процесу полягає в поступовому пошаровому відтворенні об'єктів. У цьому процесі застосовується спеціальний електронний пристрій - 3D принтер, який друкує певними видами матеріалів. Більш детально про нього написано тут. Інші назви технології – швидке прототипування або адитивное виробництво. Часто словосполучення «адитивні технології» використовується в значенні «3D технології».

Відтворення об'єктів відбувається поступово. За необхідної форми шар за шаром наноситься обраний матеріал, формуючи готову модель. Варто відзначити, що можливості 3Д-друку практично безмежні, тобто виготовити можна все що завгодно. У деяких технологіях для дуже тонких нависаючих елементів передбачено наявність підтримок, завдяки яким можна уникнути їх провисання.

Література

1. Огляд технологій швидкого прототипування для автомобільної сфери та інтеграція 3D принтерів в навчальний процес університету. Електронний ресурс. Режим доступу: [https://www.khadi.kharkov.ua/fileadmin/P_vcheniy_secretar

2. 3D-моделювання: програми та реалізація. Електронний ресурс. Режим доступу: [https://pro3d.com.ua/a358911-scho-take-druk.html]

3. Що таке 3D друк? Електронний ресурс. Режим доступу: [https://sites.google.com/site/3dmodeluvana/so-take-3d-modeluvanna]

4.Що таке 3D-друк? Електронний ресурс. Режим доступу: [https://www.0532.ua/list/225224]

УДК 004.827

ЗАСТОСУВАННЯ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ В ПОЖЕЖНО-РЯТУВАЛЬНІЙ СПРАВІ

Малець О.-С., Головатий Р., Хлевной О.
Львівський державний університет безпеки життєдіяльності

Представлено аналіз вітчизняного та закордонного досвіду використання нейронних мереж та штучного інтелекту в пожежно-рятувальній справі.
Ключові слова: *нейронні мережі, штучний інтелект, пожежа, дрони, евакуація, тепловізори*

An analysis of domestic and foreign experience in the use of neural networks and artificial intelligence in fire and rescue is presented.
Keywords: *neural networks, artificial intelligence, fire, drones, evacuation, thermal imagers*

Станом на сьогодні штучний інтелект та нейромережі широко впроваджуються для забезпечення потреб рятувальних підрозділів багатьох країн світу. Розглянемо декілька варіантів застосування штучного інтелекту для запобігання надзвичайним ситуаціям та задля допомоги рятувальним підрозділах під час їх ліквідації..

Візуалізація об'єктів в умовах погіршеної видимості (сильне задимлення).

В умовах погіршеної видимості рятувальники використовують здебільшого тепловізори, проте зображення з тепловізорів досить важко сприймати через значну колористику. Окрім того через температурні поля в зонах пожежі іноді контури розігрітих майже до однакової температури предметів ідентифікувати майже неможливо. Отже, розробка засобів та технологій, здатних покращувати орієнтування рятувальника в умовах поганої видимості є важливим завданням.

Для вирішення цієї проблеми використовується технологія комп'ютерного зору. Тепловізійна камера встановлюють на верхню частину шолома. Кадри зображення з камери надсилаються в процесор для обчислення простих матричних операцій. Процесор виконує операції виявлення країв і контурів, використовуючи різні фільтри, зокрема, оператор Собеля. Оброблена картинка надходить на окуляри. Картинка, яку бачить рятувальник через окуляри AR наведена на рисунку 1. За допомогою цього простого алгоритму пожежники можуть ефективно розрізняти навколишнє. Це полегшує для пожежників ідентифікацію об'єктів навколо них, тим самим прискорюючи весь процес порятунку.

Рисунок 1 – Зображення, оброблені за допомогою нейромережі

Дослідження, проведені під час тренувань у спеціальних вогневих камерах в умовах, наближених до обстановки реальної пожежі показали, що ця технологія дозволяє зменшити тривалість виконання поставлених завдань на 17-30% (в залежності від виду завдання). Особливо ефективною є ця технологія під час пошуку потерпілих в умовах задимлення.

Система AUDREY

Робота рятувальників супроводжується значними фізичними навантаженнями. За таких умов виникає ризик погіршення самопочуття (тепловий удар, отруєння продуктами горіння, порушення серцево-судинної системи, тощо). Для недопущення подібних випадків необхідним є постійний моніторинг показників життєдіяльності рятувальників.

Система AUDREY (абревіатура від Assistant for Understanding Data through Reasoning, Extraction, and Synthesis) дає можливість аналізувати показники життєдіяльності рятівників та надавати рекомендації щодо подальших дій. Зокрема, система визначає температуру, тиск, концентрацію чадного та вуглекислого газу в крові, пульс. Користувач, який працює в умовах пожежі, отримує попередження про можливу небезпеку та вказівки щодо подальших дій. Початково технологію розробляли для NASA, але удосконалення технологій роботи з нейромережами та штучним інтелектом, розробка методик машинного навчання дали змогу впроваджувати **AUDREY** для потреб пожежогасіння.

Досліди, проведені спеціалістами NASA довели, що система створює можливість раннього виявлення загрози подальшого погіршення стану здоров'я людини та у близько 80% випадків здатна попередити про загрозу настання критичного стану та запобігти його виникненню шляхом своєчасного інформування.

Сумісне застосування дронів та систем штучного інтелекту для виявлення та прогнозування розвитку пожеж в природніх екосистемах

В умовах спеки суттєво зростає пожежна небезпека природних екосистем. При цьому виявлення пожеж на ранніх стадія розвитку є запорукою мінімізації збитків. Виявлення та прогнозування пожеж в природніх

екосистемах на основі обробки зображень, що надходять з камер відеоспостереження дронів (безпілотних літальних апаратів). При такому підході нейромережі систем штучного інтелекту навчають розпізнавати ознаки пожежі. Процес навчання передбачає визначення основних ознак (критеріїв) пожежі, тренування мережі та перевірка валідації. Після навчання, нейромережі матимуть змогу виявляти осередки загоряння на ранніх стадіях, передавати результати на пульт спостереження та запобігати розповсюдженню пожежі шляхом свочасного реагування на неї.

Також системи штучного інтелекту із технологіями нейромережевого навчання можуть виявляти ознаки пожежі в природніх екосистемах на основі даних різних датчиків (вміст в повітрі вуглекислого газу, чадного газу, інших хімічних сполук), що також розміщуються на безпілотних літальних апаратах.

За схожими принципами функціонують системи не тільки для контролю за лісовими пожежами, а і в агропромисловому комплексі тощо.

У Канаді, Австралії, США та на півдні Європи (Іспанія, Італія, Греція тощо) подібні системи використовуються для моніторингу обстановки, проведення розвідки та виявлення пожеж у природніх екосистемах. Дослідження, проведені провідними установами США та Євросоюзу показують, що економічний ефект від впровадження подібних технологій становить десятки мільйонів доларів щороку.

Література

1. Vedant Kumar. Applications of Artificial Intelligence in Fire & Safety. Overview of the applications of AI in mitigating the dangers due to fire.

2. Eric Wai Ming Lee. Application of Artificial Neural Network to Fire Safety Engineering https://link.springer.com/chapter/10.1007/978-3-642-13639-9_15

3. Chrysanthos Maraveas, Dimitrios Loukatos, Thomas Bartzanas, Konstantinos G. Arvanitis. Applications of Artificial Intelligence in Fire Safety of Agricultural Structures.

4. European Parliament Committee on Legal Affairs. 2017. REPORT with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) A8-0005/2017 27 January.

5. US National Institute of Standards and Technology

УДК 004.451

ОПЕРАЦІЙНІ СИСТЕМИ: ІСТОРІЯ РОЗВИТКУ

Малькевич Р., Карабин О.
Львівський державний університет безпеки життєдіяльності, Львів

Розглянуто історичні аспекти розвитку операційних систем від початку становлення до сучастості, наведено особливості найпоширеніших операційних систем чотирьох поколінь комп'ютерів.
***Ключові слова**: операційна система, процесор, програмне забезпечення.*

The historical aspects of the development of operating systems from the beginning to the present are considered, the features of the most common operating systems of four generations of computers are given.
***Keywords:** operating system, processor, software.*

Операційна система - це основне програмне забезпечення, яке керує всіма апаратними та іншими програмами на комп'ютері. Операційна система взаємодіє з апаратним забезпеченням комп'ютера і надає послуги, які можуть використовувати програми. Вона обробляє вхідні та вихідні пристрої, тобто все, від клавіатури і миші до радіо, Wi-Fi, пристроїв зберігання даних і дисплея та використовує драйвери пристроїв, написані творцями апаратних засобів для зв'язку зі своїми пристроями.

Історія розвитку операційних систем налічує багато років. Так як операційні системи з'явилися і розвивалися в процесі конструювання комп'ютерів, то ці події історично тісно пов'язані. Програмне та апаратне забезпечення еволюціонували спільно, здійснюючи взаємний вплив один на одного. Поява нових технічних можливостей призводила до прориву в області створення зручних, ефективних і безпечних програм, які в свою чергу були спрямовані на пошук нових технічних рішень. Розглянемо коротко історичну еволюцію обчислювальних систем.

Перше покоління (1945-1955): електронні лампи і комутаційні панелі. Операційних систем немає.

Друге покоління (1955 - початок 60-х): транзистори і системи пакетної обробки, пакетні операційні системи. Вперше склалося чітке розділення між проектувальниками, збирачами, операторами, програмістами і обслуговуючим персоналом. Суть системи полягала в тому, щоб зібрати повний комплект завдань (перфокарт) в кімнаті вхідних даних і потім переписати їх на магнітну стрічку, використовуючи невеликий недорогий комп'ютер. Наприклад, комп'ютер класу IBM 1401 використовувався для зчитування карт, копіювання стрічок і друку вихідних даних, але він не підходив для числових обчислень. Великі комп'ютери другого покоління використовувалися голов-

ним чином для наукових і технічних обчислень, таких як розв'язування диференціальних рівнянь в частинних похідних, які часто зустрічаються у фізиці та інженерних задачах. В основному на обчислювальних комп'ютерах програмували на мові Фортран й Асемблері. Типовими операційними системами були FMS (Fortran Monitor System) і IBSYS (операційна система, яка була створена корпорацією IBM для комп'ютера IBM 7094).

Третє покоління (1960-1980): інтегральні схеми і багатозадачність, перші багатозадачні операційні системи. Період характеризується переходом від окремих напівпровідникових елементів типу транзисторів до інтегральних мікросхем. Найважливішим досягненням цього періоду стала багатозадачність, управління поділом спільно використовуваних ресурсів, таких як процесор, оперативна пам'ять, файли і зовнішні пристрої. Іншим досягненням операційних систем третього покоління стала здатність зчитувати завдання з перфокарт на диск - спулінг. Перша серйозна система з режимом поділу часу CTSS (Compatible Time Sharing System - сумісна система поділу часу) була розроблена в Массачусетському технологічному інституті на спеціально переробленому комп'ютері IBM 7094. Ще одним важливим моментом цього періоду був великий ріст міні-комп'ютерів, починаючи з випуску машин класу PDP-1 корпорацією DEC в 1961 році, які мали дуже маленьку оперативну пам'ять, але коштували дешево і тому користувалися великим попитом. Деякі види робіт вони виконували з такою ж швидкістю, що і IBM 7094, що дало поштовх до появи нової індустрії міні комп'ютерів. Кен Томпсон (Ken Thompson), один з фахівців з комп'ютерів в Bell Labs, який працював над проектом MULTICS, вирішив для міні-комп'ютера PDP-7 написати усічену однокористувацьку версію операційної системи MULTICS, яка пізніше розвинулася в операційну систему UNIX.

Четверте покоління (з 1980 року по наші дні): персональні комп'ютери, класично мережеві і розподілені системи. Цей період в еволюції операційних систем пов'язаний з появою великих інтегральних схем (LSI, Large Scale Integration) - кремнієвих мікросхем, що містять тисячі транзисторів у одному квадратному сантиметрі. У 1974 році, коли компанія Intel випустила перший універсальний 8-розрядний центральний процесор Intel 8080, в рамках операційної системи CP / M було створено програмне забезпечення значного обсягу, що включало транслятори з мов Бейсік, Паскаль, Сі, Фортран, Кобол, Лисп, Ада і ін., текстові і табличні процесори, системи управління базами даних, графічні пакети, символьні пакети і інші проблемно орієнтовані програми. Успіх системи в значній мірі був зумовлений її простотою і компактністю, можливістю швидкого налаштування на різні конфігурації ПЕОМ. Перша версія системи займала всього 4 КБ, що було вельми важливо в умовах обмеженості обсягів пам'яті ПЕОМ того часу. Пізніше було написано безліч прикладних програм, що працюють в операційній системі CP/M, що дозволило їй займати вищу позицію в світі

мікрокомп'ютерів протягом 5 років. З появою ПЕОМ, що використовують 16-розрядні мікропроцесори типу Intel 8088 і 8086, операційна система MS DOS стала домінуючою і найбільш довголітньою. З моменту появи в 1981 році MS DOS поширилася настільки широко, що завоювала право вважатися найпопулярнішою в світі. Коли в 1983 році з'явився комп'ютер IBM PC/AT з центральним процесором Intel 80286, операційна система CP/M доживала свої останні дні. Пізніше система MS-DOS широко використовувалася на комп'ютерах з процесорами 80386 і 80486. Хоча первісна версія MS-DOS була досить примітивна, наступні версії системи виходили більш досконалими з новими властивостями, включаючи багато запозичень від UNIX. В даний час для MS DOS розроблений величезний фонд програмного забезпечення. Операційні системи CP/M, MS-DOS та інші для перших мікрокомп'ютерів повністю ґрунтувалися на введенні команд з клавіатури. Потім завдяки дослідженням, проведеним в 60-і роки Дагом Енгельбартом (Doug Engelbart) в науково-дослідному інституті Стенфорда (Stanford Research Institute) ця властивість операційної системи змінилася. Енгельбарт винайшов графічний інтерфейс користувача (GUI, Graphical User Interface), що складається з вікон, значків, різних меню і миші. Одного разу Стів Джоб (Steve Jobs), який винайшов комп'ютер Apple, відвідав PARC і побачив GUI. Він усвідомив його потенційну цінність і приступив до створення Apple з графічним інтерфейсом. Це призвело до проекту Lisa, який був дуже дорогий і зазнав комерційну невдачу. Друга спроба Джобса Apple Macintosh мала величезний успіх не тільки через невисокі ціни, а й тому, що на ньому працював дружній інтерфейс, тобто призначений для користувачів, які нічого не знають про комп'ютери і не бажають чогось навчатися. Коли корпорація Microsoft вирішила створити наступника MS-DOS, вона перебувала повністю під впливом успіхів компанії Macintosh. Була розроблена система, що отримала назву Windows, яка протягом 10 років, з 1985 до 1995 року, виконувала роль графічного середовища поверх операційної системи MS-DOS. У 1995 році вийшла в світ автономна версія Windows 95, яка включила в себе безліч особливостей операційної системи MS-DOS.

По мірі того, як ці операційні системи стають повсякденними речами та кожну секунду попереджають наш наступний крок, виникають нові питання про те, які ж насправді в них повинні бути обов’язки. Операційні системи майбутнього будуть функціонувати не лише для одного пристрою. Вона буде підтримувати цілу екосистему.

УДК: 378.147

ФОРМУВАННЯ ІНФОРМАЦІЙНОГО ОСВІТНЬОГО СЕРЕДОВИЩА МОЛОДІ

Мельникова І., Бобирєва Т.
ВСП «Машинобудівний фаховий коледж Сумського державного університету», м. Суми.

Інформатизація сучасного суспільства зумовила необхідність формування в молоді інформаційної компетентності як під час навчального процесу, так і в майбутній професійній діяльності. Нині суспільство зацікавлене в тому, щоб громадяни були здатні самостійно, активно діяти, приймати рішення, гнучко адаптуватися до умов життя, які стрімко змінюються. Зміна парадигми освіти останніми роками висуває перед навчальними закладами вдосконалення підготовки майбутніх фахівців, становлення їх як компетентних професіоналів, здатних використовувати інноваційні форми, засоби й методи навчання чи роботи.

Ключові слова: *інформаційні технології, інформаційне суспільство.*

Informatization of modern society has necessitated the formation of information competence of young people both during the educational process and future professional activity. Today, society is interested in the fact that citizens can act independently, actively, make decisions, flexibly adapt to rapidly changing living conditions. The paradigm shift in education in recent years has put forward for educational institutions to improve the training of future professionals, becoming them as competent professionals, able to use innovative forms, tools and methods of teaching or working.

Key words: *information technologies, information society.*

Постановка проблеми. XXI століття – характеризується наявністю інформаційного суспільства, головною рисою якого є перетворення інформації в один із головних виробничих ресурсів. Оскільки в сучасному світі інформація є стратегічним національним ресурсом, одним із основних багатств держави, який відіграє дедалі більшу роль у системі державного управління. Сучасна молодь існує в інформаційну еру, де оточуючий світ все більше втрачає рис матеріального світу і перетворюється на світ інформаційно-цифровий. Як наслідок змінюються засоби навчання, навчальний процес являє собою взаємодію «людина-матеріальний носій інформації», тому, наприклад, уявне моделювання явищ природи значно розширюється за рахунок інформаційно-комунікативних технологій. Традиційні форми навчального процесу швидко адаптуються до вимог часу та переходять до дистанційних, хмарних технологій [2].

Проблема інформатизації освіти зосереджена в робота наступних вчених: В. Биков, Р. Гуревич, М. Жалдак, І. Захарова, Ю. Машбиць, Н. Морзе.

Метою статті є дослідження шляхів формування інформаційного освітнього середовища молоді враховуючи сучасну парадигму освіти.

Виклад матеріалу. Інформатизація освіти – це сукупність взаємопов'язаних організаційно-правових, соціально-економічних, навчально-методичних, науково-технічних, виробничих та управлінських процесів, спрямованих на задоволення інформаційних, обчислювальних і телекомунікаційних потреб учасників навчально-виховного процесу, а також тих,

хто цим процесом керує та його забезпечує. Матеріальною основою інформаційних технологій, за допомогою яких здійснюється збирання, зберігання, передача та обробка інформації є програмно-технічні засоби, що використовують відповідні програмні продукти.

Наше сьогодення неможливо уявити без комп'ютерів, які увійшли не лише в усі галузі виробництва, культури, освіти, а й практично у кожну оселю. Значним попитом серед людей різного віку та соціального стану користуються комп'ютерні ігри. Отож світові фірми-гіганти щорічно змагаються на споживчому ринку, виносячи на суд вимогливих геймерів нові ігри. Зараз комп'ютерні ігри просто вражають масштабністю та наближенням до реального життя. Крім цього, студент перебуває у віртуальному оточенні, яке згенероване комп'ютером і яке може інтерактивно взаємодіяти з одним або декількома користувачами, впливаючи на їхні органи чуття з метою створення ілюзії занурення в світ гри [2].

Інформаційні технології можуть розв'язувати проблеми навчання, професійного спілкування, інтенсифікувати навчальний процес за рахунок підвищення темпу, індивідуалізації навчання, моделювання ситуацій, збільшення активного часу кожного, хто навчається, підвищення наочності. Варто виокремити деякі переваги використання інформаційних технологій у навчальному процесі: організація пізнавальної діяльності шляхом моделювання; імітація типових професійних ситуацій за допомогою мультимедіа; застосування одержаних знань у наукових дослідженнях; ефективне тренування знань, умінь і навичок; автоматизований контроль результатів навчання; здійснення зворотнього зв'язку; розвиток творчого мислення; можливості об'єднання в навчальних програмах візуальної та звукової форм.

Інноваційні процеси в освіті виникали в різні історичні періоди і визначали її розвиток. Перший етап – електронізація, він характеризувався широким впровадженням електронних засобів, обчислювальної техніки в навчальний процес (60-70 роки XX ст.). Другий етап – комп'ютеризація освіти – пов'язаний з використанням потужних комп'ютерів, програмного забезпечення. Для цього етапу притаманна діалогова взаємодія людини з комп'ютером. Діалогове спілкування людини з комп'ютером відкрило нові широкі можливості в освітній галузі. Третій, сучасний етап інформатизації освіти характеризується широким використанням сучасних комп'ютерів, швидкодіючих накопичувачів значної ємності, нових інформаційно-комунікаційних технологій, соціальних мереж і сервісів [2].

Саме сучасний етап інформатизації освіти характеризується активним використанням засобів комунікації: електронної пошти, глобальної, регіональної та локальної мережі відкриває для навчання можливість здійснювати:

− оперативне передавання на відстані інформації будь-якого обсягу і виду;
− інтерактивний, оперативний зв'язок;
− доступ до різноманітних джерел інформації;
− організацію спільних телекомунікаційних проектів;
− спілкування та обговорення проблем, участь у телеконференціях, вебінарах, чатах, форумах, блогах та ін.

У системі освіти широкого поширення набули універсальні офісні прикладні програми і засоби інформаційно-комунікаційних технологій: текстові процесори, електронні таблиці, програми підготовки презентацій, системи управління базами даних, органайзери, графічні пакети та ін.

Зараз в професійній освіті відбувається формування фахівців нового покоління, які володіють інформаційними копметентностями та вміло реалізують свої можливості в інформаційному просторі. Навіть вже зараз, особливо в карантинних умовах навчання, інформаційне освітнє середовище дає змогу здобувачам освіти мати доступ до навчання в будь-який час з використанням будь-яких інформаційних ресурсів.

