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

ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

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

28 листопада 2019 року

Львів – 2019

ББК 32.81+78.362

*Захист інформації в інформаційно-комунікаційних системах: з*бірник тез доповідей ІІІ Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 28 листопада 2019 року. Львів, ЛДУ БЖД, 2019, 290 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

Напрям 1

Управління інформаційною безпекою

СУТНІСТЬ ПОТЕНЦІЙНИХ ТА РЕАЛЬНИХ ЗАГРОЗ ІНФОРМАЦІЇ

Дмитренко А., Мирошниченко В.
Дніпропетровський державний університет внутрішніх справ

Анотація. В роботі розглянуто шляхи забезпечення надійності роботи інформаційних систем, небезпечні впливи та основні вимоги поводження з інформаційними ресурсами.

Ключові слова: захист інформації, класифікація загроз, інформаційні системи, розмежування доступу.

Summary. The paper considers ways to ensure the reliability of information systems, dangerous influences and basic requirements for the management of information resources.

Keywords: information security, threat classification, information systems, access delimitation.

Одним з найважливіших аспектів проблеми створення ефективного гарантованого захисту інформації є визначення, аналіз і класифікація можливих загроз безпеки інформації.

Під ***загрозою безпеки*** розуміється потенційно можлива подія, процес або явище, які можуть привести до знищення, втрати цілісності, конфіденційності або доступності інформації.

Загрози можна класифікувати по відношенню джерела загрози:

до об'єкта захисту (зовнішні й внутрішні),

по виду джерела загроз (фізичні, логічні, комунікаційні, людські),

по ступеню злого наміру (випадкові й навмисні).

Усю множину загроз можна розділити на два класи: ***випадкові або ненавмисні, та навмисні***. Загрози, які не пов'язані з навмисними діями зловмисників і реалізуються у випадкові моменти часу, називають ***випадковими*** або ненавмисними.

Реалізація загроз цього класу приводить до найбільших втрат інформації (за статистичним даними – до 80% збитків від усіх можливих загроз) [1]. При цьому можуть відбуватися знищення, порушення цілісності й доступності інформації. Рідше порушується конфіденційність інформації, однак при цьому створюються передумови для злочинного впливу на інформацію.

У результаті порушується працездатність технічних засобів, знищуються й спотворюються дані й програми. Порушення роботи окремих вузлів і пристроїв можуть також призвести до порушення конфіденційності інформації.

Стихійні лиха й аварії чреваті найбільш руйнівними наслідками для матеріальних джерел зберігання інформації, тому що останні зазнають фізичному руйнуванню, інформація втрачається або доступ до неї стає неможливий.

Помилки при розробці інформаційної системи, алгоритмічні й програмні помилки приводять до наслідків, аналогічних наслідків збоїв і відмов технічних засобів. Крім того, такі помилки можуть бути використані зловмисниками для впливу на ресурси інформаційної системи. Особливу небезпеку становлять помилки в операційних системах і в програмних засобах захисту інформації.

Згідно даним Національного інституту стандартів і технологій США, 65% випадків порушення безпеки інформації відбувається в результаті помилок користувачів і обслуговуючого персоналу [2]. Некомпетентне, недбале або неуважне виконання співробітниками функціональних обов'язків призводять до знищення, порушення цілісності й конфіденційності інформації, а також компрометації механізмів захисту.

Характеризуючи загрози інформації, не пов'язані з навмисними діями, у цілому, слід зазначити, що механізм їх реалізації вивчений досить добре, накопичений значний досвід протидії цим загрозам. Сучасна технологія розробки технічних і програмних засобів, ефективна система експлуатації інформаційних систем, що включає обов'язкове резервування інформації, дозволяють значно знизити втрати від реалізації загроз цього класу.

Другий клас загроз безпеки інформації становлять ***навмисно створювані*** загрози. Даний клас загроз вивчений недостатньо, дуже динамічний і постійно поповнюється новими загрозами. Загрози цього класу відповідно до їхньої фізичної сутності й механізмів реалізації можуть бути розподілені по п'ятьом групах:

- традиційне шпигунство й диверсії;
- несанкціонований доступ до інформації;
- електромагнітні випромінювання й наведення;
- модифікація структур інформаційних систем;
- шкідницькі програми.