У зв'язку з цим формуються тенденції, що характеризують перспективні шляхи розвитку сучасної освіти України на засадах інформаційно-цифрового суспільства зі звичним вже повсюдно штучним інтелектом. Зокрема, все більше насичення освітнього простору приладами віддаленого керування, зростання ролі комп'ютерної грамотності всі учасників навчального процесу при опанування цифрових засобів навчання нового покоління [3].

Висновки. Отже, інформаційне освітнє середовище сучасної молоді ілюструє запити суспільства на формування компетентної особистості, яка вміло в своїй навчальній діяльності чи роботі використовує інформаційні ресурси для досягнення бажаних цілей. Інформатизація освітнього середовища дала значний поштовх до нового етапу надання освітніх послуг в Україні. Незважаючи на те, що наша держава є одним із лідерів в Європі за кількістю здобувачів вищої освіти, все ще залишається ряд невирішених проблем освітньої сфери при підготовці молодих фахівців. Тому, інформаційні технології організації навчального процесу є якісним, і головне результативним шляхом у подоланні перешкод в наданні сучасних освітніх послуг, враховуючи всі можливі варіанти роботи учасників навчального процесу.

Література:

1. Буров О. Ю. Інформаційна ера та вимоги до засобів навчання / О. Ю. Буров // Інформаційно-ресурсне забезпечення освітнього процесу в умовах діджиталізації суспільства: збірник матеріалів Міжнародної науково-практичної конференції, 11 листопада 2020 р. – Київ : Науково-методичний центр ВФПО, 2020. – 353 с.

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

3. Мельникова І. В. Використання ГІС у курсі географії 11 класу як складова особистісно-професійної компетентності педагога в умовах інноваційних змін / І. В. Мельникова // Інноваційні технології розвитку особистісно-професійної компетентності педагогів в умовах післядипломної освіти. – Суми, 2021. – 656 с.

УДК: 378.046

РЕЗУЛЬТАТИВНІСТЬ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ НА ЗАНЯТТЯХ ГЕОГРАФІЇ В КОЛЕДЖІ.

Мельникова І., Влезько О.
ВСП «Машинобудівний фаховий коледж Сумського державного університету», м. Суми.

Сучасне інформаційне суспільство постійно має запит на формування компетентних, кваліфікованих фахівців. Головним ресурсом сучаної освіти є інформація в будь-якому її вигляді. Як наслідок, сучасна освітня діяльність має на меті формування майбутнього компетентного фахівця в умовах пришвидшеної інноватизації та мережевих зв'язків інформаційного простору. Для сучасних викладачів головним є розвиток інформаційно-цифрової компетентності, що передбачає впевнене застосування інформаційно-комунікаційних технологій як в повсякденному житті, так і у професійній діяльності.

Ключові слова: *інформаційні технології, геоінформаційні ресурси.*

The modern information society is constantly in demand for the formation of competent, qualified professionals. The main resource of modern education is information in any form. As a result, modern educational activities aim to form a future competent specialist in the conditions of accelerated innovation and network connections of the information space. For modern teachers, the main thing is the development of information and digital competence, which involves the confident use of information and communication technologies in everyday life and in professional activities.

Key words: *information technology, geoinformation resources*.

Проблематика дослідження. Інформаційні технології все частіше проникають у різні сфери життя та стали стандартом у сфері освіти, науки і досліджень в багатьох розвинених країнах. Впровадження інформаційний технологій в освіту потребує систематичної та всебічної підтримки, яка має бути спрямована на практику їх використання так і на сучасні форми та методи навчання. Педагог без застосування сучасних інструментів вже не може організовувати навчальний процес, оскільки учням чи студентам потрібно навчитися працювати з інформацією, оцінювати інформаційні джерела, вміти працювати в команді, аналізувати і представляти кінцевий продукт використовуючи сучасні цифрові засоби представлення результатів. Відповідно, для вирішення цих завдань, викладачі та вчителі мають володіти відповідници інформаційно-цифровими й електронними інструментами та застосовувати їх для досягнення педагогічної мети, що потребує підвищення їх фахового рівня.

Інформаціні технології навчання як засоби формування інформаційної компетентності всіх учасників навчального процесу розглядаються в працях відомих вітчизняних та зарубіжних науковців: Р. Гуревич, М. Кадемія, Л. Шевченко, О. Абдалова, Л. Гозман.

Метою статті є дослідження результативності використання інформаційних технологій на заняттях географії, застосовуючи геоінформаційні ресурси в навчальному процесі.

Виклад основного матеріалу. Інформаційні технології є сукупністю методів, виробничих процесів і програмно-технічних засобів, інтегрованих з метою збирання, опрацювання, зберігання, розповсюдження, показу і використання інформації в інтересах її користувачів. Вагомість використання інформаційних технологій в навчальному процесі означає наявність знань, вмінь та навичок в галузі даних технологій та здатність їх застосування в професійній діяльності [1].

Інформаційні технології навчання вже змінили традиційну систему освіти у напрямку формування її нової якості. Ця якість полягає в збільшенні кількості віртуальних освітніх платформ для організації навчального процесу, або ж один електронний ресурс може бути використаний багато разів для надання різних освітніх послуг, тощо.

Організовуючи навчальний процес на заняттях географії в коледжі, інформатизації освітнього середовища можна досягти завдяки використання геоінформаційних технологій. Дані технології являють собою сучасну комп'ютерну технологію, що дозволяє поєднати модельне зображення території (електронне відображення карт, схем, космо-, аерозображень земної поверхні) з інформацією табличного типу (статистичні дані, списки, економічні показники тощо). Тому, наприклад, наявність цифрових карт, космічних знімків та інструментів роботи з ними забезпечує широке інформаційне поле для всіх учасників навчального процесу [3].

Під час опанування студентами навчального матеріалу курсу географії 11 класу, активне впровадження геоінформаційних ресурсів варто здійснювати, наприклад, при вивченні теми «Сучасні картографічні твори» для формування чіткої картини сучасних можливостей зібрання, аналізу і подання географічної інформації як про природні, так і соціально-економічні об'єкти будь-якої точки світу. Так, доцільно навести переваги використання безкоштовного додатку від Goggle – програми Google Earth.

Google Earth являє собою віртуальний глобус, використовуючи який можна значно урізноманітнити навчальний процес чітким наочним показом елементарних природних чи господарських процесів світу у поєднанні з їх просторовим розміщенням, без застосування додаткових засобів. У даному випадку перевагою використання Google Earth у навчальному процесі є якраз формування взаємопов'язаної картини існування будь-якого географічного явища чи процесу, що досягається наочним встановленням причинно-наслідкового зв'язку, чого дуже важко досягти. Наприклад, за допомогою Google Earth збільшуючи чи зменшуючи масштаб місцевості на віртуальному глобусі, при виборі

конкретного інструменту чітко можна розгледіти поширення різних форм рельєфу у поєднанні із господарськими об'єктами, що до них приурочені. Також, дана програма, наприклад, дає можливість змоделювати рух повітряних мас по земній кулі в даний момент [3].

Висновки. Таким чином, інформаційні технології на заняттях географії забезпечують процеси пошуку, збору, передачі та збереження великого обсягу інформації в оцефрованому вигляді за допомогою різних програмних додатків. Використання інформаційних технологій передбачає результативне їх застосування на заняттях в коледжі, що значно полегшує сприйняття та засвоєння навчального матеріалу здобувачами освіти. Тому, саме на заняттях географії використання інформаційних технологій у вигляді геоінформаційних ресурсів дає можливість урізноманітнити засвоєння та закріплення навчального матеріалу, як наслідок зацікавлення, враховуючи активне використання гаджетів студентами у повсякденні. Вагомою перевагою застосування інформаційних технологій у ході заняття є не вибагливість програмного забезпечення що до їх використання на гаджетах всіх учасниках навчального процесу, використовуючи різні операційні системи, що значно скорочує час на встановлення необхідних програм чи ознайомлення з ними.

Література

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

2. Коваль Т. І. Професійна підготовка з інформаційних технологій майбутніх інженерів-економістів: монографія / Тамара Іванівна Коваль. — К. : Ленвіт, 2007. — 264 с. — Бібліогр.: С. 202-232.

3. Мельникова І. В. Використання ГІС у курсі географії 11 класу як складова особистісно-професійної компетентності педагога в умовах інноваційних змін / І. В. Мельникова // Інноваційні технології розвитку особистісно-професійної компетентності педагогів в умовах післядипломної освіти. – Суми, 2021. – 656 с.

4. Навчальна програма з географії для 10-11 класів (Рівень стандарту) «Затверджено Міністерством освіти і науки України» (Наказ МОН України від 23.10.2017 № 1407) – 25 с.

УДК 378.147

ГЕЙМІФІКАЦІЯ В НАВЧАЛЬНОМУ ПРОЦЕСІ

Мечус Х., Смотр О.
Львівський державний університет безпеки життєдіяльності, м. Львів

У роботі систематизовано теоретичні дослідження проблеми гейміфікації у навчальному процесі на підставі чого зроблені рекомендації щодо їх використання в умовах сучасного навчання.

Ключові слова: *інформаційні технології, інформатизація освіти, гейміфікація, мотивація.*

The Tpaper systematizes theoretical studies of gamification in the educational process is carried out in the work on the basis of which recommendations concerning their use in the conditions of modern training are made.

Keywords: *information technologies, informatization of education, gamification, motivation.*

Однієї з основних проблем навчання є складність залучення студентів у навчальний процес. З кожним роком збільшується прірва між рівнем підготовки майбутніх студентів і якістю освітніх програм у вищому навчальному закладі. І проблема не лише у небажанні студентів сприймати нову інформацію, її джерелом є те, що вони ростуть і навчаються в іншому освітньо-соціальному просторі – інтерактивно-ігровому. Основною ідеєю гейміфікації є мотивація користувача, спонукання його до певної дії, аніж навчання чому-небудь.

Гейміфікація (від англ. слова gamification, game - гра) - це процес використання ігрового мислення і динаміки ігор для залучення аудиторії і вирішення завдань, перетворення чого-небудь у гру [1]. Гейміфіковане навчання означає додавання елементів ігрового процесу до існуючих навчальних курсів, щоб залучити учнів, мотивувати їх дії, сприяти навчанню. Гейміфікація допомагає реалізовувати соціальні зв'язки в процесі навчання, удосконалювати майстерність, не забувати про конкуренцію, дбати про досягнення і статус [2, 3].

Гейміфікація пов'язана не зі створенням повноцінної гри, а з використанням елементів гри. Працюючи на рівні елементів, гейміфікація в порівнянні з грою дає більше гнучкості. Тому завдання гейміфікації полягає в тому, щоб взяти елементи, які зазвичай працюють у світі ігор, і ефективно застосувати їх у реальному світі [4,5].

Мотивація студента – це важлива частина успіху студента в навчанні і в його подальшому житті. Гейміфікація в навчанні залучає людей значущими і цікавими способами, з прицілом на узгодження особистих мотивів людини з його цілями. Складовими мотивації є:

1. Компетентність – студент вважає, що має можливість для виконання завдання, яке було поставленого перед ним/нею.
2. Контроль / автономія - студент відчуває себе під контролем, коли бачить прямий зв'язок між своїми діями і їх результатом, і зберігає автономію, маючи деякий вибір в тому, як виконати завдання.
3. Інтерес / значення (ціннісне) - студент має деякий інтерес до задачі або бачить сенс у її завершенні.
4. Зв'язаність - завершення завдання приносить студенту соціальні нагороди, такі як почуття приналежності до класу або до іншої бажаної соціальної групи, або хтось підтверджує соціальну значимість студента.

Взаємодія цих складових, поряд з іншими, такими як клімат у навчальному закладі та умови вдома, є досить складною і змінюється не тільки серед різних студентів, а й у одного і того ж студента в різних ситуаціях. Тим не менш, ці складові є корисними на етапі проектування, або при аналізі впливу різних стратегій на підвищення мотивації студентів.

Конкуренція – це ще один елемент, який можна використати у гейміфікації. Надати можливість всім учасникам бачити нагороди інших, або отримувати бонуси лідерам і таким чином стимулювати інших виконувати завдання.

Альтернативний підхід до гейміфікації - надати реальним завданням характеристик ігрового світу [6]. Наприклад, запропонувати декілька можливих варіантів розв'язання задачі, повторити із прикладу, поступово ускладнювати, ще можна додати розповідь чи передісторію, для поглиблення в процес та розвиток виконання завдань.

Можемо стверджувати, що сучасний інструментарій ІТ-технологій здатен забезпечити впровадження методів гейміфікації в освітній процес, з метою підвищити мотивацію студента до навчання. Серед найбільш популярного інструментарію ІТ-технологій, що використовується на сьогодні в процесі здобуття знань, можемо виокремити: Zoom, Meet, Teams, Viber, Telegram, Kahoot, Mentimeter, Canva, Google Keep, Quizziz, 101 Planners, MineTest, Learningapps, VR-системи.

- *Додатки й чат-боти*. Охочі отримувати нові знання часто використовують смартфон для цих цілей, адже він завжди в руці. Використання додатків допомагає структурувати навчальний процес та урізноманітнити його через зміну формату навчання.
- *Vr/ar-формати*. Забезпечують передачу досвіду й картинки за допомогою віртуальної та доповненої реальності. І це в рази підвищує залученість студента та його мотивацію до здобуття нових знань.
- Навчальні платформи, що надають можливість забезпечити формат мікронавчання (microlearning). Це методика, що передбачає розбивку складної теми на маленькі частини. Інструмент особливо ефективний для вивчення складних об’ємних тем та в довгострокових програмах навчання. Принципи мікронавчання можна (і потрібно) застосовувати щоденно для досягнення найкращих результатів. Прослухати 20-хвилинну лекцію, ви-

вчити всього 3 нових іноземних слова або одну формулу не так складно, але дієво — якщо робити це щодня та ще й у ігровій формі, у форматі квесту, розвязку кросворду, гри, тощо.

Персоналізація та адаптивне навчання. Це модель автоматизованого навчання, за якого система підлаштовується під здібності, знання й навички кожного студента. Спершу адаптивні технології збирають інформацію про індивідуальну поведінку студента. Залежно від того, як студент взаємодіє з матеріалом та як відповідає, змінюється те, що він бачить на екрані — підказки, запитання, послідовність завдань і тем.

Найцінніший потенціал ігрового навчання криється в тому, що воно допомагає бачити завдання, тему або модель в контексті – як частину системи. На відмінну від запам'ятовування, зазубрювання і опитувань, які часто критикують, тому що вони спрямовані на окремі факти, ігри змушують учнів бачити предмети і явища в їхніх зв'язках. Будь-яке завдання стає корисним, оскільки воно є частиною більш великої мульти-системи.

Література

1. Гейміфікація. Електронний ресурс https://dl.khadi.kharkov.ua/mod/book/tool/print/index.php?id=37552

2. Гейміфікація в освіті. Електронний ресурс https://osvitanova.com.ua/posts/2596-heimifikatsiia-v-osviti

3. Левин М. Як технології змінять освіту: П'ять головних трендів / М.Левин [Електронний ресурс]. – Режим доступу: https://www.forbes.ru/tehno/budushchee/82871-kak-tehnologii-izmenyat-obrazovanie-pyat-glavnyh-trendov

4. Жолубак Л.В. Гейміфікація як інструмент підвищення мотивації студента до навчання / Л.В. Жолубак, Х.В. Мечус, О.О. Смотр // збірник матеріалів Десятої Міжнародної наукової конференції студентів та молодих вчених «Сучасні інформаційні технології - 2020» «Modern Information Technology - 2020» (14-15 травня 2020 р., м.Одеса) / МОН України; Одес. Нац. політех. ун-т ; Ін-т комп'ют. систем. – Одеса : Наука і техніка, 2020. – с. 220-221.

5. Тарапата Н. Комп'ютерна гра. Інструменти і методологія створення комп'ютерних ігор. / Н. Тарапата, М. Семьонова, О. Смотр // ІІ міжвузівська науково-практична конференція курсантів та студентів «Захист інформації в інформаційно-комунікаційних системах» 24 листопада 2017 року –Львів. – С. 55-56.

6. Малець І.О. Використання сервісів Microsoft Office 365 для мотивації активності студентів // І.О. Малець, О.О. Смотр // Міжнародна наукова конференція ISDMCI'2018 "Інтелектуальні системи прийняття рішень та проблеми обчислювального інтелекту" 21-27 травня 2018 року смт. Залізний Порт, Україна – С. 176-177.

УДК 004.42

РОЗРОБКА TELEGRAM БОТУ ДЛЯ АВТОМАТИЗАЦІЇ ПРОЦЕСУ ОТРИМАННЯ РОЗКЛАДУ В НАВЧАЛЬНОМУ ЗАКЛАДІ

Мигасюк Р. Смотр О.
Львівський державний університет безпеки життєдіяльності, м. Львів

Робота присвячена розробці Telegram Боту для автоматизації процесу отримання розкладу в навчальному закладі, розсилці новин тощо. Розроблено та реалізовано проект на основі мови програмування Python з використанням бібліотеки aiogram, бази даних Postgresql та хостингом Heroku.

Ключові слова: *чат-бот, Telegram, Python, он-лайн сервіс, хостинг Heroku*

This work is devoted to the development of Telegram bot that aims to automate the process of obtaining the university schedule and receiving relevant news and updates. The project is created using Python programming language, aiogram library, Postgresql database and Heroku hosting.

Key words: *Bot, Python, DBMS, Telegram, online service, hosting Heroku.*

Розвиток інформаційних технологій, діджиталізація суспільства, а в останні роки, ще й пандемія Covid-19 – усі ці фактори, значно перемістили вектор спілкування та діяльності нашого суспільства із оф-лайн середовища у он-лайн. Ми уже не уявляємо свого життя без онлайн сервісів, адже це зручно та дозволяє суттєво заощадити час. За допомогою онлайн сервісів можна робити будь-що: проводити грошові операції, спілкуватися, шукати інформацію, пересилати та публікувати інформацію зберігати послуги тощо. Кількість клієнтів, що користуються онлайн сервісами щодня зростає. Відповідно компаніям (організаціям), що надають ці послуги доводиться опрацьовувати все більше запитів, не ігноруючи при цьому жодного з потенційних клієнтів. Для вирішення цієї проблеми на сьогодні використовують передові технології, які пропонують такий варіант спілкування, як чат-бот.

Чат-бот (англ. Chatbot) − комп'ютерна програма, розроблена на основі нейромереж та технологій машинного навчання, за допомогою якої можливо здійснювати комунікацію в аудіо- або текстовому форматі [1]. Чат-бот використовують для виконання конкретних завдань (наприклад, отримання довідкової інформації, виконання розрахунків) або задля розваги. Він створюється людиною для людей та навчається під певне коло цілей. Чат-бот імітує розмову з людиною в Інтернеті, саме тому даний сервіс найкраще зарекомендував себе в месенджерах. Месенджери це програми

для обміну повідомленнями в реальному часі через інтернет. Найпопулярнішими месенджерами в Україні є Viber, Telegram, Facebook Messenger, WhatsApp [2]. З кожним роком тенденція використання чат-ботів у сфері надання послуг(замовлення їжі, товару, запис до перукаря, тощо), зростає.

Виникає питання, чому не використовувати чат-ботів у навчальному процесі. Хоча б, для прикладу, для автоматизації сервісу отримання розкладу занять в навчальному закладі, розсилки новин закладу тощо. Звісно ж у нашому університеті є сайт з електронним розкладом, працює правильно, але не «запам'ятовує» ні курс, ні групу. Отож, щоразу необхідно заходить в браузер, шукати сайт, вводить одне групу, дату, тобто займатися монотонною роботою та затрачати час. Тому було прийнято рішення розробити чат-бот, що допоможе вирішити ці проблеми та надасть можливість зреалізувати, ще ряд корисних послуг, для прикладу, нагадування, за годину до початку пари, про необхідність підключитись до «онлайн-мітингу» чи надсилання щоденного розкладу, тощо. Розроблятимемо Telegram бот.

Чому Телеграм? Telegram - останнім часом зарекомендував себе як один з месенджерів з найбільш швидко зростаючою аудиторією, Адже, більшість студентів мають свої бесіди груп саме у Telegram, тому можливість адаптації Бота під чат є перспективною та цікавою. Окрім цього, Telegram API надає користувачу великий спектр можливостей у реалізації чат-бота [3], а саме:

- Багатомовність, у написанні чат-ботів, можна використовувати такі мови як: Python; Java; Node.js; C#; PHP; Rust; Ruby; Swift; Kotlin; C++; Go.
- Сервіси конструктори Ботів та сервіси з готовими шаблонами.
- Кросплатформність, Телеграм реалізований на IOS, Android як мобільний додаток та десктопні ОС Windows, MacOS, Linux.

Для написання чат-боту ми вирішили використовувати Python, зважаючи на великий вибір бібліотек для написання(telebot, aiogram), простоту та структурованість коду. Та обрали саме aiogram бібліотеку.

Чому aiogram?

- Асинхронність – процес обробки введення\виведення, що дозволяє продовжити обробку інших завдань, не чекаючи завершення попереднього завдання.
- Підтримка розробників, часті оновлення, бібліотека не стоїть на місці, а постійно розвивається, додаються нові можливості для розробки.

Розгортатимемо свій проект на cloud платформі Heroku. ***Чому Heroku?***

- Зручний інтерфейс;
- Розгортання проекту через GitHub;

– Хостинг надає безкоштовну можливість створення додатку;
– Heroku Postgresql надає найдосконалішу в світі базу даних з відкритим вихідним кодом як надійний, безпечний і масштабований сервіс, оптимізований для розробників.