Організація забезпечення захисту інформації повинна передбачати обов'язкову ідентифікацію можливих джерел загроз, факторів, що сприяють їх прояву (вразливості) і, як наслідок, визначення актуальних загроз.

У якості джерел небажаного впливу на інформаційні ресурси як і раніше актуальні методи й засоби шпигунства й диверсій, які використовувалися й використовуються для добування або знищення інформації на

об'єктах, що не мають інформаційних систем. Ці методи також діючі й ефективні в умовах застосування інформаційних систем. Найчастіше вони використовуються для одержання відомостей про систему захисту з метою проникнення в інформаційну систему, а також для розкрадання й знищення інформаційних ресурсів.

Для деяких об'єктів інформаційних систем і зберігання інформації існує загроза збройного нападу терористичних (диверсійних) груп. При цьому можуть бути застосовані засоби вогневої поразки.

Термін несанкціонований доступ до інформації (НСД) визначений як доступ до інформації, що порушує правила розмежування доступу з використанням штатних засобів обчислювальної техніки або автоматизованих систем.

Під правилами розмежування доступу розуміється сукупність положень, що регламентують права доступу осіб або процесів (суб'єктів доступу) до одиниць інформації (об'єктів доступу).

У результаті збоїв або відмов засобів системи, а також помилкових дій обслуговуючого персоналу й користувачів можливі стани системи, при яких спрощується НСД.

Реалізація безперервного процесу захисту інформації можлива тільки на основі систем концептуального підходу й промислового виробництва засобів захисту, впровадження надійних механізмів захисту й забезпечення їх сталого функціонування й високої ефективності, провадження відповідних робіт тільки фахівцями високої кваліфікації в області захисту інформації.

Література:

1. Ленков С.В., Перегудов Д.А., Хорошко В.А., Методы и средства защиты информации/ под. ред. В.А.Хорошко. – К.: Арий, 2008. – Том 1. Несанкционированное получение информации, – 464 с.

2. Богуш В.М., Юдін О.К., Інформаційна безпека держави. –К.: «МК-Прес», 2005. – 432с.

3. Мельников В.П., Клейменов С.А., Петраков В.М., Информационная безопасность и защита информации: учебное пособие для студентов высших учебных заведений / под. ред. С.А.Клейменова. – М.: Изд. центр «Академия», 2009. – 336 с.

СИСТЕМИ ЗБОРУ ІНФОРМАЦІЇ ПРО БЕЗПЕКУ ТА УПРАВЛІННЯ ПОДІЯМИ

Довганик С., Полотай О.
Національний університет «Львівська політехніка»

Описано основне призначення та особливості SIEM-систем для збору інформації та управління подіями. Показано основні джерела інформації, які використовуються для таких систем. Наведено перелік сучасних SIEM-систем.
Ключові слова: захист інформації, SIEM-системи, управління подіями.

The main purpose and features of SIEM systems for information gathering and event management are described. The main sources of information used for such systems are shown. The list of modern SIEM-systems is given.
Keywords: information security, SIEM systems, event management.

Оскільки практично більшість підприємств працюють в Інтернеті, все важливіше використовувати інструменти кібербезпеки та виявлення загроз для запобігання простоїв роботи. На жаль, у мережі багато активних недобросовісних зловмисників, які лише чекають удару по вразливих системах. Інформація про безпеку та управління подіями (SIEM) стали основною частиною виявлення та подолання кібератак.

Системи захисту, відомі під абревіатурою SIEM, з'явилися в результаті еволюції і злиття SEM і SIM.

SEM – Security Event Management – система захисту, яка працює в режимі реального часу. Вона самостійно спостерігає за подіями в інформаційних потоках, збирає їх, виробляє кореляцію і генерує превентивні повідомлення.

SIM – Security Information Management – система, яка відповідає за аналіз відомостей на основі статистики та девіацій від встановлених правил безпеки.