На рисунку 1 відображено процес реєстрації у Telegram-боті «Розклад ЛДУ БЖД».

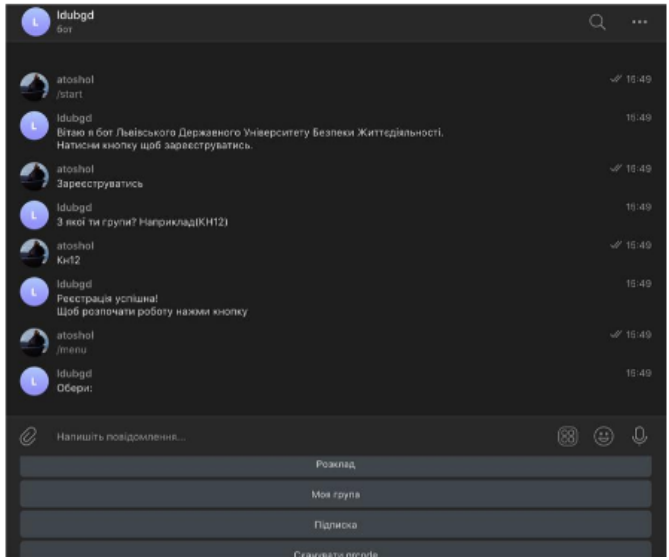


Рисунок 1. Процес реєстрації у Telegram –боті «Розклад ЛДУ БЖД»

Підсумовуючи вищенаведене, можна стверджувати, що на сьогодні, розробка власного чат-бота є актуальною, цікавою та технічно здійсненною задачею. Вибір Telegram месенджера та cloud платформи Heroku для розробки та хостингу чат бота є обґрунтованими.

Література

1. Чат-бот. URL: https://uk.wikipedia.org/wiki/%D0%A7%D0%B0%D1
2. Юдін А. Топ месенджерів в Україні та світі 2020. URL: https://marketer.ua/ua/top-messengers-in-ukraine-and-the-world/ https://marketer.ua/ua/top-messengers-in-ukraine-and-the-world/
3. Офіційний сайт Telegram. Електронний ресурс Telegram API. URL:https://core.telegram.org/api
4. Офіційний сайт Heroku. URL: https://www.heroku.com/

УДК 515. 2 + 519.5

РОЗРОБКА 3D ОТОЧЕННЯ ДЛЯ ОФОРМЛЕННЯ ТА РЕТУШІ ФОТОПРОЄКТІВ

Морозова М., Сидоренко О.
Національний Технічний Університет «Харківський Політехнічний Інститут», м. Харків

***Анотація**. Робота присвячена дослідженню поєднання галузей двовимірної і тривимірної комп'ютерної графіки на прикладі пошуку нових методів застосування тривимірного комп'ютерного моделювання та візуалізації оточення у сферах фотографії та фотомонтажу з урахуванням потреб сучасної культури.*

***Annotation**. The work is devoted to research of combination between two-dimensional and three-dimensional computer graphics using as an example search for new methods of applying three-dimensional computer modeling and visualization of the environment in the field of photography and photomontage considering the needs of modern culture.*

***Ключові слова**: комп'ютерна графіка, 2D графіка, 3D моделювання, 3D оточення, композитинг, CGI, фотографія, фотомонтаж.*

***Keywords**: computer graphics, 2D graphics, 3D modeling, 3D environment, compositing, CGI, photography, photomontage.*

На сучасному етапі розвитку галузь комп'ютерної графіки є потужним інструментом вирішення споживчих потреб суспільства. Сьогодні методи мультимедійних технологій, зокрема поєднання двовимірної графіки і тривимірного моделювання, візуалізації та рендерингу, дозволяють здійснити створення нових або неіснуючих з об'єктивних причин реальностей.

На сьогодні сфера комп'ютерного монтажу становить значну частину продуктів елітарної та масової культур, задовольняючи потреби як високих мистецьких жанрів, так і індустрії розваг: кіно- та фотомистецтва, засобів масової інформації, реклами, комп'ютерних та мобільних ігор і додатків тощо.

Метод композитингу – це створення цілісного зображення за допомогою суміщення кількох видів графіки (2D, 3D тощо) та її подальших шарів. Процес композитингу означає безпосередню роботу над матеріалами сцени, обробку отриманого зі сцени зображення у вигляді поєднання, редагування, накладання спеціальних та візуальних ефектів, стикування декількох зображень та моделей, тобто елементів сцени в єдине ціле, відділення елемента від фону, налаштування кольору та світлотіні. У сучасній галузі комп'ютерної графіки сумісно з таким методом часто використовуються технології **Computer-Generated Imagery** (далі – **CGI**) [1].

Фотографія, доповнена технологією **CGI**, – це процес створення реалістичних зображень на основі технологій тривимірної комп'ютерної графіки. Вона дозволяє отримувати швидкі та ефективні результати. Викорис-

тання **CGI** у процесі доповнення фотозображень дає можливість розширити спектр пропонованих ідей та послуг, зводить їх кількість до необмеженого рівня для спеціаліста у галузі ретуші та тривимірної графіки.

Синергічне поєднання фотографії та **CGI** дозволяє отримати не лише реалістичне зображення об'єкту, але й досягти сюрреалістичних візуальних ефектів, виділити продукт чи бренд, реалізувати процес зйомок, які раніше були неможливими, ігноруючи закони фізики матеріального світу.

Поєднання двовимірного зображення, зокрема, фотографічних зображень з тривимірними об'єктами у дизайні проектів дозволяє створювати оточення для задоволення будь-яких потреб вищеназваних галузей. Успіх методу полягає у створенні та обробці зображень для досягнення реалістичних результатів економічно-виваженої вартості за відносно невеликий проміжок часу. Створення реальних об'єктів оточення для фото- чи відеозйомок, як правило, займає значний часовий обсяг, часто є економічно невиправданим, або ж взагалі неможливим [2,3]. Тому на сучасному етапі розвитку мультимедійних технологій спеціалісти в галузі тривимірної комп'ютерної графіки мають можливість розробки та розвитку креативних рішень для власних проектів.

Серед беззаперечних переваг методу можна назвати його практичну гнучкість та широку інтегрованість. Сьогодні метод композитингу поширився у багатьох сферах мистецтва та бізнесу, що дало змогу компаніям-розробникам поширювати власне програмне забезпечення (далі – ПЗ), створене для задоволення потреб методу та реалізації його алгоритмів. Незважаючи на це, в основі процесу композитингу лежить гнучкість планування та комплексний підхід, що роблять можливими його реалізацію у більшості графічних двовимірних та тривимірних редакторів без необхідності звернення до спеціалізованого ПЗ.

Ще одним з плюсів методу є його ергономічність та екологічність. Сучасні редактори комп'ютерної графіки мають широкий внутрішній інструментарій для редагування об'єктів зображень, що дозволяє змінювати їх характеристики та зовнішній вигляд (розмір, колір, розташування, перспектива тощо), тому 3D моделі та сцени можуть бути скореговані на будь-якому етапі роботи та використані необмежену кількість разів. Це дозволяє уникнути надлишків незатребуваних та одноразових штучних матеріалів (пластик, поліетилен, силікон тощо), які використовуються при створенні реальних декорацій, реквізиту та при складному гримуванні.

Для досягнення високих результатів процес роботи з цим методом доцільно розподілити на декілька етапів. Як правило, основна ідея, схема розташування об'єктів та вигляд готового зображення продумуються заздалегідь аби усунути проблеми поєднання 2D та 3D об'єктів на сцені у процесі роботи. Завчасне планування, до якого входять теоретична (вибір теми, розробка ідеї, постановка задачі) та практична (створення ескізів) частини дає змогу вирішити вищеназвані проблеми галузі комп'ютерної графіки.

Наступний етап також є підготовчим проте націленим на отримання практичних результатів. Відбувається попередня підготовка графічних матеріалів: 2D зображення редагуються відповідно до поставлених задач (ретуш зображених об'єктів, фотопластика, кольорова корекція, редагування перспективи тощо), відбувається створення 3D об'єктів сцени.

Третій етап полягає в безпосередньому суміщенні 2D та 3D об'єктів для отримання необхідного вигляду у тривимірному графічному редакторі. На цьому етапі є можливим використання технології хромакею, однотонного зеленого, синього або білого тла, що розширює можливості інструментарію заміни фону в графічних редакторах.

Четвертий етап включає процес рендерингу, завданням якого є створення 2D зображення на основі отриманої завдяки суміщенню сцени. Заключний етап роботи з методом означає додаткову постобробку отриманого після рендерингу зображення, яка може бути виконана у 2D редакторах (додаткова кольорова корекція, додавання написів, готових растрових та векторних зображень тощо).

Таким чином, поєднання двовимірних фотографічних зображень із тривимірними об'єктами є актуальним прикладом складного творчо-технічного процесу, реалізація якого дозволяє досягти необмежених результатів, задовольняє потреби сучасної культури і є уособленням понять ергономіки та екологічності.

Література

1. Jon Gress. Digital Visual Effects and Compositing: 1st Edition. / Jon Gress. – New Riders Pub, 2014. – 530 p.

2. Ron Brinkmann. The Art and Science of Digital Compositing: Techniques for Visual Effects, Animation and Motion Graphics. /Ron Brinkmann. – Elsevier Science & Technology, 2008. – 704 p.

3. Kevin Karsch et al. Automatic Scene Inference for 3D Object Compositing / Kevin Karsch, Kalyan Sunkavalli, Sunil Hadap, Nathan Carr, Hailin Jin, Rafael Fonte, Michael Sittig, David Forsyth // ACM Transactions on Graphics. – 2014. – № 3. – P. 1–15

УДК 514.18

ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ У 3Д МОДЕЛЮВАННІ ВОГНЕГАСНИКА

Назарко М.Б., Мартин Є.В.
Львівський державний університет безпеки життєдіяльності

У сучасному світі всі знають що таке комп'ютер, а лише кілька десятиліть тому людство навіть не могло уявити собі подібні технології. Сьогодні за допомогою Інтернету та комп'ютера ми можемо за хвилину опинитись в будь якій частині нашої планети, та навіть за її межами.

Раніше дизайнерам доводилось все малювати за допомогою звичайних олівців та пензликів, художники малювали лише на папері чи тканині. В сучасному світі вони можуть увімкнути комп'ютер, завантажити кілька програм і почати роботу з ними. Доволі просто можна поміняти колір чи форму стола, а не перемальовувати все з початку. Подібні програми можуть бути як і для операційних систем **Windows, Mac OC, Linux Android, Ios**, прикладом такої програми може бути - **Blender** [1,2].

Перш за все слід відмітити, що програма **Blender** (рис.1) є безкоштовним, доволі потужним і багатофункціональним інструментом для роботи з тривимірною графікою [3,4,5]. Кількістю своїх функцій він практично не поступається великим і дорогим програмам. Ця система цілком підійде як для створення 3Д-моделей, так і для розробки відеороликів і мультфільмів. Незважаючи на деяку нестабільність роботи і відсутність підтримки великого числа форматів 3Д-моделей, **Blender** може похвалитися перед тим же **3ds Max** більш просунутим інструментарієм створення анімацій [6].

Блендер може виявитися складним у вивченні, так як має відносно складний інтерфейс, та незвичну логіку роботи. Зате завдяки відкритій ліцензії він може успішно використовуватись в комерційних цілях та розробці 3Д моделей пожежно-технічних об'єктів.

Рис.1. Логотип **Blender**

Основу інтерфейсу складають горизонтальні вкладки, кожна з яких відведена під певну категорію функцій, що дозволяє легко перемикатися між різними завданнями, забезпечуючи різні дії над 3D моделями в одному вікні. Праворуч у кожній вкладці містяться панелі інструментів, які мають власні вкладки, розташовані вертикально. Практично кожна функція має відповідне їй поєднання клавіш, і враховуючи кількість наданих можливостей у **Blender**, кожна клавіша включена в більш, ніж одне поєднання. З того часу як **Blender** став проєктом з відкритим вихідним кодом, було додано повні контекстні меню до усіх функцій, а використання інструментів зроблене

логічнішим та гнучкішим. Користувацький інтерфейс підтримує колірні схеми оформлення, прозорі плаваючі елементи, які розширюють функціональність **Blender**. До окремих об'єктів і навіть їх полігонів можна прикріплювати нотатки [1].

У цій програмі ми спробували зробити 3Д модель вогнеганика (рис.2). Об’єкт складається:

– важіль;
– ручка;
– корпус;
– шланг;
– насадка на розпилювач.

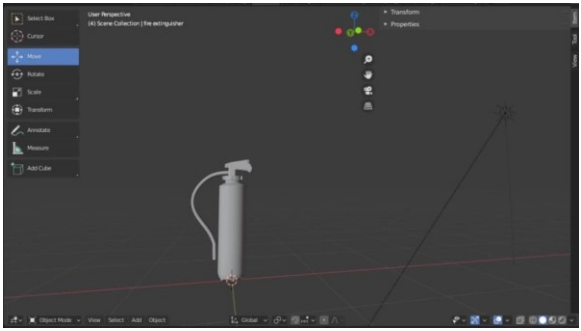


Рис. 2. Модель вогнегасника

Отже, не зважаючи на те, що **Blender** є складнішим у вивчені, проте не менш перспективний. Тому що він майже не відрізняється функціоналом і до того ж безкоштовний на відміну від інших платних програм, що значно зменшує їх доступність для студентів та інших користувачів.Тому краще використовувати абсолютно безкоштовну програму **Blender**, за допомогою якої нам вдалось розробити 3Д модель вогнегасника.

Література

1. https://uk.wikipedia.org/wiki/Blender.
2. Михайленко В.Є. Інженерна та комп’ютерна графіка / В.Є. Михайленко, В.М. Найдиш, А. М.Підкоритов, І.А. Скидан. – К.: Видавничий дім «Слово. – 352с.
3. Джеймс Кронистер. Blender Basics 4rd edition / /BlenderBasics_4thEdition2011.pdf 2011. – 178с.
4. Джеймс Кронистер. Blender Basics 3rd edition / blender-basics-3-rd-edition/download/ 2010. – 153с.
5. Роме Кодрон, П’єр-Арманд Нік. Blender 3D: Designing Objects / Blender-3D-Designing-Objects 2016. – 1281с.
6. https://blender.ru.uptodown.com/windows.

УДК 35:004.896:17

ПІДХОДИ ДО ВИКОРИСТАНЯ ШТУЧНОГО ІНТЕЛЕКТУ У РІЗНИХ ГАЛУЗЯХ ЖИТТЄДІЯЛЬНОСТІ СУСПІЛЬСТВА

Олійник А., Бурак Н.
Львівський державний університет безпеки життєдіяльності, м. Львів

У роботі досліджено можливості штучного інтелекту, які могли б бути ефективно використані в сучасному суспільстві. Розглядаються сфери у яких активно застосовується штучний інтелект, що свідчить про глибоке осмислення потреби його використання.

Ключові слова: *машинне навчання, інтелектуальний аналіз даних, автоматизація, штучний інтелект.*

The possibilities of artificial intelligence that could be effectively used in modern society are investigated in the work. Areas in which artificial intelligence is actively used are considered, which indicates a deep understanding of the need for its use.

Keywords: *machine learning, data mining, automation, artificial intelligence.*

У теперішній час організація управління багато у чому залежить від характеристик нової інформаційної економіки, завдяки комп'ютеризації суспільства та його інститутів. Характеристики нового інформаційного середовища включають підвищення ролі інформації і знань в житті суспільства й індивіда, а також уречевлення інформації і перетворення її в ключовий чинник економічного розвитку. Маркетинг різко змінився, коли з'явилися такі технології, як телефон, комп'ютер, Інтернет, а тепер і штучний інтелект.

Штучний інтелект— розділ комп'ютерної лінгвістики та інформатики, що опікується формалізацією проблем та завдань, які подібні до дій, що виконує людина.

Штучний інтелект (далі – ШІ) давно став частиною життя людини. Він допомагає відпочивати, вчитися і працювати. Сьогодні машини вже вміють розпізнавати мову, володіють технічним зором, який дозволяє їм з точністю визначати вік, стать, емоції людини, розпізнавати об'єкти (машини відповідають, які предмети бачать на малюнках, яка їхня кількість, до якого класу вони належать) і тому подібне.

Штучний інтелект має широке застосування в сучасному суспільстві. Більш конкретно, використовується для медичної діагностики, електронної комерції, дистанційного керування роботами та дистанційного зондування Землі. ШІ використовується для розробки та розвитку численних галузей, включаючи фінансування, охорону здоров'я, освіту, транспорт та інші.

Для чіткого розуміння етичних аспектів впровадження штучного інтелекту варто класифікувати їх алгоритми за інтелектуальними можливостями на прості, складні та суперінтелектуальні (див. рис.1).

Рис.1. – Класифікація алгоритмів систем штучного інтелекту

До простих відносять елементарні (локальні) інтелектуальні програми, які створені для спрощення повсякденного життя людей (наприклад навігатори, «смарт-техніка», голосові помічники). Такі програми можуть вирішувати лише локальні завдання і ніколи не зможуть вийти за їх межі. Основою складного ШІ є створення такої системи, яка могла б бути розумнішою і думати на рівні людського розуму. Алгоритми складного ШІ зможуть вирішувати будь-які інтелектуальні завдання так само, як і людина. Вони запрограмовані на самонавчання, аналіз та накопичення інформації. У свою чергу, до ключових характеристик суперінтелекту відносять здатність дума- ти, міркувати, вирішувати головоломки, виносити судження, управляти, планувати, вчитися і спілкуватися самостійно.

Розумна промисловість. Провідні світові компанії і фірми, які виявляють бажання бути конкурентоспроможними, звертають увагу на інтелектуальні рішення для виробництва:

- Автоматизація. Участь людини в налагоджених виробничих процесах скорочується до мінімуму. Завдяки автоматизації постійних дій, скорочується час виробництва і збільшуються потужності.
- Аналіз даних. Штучний інтелект не втомлюється і менше помиляється, коли потрібно обробити велику кількість даних. Наприклад, здійснювати бухгалтерські розрахунки.
- Роботизація. Роботи здатні збирати конструкції з різних деталей, бурити, досліджувати, класифікувати і тестувати. Існують роботи, які здатні аналізувати поведінку людини на виробництві і упереджувати нещасні випадки.

Найбільш активно застосовуються ШІ-технології в таких країнах, як Америка, Японія, Китай, Німеччина. Відома компанія з випуску мотоциклів Harley-Davidson за допомогою розумних систем скоротила час збирання мотоцикла з 21 дня до 6 годин. Техногігант Samsung планує повністю перевести один із заводів на виробництво, яке використовує штучний інтелект, у 2023 році.

Військова справа. ШІ є важливою технологією перспективних систем управління поля бою та озброєнням. За допомогою ШІ можливо забезпечити оптимальний та адаптивний до загроз вибір комбінації сенсорів і засобів ураження, скоординувати їх сумісне застосування, виявляти та ідентифікувати загрози, оцінювати наміри противника.

Державний сектор і штучний інтелект. Системи ШІ за допомогою камер і датчиків руху здатні стежити за порядком на вулицях міста і в місцях масового скупчення людей, прогнозувати виникнення небезпечних ситуацій і навіть впізнавати злочинців. Також розумні системи здатні з точністю проводити звірку документів, упереджувати крадіжки.

Так само технології штучного інтелекту працюють і в службах пожежної безпеки, самостійно перевіряючи, попереджаючи і приймаючи рішення щодо виклику бригади пожежників.

Розумний побут. Найпопулярніший продукт, створений із застосуванням технології ШІ, – це смарт-хаус. Не дивно, адже концепція його застосування вже відома: розумний будинок робить побут більш комфортним, упорядкованим. Система здатна стежити за безпекою житла, витратою води і світла, кліматом, контролювати стан мереж, автоматично прибирати.

Допомагають в повсякденному житті і портативні розумні пристрої – ті, які опановують переклади, фітнес-браслети, смарт-годинник.

Отже, від того наскільки швидко і результативно впроваджуватимуться інтелектуальні системи в повсякденне життя, залежить від конкретних проектів і завдань. Звичайно, штучний інтелект неможливо убезпечити від помилок і впливу зовнішніх чинників. Тож приймати важливі рішення і нести за них відповідальність, як і раніше, буде людина, але за допомогою розумних машин і програм люди зможуть працювати швидше, а також зробити своє життя більш комфортним і безпечним.

Література

1. McCarthy J. What is artificial intelligence? [Електронний ресурс] / John McCarthy. – 2007. – Режим доступу до ресурсу: http://www-formal.stanford.edu/ jmc/whatisai/.

2. Roetzer P. Content Marketing: The Path to a More (Artificially) Intelligent Future [Електронний ресурс] / Paul Roetzer. – 2017. – Режим доступу до ресурсу:
http://contentmarketinginstitute.com/2017/04/cognitivecontent-marketing-ai/.

3. Гаврилова Т. А. Базы знаний интеллектуальных систем / Т. А. Гаврилова, В. Ф. Хорошевский. – СПб: Питер, 2000. – 384 с.

4. Осипов Г. С. Искусственный интеллект: состояние исследований и взгляд в будущее / Г. С. Осипов // Новости искусственного интеллекта. – 2001. – № 1. [Електронний ресурс] / Г. С. Осипов – Режим доступу до ресурсу: http://www.raai.org/about/persons/osipov/ pages/ai/ai.html.

УДК 519.832

МІНІМАКСНИЙ ПІДХІД ДО РОЗВ'ЯЗАННЯ СТАТИСТИЧНИХ ІГОР

Павлова В. Г.
Маріупольський державний університет, м. Маріуполь

Метою даної роботи є розгляд критерію Севіджа, як інструменту моделювання в умовах невизначеності. Критерій безпосередньо пов'язаний з розв'язанням статистичних ігор та теоремою про мінімакс. Крім цього, розглянуті наступні питання: визначення поняття мінімаксної та оптимальної стратегії, а також матричної та статистичної гри.

Ключові слова: *системний аналіз, мінімаксна стратегія, статистична гра, оптимальна стратегія, матрична гра, критерій Севіджа, мінімаксний ризик.*

The purpose of this paper is to consider the Savage criterion as a modeling tool under uncertainty conditions. The criterion is directly related to the solution of statistical games and the minimax theorem. In addition, the following issues are considered: definition of the concept of minimax and optimal strategy, as well as matrix and statistical game.

Key words: *system analysis, minimax strategy, statistical game, optimal strategy, matrix game, Savage criterion, minimax risk.*

Важливим результатом професійної підготовки бакалаврів системного аналізу виступає спеціальна професійна компетентність, яка формується на основі інтеграції математичних і спеціальних інформатичних дисциплін та забезпечує їм здатність розв'язувати складні спеціалізовані задачі та практичні проблеми системного аналізу в професійній діяльності. Професійна компетентність бакалаврів системного аналізу виявляється в засвоєнні інтегрованої сукупності знань про способи професійної аналітичної діяльності та передбачає наявність в них узагальнених інтегрованих знань з теорії ігор та конфліктів [1]. Ці знання надають якісний інструмент для моделювання систем в умовах невизначеності.

Теорему мінімаксу було доведено Джоном фон Нейманом у 1928 р. Ця стратегія з часом не втратила своєї актуальності, її широко використовують в теорії ігор, теорії прийняття рішень, дослідженні операцій, статистиці та філософії.

Мінімакс – це стратегія завжди мінімізувати максимально можливі втрати, які можуть бути результатом вибору гравця. Назва «мінімакс» походить від мінімізації втрат, що виникають, коли противник вибирає стратегію, яка дає максимальні втрати, і корисно при аналізі рішень першого гравця, коли гравці рухаються послідовно або одночасно [2]. Стратегія, яка відповідає мінімаксу називається мінімаксною, та є найвідомішою стратегією гри двох гравців з нульовою сумою.

Матричною грою в математичній теорії ігор називається гра двох осіб з нульовою сумою, в якій в розпорядженні кожного з них є кінцевий безліч стратегій. Правила матричної гри визначає платіжна матриця, елементи якої - виграші першого гравця, які є також програшами другого гравця.

Матрична гра є антагоністичною грою. Перший гравець отримує максимальний гарантований (що не залежить від поведінки другого гравця) виграш, рівний ціні гри. Другий гравець намагається отримати мінімальний гарантований програш [3].

Статистична гра є специфічним видом матричних ігор. У них один з гравців є нейтральним, тобто не веде активної протидії іншому учаснику гри, та зберігає потай свою стратегію. Зазвичай такого гравця називають «природою», навколишнім середовищем або обстановкою. «Природа» не прагне використовувати в своїх інтересах помилки противника або інформацію про його стратегії [4].

Оптимальною стратегією гравця в матричній грі називається така, яка забезпечує йому максимальний виграш. Якщо гра повторюється неодноразово, то оптимальна стратегія повинна забезпечувати максимальний середній виграш.

При виборі цієї стратегії основою міркувань є припущення, що противник є, щонайменше, так само розумний, як і ми самі, і робить все, щоб добитися такої ж мети.

Розрахунок на розумного противника - лише одна з можливих позицій в конфлікті, але в теорії ігор саме вона кладеться в основу [5].

На практиці, вибираючи одне з можливих рішень, часто зупиняються на тому, здійснення якого призведе до найменш тяжких наслідків, якщо вибір виявиться помилковим. Цей підхід до вибору рішення математично був сформульований американським статистиком Севіджем в 1954 році і отримав назву «принцип Севіджа». Він особливо зручний для економічних задач і часто застосовується для вибору рішень в іграх людини з природою.

За принципом Севіджа кожне рішення характеризується величиною додаткових втрат, які виникають при реалізації цього рішення, у порівнянні з реалізацією рішення, правильного при даному стані природи. Правильне рішення не тягне за собою ніяких додаткових втрат, і їх величина дорівнює нулю. При виборі рішення слід брати до уваги тільки додаткові втрати, які, по суті, будуть наслідком помилок вибору.

Для вирішення завдання будується так звана «матриця ризиків», елементи якої показують, який збиток понесе гравець в результаті вибору неоптимального варіанта рішення.

Ризиком гравця при виборі стратегії в умовах (станах) природи називається різниця між максимальним виграшем, який можна отримати в цих умовах, і виграшем, який отримає гравець в тих же умовах, застосовуючи стратегію.

Критерій Севіджа – це критерій мінімаксного ризику, мінімізації «жалю». Цей критерій є максимально обережним і песимістичним.

У критерії Севіджа песимізм проявляється наступним чином: гіршим вважається не мінімальний виграш, а максимальна втрата виграшу в порівнянні з тим, що можна було б досягти в даних умовах (максимальний ризик) [6].

Підсумовуючи, можна зробити висновок, що мінімаксна стратегія дає змогу мінімізувати максимально можливі втрати. Якщо один із гравців дотримується оптимальної стратегії, то для другого відхилення від його оптимальної стратегії не може бути вигідним.

Для того, щоб стратегія давала якомога максимальний результат, повинні виконуватися наступні чинники:

- Гравець повинен дійсно намагатися виграти. Випадкові та необдумані дії можуть значною мірою позначитися на ефективності методу;
- Гра повинна бути суто стратегічною та виключати будь-які випадкові компоненти.

Тобто алгоритм розв'язання гри за допомогою цієї стратегії полягає у тому, щоб гравець знайшов можливі майбутні ходи, вирішив, наскільки вони ефективні та передбачив, чи зробить опонент усі правильні дії, щоб привести його до бажаного результату.

Ігри, в яких один учасник – «природа», тобто є нейтральним і його стратегія невідома, а інший – особа, яка приймає рішення, називають іграми з природою або статистичними іграми.

Критерій Севіджа дозволяє знайти найкраще рішення, яке зможе максимізувати можливий прибуток та мінімізувати можливий збиток. Критерій мінімаксного ризику корисно використовувати при розв'язанні економічних питань, бо він дає змогу отримати найбільш вигідний результат серед представлених.

Отже, головна ідея полягає у тому, щоб знайти оптимальну стратегію, яка призводить до найменш тяжких наслідків, та дотримуватися її на всіх етапах гри, саме це зможе забезпечити гравцю максимальний виграш.

Література

1. Дяченко О.Ф. Проблема проектування змісту професійної підготовки майбутніх бакалаврів з системного аналізу. *Математичні методи, моделі та інформаційні технології у науці, освіті, економіці, виробництві*: збірник тез III Всеукраїнської науково-практичної Інтернет-конференції з проблем вищої освіти і науки, м. Маріуполь, 28 квітня 2021 р. С. 12 – 13.

2. Minimax | Brilliant Math & Science Wiki. [Електронний ресурс]: https://brilliant.org/wiki/minimax/

3. Матричные игры: примеры решения задач. [Електронний ресурс]: https://function-x.ru/games_matrix_games.html

4. Понятие статистической игры. [Електронний ресурс]: https://lektsii.com/1-32920.html

5. Принцип максиміну в антагоністичних іграх. Сідлова точка. [Електронний ресурс]: https://matica.org.ua/metodichki-i-knigi-po-matematike/teoriia-igr/06-printcip-maksimina-v-antagonisticheskikh-igrakh-sedlovaia-tochka

6. Критерій Севіджа приклад рішення. Прийняття рішень в умовах невизначеності. Розрахунок платіжної матриці і матриці ризиків. [Електронний ресурс]: https://multfishki.ru/kriterii-sevidzha-primer-resheniya-prinyatie-reshenii-v-usloviyah.html.

УДК 004.622, 004.048

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ПОШУКУ КОРЕЛЯЦІЇ МІЖ ПАРАМЕТРАМИ COVID В УКРАЇНІ

Павлюк О., Стронціцька А.-О.
Національний університет «Львівська політехніка», Львів

COVID-19 спричинив серйозні проблеми та занепокоєння по всьому світі. Стан громадського здоров'я призвів до збільшення уваги у пошуковій системі Google та його активнішого висвітлення як у ЗМІ так і в глобальній мережі Internet. Це дало велику перспективу по дослідженню застосування інформаційних технологій для пошуку кореляції з COVID в Україні, по здійснених запистах у Google в Україні. Цей вплив можна кількісно оцінити, використовуючи засоби Big Data.

За допомогою такого засобу Data Mining, як компонента Google Trends здійснено пошук по 5-ти фразах які найчастіше використовувалися в пошуковій системі Google. Побудову графіків здійснили за допомогою інструменту Pandas. Весь період пандемії корона вірусу в Україні розбили на 3-ри хвилі. Для кожної з них визначили коефіцієнт кореляції Пірсона, побудувавши матриці кореляційних залежностей. По результатах обчислень доведено кореляційний зв'язок між кількістю підтверджених випадків та запитів в пошуковій системі Google по фразі «симптоми Covid». Для кожної з хвиль обчислено кількість тижнів на які здійснено випередження запитів відносно лабораторно підтверджених тестів.

Ключові слова: Covid; кореляція; хмарні сервіси; коефіцієнт кореляції Пірсона; Google Trends; Pandas; Data Mining.

COVID-19 has caused serious problems and concerns around the world. The state of public health has led to increased attention in the Google search engine and its more active coverage in both the media and the global Internet. This gave great prospects for the study of the use of information technology to find a correlation with COVID in Ukraine, according to the records made in Google in Ukraine. This impact can be quantified using Big Data tools.

Using the Data Mining tool as a component of Google Trends, we searched for 5 phrases that were most often used in the Google search engine. Graphing was done using the Pandas tool. The entire period of the coronavirus pandemic in Ukraine was divided into 3 waves. For each of them, the Pearson correlation coefficient was determined by constructing matrices of correlation dependences. The calculations show a correlation between the number of confirmed cases and queries in the Google search engine for the phrase "Covid symptoms". For each of the waves, the approximate number of weeks that separate dates of google search spikes and large numbers of positive laboratory-validated tests were calculated.

Keywords: Covid; correlation; cloud services; Pearson correlation coefficient; Google Trends; Pandas; Data Mining.

21 лютого 2020 року в Україні вперше лабораторно підтвердили COVID-19 спричинений вірусом SARS-CoV-2. А на початку листопада 2021 року Україна посіла друге місце у світі за кількістю смертей спричинених коронавірусом. За весь період в Україні спостерігали три хвилі пандемії коронавірусу. Перша тривала майже рік: з 21 лютого 2020 року до середини лютого 2021 року. Друга до середини липня 2021 року. Далі - 3-

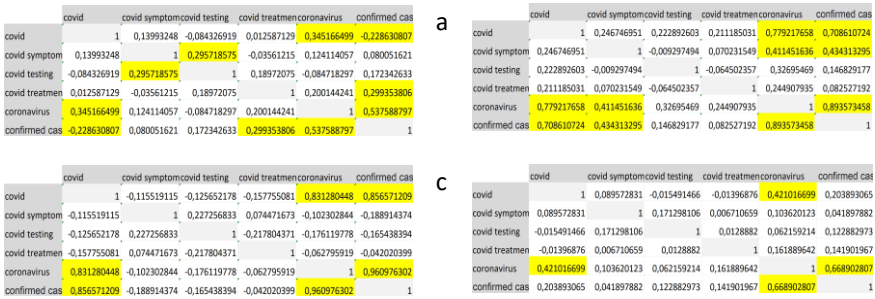
тя хвиля, яка триває й досі. Очевидно, що інтерес користувачів глобальної мережі Internet зростає із збільшенням розмаху пандемії.

Поява нового вірусу сприяла збільшенню пошуків в пошуковій системі Google. Великі черги до сімейних лікарів також спонукали до того, що багато користувачів вважали за потрібне спочатку здійснити пошук інформації про симптоми в пошуковій системі Google, а потім звернутися до лікарів. Отже, на пошуковому сервері Google була зібрана статистика по запитах користувачів із фразами пов'язаними з COVID. Також є загальнодоступна "стандартна" статистична інформація по covid яка включає: кількість лабораторно підтверджених випадків; кількість смертей; кількість здійснених вакцинувань та ін. По цій інформації можна здійснювати прогнозування вищеперерахованих параметрів. Часто для цього використовують саме штучні нейронні мережі [1, 2, 3, 4]. Вони дають досить високу точність прогнозів при значному обсязі статистичної інформації. Проте на перших хвилях пандемії, коли кількість "стандартної" статистичної інформації була малою, виникла необхідність у додаткових даних. Всі дані можна отримати за допомогою засобів Data Mining з пошукового сервера Google.

Google Trends – це корисний інструмент Data Mining для відстеження соціальних тенденцій [5, 6, 7]. Дані Google Trends на тему «COVID» використано для дослідження кореляції між параметрами пов'язаними з коронавірусом в Україні. У цьому дослідженні були зроблені підготовчі кроки для розробки експериментального інструмента пошуку кореляційних залежностей у даних по коронавірусу в Україні. А також пошуку основних механізмів, що впливають на поширення та розвиток хвороби.

«Стандартні» статистичні дані про «Covid» отримані з відкритих джерел сайту https://ourworldindata.org/coronavirus/country/ukraine. Із цієї статистики відвільтрували лабораторно підтверджені випадки корона вірусу в Україні. Додаткові дані отримані по 5-ти фразах, які найчастіше використовувалися при пошуку в Google: «covid»; «covid symptoms»; «covid testing»; «covid treatment»; «coronavirus». Дані зчитали засобом Pandas. Їх посортували за датою. Далі проведено імпорт даних Google Trends і зроблено перевірку, що вони мають числовий формат. Дані користувачів з пошуків у Google зняті щотижня, а дані Covid - щодня. Тож потрібно усереднити дані Covid таким чином, щоб отримати сукупні випадки за кожен тиждень.

По 6-тьох параметрах: «covid»; «covid symptoms»; «covid testing»; «covid treatment»; «coronavirus»; «confirmed cases» складено матриці кореляційних залежностей для кожної хвилі пандемії коронавірусу в Україні. На перетині комірок матриці записано порахований коефіцієнт кореляції Причому додатні значення коефіцієнта кореляції Пірсона свідчать про пряму залежність: із зростанням одного параметра – зростає й інший. она для двох параметрів розміщені у відповідному рядку та стовбці. Матриці кореляційних залежностей наведені рис. 1.



	covid	covid symptom	covid testing	covid treatmen	coronavirus	confirmed cas
covid	1	0,13993248	-0,084326919	0,012587129	0,345166499	-0,228630807
covid symptom	0,13993248	1	0,295718575	-0,03561215	0,124114057	0,080051621
covid testing	-0,084326919	0,295718575	1	0,18972075	-0,084718297	0,172342633
covid treatmen	0,012587129	-0,03561215	0,18972075	1	0,200144241	0,299353806
coronavirus	0,345166499	0,124114057	-0,084718297	0,200144241	1	0,537588797
confirmed cas	-0,228630807	0,080051621	0,172342633	0,299353806	0,537588797	1

a

	covid	covid symptom	covid testing	covid treatmen	coronavirus	confirmed cas
covid	1	0,246746951	0,222892603	0,211185031	0,779217658	0,708610724
covid symptom	0,246746951	1	-0,009297494	0,070231549	0,411451636	0,434313295
covid testing	0,222892603	-0,009297494	1	-0,064502357	0,32695469	0,146829177
covid treatmen	0,211185031	0,070231549	-0,064502357	1	0,244907935	0,082527192
coronavirus	0,779217658	0,411451636	0,32695469	0,244907935	1	0,893573458
confirmed cas	0,708610724	0,434313295	0,146829177	0,082527192	0,893573458	1

	covid	covid symptom	covid testing	covid treatmen	coronavirus	confirmed cas
covid	1	-0,115519115	-0,125652178	-0,157755081	0,831280448	0,856571209
covid symptom	-0,115519115	1	0,227256833	0,074471673	-0,102302844	-0,188914374
covid testing	-0,125652178	0,227256833	1	-0,217804371	-0,176119778	-0,165438394
covid treatmen	-0,157755081	0,074471673	-0,217804371	1	-0,062795919	-0,042020399
coronavirus	0,831280448	-0,102302844	-0,176119778	-0,062795919	1	0,960976302
confirmed cas	0,856571209	-0,188914374	-0,165438394	-0,042020399	0,960976302	1

c

	covid	covid symptom	covid testing	covid treatmen	coronavirus	confirmed cas
covid	1	0,089572831	-0,015491466	-0,01396876	0,421016699	0,203893065
covid symptom	0,089572831	1	0,171298106	0,006710659	0,103620123	0,041897882
covid testing	-0,015491466	0,171298106	1	0,0128882	0,062159214	0,122882973
covid treatmen	-0,01396876	0,006710659	0,0128882	1	0,161889642	0,141901967
coronavirus	0,421016699	0,103620123	0,062159214	0,161889642	1	0,668902807
confirmed cas	0,203893065	0,041897882	0,122882973	0,141901967	0,668902807	1

Рис. 1. Матриці кореляційних залежностей між параметрами по Covid в Україні (a, b, c, d – першої, другої, третьої, та всії разом хвилі пандемії відповідно)

У всьому періоді пандемії коронавірусу в Україні корелювали такі пари параметрів: coronavirus - confirmed cases; covid – coronavirus. Решту залежностей між параметрами не носять такого явно вираженого характеру. У першій хвилі пандемії найбільшу кореляційну залежність мали такі пари параметрів: coronavirus - confirmed cases; coronavirus – covid; covid symptoms- covid testing; confirmed cases - covid. Оскільки у цій хвилі пандемії Covid-19 це була нова вірусна хвороба про яку досі більшість користувачів глобальної мережі Internet не знали. Тому їх більше цікавили саме симптоми цієї хвороби, скільки людей нею захворіло (клінічно підтверджені випадки), де можна протестуватись на її наявність, а також як вилікуватися від неї.

У другій хвилі пандемії найбільше корелюють такі пари параметрів: coronavirus – confirmed cases; coronavirus – covid; confirmed cases- covid symptoms; coronavirus - covid symptoms. У ній зросла кількість параметрів, що корелюють з клінічно підтвердженими випадками хвороби і прямопропорційна залежність стала ще на 40% більш вираженою.

Третя хвиля пандемії триває й досі. Тому коефіцієнти кореляції Пірсона можуть змінюватися. Станом на початок листопада виявлена така залежність між парами параметрів: coronavirus - confirmed cases; confirmed cases – covid; covid – coronavirus.

Проведений огляд проблеми застосування інформаційних технологій для пошуку кореляції між кількістю підтверджених випадків та запитів в пошуковій системі Google по Covid. Проаналізовано попередні дослідження, які показали зв'язок між тенденціями веб-пошуку та традиційними показниками Covid-19. Дослідження показало, що висвітлення інформації про коронавірус у мережі Інтернет призвело до активізації пошуків про можливі симпотоми даної хвороби. Цей вплив можна кількісно оцінити, використовуючи засоби Big Data. За допомогою коефіцієнта кореляції Пірсона доведено кореляційні залежності між параметрами, що описують Covid. Отже, ефективність застосування інформаційних технологій для пошуку кореляції між параметрами Covid в Україні була підтверджена.

Література

1. Jiachen Sun, Peter A. Gloor. Assessing the Predictive Power of Online Social Media to Analyze COVID-19 Outbreaks in the 50 U.S. States // Future Internet 2021, 13(7), 184; https://doi.org/10.3390/fi13070184
2. Rabiolo A, Alladio E, Morales E, Marchese A. Forecasting the COVID-19 Epidemic by Integrating Symptom Search Behavior Into Predictive Models: Infoveillance Study doi:10.2196/28876
3. Pavliuk O., Strontsitska A., Dunaev R., Derkachuk R. Forecast of the number of new patients and those who died from COVID-19 in Bahrain // Decision aid sciences and applications : International conference, (7–9 November 2020, Sakheer, Bahrain, 2020). – 2020. – С. 422–426 https://doi.org/10.1109/dasa51403.2020.9317122
4. Borghi P.H., Zakordonets, O., Teixeira, J.P. A COVID-19 time series forecasting model based on MLP ANN. // Procedia Computer Science Volume 181, 2021, Pages 940-947// DOI: 10.1016/j.procs.2021.01.250
5. Tseng Q. Reconstruct Google Trends Daily Data for Extended Period. towards data science. 2019. https://towardsdatascience.com/reconstruct-google-trends-daily-data-for-extended-period-75b6ca1d3420
6. Cervellin G, Comelli I, Lippi G. Is Google Trends a reliable tool for digital epidemiology? Insights from different clinical settings. J Epidemiol Glob Health 2017 Sep;7(3):185-189. https://doi.org/10.1016/j.jegh.2017.06.001
7. U Venkatesh, Periyasamy Aravind Gandhi. Prediction of COVID-19 Outbreaks Using Google Trends in India: A Retrospective Analysis // Healthc Inform Res. 2020 Jul; 26(3): 175–184. doi: 10.4258/hir.2020.26.3.175

УДК 004.42

РОЗРОБКА ДОДАТКУ «БІРЖА АГАРНИХ ПОСЛУГ»

Пенхерський М., Мозуль Х., Татомир А.
Львівський національний аграрний університет, м. Дубляни

У роботі представлено аспекти та особливості розробки програмного додатку «Біржа агарних послуг». Подано основні технології використанні для створення сервісів серверної сторони додатку та клієнтського відображення даних. Відображено взаємодію користувачів між собою у формі замовник-виконавець.