Абревіатура SIEM означає «Система Збору та Кореляції Подій». Як можна судити з назви, самі по собі такі системи не здатні що-небудь запобігати або захищати. Їх завдання в іншому – аналізувати інформацію, що надходить від різних систем, таких як антивіруси, DLP, IDS, маршрутизатори, міжмережеві екрани, операційні системи серверів і призначених для користувача ПК, і при цьому детектувати відхилення від норм по якимось критеріям. Якщо таке відхилення виявлено – система генерує інцидент. Варто відзначити, що в основі роботи SIEM лежать, в основному, статистичні та математичні технології, схожі на ті, що використовуються, наприклад, в BI-системах.

До речі, SIEM-система не тільки автоматизує аналіз різних системних подій. Важливо, що з її допомогою можна виявити дії, які зовні виглядають цілком нешкідливими, але в сукупності становлять загрозу. Наприклад, якщо довірений користувач відправляє конфіденційні дані на email-адресу, що лежить поза звичного кола адресатів, то DLP-система не завжди відловлює такі дії, проте SIEM згенерує інцидент на базі накопиченої статистики.

Діапазон завдань, які здатна вирішити SIEM-система, дійсно дуже широкий. По-перше, про що вже згадувалося раніше, це автоматизація моніторингу та аналізу всіх подій, які відбуваються в численних системах захисту. Друге важливе завдання, цілей, заради якої використовуються SIEM-технології: в разі інциденту SIEM здатна надати всю необхідну доказову базу, придатну як для внутрішніх розслідувань, так і для суду. Третє важливе призначення системи – SIEM допомагає проводити аудити на відповідність різним галузевим стандартам.

Більше число джерел даних означає більш повне і ретельне охоплення всіх подій, що реєструються в IT-інфраструктурі підприємства. Для виконання свого завдання сучасні SIEM-системи використовують такі джерела інформації:

- ***Access Control, Authentication.*** Застосовуються для моніторингу контролю доступу до інформаційних систем і використання привілеїв.
- ***DLP-системи.*** Відомості про спроби інсайдерських витоків, порушення прав доступу.
- ***IDS / IPS-системи.*** Несуть дані про мережеві атаки, зміни конфігурації і доступу до пристроїв.
- ***Антивірусні програми.*** Генерують події про працездатність ПО, базах даних, зміні конфігурацій і політик, шкідливий код.
- ***Журнали подій серверів і робочих станцій.*** Застосовуються для контролю доступу, забезпечення безперервності, дотримання політик інформаційної безпеки.
- ***Міжмережеві екрани.*** Відомості про атаки, шкідливі програми та інше.
- ***Мережеве активне обладнання.*** Використовується для контролю доступу, обліку мережевого трафіку.
- ***Сканери вразливостей.*** Дані про інвентаризацію активів, сервісів, ПО, вразливостей, поставка інвентаризаційних даних і топологічної структури.
- ***Системи інвентаризації та asset-management.*** Поставляють дані для контролю активів в інфраструктурі і виявлення нових.
- ***Системи веб-фільтрації.*** Надають дані про відвідування співробітниками підозрілих або заборонених веб-сайтів.

SIEM-системи стали основним компонентом безпеки сучасних організацій. Основна причина полягає в тому, що кожен користувач або трекер залишає після себе віртуальний слід у даних журналу мережі. Системи SIEM розроблені для використання цих даних журналу, щоб генерувати уявлення про минулі атаки та події. Система SIEM не тільки визначає, що стався напад, але дозволяє вам бачити, як і чому це сталося.

По мірі того, як організації оновлюють і покращують масштабність все більш складних IT-інфраструктур, SIEM набуває ще більшого значення в останні роки. Всупереч поширеній думці, брандмауерів та антивірусних пакетів недостатньо для захисту мережі в цілому. Нульові атаки все ще можуть проникнути в захисні сили системи навіть при застосуванні цих заходів безпеки.

Серед сучасних SIEM систем, варто виділити такі:

- ManageEngine EventLog Analyzer;
- Журнал SolarWinds & Менеджер подій;
- IBM Security QRadar.

Використання SIEM також допомагає компаніям дотримуватися різноманітних галузевих правил управління інформаційною безпекою. Системи SIEM забезпечують найкращий спосіб задоволення цієї нормативної вимоги та забезпечують прозорість журналів, щоб генерувати чітку інформацію та вдосконалення.

Література:

1. Столова О. В. Методика порівняння ефективності сучасних SIEM-систем: [Електронний ресурс]. – Режим доступу: http://ela.kpi.ua/bitstream/123456789/20810/1/13.%D0%A1%D1%82%D0%BE%D0%BB%D0%BE%D0%B2%D0%B0.163-164.pdf

2. TIM KEARY 9 Best SIEM Tools: A Guide to Security Information and Event Management. [Електронний ресурс]. – Режим доступу: https://www.comparitech.com/net-admin/siem-tools/

3. Drew Robb, Top SIEM Products [Електронний ресурс]. – Режим доступу: https://www.esecurityplanet.com/products/top-siem-products.html

4. Abhishek Sharma, Senior Technical Marketing Engineer at Securonix The Anatomy of a Modern SIEM: https://www.securonix.com/the-anatomy-of-a-modern-siem/

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Дубей С., Козловський В., Фірман В.
Львівський національний університет імені Івана Франка

Інформаційна безпека зараз, одне з найактуальніших питань сьогодення.

Будь-яке підприємство, це як мінімум опрацювання даних свої працівників, а як максимум, це опрацювання величезної кількості, статистики, електронної пошти, інформації від клієнтів, тощо.

Отже, для бізнесу вона відіграє надзвичайно важливу роль, як в забезпеченні безпеки своїх даних, так і даних працівників, користувачів та третіх сторін.

Захист інформації полягає в:

1) Забезпеченні гарантії захищеного зберігання.

2) Безпечний доступ до інформації в процесі використання, для будь-яких корпоративних цілей.

3) Компетентні співробітники

Під поняттям інформація, мається на увазі: файли будь-якого вмісту, ресурси в корпоративній мережі, корпоративна мережа, працівники.

Забезпечення захищеного зберігання, може бути при умові:

1) Шифрування даних з використанням надійних симетричних шифрів(AES, RS4,DES, тощо)

2) Використання фізичних носіїв з системами захисту від механічного, програмного, фізичного впливу (радіація, магнітні поля, тощо).

3) Обмеження кола осіб, що мають доступ до фізичних носіїв

Забезпечення безпечного доступу до інформації, може бути при умові:

1) Існування системи керування доступами до ресурсів для співробітників.

2) Існування системи моніторингу стану мережі та стану корпоративних ресурсів.

3) Існування системи протидії кібер-атакам, як з ззовні, так і з середини.[1]

[1]Прикладами таких систем, є рішення по організації мережі через NAT, використання фаєрволів, як програмних, так і фізичних, фільтрація трафіку за допомогою налаштування маршрутизаторів, або тих самих фаєрволів. Накладання обмежень на корпоративні комп'ютери за допомогою антивірусів, та попередніх налаштувань відділом технічної підтримки.

4) Використання ліцензійного ПЗ, антивірусів, ліцензійних операційних систем(спеціалізованих для корпоративного використання (RedHat, CentOS, Fedora, тощо)).

5) Існування системи резервного копіювання

6) Проінструктовані, та навчені техніці інформаційної безпеки співробітники.

7) Існування відділу технічної підтримки.

Забезпечення компетентності співробітників з приводу інформаційної безпеки:

Проведення навчань та інструктажів з приводу інформаційної безпеки, на рівні користувача:

1) Проведення інструктажів на рахунок соціальної інженерії.

2) Систематичне тестування співробітників з приводу техніки інформаційної безпеки.

Втручання за допомогою соціальної інженерії може включати в себе:

1) Пошук незадоволеного, або ж морально слабкого співробітника, з метою виявлення можливих вразливостей в системі офісної безпеки.

2) Видавання себе за співробітника підприємства, або працівника того чи іншого відділу.

3) Використання чужих, або ж підроблених пропусків, паролів, тощо.

4) Збір будь-якої не знищеної інформації що може нашкодити клієнтам, підприємству, співробітникам.

5) Збір знищеної інформації на паперових носіях, з метою її відновлення.

Забезпечення безпеки життєдіяльності може бути при:

1) Існуванні системи відеоспостереження.

2) Існування системи резервного енергопостачання генераторів і відповідно її належна охорона, для забезпечення безпеки життєдіяльності персоналу.