Ключові слова: розробка, програмний додаток, біржа, агарні послуги.

The paper presents aspects and features of the development of the software application "Agar Services Exchange". The basic technologies used to create services on the server side of the application and client data display are presented. The interaction of users with each other in the form of the customer-executor is displayed.

Keywords: development, software application, exchange, agar services.

Інформаційні технології взаємодіють та впливають на продуктивність сільського господарства різними способами [1, 2]. Це може допомогти у прийнятті рішень щодо використання земель, працівників, технічного устаткування, капіталу та управління. Продуктивність діяльності у сільському господарстві може бути покращена за допомогою відповідної, надійної, зручної та швидкої технології для обміну інформацією про доступні ресурси та працівників [3, 4].

Сьогодні інноваційні інформаційні технології в сучасному сільському господарстві важливі як ніколи раніше. Галузь стикається з величезними проблемами – від зростання витрат на поставку, зміни в уподобаннях споживачів щодо прозорості та стійкості, до найважливішої проблеми – нестачі робочої сили. Сільськогосподарські компанії дедалі більше усвідомлюють необхідність вирішення цих проблем завдяки впровадженню інноваційних інформаційних технологій. За останні 10 років сільськогосподарські технології зафіксували величезний ріст інвестицій у розвиток інформаційних технологій. Основні технологічні інновації в космосі зосереджені на таких сферах, як вертикальне землеробство в приміщеннях, автоматизація та робототехніка, технології тваринництва, сучасні тепличні практики, точне землеробство та штучний інтелект та блокчейн.

Оглядаючи ринок інформаційних технологій пов’язаних з аграрними технологіями нами встановлено, що на ринку дуже мало дещо схожих аналогів до пропонованого нами додатку «Біржа агарних послуг». Яскравим прикладом використання інформаційних систем і технологій в аграрній сфері є NASA World Wind – безкоштовна Open-Sorce API для візуалізації світу в 4D, такі як супутникове відстеження та сейсмічна історія. Команда спеціалістів NASA World Wind 2017 розробила освітню вебпрограму, яка візуалізує вплив зміни клімату на сільське господарство, використовуючи велику колекцію глобальних даних про сільське господарство та клімат та Web World Kit Software Development Kit (SDK).

Серверна сторона будь якої інформаційної системи грає велику роль у збереженні, захисті та обробці даних користувача. Нами пропонується додаток «Біржа агарних послуг», який за основу для розробки серверної сторони передбачає використання платформи Node.js. Node.js – це платформа створена для розширення застосування вузько направленого асинхронного коду на JavaScript для загального використання.

Також передбачається використання Apollo Server – це сервер GraphQL із відкритим вихідним кодом, сумісний зі специфікаціями та з будь-яким клієнтом GraphQL, включаючи Apollo Client. Це найкращий спосіб створити готовий до самостійного самодокументування API GraphQL, який може використовувати дані з будь-якого джерела рис. 1.

Також важливу роль при створенні додатку відіграє швидке повідомлення користувача про певні дії додатку або інших користувачів, які можуть бути пов’язанні з ними. Саме таку роль в додатку передбачено частині під назвою notification service. Це реалізовано на основі технологій Websoket. Обгорткою для цієї технології буде служити бібліотека Socket.io.

Одним із головних компонентів будь якої інформаційної системи є база даних для зберігання даних користувачів, дій сервісу та багатьох інших операцій. У запропонованому додатку використовуватиметься зразу дві бази даних. Одна як основна для зберігання усього масиву даних. Найкращим та найзручнішим варіантом є Mongodb.

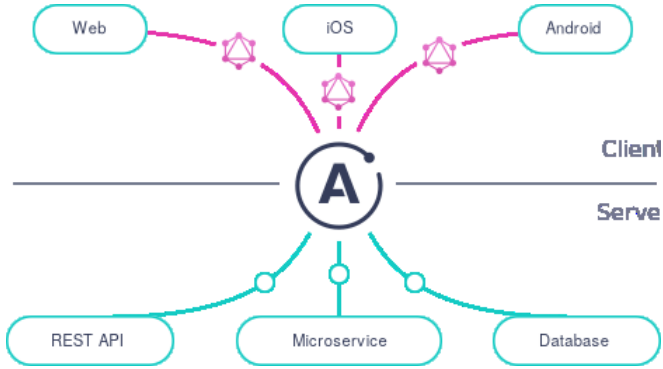


Рис. 1. Схема зв'язків за допомогою Apollo Graphql

MongoDB – документована база даних на основі формата JSON, є найяскравішим прикладом NoSQL-систем. JSON – це формат обміну та зберігання інформації на основі об'єктів Jsvascript (JavaScript Object Notation). На рисунку 2 показано приклад зберігання інформації у базі даних MongoDB в форматі JSON.


```
_id: ObjectId("5fd9e7cd61c3a955b8025b5b")
type: "customer"
active: true
› profile: Array
email: "JohnWick@gmail.com"
name: "Keanu Reeves"
provider: "email"
createdAt: 2020-12-16T10:56:13.757+00:00
updatedAt: 2021-02-10T07:01:26.444+00:00
__v: 0
birthday: 1984-01-11T00:00:00.000+00:00
› categoriesId: Array
description: "Киа́ну Чарльз Ривз (англ. Keanu Charles Reeves, [kiˈɑːnuː]; род. 2 сен..."
firstName: "Keanu"
lastName: "Reeves"
middleName: "Charles"
deleted: false
```


Рис. 2. Формат даних JSON

Практичне використання додатку «Біржа агарних послуг» полягає у тому, щоб створити зручний швидкий та безпечний інструмент поєднання працівників та роботодавців в аграрній сфері. Додаток «Біржа агарних послуг» дозволить замовникам швидко знаходити потрібних їм працівників, робоче устаткування та ресурси для вирішення їхніх проблем при роботі. У свою чергу багато працівників зможуть без проблем надавати послуги та отримувати плату за них.

Література

1. Тригуба А.М., Шелега О.В., Пукас В.Л., Михайлюк В.М. Узгодження конфігурацій інтегрованих проектів аграрного виробництва. *Вісник Національного технічного університету «ХПІ». Серія : Стратегічне управління, управління портфелями, програмами та проектами*. 2015. 2. С. 135-140. Режим доступу: http://nbuv.gov.ua/UJRN/vntux_ctr_2015_2_27. (Last accessed: 12.05.2021).

2. Tryhuba A., Ratushny R., Tryhuba I., Koval N. and Androshchuk I., The Model of Projects Creation of the Fire Extinguishing Systems in Community Territories, in: Acta universitatis agriculturae et silviculturae mendelianae brunensis. 68, 2, 2020, pp. 419-431.

3. Tryhuba A., Bashynsky, I. Garasymchuk, O. Gorbovy et al., Research of the variable natural potential of the wind and energy energy in the northern strip of the ukrainian carpathians, in: 6th International Conference : Renewable Energy Sources (ICoRES 2019). E3S Web of Conferences 154, 06002, 2020.

4. Tryhuba A., Tryhuba I., Bashynsky O., et al., Conceptual model of management of technologically integrated industry development projects, in: 15th International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT), 2, pp. 155-158, September 2020.

УДК 004.9

ДОДАТКОВИЙ ФУНКЦІОНАЛ ДЛЯ САЙТУ ZNYMKYHUB ВИКОРИСТОВУЮЧИ MICROSOFT AZURE (FACE API)

Романчук В.
Львівський національний університет імені Івана Франка, м. Львів

У роботі реалізовано додатковий функціонал, а саме фільтрація фото за допомогою Microsoft Azure (Face API), до сайту «ZnymkyHub», який був розроблений минулого року.
Ключові слова: *сайт, Microsoft Azure, аналіз обличчя, хмарний сервіс.*

The paper presents an additional functionality: photo filtering using Microsoft Azure (Face API), for site "ZnymkyHub", which was developed last year.
Keywords*: site, Microsoft Azure, facial analysis, cloud service.*

Робота над сайтом «ZnymkyHub» триває вже тривалий час і було вирішено вдосконалювати і розвивати його. У ході теоретичного аналізу досліджено, що найбільш зручно і надійно використовувати багатофункціональний фреймворк ASP.NET Core, який надає можливість розробки швидких API для веб-сайтів. Для створення бази даних використовувався принцип Code First, для створення інтерфейсів – Vue.js та для можливості спілкування – SignalR. У результаті, користувачі мають наступні можливості:

- зареєструватися як фотограф і створити своє портфоліо (додавання фотографій);
- зареєструватися як клієнт і мати змогу знайти фотографа, який підходить по місці знаходження, ціні та іншим вимогам; відмічати фотографії, які сподобались найбільше, зберігати їх;
- можливість обговорювати різні питання між клієнтами та фотографами за допомогою форуму.

Новий функціонал сайту допомагає користувачам відфільтрувати фото за обличчям за допомогою Microsoft Azure [1][2]. Чому саме такий функціонал було вирішено реалізувати? Наприклад, на різні події такі як: день народження, весілля, перше причастя тощо, зазвичай запрошують фотографа, для того щоб зафіксувати всі важливі моменти. Здається вже не мало б виникнути ніяких проблем, та коли ви отримуєте фото, то це не тільки ваші світлини, а й всіх інших людей, які були на святі. Таким чином, приходиться перебирати дуже багато фотографій і відсортовувати ваші фото. Тому для того, щоб не робити це вручну, ви можете на сайті завантажити фото людини, яку вам потрібно знайти і також завантажити фотографії, серед яких потрібно здійснити пошук. У результаті отримаєте архів з фотографіями на яких є людина, яку ви шукали.

Також для зручнішого користування, реалізовано підвантаження фото з хмарних середовищ, так як фотографи зазвичай скидують фотографії саме на них. Таким чином, робота з даним фільтром стає ще простішою. Ера дисків та флешок відходить у минуле, а актуальність хмарних сервісів важко переоцінити.

Висновки. У результаті, використовуючи Microsoft Azure Face API, було реалізовано зручний функціонал для фільтрування фотографій. Користувач завантажує головну фотографію особи, за якою система буде шукати її серед набору фото, які також повинен завантажити користувач або підвантажити їх з хмарного середовища. У результаті повертається архів з потрібними вам фотографіями.

Література

1. *Що таке Microsoft Azure?* : веб-сайт. URL: https://ua.phhsnews.com/articles/howto/what-is-microsoft-azure-anyway.html
2. *Azure Cognitive Services REST API for Face Analysis* веб-сайт. URL: https://medium.com/microsoftazure/azure-cognitive-services-rest-api-for-computer-vision-cf782e975837

УДК 004.4'2

РОЗВИТОК ОБЧИСЛЮВАЛЬНОГО МИСЛЕННЯ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ В ПРОЦЕСІ НАВЧАННЯ ДИСКРЕТНОЇ МАТЕМАТИКИ

Ротаньова Н., Мараховський Д.
Маріупольський державний університет, м. Маріуполь

У дослідженні на основі аналізу вітчизняних та зарубіжних наукових праць визначено сутність поняття «обчислювальне мислення» як багаторівневого мисленнєвого утворення, сформованість якого відбиває здатність людини вирішувати складні (освітньо-наукові, виробничі) завдання. З'ясовано, що вивчення навчальної дисципліни «Дискретна математика» уможливлює розвиток обчислювального мислення здобувачів вищої освіти.

Ключові слова: *обчислювальне мислення, дискретна математика, здобувачі вищої освіти.*

The present study is aimed at exploring the concept of computational thinking in domestic and foreign research. Computational thinking has been defined as a multifaceted mental formation which reflects person's ability to solve complicated (educational, scientific and job-related) problems. It has been found that learning Discrete Mathematics enables to develop computational thinking of higher education seekers.

Key words: *computational thinking, Discrete Mathematics, higher education seekers.*

В умовах цифрової трансформації освіти набуває актуальності розвиток обчислювального мислення майбутніх фахівців. Сутність поняття «обчислювальне мислення» (computational thinking) розкрито вітчизняними та зарубіжними дослідниками. Зокрема українські вчені Т. Тихонова та Г. Кошкіна інтерпретують його як розумову здатність особистості вирішувати складні проблеми через конструювання систем та процесів за допомогою комп'ютерів. Авторки виокремлюють наступні компоненти обчислювального мислення: декомпозицію, розпізнавання шаблонів, абстракцію і алгоритми, й зазначають, що цей вид мислення охоплює всі інші його види, а саме: процесуальне, алгоритмічне, структурне й критичне [1, с. 210].

Відзначимо, що поняття «обчислювальне мислення» є найбільш вивченим у зарубіжній науці. Уперше в науковий обіг його було введено американською дослідницею Дж. Уінг, яка спочатку визначила обчислювальне мислення як підхід до вирішення проблем, проєктування систем та розуміння людської поведінки, який спирається на фундаментальні обчислювальні поняття. У наступних наукових працях дослідниця уточнила, що обчислювальне мислення являє собою процеси, які беруть участь у формулюванні проблем та їх розв'язанні [6-8]. Сформоване обчислювальне мислення, на думку Дж. Уінг та її колег, дозволяє вирішувати відкриті або напіввідкриті завдання, в яких і процес, і результат є невизначеними, й таким чином розвиває готовність до непередбачуваних ситуацій [9]. Отже, на відміну від вітчизняних учених зарубіжні дослідники визначають обчислювальне мислення не як здатність, а як мисленнєвий процес, та вказують, що цей тип мислення охоплює абстрактне, логічне, моделююче та конструктивне мислення [2, с. 413]. На процесуальній та, зокрема творчій, природі обчислювального мислення акцентовано і в інших визначеннях: наприклад, його розуміють як комплекс когнітивних і метакогнітивних стратегій з метою проєктування та конструювання обчислювальних систем, й у широкому значенні – як процес генерування ідей, альтернатив чи можливостей для вирішення проблем, інтегрування технологій інноваційним способом [4].

Учені наголошують, що в XXI столітті обчислювальне мислення є фундаментальним та необхідним для фахівця інженерно-технічного напряму, тому важливою є орієнтація математичної освіти на розвиток обчислювального мислення у майбутніх учених, математиків та інженерів [3, с. 99]. Цінною є думка, що ідеальна методологія математичної освіти має бути спрямованою на глибоке розуміння здобувачами ключових математичних понять та формування їхніх умінь застосовувати комп'ютерні технології для вирішення складних завдань. Опанування комп'ютерних алгоритмів без необхідної математичної бази знань може призвести до неправильної інтерпретації результатів. І навпаки, вивчення математики без технологічного супроводу може в значній мірі обмежити коло проблем, котрі вирішують студенти за допомогою викладачів на заняттях [5, с. 429].

Вважаємо, що розвиток обчислювального мислення, зокрема здобувачів вищої освіти спеціальностей 124 Системний аналіз та 125 Кібербезпека, буде ефективним у процесі опанування навчальної дисципліни «Дискретна математика». Відомо, що в процесі її вивчення систематизуються попередні знання з класичної та вищої математики, й водночас усвідомлюється роль математичних методів у створенні комп'ютерних систем та програмного забезпечення. Дискретна математика має справу з числами, графіками, іграми та іншими об'єктами, які є дискретними, а не безперервними; слугує основою для інформатики та охоплює криптографію, комбінаторику, теорію ігор, логіку, теорію чисел, дослідження операцій та теорію множин, тому її вивчення сприятиме розвитку обчислювального мислення здобувачів, готуючи їх до опанування інших навчальних дисциплін (інформатики, теорії алгоритмів, алгоритмічних мов, програмування, конструювання тощо), орієнтуванню в інформаційному просторі та вирішенню за-

вдань системного аналізу та кібернетичної безпеки за допомогою методів дискретної математики (графічних, логічних, теоретико-множинних).

Результати педагогічних спостережень свідчать про те, що часто здобувачі вищої освіти ІТ-спеціальностей не повною мірою усвідомлюють прикладне застосування дискретної математики й доцільність розвитку обчислювального мислення в процесі її вивчення. У зв'язку із цим важливо продемонструвати, що опанування теорії чисел є значущим для створення, зламування та відтворення цифрових паролів у криптографії; також засвоєння теорії графів допоможе вирішувати складні логістичні завдання; групувати та впорядковувати інформацію для баз даних організацій, компаній та підприємств; окрім того, основні положення дискретної математики використовуються для розроблення алгоритмів і комп'ютерних програм.

Узагальнюючи думки вітчизняних та зарубіжних учених, необхідним є надати комплексне визначення поняття «обчислювальне мислення», яке б розкривало його як якісний стан та процесуальне явище. Отже, на наш погляд, обчислювальне мислення здобувача вищої освіти – це багаторівневе мисленнєве утворення, що включає репродуктивне та продуктивне (творче) мислення, й сформованість якого відбиває здатність майбутнього фахівця вирішувати складні (освітньо-наукові, виробничі) завдання.

Література

1. Тихонова Т., Кошкіна Г. Computational thinking як сучасний освітній тренд. *Електронне наукове фахове видання «Відкрите освітнє середовище сучасного університету»*. 2018. № 5. С. 210-221.

2. Liu J., Wang L. Computational Thinking in Discrete Mathematics. 2010. Vol. 1. P. 413-416.

3. Rambally G. Emerging Research, Practice, and Policy on Computational Thinking. 2017. P. 99-119.

4. Romero M., Lepage A., Lille B. Computational thinking development through creative programming in higher education. *International Journal of Educational Technology in* ***Higher*** *Education*. Vol. 14. № 42. 2017. URL: https://doi.org/10.1186/s41239-017-0080-z

5. Sinkovits R., Soto O. Introducing Computing and Technology through Problem-Solving in Discrete Mathematics. *Practice and Experience in Advanced Research Computing*. 2020. P. 429-435.

6. Wing J. Computational thinking. *Communications of the ACM*. 2006. Vol 49. № 3. P. 33–35.

7. Wing J. Computational thinking and thinking about computing. *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences.* 2008.Vol. 366. № 1881. P. 3717–3725.

8. Wing J. Research notebook: Computational thinking-What and why? *The Link Newsletter*. 2011. № 6. P. 1–32. URL: http://link.cs.cmu.edu/files/11-399_The_Link Newsletter-3.pdf.

9. Zhong B., Wang Q., Chen J., Li Y. An exploration of three-dimensional integrated assessment for computational thinking. *Journal of Educational Computing Research.* 2016. Vol. 53. № 4. P. 562–590.

УДК 004.94+614

ЗАСТОСУВАННЯ НЕЙРОМЕРЕЖ ДЛЯ ДОСЛІДЖЕННЯ ПАРАМЕТРІВ ЕВАКУАЦІЇ ПІД ЧАС ПОЖЕЖІ

Сировий В., Хлевной О.
Львівський державний університет безпеки життєдіяльності

Проаналізовано вітчизняний та закордонний досвід моделювання процесів евакуації з будівель різного призначення під час пожежі та розкрито перспективи застосування нейромереж для визначення основних параметрів руху евакуаційних потоків.

Ключові слова: *нейронна мережа, евакуація при пожежі, тривалість евакуації, штучний інтелект*

Ukrainian and foreign experience in modeling the evacuation processes during a fire has been analyzed and the prospects of using neural networks to determine the basic parameters of evacuation flows have been revealed.

Keywords: *neural network, fire evacuation, evacuation duration, artificial intelligence*

Нещодавно вчені університету Мічігану представили алгоритм, який допомогає автомобілям, що використовують автопілот, розпізнавати напрямок і передбачати рухи пішоходів. Зібравши дані за допомогою камер, лідарів та GPS, розробники створили датасет та навчили рекурентну нейронну мережу передбачати рухи людини з точністю до 10 см.

Модель називається Bio-LSTM. Це рекурентна нейронна мережа з LSTM, яка може передбачити розташування та 3D-позу пішохода на основі попереднього кадру. Мережа здатна прогнозувати позу з відривом до 45 метрів для кількох пішоходів одночасно. Підхід спирається на аналіз темпу людини, включаючи дзеркальну симетрію тіла та вивчення того, як становище ніг впливає на стійкість під час ходи.

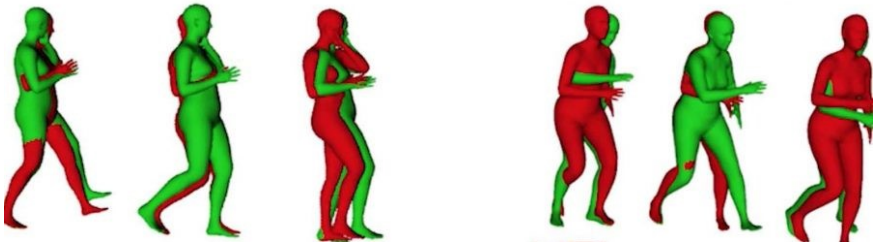


Рисунок 1 – Прогнозування нейромережею рухів людини

Нейромережу навчили на наборі даних PedX, який був зібраний у реальних міських умовах на перехрестях. Автомобілі з четвертим рівнем автономності записували дані за допомогою камер, лідерів та GPS. Використовуючи відеозаписи з рухами завдовжки кілька секунд, мережа навчилася прогнозувати рух. Спочатку їй показувався перший фрагмент відео з початком руху, потім система прогнозувала, після чого перевіряла точність, звіряючи свій результат з інформацією з другої частини відео.

Розробники протестували метод на датасеті PedX та даних з mocap. Результати показують, що метод можна використовувати для передбачення та класифікації рухів пішоходів. Точність можна порівняти з іншими сучасними методами.

Результати таких досліджень наштовхують на перспективи застосування нейронних мереж для моделювання руху людських потоку різного складу під час евакуації з будівель і споруд при пожежі.

Моделювання процесів евакуації під час пожежі з будівель різного призначення передбачає формування баз емпіричних даних, що характеризують параметри руху людських потоків різного складу. Склад потоків (віковий, гендерний тощо) для різних об'єктів суттєво відрізняється, відтак, виникає одразу дві потреби. Перша – створення адекватних моделей для прогнозування руху потоків і, відтак, точного розрахунку тривалості евакуації. Друге – для формування баз даних параметрів руху необхідно провести велику кількість натурних досліджень та здійснити їх обробку. Це кропітка механічна праця, яка потребує автоматизації. Саме нейронні мережі здатні забезпечити реалізацію обох потреб.

Висновок. Технології машинного навчання дають змогу навчати нейромережі аналізувати структуру потоків в громадських будівлях та визначати основні параметри – залежність швидкості руху потоку від щільності. Це досить актуально при організації евакуації людей з громадських місць. Нейромережа за даними камер відеоспостереження підраховує загальну кількість людей та у разі виникнення пожежі може прогнозувати напрямки та тривалість руху евакуаційних потоків. Ці технології можуть використовуватись у системах оповіщення та управління евакуацією задля запобігання утворення скупчень та тисняви.

Література

1. Vedant Kumar. Applications of Artificial Intelligence in Fire & Safety. Overview of the applications of AI in mitigating the dangers due to fire.

2. Eric Wai Ming Lee. Application of Artificial Neural Network to Fire Safety Engineering https://link.springer.com/chapter/10.1007/978-3-642-13639-9_15

УДК 004.94

СУЧАСНІ ЗАСОБИ ВІЗУАЛІЗАЦІЇ ДАНИХ

Сировий В., Борзов Ю.
Львівський державний університет безпеки життєдіяльності, м. Львів

У роботі розглянуто поняття перспективи як невід'ємної складової зображення даних. Наведено приклади візуалізації в різних сферах діяльності та описано способи ілюстрації даних різних типів.

Ключові слова: *візуалізація даних; цифрова візуалізація; графіки; розподіли; пропорції; геопросторові дані*

The article considers the concept of perspective as an integral part of of data visualization. Examples of visualization in different areas of activity are given and methods of illustrating data of different types are described.

Key words: *data visualization; digital visualization; graphics; distribution; proportions; geospatial data*

З розвитком інформаційних технологій значно збільшилися об'єми інформації, а відтак способи її зберігання та обробки. Нові методики відчутно полегшують роботу та підвищують ефективність під час роботи з даними. Розвиток інформаційних інструментів призвів до зміни подання інформації, зокрема до її візуалізації – графічного представлення даних, завдяки якому в лаконічній формі можна представити те, що на папері займе не один абзац. Завдяки своїй наочності, графічна презентація підвищує ефективність сприйняття та допомагає сконцентрувати увагу на головному. Дослідження показали що люди, які читали лише текстову інструкцію ліків засвоїли 70% від прочитаного. Натомість етикетки із зображеннями освоїли 95% опитуваних. Сьогодні візуальне представлення даних набуло великої популярності, проте мало людей замислюються над тим, чому графіки та гістограми є більш ефективні за текст та числа. З усього вище сказаного випливає необхідність правильного обґрунтування способів та вибору візуалізації.

Розширення людського сприйняття є головним завданням візуалізації. Вона повинна створити об'ємнийсвіт, в якому інформація буде сприйматися максимально повно, у трьох вимірах: ширині, висоті, довжині. У вирішенні цього завдання нам допоможе прийом для створення об'ємності доби Ренесансу – перспектива. Вона змушує людину відчувати окремі елементи та звертати на них увагу. Перспектива завжди залучається під час створення діаграм, гістограм, графіків та карт – найбільш популярних технологій візуалізації інформації, де кожен компонент має своє місце, а дані розташовані відносно один одного.

Діаграма є одним з найпоширеніших способів візуалізації даних, тому сьогодні існує їхнє велике різноманіття:

Для зображення прогресу та тенденції рекомендовано використовувати лінійну діаграму. Вона також використовується для візуального зо-

браження різних категорій даних, абопід час побудови графіка, заснованого на тривалому зборі даних.

Обласна діаграма (діаграма площ) заповнює кольором або малюнком простір між лінією та віссю абсцис.Такий спосіб візуалізації підходить для демонстрації відносин між частинами одного цілого,.

Діаграма з подвійною віссю дозволяє видобувати дані з використанням двох осей – осі абсцис та осі ординат. Такий варіант дозволяєпроілюструвати кореляцію або її відсутність між різними показниками.

Для порівняння великої кількості різних складових використовують штабельну діаграму. Зокрема, щоб зобразити кількість відвідувачів декількох сторінок та кожного сайту окремо.

Щоб зобразити склад чого-небудь, тобто як частини складаються в одне ціле, використовують кругову діаграму. Такий варіант візуалізації показує числа у відсотках, де загальна сума всіх компонентів повинна дорівнювати 100%

Діаграма-водоспад використовується для зображення того, як проміжні значення – негативні й позитивні – впливають на початкове значення і призводять до фінального результату. Зокрема, за допомогою цієї діаграми можна показати залежність загального доходу компанії від різних відділів.

Щоб зобразити зв'язок між двома змінними використовують точкову діаграму. Вона підходить, якщо ви хочете знайти загальне в наборі різних точкових даних.

Для порівняння між різними елементами використовують гістограму. Вона порівнює компоненти за певний проміжок часу. Такий спосібрекомендовано використовувати для відстеження динаміки кількості клієнтів за певний період.

Горизонтальну гістограму слід використовувати в разі порівняння більше 10 елементів, або для того, щоб уникнути плутанини, коли одна смужка даних занадто довга.

Щоб показати прогрес в досягнені мети, порівняти його за різними критеріями і зобразити результат як рейтинг або продуктивність використовують шкалу зі значеннями.

Теплова карта надає рейтингову інформацію та показує взаємозв’язок між двома елементами. Інформація про рейтинг зображується з використанням різних кольорів або різної насиченості.

З давніх давен візуалізація даних використовувалася людьми для наочності в інформаційних картах, кресленнях, моделях тощо. З плином часу з’являлись нові методи та прийоми для відображення даних. Одним з таких методів стала перспектива, яка надала елементам відчуття власного місця серед інших та надала можливість відображати предмети об’ємно. За допомогою перспективи створюються графіки, діаграми, гістограми, тривимірні простори, теплові карти, в яких людина може легко сприймати та засвоювати інформацію.

Література

1. Тютюнник А. В. ТЕХНОЛОГІЇ ВІЗУАЛІЗАЦІЇ У СВІТОВИХ ДОСЛІДЖЕННЯХ [Електронний ресурс] / Анастасія Володимирівна Тютюнник. – 2020. – Режим доступу до ресурсу: https://elibrary.kubg.edu.ua/id/eprint/34241/1/A_Tiutiunnyk_OPENEDU_9_NDLIO.pdf.
2. Візуалізація даних: як правильно вибрати діаграму або графік для річного звіту [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://toplead.com.ua/ru/blog/id/vizualizacija-dannyh-kak-pravilno-vybrat-diagrammu-ili-grafik-dlja-godovogo-otcheta-212/.
3. WhatisDataVisualizationandWhyIsItImportant?. [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://searchbusinessanalytics.techtarget.com/definition/data-visualization.
4. WhatIsDataVisualization? Definition, Examples, AndLearningResources [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://www.tableau.com/learn/articles/data-visualization.
5. 13 ScientificReasonsWhyYourBrainCravesInfographics[Interactive] [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://neomam.com/interactive/13reasons/.

УДК 351.861

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ПРОЦЕСУ ЗНИЩЕННЯ ВИБУХОНЕБЕЗПЕЧНИХ ПРЕДМЕТІВ ПІД ВОДОЮ

Соловйов Ю.
Національний університет цивільного захисту України, Харків

Проведено експериментальні дослідження. Результати статистичного аналізу експериментальних результатів, які були отримані в процесі оперативної діяльності особового складу відділення підводного розмінування показали, що при рівні значимості α=0,05 результати розходу повітря у водолазів-саперів описуються нормальним розподілом. При цьому розхід повітря суттєво відрізняється від глибини знищення вибухонебезпечного предмету.
Ключові слова: *підводне розмінування, водолаз-сапер, математична модель.*

Experimental researches are carried out. The results of statistical analysis of experimental results obtained during the operational activities of the personnel of the submarine demining department showed that at the level of significance α = 0.05 the results of air flow in sapper divers are described by the normal distribution. The air flow rate differs significantly from the depth of destruction of an explosive object.
Key words: *underwater demining, diver-sapper, mathematical model.*

Незважаючи на те, що існуючий рівень технологічного прогресу дозволяє на протязі між 2021 та 2030 роками на 100% збільшити використання водних ресурсів, всі прибережні країни ЄС зіткнулись з викликами, що пов’язані із повоєнними залишками вибухонебезпечних [1] та хімічних речовин у вод-

них акваторіях. Крім цього у всьому світі на цей час встановлено біля 70 мільйонів мін, з яких, ймовірно, 15% встановлені на мілководні ділянки внутрішніх водоймищ. В Україні ці виклики усугубляються як значною кількістю вибухонебезпечних предметів на узбережжі Чорного та Азовського морів, характерним прикладом чого є Херсонська область [2], так і збільшенням вибухонебезпечних предметів, які забруднюють мирні водні акваторії внаслідок агресії Росії. З урахуванням того, що в нашій країні питання підвищення розвідки та розмінування водного середовища у порівнянні з ліквідацією вибухонебезпечних предметів на суходолі, де накопичено величезний досвід, потребують подальшою розробки, проблема підвищення ефективності попередження надзвичайних ситуацій (НС), пов'язаних з підводним розташуванням вибухонебезпечних предметів, є актуальною.

В доповіді показано, що процес підводного розмінування здійснюється умовною системою «НС, що пов'язана із підводним розташуванням вибухонебезпечного предмету – спеціальні засоби підводного розмінування – водолаз-сапер». Цю «умовну систему» надалі будемо називати як система [3].

В цій системі в якості вихідних даних присутні виступають показники, що характеризують безпосередньо водолазів-саперів (множина ХВС), спеціальні засоби підводного розмінування (множина ХСЗПР), надзвичайну ситуацію та умови проведення підводного розмінування, тобто навколишнє середовище (множина ХС).

$$X = X_{ВС} \cup X_{СЗПР} \cup X_{С}. \qquad (1)$$

Ефективність проведення конкретного варіанту підводного розмінування Y* відображає оперативно-технічний характер підводного розмінування і цю ефективність можна розглядати як закономірність підводного розмінування

$$Y^{*} = F^{*}(X) \qquad (2)$$

З урахуванням вищевикладеного доцільним є вибір плану 3х3х2 для проведення багатофакторного експерименту. В цьому випадку поліноміальна модель підводного розмінування має вигляд

$$Y = a_0 + a_1 X_{ВС} + a_2 X_{СЗПР} + a_3 X_{С} + a_{11} X_{ВС}^2 + a_3 X_{С}^2 + \\ + a_{12} X_{ВС} X_{СЗПР} + a_{13} X_{ВС} X_{С} + a_{23} X_{СЗПР} X_{С}, \qquad (3)$$

де $X_{ВС}, X_{СЗПР}, X_{С}$ – обрані для дослідження фактори.

Оскільки порівняльна оцінка обраних для розгляду факторів повинна виконуватись в нормованих перемінних , необхідно отримати тотожній (3) вираз

$$y = b_0 + b_1 x_1 + b_2 x_2 + b_3 x_3 + b_{11} x_1^2 + b_3 x_3^2 + b_{12} x_1 x_2 + b_{13} x_1 x_3 + b_{23} x_2 x_{3n}. \qquad (4)$$

В цьому випадку обґрунтування пропозицій щодо підвищення ефективності функціонування системи здійснюється за результатами ранжування факторів x_i за ступенем впливу на ефективність проведення підводного розмінування шляхом аналізу відповідних однофакторних моделей, отриманих при стабілізації інших факторів.

$$y = b_0 + b_1x_1 + b_2x_2 + b_3x_3 + b_{11}x_1^2 + b_3x_3^2 + b_{12}x_1x_2 + b_{13}x_1x_3 + b_{23}x_2x_{3n}$$
$$\Downarrow \qquad (5)$$
$$\left(x^{(1)}_{i\in(1,\,3)} \geq x^{(2)}_{j\in(1,\,3;\;j\neq i)} \geq x^{(3)}_{\gamma\in(1,\,3;\gamma\neq i\neq\ldots\neq j)}\right)$$

Упорядкування результатів багатофакторного експертного моделювання дозволяє суттєво спростити побудову конкретних поліноміальних моделей, які необхідно знайти, оскільки в результаті цього під час розрахунку оцінок коефіцієнтів b_0, b_i, b_{ii}, b_{ij} можна використовувати [4] готові формули

$$b_0 = A_0(0Y) - \sum A_{0i}(ii0Y), \qquad (6)$$
$$b_i = A_i(iY), \qquad (7)$$
$$b_{ij} = A_{ij}(ijY), \qquad (8)$$
$$b_{ii} = A_{ii}(iiY) - A_{0i}(0Y), \qquad (9)$$

де A_0, A_{0i}, A_i, A_{ij}, A_{ii} – постійні для розрахунку коефіцієнтів регресії при симетричних планах.

Це дозволило, використовуючи (6)-(9), розрахувати коефіцієнти трифакторної квадратичної моделі, які встановлюють кількісний зв'язок між часом знищення вибухонебезпечного предмету (в нормованих перемінних) та обраними факторами

$$y_{підрив} = 0,412 - 0,153\cdot x_1 - 0,307\cdot x_2 - 0,043\cdot x_3 + \\ +0,043\cdot x_1^2 + 0,065\cdot x_2^2 - 0,029\cdot x_1\cdot x_2 - 0,001\cdot x_1\cdot x_3 - 0,0005\cdot x_2\cdot x_3 \qquad (10)$$

Результати, які були визначені за допомогою математичної моделі (10) знищення вибухонебезпечного предмету водолазами-саперами під водою, співпадають з результатами натурних експериментів та укладаються в довірчі інтервали, які розраховані з надійністю 0,95, що підтверджує надійність розробленої математичної моделі підриву вибухонебезпечного предмету під водою при ліквідації відповідної надзвичайної ситуації.

Література

1. Про реалізацію основних заходів з протимінної діяльності у 2020 році та проведення спеціальних вибухових робіт: наказ ДСНС України від 21 січня 2020 року № 68. С. 1-7.

2. Соловйов І.І., Стрілець В.М. Проблемні питання виконання робіт з підводного розмінування. Енергозбереження та промислова безпека: виклики та перспективи. Третя міжнародна науково-практична конференція. Київ: КПІ, ННДІ ПБтаОП. 2020. С.225-231

3. Long, Terrance P. (2013). An International Overview of Sea Dumped Chemical Weapons: The Way Forward. Conventional Weapons Convention Coalition. Available at: http://www.cwccoalition.org/wp-content/uploads/2010/12/longpaper.pdf

4. Вознесенский В.А. Статистические методы планирования эксперимента в технико-экономических исследованиях. – М.: Финансы и статистика, 1981. – 263 с.

УДК 004.05

ОЦІНКА ЯКОСТІ ВЕБ-ЗАСТОСУНКУ ДЛЯ ОСББ

Уханський М.
Факультет математики та інформатики
ДВНЗ «Прикарпатський національний університет
імені Василя Стефаника», м. Івано-Франківськ, Україна

I. ВСТУП

В теперішній час спостерігається тенденція щодо менеджменту і здійснення адміністрування будь-яких сфер діяльності та підприємств у мережі інтернет. Веб-застосунки, з допомогою яких виконуються адміністрування, потребують оцінки параметрів якості аплікації для задоволення конкурентного попиту продукції у порівнянні з відповідними базовими показниками за фіксованих умов. Від того, наскільки вдало зроблено програмний продукт, в кінцевому результаті залежить його життєздатність. Вимоги та параметри допомагають замовникам оцінити аплікацію, визначити її конкурентоспроможність, перевірити необхідність в оплаті основного або ж всього функціоналу застосунку. Саме тому, було вирішено розробити оцінювання якості програмного забезпечення на прикладі розробленого сайту здійснення менеджменту і адміністрування для об'єднання співвласників багатоквартирного будинку (ОСББ).

II. АНАЛІЗ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Стандарт [1] об’єднує характеристики якості програмного забезпечення (ПЗ) з різних стандартів і пропонує модель якості програмного застосунку, зображену на рис. 1.

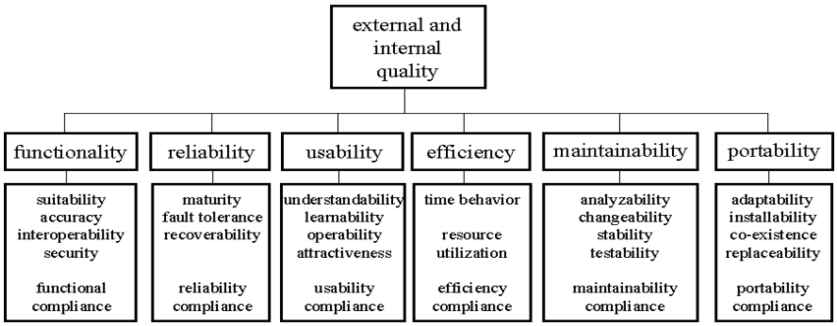


Рисунок 1 – ISO/IEC 9126 модель якості програмного забезпечення

Очевидно, що якість ПЗ залежить від шести основних характеристик, а саме: ефективності, функційної придатності, надійності, зручності використання, супроводжуваності, можливості перенесення. Досягаючи найвищого значення кожної з восьми характеристик якості, ми можемо досягти максимальної оцінки якості ПЗ.

В даний час оцінювання характеристик якості ПЗ відбувається наступним чином: оцінюються показники якості ПЗ – обирається метрика, градуюється шкала оцінки, залежно від можливих ступенів відповідності показника накладеними обмеженнями. Перелік «вимірюваних» показників становить критерій для оцінки.

Здійснити порівняння якісних характеристик однотипного програмного забезпечення документом ISO/IEC неможливо, оскільки вони не містять методики визначення узагальненого показника якості [2, 3].

III. Виклад основного матеріалу

Основну ідею дослідження зображено на рис. 2, де показано схематично алгоритм, який описує послідовність основних дій, необхідних для оцінювання ПЗ для різних ОСББ. Отже, першим кроком є оцінювання якості ПЗ за міжнародним стандартом ISO/IEC 9126. Наступним кроком є пошук пріоритетних властивостей для ОСББ. Після цього варто визначити вагові коефіцієнти, а також оцінки для новостворених властивостей за формулами ISO/IEC метрики. Коли оцінки будуть обчислені, потрібно просумувати значення стандартів і новостворених характеристик для ОСББ таких як синхронізація платежів, частота оновлення даних, інтеграція з соціальними мережами, звітність по ОСББ, верифікація учасників ОСББ. Загальна оцінка якості отримується шляхом усереднення.

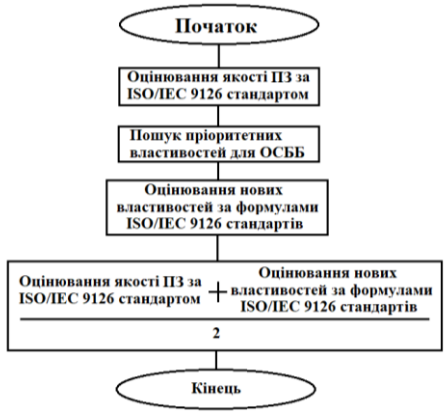


Рисунок 2 – Алгоритм оцінювання програмного забезпечення для ОСББ

IV. Висновки

З поданого вище матеріалу випливає, що оцінювання якості ПЗ як сукупності функцій основних шести характеристик є суб'єктивним, оскільки різні організації вибирають вигідні для них метрики та інтерпретують отримані значення як максимальні. Дане дослідження допоможе замовникам вибрати важливі пункти й оцінювати програми на ринку з вагомими для них характеристиками. Крім того, це сприятиме визначенню конкурентоспроможних аплікацій, спрямованих під вимоги користувачів ОСББ.

Література

1. ISO/IEC 9126. Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE). – System and software quality models / ISO/IEC.
2. Андрейко В.М. Кваліметрія програмного забезпечення засобів вимірювань: монографія. Івано-Франківськ: Симфонія форте, 2016. 120 с.
3. Кузь М.В., Соловко Я.Т., Андрейко В.М. Методологія формування узагальненого критерію якості програмного забезпечення в умовах невизначеності. Вісник Вінницького політехнічного інституту. 2015. № 5. С. 104–107.

УДК 681.51

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ СТВОРЕННЯ ГІС ДЛЯ КОНТРОЛЮ ГРАНИЧНОГО РІВНЯ ВОДИ У ВОДОЙМАХ

Федерляйн М., Сікора Л.
Національний університет "Львівська політехніка", м. Львів

У статті розглянуто створення інформаційної системи для контролю граничного рівня водних ресурсів на основі ГІС - технологій. Використання розробленої структури та функціонального елементного складу при реалізації системи обробки інформації для попередження і ліквідації стихійного лиха територіального рівня дозволяє підвищити оперативність і ефективність прийнятих рішень щодо попередження та ліквідації наслідків стихії.