3) Спеціальний персонал, що забезпечує охорону офісів , спеціальних об'єктів особливої важливості, таких як система резервного енергопостачання, або ж дата-центри.

Отже підсумовуючи вище наведене, інформаційна безпека, наряду з охороною праці, та охороною безпеки життєдіяльності на підприємстві, має бути першим пріоритетом для підприємства, та співробітників.

Тільки строге дотримання стандартів техніки безпеки , може забезпечити, безперебійну, продуктивну працю на підприємстві, зекономити кошти власнику, зберегти репутацію перед клієнтами, та здоров'я своїх співробітників.

Адже, техніка безпеки, в тому числі інформаційна, писана кров’ю.

Література:

1. Кевин Митник Искусство обмана: Компания АйТи; 2004 ISBN 5-98453-011-2, 0-471-23712-4
2. Низенко Е. І., Калиняк В. П. Забезпечення інформаційної безпеки підприємництва: Навч. посіб. — К. : МАУП, 2006. — 134 с. — Бібліогр.: С. 124–130.
3. Сороківська О. А. , В. Л. Гевко Інформаційна безпека підприємства: Нові загрози та перспективи. 14.06.2010
4. Стандарт ISO/IEC 27001:2013 : https://www.iso.org/standard/54534.html

УДК 636.5252

ПРОГРАМНА СИСТЕМА ФОРМУВАННЯ АГРЕГОВАНИХ ДАНИХ

Поворозник Ю.П., Малець І.О.
Львівський державний університет безпеки життєдіяльності, Львів

Роботу присвячено актуальній проблемі створення програмної системи формування агрегованих даних.

Процес формування агрегованих даних є дуже важливим для сучасного управління бізнес-процесами і на основі цих даних підприємства різноманітних галузей можуть сформувати результуючі звіти за певний період часу і побачити реальний розвиток свого підприємства. Використовуючи агреговані дані, керівництво підприємств здатне прийняти необхідні рішення для подальшого успішного їх розвитку.

В наші часи без ефективних програмних систем збереження даних не обійдеться практично жодне підприємство. Це можуть бути різного роду підприємства: банки, страхові, транспортні компанії, мережі супермаркетів, телекомунікаційні та маркетингові фірми, організації, що задіяні в сферах послуг тощо [3]. Всі вони здійснюють збір, обробку та збереження даних, які містять колосальний об’єм даних. На основі цих даних вирішуються найбільш різноманітні завдання, пов’язані з взаємодією з клієнтами або ж для розв’язання аналітичних задач. Проблеми обробки і збереження даних підприємства стають все більш актуальними, і багато спеціалістів в галузі інформаційних технологій намагаються постійно покращувати засоби роботи з цими даними. Спеціалісти, які займаються аналізом даних повинні мати доступ до всієї інформації, яка їх цікавить, а також використовувати зручні і прості засоби для представлення і роботи з цією інформацією.

Задачі технологій сховищ даних (Data Warehouse) та бізнес-інтелекту (Business Intelligence) направлені на вирішення цих проблем. Бізнес-інтелект – це процес прийняття «інтелектуальних» бізнес-рішень шляхом аналізу доступних даних. З технологічної точки зору, бізнес-інтелект об’єднує в собі області сховищ даних, розробку OLAP та Data Mining систем, формування звітів, візуалізації та аналізу даних [5].

Сховище даних – це організований масив даних підприємства, що обробляється і зберігається в єдиному апаратно-програмному комплексі, що забезпечує швидкий доступ до даних підприємства, багатовимірний аналіз даних, створення звітів з метою відображення статистичних даних [1].

Сховище даних містить величезний обсяг даних. Деякі сховища даних містять десятки терабайт і навіть петабайт даних. Крім цього, оскільки ці дані повинні охоплювати все підприємство, реалізація сховищ даних

зазвичай займає багато часу, обсяг якого залежить від розміру підприємства. Внаслідок цих недоліків, багато компаній починають з менших рішень, які називаються кіоском даних.

Кіоск даних (Data Mart) являє собою склад даних, що містить всі дані на рівні відділу, що дозволяє користувачам мати доступ до даних, які зачіпають лише окрему частину їх компанії. Наприклад, відділ збуту зберігає всі свої дані по збуту в своєму власному кіоску даних, дослідний відділ зберігає дані з досліджень в своєму кіоску даних тощо. В структурах сховищ даних підприємств використовують проміжну базу даних (Staging), в якій здійснюється безпосередня обробка даних, що надійшли з систем оперативної обробки транзакцій OLTP перед завантаженням цих даних в сховище даних. Агрегація даних – це процес збирання вихідних даних з метою представлення цих даних у зведеній формі для статистичного аналізу. Наприклад, вихідні дані можуть бути агреговані протягом певного періоду часу шляхом застосування статистичних функцій над даними, такими як визначення середнього арифметичного, максимального або мінімального значення, суми значень, підрахунок кількості значень. Після виконання процедури агрегування даних вони можуть бути представлені засобами формування звітів з метою прийняття бізнес-рішень [4].

В сучасних програмних системах процес агрегування даних реалізовується за допомогою технології OLAP. Технологія OLAP дозволяє користувачеві здійснювати різноманітні аналітичні операції, такі як консолідація, деталізація, зріз даних [2]. Ключовою структурою даних технології OLAP є куб.

OLAP-куб є аналітичною структурою даних, що створена з робочих даних підприємства. Куб включає в себе чисельні дані, які називаються фактами, до яких застосовується агрегація, а також містить інформацію про виміри, що описують факти та здійснюють їхнє розподілення. Існує три типи схем за якими формується куб:

1) Схема «Зірка» – існує одна таблиця фактів, до якої посилаються декілька таблиць вимірів;

2) Схема «Сніжинка» – існує одна таблиця фактів, до якої посилаються декілька таблиць вимірів, до яких посилаються таблиці інших вимірів;

3) Схема «Сузір'я» – існує декілька таблиць фактів та таблиць вимірів, які між собою взаємопов'язані.

Структура OLAP технологій надає можливість багатовимірного аналізу даних, що суттєво спрощує формування результуючих звітів.

Програмна система формування агрегованих даних будується за технологіями бізнес-інтелекту і включає в себе такі компоненти як: джерело даних, база даних, сховище даних, кіоск даних, аналітична структура даних (в якій безпосередньо формуються агреговані дані) та засоби створення звітів на основі сформованих агрегованих даних.

Процес міграції даних з однієї структури в іншу називається процесом збору, трансформації та завантаження даних – ETL. Мета ETL процесу: забезпечити якісну та надійну обробку та переміщення даних в місце призначення.

Актуальність даної тематики є дослідження сучасних проблем обробки даних великого об'єму та можливість покращення результуючих звітів, що сформовані на основі агрегованих даних. Запропоновано альтернативний принцип побудови системи сховища даних шляхом покращення показників якості та швидкості процесу формування агрегованих даних, що дозволяє підприємству з меншими витратами отримувати результуючі дані.

Для досягнення сформульованої мети програмна система повинна відповідати наступним вимогам:

- можливість централізованого управління та моніторингу процесу збору, трансформації та завантаження даних та можливість автоматизації процесу завантаження даних;
- можливість формування звітів на основі завантажених даних та забезпечення можливості масштабування системи;
- забезпечити систему необхідними програмними засобами захисту інформації.

В рамках технології аналітичних структур даних запропоновано новий підхід до формування агрегованих даних, удосконалено сучасні принципи побудови систем сховищ даних.

Література:

1. Батьков В.О. - Анализ проблем современных хранилищ данных // Батьков В.О. – Московский государственный университет экономики, статистики и информатики, 2013. – 3 с.

2. Горбань Г.В. Методи та об'єктно орієнтована інформаційна технологія інтелектуального аналізу багатовимірних даних / Горбань Г.В. – Чорноморський державний університет імені Петра Могили: «05.13.06 – Інформаційні технології», 2016. – 229 с.

3. Корнилов Е.Г. Современное применение OLAP и OLTP технологий в экономике // Корнилов Е.Г., Долгова Т.Г. – Красноярск: сибирский государственный аэрокосмический университет, Секция «Информационно-экономические системы», 2010. – С.419-420

4. Data aggregation [Електронний ресурс] / ibm. – Режими доступу: https://www.ibm.com/support/knowledgecenter/en/SSBNJ7_1.4.4/dataView/Concepts/ctnpm_dv_use_data_aggreg.html.