Ключові слова: *ГІС, стихійне лихо, ліквідація наслідків стихії.*

The article considers the creation of an information system for the control of the limit level of water resources on the basis of GIS - technologies. Using of the developed structure and functional elemental composition in the implementation of the information processing system for the prevention and elimination of natural disasters at the territorial level allows to increase the efficiency and effectiveness of decisions to prevent and eliminate the consequences of the disaster.

Key words: *GIS, disaster, elimination of the consequences of the disaster.*

В даний час світовий досвід з усією очевидністю показує, що найефективнішим способом зниження втрат від природних, техногенних, в цілому і соціально-економічних надзвичайних ситуацій та катастроф є їх прогнозування, інформування та управління. Базовою основою попередження катастрофічних ситуацій при природних катаклізмах, які призводять до повеней є їх моніторинг і управління, який можна проводити за допомогою ГІС-систем.

Аналізуючи еволюцію розвитку ГІС, можна виділити кілька значущих етапів:

- перехід до багатокористувацьких систем;
- істотне скорочення часу на отримання і збір первинної просторової інформації;
- повсюдний і полегшений доступ до електронних веб- і мобільних карт.

Сьогодні це призвело до появи таких взаємопов'язаних технологій, як «хмарні» обчислення, обробка «великих даних», прийом даних в режимі реального часу, гетерогенні сенсорні мережі, та ін. Мабуть, вже можна говорити, що настав черговий етап розвитку – перехід від інформації до знань, що дозволяє дійсно розуміти яким чином протікають процеси, явища і приймати найкращі рішення [1].

Оцінка наслідків екстремальних паводкових ситуацій включає в себе набір операцій просторового аналізу, мета якого є виявлення об'єктів (населені пункти, дороги, угіддя, ділянки забудови тощо), які можуть бути затоплені внаслідок очікуваної повені або паводку.

До них ми можемо віднести:

- перелік населених пунктів, що потрапили в зону затоплення та орієнтовно кількість жителів у них;
- перелік промислових підприємств та потенційно небезпечних об'єктів, що потрапили в зону затоплення;
- кількість кілометрів автомобільних та залізничних шляхів, ліній зв'язку та інженерних комунікацій, що попали в зону затоплення тощо [2].

Використання такого потужного інструменту просторового аналізу, як ГІС у більшості випадків обмежуються створенням картографічної основи для відображення і графічного зіставлення елементів, що зумовлюють розподіл небезпек на території досліджень. Проте, оцінка ризиків є досить складним технологічним процесом, який потребує одночасного зіставлення просторового положення багатьох чинників, що визначають рівень небезпеки на кожній ділянці території досліджень. Графічне порівняння контурів розповсюдження кожного з чинників може лише дати уяву про їх приблизне співвідношення у просторі. Справжній ефект може дати лише впровадження автоматизованої системи комплексної кількісної оцінки кожного елементу території за багатьма критеріями одночасно. Саме на вирішення проблем такого типу націлені засоби просторового аналізу та моделювання ГІС [3].

Література

1. Геоинформатика: в 2 кн. / учебник для студ. высш. учеб. заведений / Е.Г. Капралов, А.В. Кошкарев, В.С. Тикунов и др.; под ред. В.С. Тикунова. – 2-е изд., перераб. и доп. – М.: Издательский центр «Академия», 2010. – 384 с.

2. Ищук А.А. Концептуальные модели местности как инструмент комплексной оценки территории /А.А. Ищук // Ученые записки Таврического университета им. В.И. Вернадского. География. Т.16(55). – 2003. – №2 – С. 94-101.

3. Краснощеков А.Н. Геоинформационные системы в экологии: учеб. пособие / А. Н. Краснощеков, Т. А. Трифонова, Н. В. Мищенко. Владимир : б. и., 2004. – 151 с.

УДК 004.584

РОЗРОБКА ЧАТ-БОТУ РОЗКЛАДУ ЗАНЯТЬ У ЛЬВІВСЬКОМУ НАЦІОНАЛЬНОМУ АГРАРНОМУ УНІВЕРСИТЕТІ ДЛЯ МЕССЕНДЖЕРА «TELEGRAM»

Фіялковський В.[1], Білецький Р.[1], Тригуба А.[1,2]
[1]Львівський національний аграрний університет, м. Дубляни
[2]Львівський держаний університет безпеки життєдіяльності, м. Львів

Проведений огляд інформаційних систем аналогів та обґрунтовано особливості запропонованого чат-боту розкладу занять у Львівському національному аграрному університеті для мессенджера «Telegram». Створено базу даних та змодельована архітектура чат-боту. Запропонований виконує чат-бот функцію надання розкладу у мессенджері «Telegram» для користувачів.
Ключові слова: *база даних, інформаційна системи, розробка, чат, бот.*

The review of information systems of analogues is carried out and the peculiarities of the proposed chat-bot of the schedule of classes at the Lviv National Agrarian University for the messenger "Telegram" are substantiated. A database has been created and the chatbot architecture has been modeled. The proposed chatbot performs the function of providing a schedule in the messenger "Telegram" for users.
Keywords: *database, information systems, development, chat, bot.*

На теперішній час існує багато способів доставлення інформації від освітніх структур до користувача [1, 2]. Кожен університет має свої варіанти доставлення розкладу занять до студента. Сьогодні найчастіше це є використання сайту освітнього закладу, які мають свої недоліки для користувачів. При цьому студенти потребують покращення доступу до отримання розкладу занять від освітнього закладу, який буде враховувати їх потребу у інформації та її збереженні [3].

У нашій роботі особлива увага приділена створенню інформаційної системи, яка допоможе студентам покращити отримання розкладу занять у освітніх закладах завдяки мессенджерам «Telegram». Також це дасть змогу користувачу власноруч вибрати потрібно йому дату та отримати розклад занять. Розробка чат-бота у запропонованій інформаційній системи є однією з головних завдань.

Для того щоб забезпечити правильну та стабільну роботу інформаційної системи, необхідно буде обрати адекватні інструменти взаємодії системи реалізації. Враховуючи поставлену задачу, раціональною мовою програмування для створення бота – Java, інструмент управління та розуміння – Maven, комплексна модель програмування та конфігурації – Spring Framework. Spring Framework це хмарна платформа, яка дозволяє створювати, доставляти, контролювати та масштабувати програми Heroku та бази даних PostgreSQL.

```
server.port=5432
localeTag=ua-UA

pingtask.ulr= https://www.google.com
pingtask.perion= 1200000

telegrambot.botUserName=@StudyLnauBot
```

Рис. 1. Приклад використання Spring Framework

Нами виконано моделювання інформаційної системи, що забезпечило побудову контекстної діаграми IDEF0. Функціональна модель запропонованої інформаційної системи у нотації IDEF0 представлена на рис. 2.

Контекстна діаграма містить узагальнений блок «Створення системи розкладу в Telegram». Згідно з методологією функціонального моделювання IDEF0 для роботи потрібно визначити вхідні дані, результуючі дані, дані управління і дані механізмів, які зображуються на діаграмі стрілками. При цьому виконується 5 етапів її функціонування.

Етап 1. Введення вхідних даних – адміністратор, на основі створеного розкладу на сайті закладу освіти, вводить дані в систему.

Етап 2. Створення факультетів –на основі введених проводить аналіз та створюються блоки із факультетами.

Етап 3. Створення спеціальностей – проводиться аналіз окремих блоків створених факультетів та додаються спеціальності у кожний створений факультет звіряючись з інформацією яку надав адміністратор.

Етап 4. Збереження результатів до БД – після повної перевірки системою даних, проводиться збереження їх у базу даних.

Етап 5. Передавання інформації боту – після завершення дії з базою даних система передає готову інформацію у сам Telegram, де чат-бот використовує її для пошуку відповіді на запит користувачів.

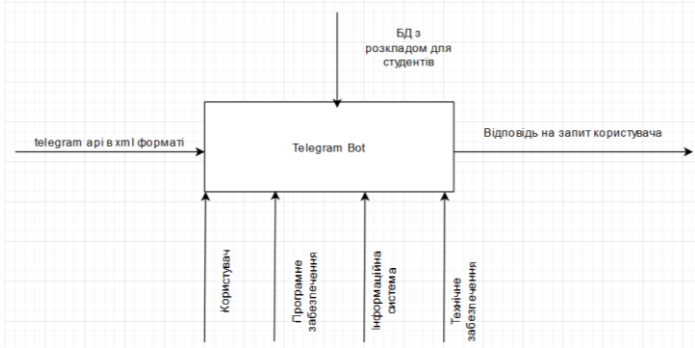


Рис. 2. Контекстна діаграма IDEF0 чат-боту розкладу занять для мессенджера «Telegram»

Для того щоб інформаційна системи працювали, для неї потрібно створити базу даних, яка буде зберігати інформацію про викладача, заняття, час початку та аудиторію (рис. 3).

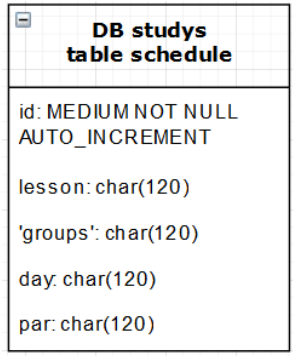


Рис. 3. Структура бази даних інформаційної системи

База даних яка буде складати частину інформаційної системи складається з 1 таблиці, що вміщує: id – первинний ключ; lesson – назва заняття; groups – назва групи та спеціальності; day – день, котрий студент сам зможе вибрати; par – містить у собі інформацію про аудиторію, викладача та час початку заняття.

Література

1. Tryhuba, A., Boyarchuk, V., Tryhuba, I. et al. (2020). Method and Software of Planning of the Substantial Risks in the Projects of Production of raw Material for Biofuel. CEUR Workshop Proceedings. Published in ITPM.

2. Tryhuba, A., Tryhuba, I., Bashynsky, O. et al. (2020). Conceptual model of management of technologically integrated industry development projects. 15th International Scientific and Technical Conference on Computer Sciences and Information Technologies (CSIT), 2, 155-158. doi: 10.1109/CSIT49958.2020.9321903

3. Розклад занять завжди в телефоні: університет запустив на Telegram чат-бота для студентів URL: https://nupp.edu.ua/news/rozklad-zanyat-zavzhdi-v-telefoni-universitet-zapustiv-na-telegram-chat-bot-dlya-studentiv.html (дата звернення 20.03.2021)

УДК 004

ДОСЛІДЖЕННЯ ТА АНАЛІЗ СУЧАСНИХ ТЕХНОЛОГІЙ РОЗРОБКИ ВЕБ-ДОДАТКІВ

Хорошайло А., Сімонова О.
Національний технічний університет «Харківський політехнічний інститут», Харків

Робота присвячена дослідженню сучасних технологій розробки веб-додатків для проєктування системи обліку співробітників компанії. Аналіз різних типів веб-додатків і технологій їх розробки. Огляд аналогів та виявлення недоліків існуючих рішень. Вибір підходу для реалізації поставлених задач.

The work is devoted to the study of modern technologies for developing web applications for engineering the accounting system of the company's employees. Analysis of different types of web applications and technologies for their development. Review of analogues and identification of shortcomings of existing solutions. Choice of approach for realization of the set tasks.

Ключові слова: *веб-додаток, SPA, MPA, PWA, сучасні технології.*

На сьогоднішній день існує два принципових типів веб-додатків: традиційні веб-додатки (MPA), велика частина логіки яких виконується на сервері, і односторінкові додатки (SPA), логіка призначеного для користувача інтерфейсу яких виконується переважно в веб-браузері, а взаємодія з веб-сервером здійснюється головним чином через веб-API. Також можливий гібридний підхід, при якому в простому випадку в рамках великого традиційного веб-додатку розміщуються одне або кілька повнофункціональних підлеглих додатків, побудованих на основі односторінкової моделі.

Розробка того чи іншого типу додатку повинна бути обумовлена функціями, які повинна виконувати програма та вимогами до неї. Існують ситуації, в яких доцільно саме традиційний додаток або протилежний – SPA (односторінковий). При виборі підходу розробку також потрібно враховувати технології, які використовуються для створення. Компанія має оцінити бюджет проєкту та кваліфікацію співробітників у той чи іншій сфері розробки.

Традиційні додатки використовують у випадках, коли на стороні клієнта застосовуються мінімальні вимоги, наприклад, використовуються тільки функції читання, додаток має працювати в браузерах без підтримки JavaScript, а також команда розробників не знайома з принципами розробки на JavaScript або TypeScript.

Односторінкові додатки корисні при розробці додатку, в якому потрібен повнофункціональний користувальницький інтерфейс, або повинен надаватися API для інших внутрішніх або загальнодоступних клієнтів. Доцільно обрати, коли команда розробників знайома з принципами розробки на JavaScript, TypeScript або Blazor WebAssembly.

Також є ще один тип веб-додатку, який уявляє собою щось середнє між сайтом і додатком – PWA (Progressive Web Application). Головною відмінністю між цим типом і вище описаними полягає у тому, що для користування таким додатком потрібно його скачати і встановити.

На сьогоднішній день існує безліч різноманітних систем, які реалізують функціонал обліку співробітників. Далі описані деякі з них.

Сервіс «Bitrix 24» уявляє собою міцну систему керування бізнесом, у тому числі дозволяє компанії зберігати усю необхідну інформацію про співробітників. Дані можуть вноситися або адміністратором або особисто працівником. Основними технологіями розробки цієї системи є мова програмування PHP та Percona Server. Цим додатком можна користуватися як в браузері, так і встановлювати на свій пристрій.

Система «1 С» – це програма для організації обліку і зберігання даних в електронному вигляді. Майже будь-яка інформація може бути представлена у вигляді звіту. Адміністратор компанії може здійснювати аналіз кадрового составу, розраховувати заробітну плату, планувати потреби у кадрах та таке інше. Платформою можна користуватися також як онлайн, так і завантаживши її на ПК. Програма складається з багатьох складових, написаних на мові програмування C++ або JAVA в нових версіях. Для забезпечення модульності весь функціонал розділений на компоненти, які являють собою динамічні бібліотеки (* .dll під Windows, * .so - під Linux). Платформа забезпечує операції виконання запитів, опису структур даних і маніпулювання даними, транслюючи їх до відповідних команди. Це можуть бути команди системи управління базами даних, в разі клієнт-серверного варіанту роботи, або команди власного движка бази даних для файлового варіанту.

Хмарна система управління трудовою дисципліною співробітників організації «TargControl» ідентифікує співробітників, автоматизує процеси планування і організації роботи персоналу, а також допомагає складати різноманітні графіки роботи, ставити завдання для співробітників. Користування системою можливо у веб-додатку, в мобільному додатку на Android або IOS та на біометричних терміналах. У розробці додатків були використанні JAVA та Kotlin.

На рисунку 1 наведений один з екранов системи «Bitrix 24».

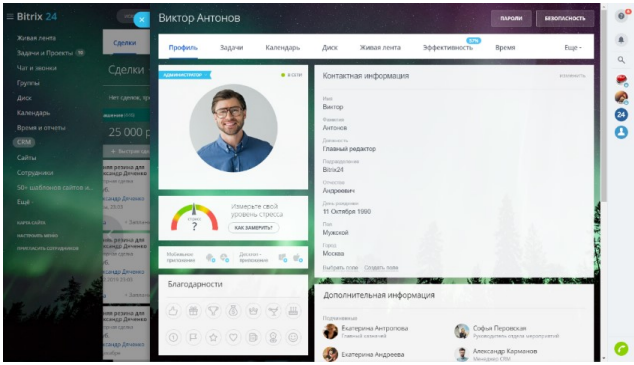


Рисунок 1 – Система «Bitrix 24»

Далі будуть розглянуть функціонал та структура майбутнього додатку та на основі проведеного аналізу обраний той тип додатку, який найбільш задовольняє нашим потребам.

1 На головній сторінці додатку повинні виводитись карточки співробітників з особистими даними про них та даними щодо компанії, а також має бути система пошуку за іменем співробітника та їх фільтрація за різними критеріями.

2 При натисканні на карточку співробітника, ця карточка повинна висуватися в центр екрана.

3 На карточці співробітника повинні бути присутні кнопки редагування та видалення. При вибору редагування має відкриватися сторінка з формою редагування даних про співробітника. При бажанні видалити має з'являтися модальне вікно підтвердження.

4 Також має бути можливість додавання співробітника за допомогою натискання на кнопку на головній сторінці додатку та переходу до форми на окремій сторінці.

5 Повинна здійснюватися обробка помилок при пошуку, а також при фільтрації списку співробітників за допомогою оповіщення модальним вікном.

Так як наш майбутній додаток має бути з багатим функціоналом на стороні клієнта та швидко реагувати на будь-які дії користувача та зміни у даних про співробітників, доцільно обрати розробку SPA.

Цей підхід дозволить працювати додатку без перезавантажень та здійснювати рендерінг компонентів та сторінок одночасно з запитом до серверу для отримання даних.

Література

1. Michael Mikowski. Single Page Web Applications, 2013. – 407 p.
2. Типи веб-додатків [Електронний ресурс] // azoft.ru – Режим доступу: https://www.azoft.ru/blog/spa-mpa-pwa/

УДК 004

ДОСЛІДЖЕННЯ ОСНОВНИХ МЕТОДІВ І ІНСТРУМЕНТІВ ЗАЛУЧЕННЯ УВАГИ В СОЦІАЛЬНИХ МЕРЕЖАХ

Хорошайло О., Сімонова О.
Національний технічний університет «Харківський політехнічний інститут», Харків

Робота присвячена дослідженню методів, що направлені на популяризацію бізнес-акаунту в соціальних мережах. Аналіз різних інструментів для реалізації поставлених задач. Виявлення недоліків існуючих рішень.

The work is devoted to the study of methods aimed at promoting a business account on social networks. Analysis of various tools for the implementation of tasks. Identifying the shortcomings of existing solutions.

Ключові слова: *SMM, соціальна мережа, автоматизація.*

Зараз соціальні мережі являються потужним рекламним інструментом, за допомогою якого можна привернути увагу до послуг, що надає автор блогу.

Присутність бренду в соціальних мережах стала необхідною. Однак, не всі компанії отримують від цього бажаний ефект, у зв'язку з тим, що навіть самий якісний контент потребує додаткового просування.

SMM (Social Media Marketing) – це метод роботи в соціальних медіа, що з'явився відносно недавно, в середині 2000-х років. Дату виникнення можна пов'язати з початком роботи перших соціальних мереж [1].

Основними методами SMM просування є:

- робота з рекламою на сайті за рахунок тематичних ресурсів, де є можливість посилатися на блог, форум або соціальну сторінку;
- можливість створити тематичний паблік в соціальних мережах з метою залучення та зацікавленості користувача для переходу на просувний сайт;
- створення провокаційних і яскравих заголовків, які привернуть увагу користувача мереж відвідати просувний сайт;
- використання ботів, та програмних додатків для збільшення кількості лайків та підписників в соціальних мережах з метою залучення уваги до контенту.

Кожен з методів, наведених вище, має також свої інструменти з розвитку і засоби здійснення. Всі ці заходи спрямовані на залучення якомога більше користувачів до свого бренду, бізнес-акаунту, чи сайту.

Портал https://target.my.com/ надає таке визначення таргетованої реклами – це спосіб просування в Інтернеті, що дозволяє показувати оголошення певної цільової аудиторії з заданими параметрами в соціальних мережах, на сайтах або в додатках [2]. Основними плюсами такого просування є:

– покази реклами тільки для цільової аудиторії, при цьому є велика кількість параметрів для налаштування, що дозволяють зібрати точний портрет потенційного клієнта;

– персоналізація оголошень: формат включає зображення або відео, заголовок і опис, що дозволяє для кожної групи створити релевантний креатив з прямим зверненням до проблеми користувача;

– легка перевірка гіпотез і швидка оптимізація: статистика оголошення вмить транслюється в кабінет, за допомогою чого можна відстежувати, які пропозиції або аудиторії працюють краще;

– підходить для просування будь-якого бізнесу: з її допомогою можна просувати масові продукти і b2b- сервіси.

Незважаючи на безліч переваг, у використанні реклами такого виду є ряд обмежень, які важливо враховувати при налаштуванні:

– необхідність формувати попит, що пов'язано з тим, що люди найчастіше використовують соціальні мережі, щоб спілкуватися і розважатися, а не задля здійснення покупок;

– у кожної мережі свої правила модерації.

Другим засобом залучення уваги є привертання уваги користувачів вручну. Плюс такого підходу в тому, що він безкоштовний, але при цьому займає дуже багато часу. Людині, зацікавленій в споживачах, доводиться самій досліджувати і знаходити потенційних клієнтів в соціальній мережі, після чого починати рекламувати свій профіль різними способами, такими як оцінка контенту, коментування записів і іншими [3].

Третім методом є просування через спеціальні сервіси, що повністю звільняють від необхідності власноруч розбиратися в рекламних алгоритмах [4].

Основною проблемою таких сервісів є ціна. На них діє невеликий період безкоштовного ознайомлення, а потім потрібно платити або за кожного залученого користувача, або за підписку на сервіс раз на місяць.

Також одним з найефективніших методів залучення уваги є використання Telegram-ботів, що являються програмами, які виконують задані дії в автоматичному режимі. Вони широко застосовуються в соціальних мережах, найчастіше – для створення ілюзії підтримки бесіди з користувачем в чаті. Також за допомогою ботів можна завантажувати і аналізувати контент, аналізувати аудиторію, підбирати хештеги і виконувати багато інших дій [5].