5. Marie-Aude Aufaure – Business Intelligence // Marie-Aude Aufaure, Esteban Zimanyi (Eds.): Second European Summer School, eBISS 2012, Brussels, Belgium, July 2012. – 234 P.

ДОСЛІДЖЕННЯ УРАЗЛИВОСТІ МІЖСАЙТОВОГО ВИКОНАННЯ СЦЕНАРІЇВ

Реутьонок О., Гарасимчук О.
Національний університет "Львівська політехніка"

Міжсайтове виконання сценаріїв (XSS) є досить поширеною вразливістю серед Web-додатків. XSS виникає, коли на сторінки, які були згенеровані сервером, потрапляють користувацькі скрипти. За допомогою XSS зловмисники можуть виконувати сценарії в браузері жертви, що дозволяють їм перехоплювати призначені для користувача сесії, підміняти сторінки сайту або перенаправляти користувачів на шкідливі сайти.

Ключові слова: міжсайтове виконаня сценаріїв, міжсайтовий скриптинг, XSS, вразливість, атака, web-додаток

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side scripts into web pages viewed by other users. Attackers can execute scripts in a victim's browser that allow them to intercept user sessions, swap site pages, or redirect users to malicious sites.

Key words: Cross-site scripting, XSS, vulnerability, attack, web-application

Міжсайтове виконання сценаріїв (Cross Site Scripting) – це тип вразливості програмного забезпечення, властивий Web-додаткам, який дозволяє атакуючому впровадити клієнтський сценарій в Web-сторінки, що переглядаються іншими користувачами. Також цю вразливість називають міжсайтовим скриптингом або XSS-вразливість. XSS є другою за поширеністю вразливістю з топ-10 OWASP і виявляється в двох третинах усіх додатків.

XSS може використовуватись для зміни налаштувань веб-додатку, перехвату сесій, крадіжки облікових записів, викрадення куків користувача, розміщення неправдивої реклами, викрадення токенів форм для проведення CSRF атак, заміни та підміни DOM-вузлів та інше.

Існує три види XSS вразливостей:

- Постійний міжсайтовий скриптинг (Stored XSS);
- Непостійний міжсайтовий скриптинг (Reflected XSS);
- Міжсайтовий скриптинг на основі об'єктної моделі документа (DOM XSS).

Постійний міжсайтовий скриптинг характеризується тим, що зловмиснику вдається впровадити на сервер шкідливий код, який виконується в браузері кожен раз при зверненні до оригінальної сторінки. Постійних XSS виникає, коли розробники здійснюють некоректну фільтрацію при збереженні вхідних даних в базу даних на сервері або при записі цих даних у файл з подальшим виводом їх в браузер користувача.

Непостійний XSS є найбільш поширеним типом міжсайтового скриптингу. Він виникає коли дані, введені користувачем у HTML формі, використовуються для генерації відповіді користувачу без попередньої обробки.

XSS у DOM-моделі виникає на стороні клієнта під час обробки даних всередині JavaScript сценаріїв. Прикладом цієї вразливості може слугувати сценарій, які отримує дані з URL через location.* DOM або за допомогою XMLHttpRequest запиту, а потім без фільтрації використовують їх для створення динамічних HTML об'єктів.

Для наглядності розберемо один приклад міжсайтового виконання сценаріїв. Викрадання куків найпопулярніший приклад XSS-атаки. У куках сайти іноді зберігають якусь цінну інформацію (іноді навіть логін і пароль (або його хеш) користувача), але найнебезпечнішою є крадіжка активної сесії. Схема виконання атаки зловмисником буде виглядати наступним чином:

1) Зловмисник використовує одну з форм веб-сайту для того, щоб вставити шкідливий рядок в базу даних веб-сайту. Шкідливим рядком може бути скрипт, який створить HTTP-запит на іншу URL-адресу, який перенаправляє браузер користувача на сервер атакуючого.

Наприклад,

```
<script>
        window.location='http://attacker/?cookie='+document.cookie
</script>
```

Програма очікує отримати звичайний текст (наприклад коментар на форумі), а не код, тому без перевірки зберігає шкідливий рядок у базу даних.