Зазвичай ботів застосовують для автоматизації процесів просування акаунтів в соціальних мережах і наповнення їх контентом. Їх використання особливо актуально при веденні декількох профілів, коли своєчасно робити публікації в кожному не вистачає часу.

Основними перевагами використання ботів для популяризації бренду у соціальних мережах є економія часу за рахунок автоматизації дій та безкоштовність використання.

Таким чином, було вирішено, що необхідно розробити бот, що дозволить безкоштовно автоматизувати дії, направлені на популяризацію бізнес-акаунту у соціальних мережах.

Література

1. SMM [Електронний ресурс] / сайт wikipedia.org – Режим доступу: https://uk.wikipedia.org/wiki/Маркетинг_у_соціальних_мережах

2. Таргетована реклама [Електронний ресурс] / сайт target.my.com – Режим доступу: https://target.my.com/pro/education/online-course/start/targeted-advertising

3. Привертання уваги вручну [Електронний ресурс] / сайт azinkevich.com – Режим доступу: https://azinkevich.com/prodvizhenie-biznesa-v-socialnyx-setyax/

4. Просування через спеціальні сервіси [Електронний ресурс] / сайт novyny.online.ua – Режим доступу: https://novyny.online.ua/smm-prosuvannya-top-5-saytiv-dlya-rozkrutki-vashogo-akkauntu-v-sotsmerezhah_n790552/

5. Використання Telegram-ботів [Електронний ресурс] / сайт novyny.online.ua – Режим доступу: https://zengram.ru/blog/post/polezne-telegram-boti-dlja-instagram

УДК 004.382.2

РОЛЬ СУПЕРКОМП'ЮТЕРІВ ТА КЛАСТЕРІВ У РОЗВИТКУ НАУКОВИХ ДОСЛІДЖЕНЬ В УКРАЇНІ ТА СВІТІ

Частило А.О., Бурак Н.Є.
Львівський державний університет безпеки життєдіяльності, м. Львів

У роботі проведено огляд сфер застосування та вирішення задач різних ступенів складності за допомогою суперкомп'ютерів та їх аналогів кластерних систем. Зазначена важливість збереження та аналізу даних у використанні сучасних комп'ютерів.

Ключові слова: *суперкомп'ютер, кластер, задачі, застосування, аналіз, дані, вузол.*

The paper reviews the areas of application and solving problems of different degrees of complexity with the help of supercomputers and their analogues of cluster systems. The importance of data storage and analysis in the use of modern computers is noted.

Keywords: *supercomputer, cluster, tasks, application, analysis, data, node.*

Термін "суперкомп'ютер" увійшов в загальновживаний лексикон завдяки поширеності комп'ютерних систем американця Сеймура Крея. Він розробляв обчислювальні машини, які, по суті, ставали основними обчислювальними засобами урядових, промислових та академічних науково-технічних проектів США з середини 60-х років до 1996 року. Не випадково в той час одним з популярних визначень суперкомп'ютера було наступне: "будь-який комп'ютер, який створив Сеймур Крей". Сам Крей ніколи не називав свої дітища суперкомп'ютерами, вважаючи за краще використовувати замість цього звичайну назву "комп'ютер".

На сьогоднішній день суперкомп'ютери є унікальними системами, створеними "традиційними" лідерами комп'ютерного ринку, такими як IBM, Hewlett-Packard, NEC і іншими, які придбали безліч ранніх компаній, разом з їх досвідом і технологіями. Компанія Cray Inc. як і раніше займає гідне місце в ряду виробників суперкомп'ютерної техніки.

Важливо мати на увазі, що суперкомп'ютер забезпечений великим обсягом пам'яті, тобто має здатність зберігати значні масиви інформації (бази даних, бази знань), що має велике значення для розв'язування задач надвисокої складності, характерних для вирішення проблем економіки, екології, космічних досліджень, вивчення біологічних та хімічних процесів, проблем матеріалознавства. Нерідко задачі, що їх треба розв'язувати в названих галузях, характеризуються десятками сотень і мільйонів незалежних змінних та відповідних обмежень, які необхідно враховувати під час розв'язання задачі. Цією обставиною й пояснюється необхідність використання ідей складних обчислювальних процесів та процесів обробки великих обсягів даних і знань, що успішно технічно реалізується на суперкомп'ютерах.

Такі задачі актуальні і в Україні. Передусім це задачі економічного характеру, проблеми технологічного передбачення, задачі економічного прогнозу, що особливо важливо для економіки перехідного періоду. Чим ретельніше, чим детальніше ми зможемо проаналізувати наші можливості, тим упевненіше окреслимо свій шлях у майбутнє.

Наша екологія надто занедбана, вона потребує постійного і всебічного моніторингу. Задачі розвитку наукових досліджень. Питання ефективного використання супутників Землі для розвитку народного господарства. Проблеми проєктування складних машин (літаків, енергетичних котлів, ракетної техніки). Задачі військового комплексу.

Багато країн з кожним роком удосконалюють суперкомп'ютери роблячи їх більш потужнішими. Наприклад, у Японії працює надпотужний комп'ютер для розв'язання задач, пов'язаних із передбаченням загрозливих стихійних явищ — землетрусів, цунамі. Ці задачі надзвичайно складні, оскільки величезні обсяги інформації про стан довкілля, що збираються в реальному часі з різних джерел, розміщених і в океані, і в космосі, мають оперативно сходитися, класифікуючись у базах даних суперкомп'ютера, щоб стати основою для складання прогнозів погоди та передбачень можливих аномалій.

У США також приділяється надзвичайно велика увага розробці аналогічних систем. Це пов'язано з необхідністю розв'язувати подібні проблеми — передбачення землетрусів, повеней. І, звичайно, задачі космічних досліджень, розвитку науки, зокрема біології та медицини, задачі ядерного синтезу тощо.

Однак унікальні рішення з рекордними характеристиками зазвичай недешеві, тому і вартість подібних систем ніяк не могла бути порівнянна з вартістю систем, що знаходяться в масовому виробництві і широко використовуваних в бізнесі. Прогрес в області мережевих технологій зробив свою справу: з'явилися недорогі, але ефективні рішення, засновані на комунікаційних технологіях. Це і зумовило появу кластерних обчислювальних систем.

Обчислювальний кластер – це сукупність комп'ютерів, об'єднаних в рамках деякої мережі для вирішення великої обчислювальної задачі. Серед вузлів зазвичай використовуються доступні однопроцесорні комп'ютери, дво- або чотирипроцесорні SMP-сервери (Symmetric Multi Processor). Кожен вузол працює під управлінням своєї копії операційної системи, в якості якої найчастіше використовуються стандартні операційні системи: Linux, NT, Solaris і т.п.

Склад і потужність вузлів може змінюватися навіть в рамках одного кластера. Даючи можливість створювати великі гетерогенні (неоднорідні) системи. вибір конкретного комунікаційного середовища визначається багатьма факторами: особливостями класу вирішуваних задач, доступним фінансуванням, необхідністю подальшого розширення кластера.

Література

1. Маценко В. Г. Суперкомп'ютери в сучасному суспільстві/ В. Г. Маценко // Науковий вісник Чернівецького університету : зб. наук. пр. Серія: Комп'ютерні системи та компоненти. – Чернівці: ЧНУ, 2010. т.Т. 1, N Вип. 1. – С.6-13

2. «Суперкомп'ютер для сучасних технологій». MirrorWeekly. [Електронний ресурс]. – Режим доступу: https://zn.ua/ukr/science/superkompyuter_dlya_suchasnih_tehnologiy.html.

3. Суперкомп'ютери і кластери [Електронний ресурс]. – Режим доступу: http://um.co.ua/2/2-15/2-153091.html.

4. «Рейтинг найбільш високопродуктивних суперкомп'ютерів очолив кластер на базі CPU ARM». [Електронний ресурс]. – Режим доступу:https://devzone.org.ua/post/reyting-naybilsh-visokoproduktivnikh-superkompyuteriv-ocholiv-klaster-na-bazi-cpu-arm.

5. Суперкомп'ютер-можливості ESET. [Електронний ресурс]. – Режим доступу: https://eset.ua/ua/blog/view/108/moshchnyye-superkompyutery-vozmozhnosti-dlya-progressa-ili-instrument-v-rukakh-kiberprestupnikov.

РОЗРОБКА ЗАСОБІВ ДОПОМОГИ У ПОШУКУ ВИХОДУ ЛЮДЕЙ З ПІДЗЕМНИХ ОБ'ЄКТІВ ІЗ ЗАЛУЧЕННЯМ МОБІЛЬНИХ ТА ВЕБ-ДОДАТКІВ

Чулкова Д., Сидоренко О.
Національний технічний університет «Харківський політехнічний інститут», м. Харків

***Анотація**: Щорічно в Україні, за даними ДСНС, в катакомбах губиться близько 2-3 особи. Хоч ця цифра є невеликою, проте через складність пошуку, тяжку орієнтацію та необізнаність потерпілих шанси на спасіння є дуже низькими. Наше дослідження надаватиме загубленим можливість зберегти своє життя, навіть не маючи жодних засобів для орієнтації на місцевості.*

***Ключові слова**: підземелля, зонування, надзвичайна ситуація, пошуково-рятувальна операція, 3Д-моделювання, мобільний додаток, веб-додаток.*

***Summary**: Every year, according to the SES, about 2-3 people are lost in the catacombs in Ukraine. Although this number is small, due to the complexity of the search, difficult orientation and ignorance of the victims, the chances of survival are very low. This study will give the lost the opportunity to save their lives, even without any means to navigate the terrain.*

***Keywords**: Dungeon, zoning, emergency, search and rescue operation, 3D modeling, mobile application, web application.*

Замкнутий простір, темінь, відсутність свіжого повітря, що може відчувати людина в таких умовах? В першу чергу, звичайно ж стрес, що є головною ознакою неспецифічної активності організму на навколишні обставини, які надають значно більші вимоги до психологічного та фізичного стану людини [1].

Навіть у місцях, що мають усі належні заходи безпеки, не можна виключати можливість нещасного випадку. Наприклад, у 2019 році в Одеських катакомбах, які є однією з найбільш привабливих туристичних пам'яток історії взаємодії людини та природи, загубилося 4 людей, а в 2020 році ще двоє глухонімих людей [2]. Пішли і не змогли вийти. І добре, що це є публічне місце і було кому повідомити про зниклих. Але ж бувають ситуації, коли люди самі організовують для себе «тури підземеллями», залазячи у відкриті люки або решітки до каналізації або печер, і зазвичай такі люди не говорять, куди саме вони йдуть. Знайти таких загублених вже набагато важче, бо з моменту зникнення до моменту звертання до ДСНС може пройти навіть декілька днів, так ще й невідомо, де починати пошуки. Шанси потерпілих вийти з пастки живими значно зменшуються.

Щоб допомогти людині у ситуації, коли вона заблукала під землею, було сформовано ідею проекту створення особливих позначок місцезнаходження людини під час блукання підземними лабіринтами [3-5]. Задум полягає у створенні об'ємних цифр з бетону, які будуть позначати номер окремої зони підземних ходів. На двох сторонах проходу буде розміщено безпосередньо номер зони, де знаходиться потерпілий, із цифр більшого розміру та стрілки з цифрами меншого розміру, що будуть вказувати напрями до сусідніх зон. Номер «1» завжди має бути розташований коло вільного неперекритого виходу, який постійно можна буде використовувати для виходу з пастки. Помітка про це також має бути поряд з номерами зон печери. Задля економії її можна зробити лише на парних числах. Об'ємність форми дозволяє через торкання зрозуміти своє положення у разі відсутності світла. Якщо людина буде мати доступ до телефону, то у спеціальному офлайн додатку вона, обираючи об'єкт, що є у базі даних, зможе подивитися розташування усіх зон всередині ходів та швидше знайти вихід з - під землі. Таке зонування території допоможе також і рятувальникам, які шукають потерпілого, бо обидві сторони будуть рухатися назустріч один одному. В додатку також будуть розміщені правила поведінки у такій ситуації та алгоритм дій, які допоможуть безпечно вийти з-під землі. А у разі можливої появи зв'язку потерпілий зможе передати диспетчеру рятувальної служби своє точне місцеположення, назвавши номер зони, де він знаходиться. Для поширення обізнаності про такі ситуації і про те, як можна собі в них допомогти, серед широкого кола людей, існуватиме web-сайт, де можна буде знайти усю необхідну інформацію з цієї теми [6,7].

Через нестачу коштів та незначний відголос таких ситуацій у суспільстві єдиним аналогом цього проекту в Україні є система каналізаційних люків. Але, на практиці, ці люки можна відкрити лише за допомогою спеціального інструменту, прикладаючи велику кількість сили, що є неможливим для знесиленого потерпілого, бо часто люки зверху ще укріплюють бетоном, чи асфальтом, щоб діти та нетверезі люди в жодному разі не змогли впасти у каналізаційний колодязь. А у катакомбах та печерах навіть поставити люки є неможливою задачею. Отже, даний проект має найбільшу кількість переваг та не

вимагає значних технічних та економічних витрат, що створює можливим його практичну реалізацію на території України.

Наочність роботи проекту залежно до поставленого завдання можна реалізувати за допомогою 3Д-моделювання ландшафту колектору або печери. Такий підхід дозволить легко проаналізувати зовнішній вигляд і можливість використання об'ємних цифр в умовах реального часу та не наражаючись на реальну небезпеку. Додаток до телефону включає в себе бібліотеку карт підземних ходів, упорядковану за різними регіонами України або іншими місцевими та типовими ознаками, таких як міська місцевість, гори, місця, віддалені від людей. Також у додатку повинна бути інструкція щодо дій потерпілого у надзвичайній ситуації та місцезнаходження виходу. Реалізація додатку в першу чергу буде для систем на базі **Android**, бо в нашій країні така операційна система телефонів є найбільш поширеною.

Подальший розвиток проекту розглядає можливість збільшення точності даних, поширення мобільного додатку на інші електроні платформи та покриття цифр фарбою, яка б відбивала світло. Це зробить цифри більш примітними і потерпілий не буде втрачати велику кількість часу на пошуки наступної цифри.

Література

1. Новини ДСНС. Загублені в безкінечному просторі катакомб – Київ, 04.09.2021.

2. Новини UA. Одеська область: знайдено двох загублених чоловіки в катакомбах – Біляївка, Одеська область, 13.08.2020.

3. Новини Радіо Свобода. Пошукова група знайшла людей, які загубилися в катакомбах на Одещині– Біляївка, Київ, 06.07.2019

4. Столяренко А. М. Экстремальная психопедагогика. – М.: Юнити, 2002. – с.72 – 74.

5. Кодекс цивільного захисту України від 2 жовтня 2012 р. Постанова Кабінету Міністрів України №841 від 30.10.2013 р. Постанова КМУ від 24.03.2004 р. №368 «Про затвердження порядку класифікації НС за їх рівнями».

6. За загальною редакцією Могильниченка В.В. Захист населення і територій від надзвичайних ситуацій, Том 1 – Київ, 2007 – с. 13 – 15.

7. Пронин К.К. Одесские катакомбы. Международный симпозиум по искусственным пещерам. – Київ-Одеса, 1998 р. – с.30-32.

УДК [004.42+005.6]:378.1

АЛГОРИТМ РОБОТИ 3D СИМУЛЯТОРА ВИЗНАЧЕННЯ ПАРАМЕТРІВ СТІЙКОСТІ ПОЖЕЖНО-РЯТУВАЛЬНОГО ТРАНСПОРТНОГО ЗАСОБУ

Яковчук В., Придатко О.
Львівський державний університет безпеки життєдіяльності, Львів

Анотація. *У роботі описано пріоритетність розробки 3D симулятора, що буде виконувати функцію візуалізації результатів руху пожежно-рятувального транспортного засобу в залежності від попередньо налаштованих та заданих результатів.*

Ключові слова. *Симулятор, пожежно-рятувальний автомобіль, рушій Unity, розробка ПЗ, керованість, стійкість.*

Abstract. *The paper describes the priority of developing a 3D simulator that will perform the function of visualizing the results of the movement of the fire and rescue vehicle depending on the pre-configured and set results.*

Keywords. *Simulator, fire and rescue vehicle, Unity engine, software development, controllability, stability.*

За більш ніж вікову історію досліджень, розроблено безліч теоретичних підходів, які дають повне фізичне розуміння процесів, що відбуваються з автомобілем як у статиці, так й у динаміці. Реалізовано безліч досліджень та шляхів підвищення стійкості і керованості транспортного засобу під час руху.

Враховуючи велику вартість експериментальних досліджень, виготовлення прототипів, витрати часу для досягнення оптимальних характеристик керованості та стійкості руху, важливо ще на стадії проектування обґрунтовано вибирати оптимальні вагові, геометричні і конструктивні параметри автомобіля. У зв'язку з цим, актуальним є аналіз конструктивних та експлуатаційних параметрів автомобілів, які впливають на стійкість руху в спектрі експлуатаційних швидкостей, а також прогнозування поведінки транспортного засобу при дії на нього зовнішніх динамічних факторів[1].

Основним недоліком досліджень, являється трудомісткість застосування інженерних розрахунків, що призводить до великої затрата часу та матеріально-технічного ресурсу. Проте, наскільки б точними не були розрахунки, головним чинником вдалого дослідження являється візуалізація одержаних результатів. Продемонструвати даний результат можливо, завдяки розробці 3D симулятора, який буде виконувати функцію візуалізації результатів, в залежності від заданих параметрів та характеристик автомобіля.

Для реалізації роботи симулятора необхідно мати алгоритм роботи, чітку структуру та архітектуру системи (рис. 1). Розрахунок математичних функцій та роботи методів реалізується за допомогою бібліотек платформи Unity де вже налаштовані розрахункові обчислення, які на вхід будуть приймати визначені параметри.

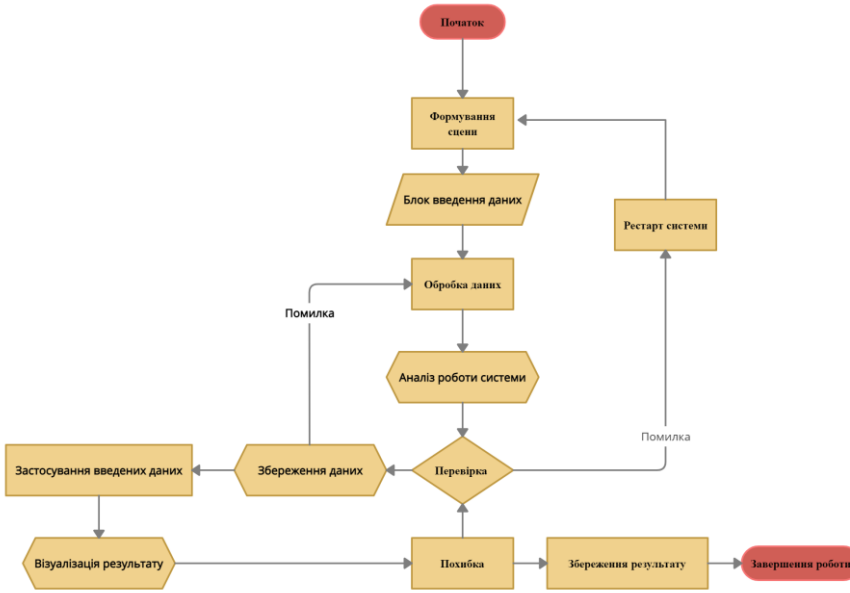


Рис. 1 Алгоритм роботи симулятора

Симулятор розроблений на рушії Unity (рис. 2), де було використано допоміжне програмне забезпечення для графічної реалізації (Adobe Photoshop, Blender), для написання коду використано об'єктно-орієнтовану мову програмування C# (середовище Visual Studio Code). Головний об'єкт дослідження – пожежна автоцистерна. Завдання розробленої системи полягає у реалізації візуалізації результатів руху пожежно-рятувального транспортного засобу, визначення стійкості та керованості.

Налаштування характеристик транспортного засобу, відбувається у вже зкомпільованій програмі, яка готова до використання, прийняття на вхід основних параметрів:

– Маса автомобіля з повним навантаженням
– Кут повороту коліс;
– Потужність двигуна;
– Сила гальмів;
– Центр маси автомобіля;

Рис. 2 Розробка програмного забезпечення на рушії Unity

Висновок. Завдяки розробленим архітектурним рішенням програмної системи та з використанням технологій C#, рушія Unity, програм графічної реалізації (Adobe Photoshop, Blender) розроблено 3D симулятор визначення стійкості пожежно-рятувального транспортного засобу під час його руху, в залежності від заданих параметрів. Головне завдання симулятора – візуалізація результатів з елементами 3D.

Література

1. Дослідження стійкості воєнного автомобіля у різних режимах руху. Електронний ресурс https://dl.khadi.kharkov.ua/mod/book/tool/print/index.php

З М І С Т

Секція 1

КІБЕРБЕЗПЕКА

Секція 2

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Наукове видання

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
V Всеукраїнської науково-практичної конференції
молодих учених, студентів і курсантів

Відповідальні за випуск **Олександр Придатко**
Ростислав Ткачук

Оригінал-макет **Ростислав Ткачук,**
Олександр Хлевной

Друк на різографі **Маріанна Климус**

Підписано до друку 12.11.2021 р.
Формат 60×84/16. Гарнітура Times New Roman.
Друк на різографі. Папір офсетний.
Ум. друк. арк. 13,4.

Друк ЛДУ БЖД
79007, Україна, м. Львів, вул. Клепарівська, 35
тел./факс: (032) 233-32-40, 233-24-79.
e- mail: mail@ubgd.lviv.ua, ndr@ ubgd.lviv.ua