2) Жертва запитує сторінку з веб-сайту.
3) Сайт включає шкідливий рядок з бази даних у відповідь і відправляє його до жертви.
4) Браузер жертви виконує шкідливий сценарій всередині відповіді, відправляючи куки жертви на сервер зловмисника.

Нагадаємо, що XSS уразливістю, що використовується атакою типу впровадження коду: введені дані користувачем помилково інтерпретуються як шкідливий програмний код. Для того, щоб не допустити цього типу ін'єкції коду, потрібно безпечна обробка введення. Для веб-розробника, існує два принципово різних способи виконання безпечної обробки введення:

- Кодування – це спосіб, який дозволяє зробити введення даних користувачем тільки як дані і не дозволяє браузеру обробляти їх як код.
- Валідація – це спосіб фільтрації введених даних користувача так, що браузер інтерпретує їх як код без шкідливих команд.

Для запобігання XSS необхідно відокремлювати неперевірені дані від активного контенту браузера. Цього можна досягти наступними способами:

– Використовувати фреймворки з автоматичним перетворенням даних, як в останніх версіях Ruby on Rails і React JS. Необхідно також проаналізувати обмеження XSS-захисту кожного фреймворка і забезпечити відповідну обробку цих винятків.

– Перетворювати недовірені дані з HTTP-запитів, грунтуючись на контексті, в HTML-коді (тілі, атрибутах, JavaScript, CSS або URL) для запобігання відбитого XSS і міжсайтового виконання збережених сценаріїв.

– Застосовувати контекстне кодування при зміні документа в браузері користувача для запобігання XSS на основі DOM. Якщо це неможливо, то застосовувати контекстне кодування до API.

– Використовувати політику захисту вмісту (CSP) для запобігання XSS. Цей захід ефективний, якщо відсутні вразливості, що дозволяють впровадити код через локальні файли

В наш час наявність цієї вразливості у web-додатках вже не для кого не секрет. Великі сайти крупних компаній досить швидко закривають цю вразливість, в той час як розробники невеликих web-додатків можуть не помічати її досить тривалий час. Саме тому XSS все ще залишається в списку найнебезпечніших уразливостей у вебі. Дотримуючись всього декількох правил у написанні логіки роботи web-додатків можливо закрити більшість уразливостей цього типу і підвищити безпеку інформації додатку.

Література:

1. Вікіпедія – вільна енциклопедія [Електроний ресурс]-Режим доступу: https://en.wikipedia.org/wiki/Cross-site_scripting -. (дата звернення 10.11.2019) – Назва з екрану

2. OWASP™ Foundation – OWASP Top 10 Most Critical Web Application Security Risks Електроний ресурс]-Режим доступу: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project -. (дата звернення 10.11.2019) – Назва з екрану

3. Полное пособие по межсайтовому скриптингу [Електроний ресурс]-Режим доступу: https://www.securitylab.ru/analytics/432835.php -. (дата звернення 10.11.2019) – Назва з екрану

4. Excess XSS: комплексный учебник по межсайтовому скриптингу [Електроний ресурс]-Режим доступу: https://defcon.ru/web-security/3428/ -. (дата звернення 11.11.2019) – Назва з екрану

ОЦІНКА ЗАХИЩЕНОСТІ ПРОМИСЛОВИХ ІНФОРМАЦІЙНИХ СИСТЕМ SCADA

Самара Н. М.
Львівський державний університет безпеки життєдіяльності, МАУ

Потреба в терміновому розв'язанні питань безпеки та оцінці захищеності пов'язаних із системою SCADA, в теперішній час є високою. На відміну від звичайних IT-систем, більшість успішних атак на системи SCADA можуть мати серйозні наслідки для економіки країни, її стабільності і, що гірше, негативно вплинути на життя людей. Так, наприклад, у 2015 році сотні тисяч українців залишилися без електроенергії майже на 6 годин через атаку на систему SCADA «Прикарпаттяобленерго», а у 2010 році мережевий комп'ютерний вірус-хробак Stuxnet завдав нищівного удару по ядерній програмі Ірану, через яку було тимчасово припинено роботи зі збагачення урану.

SCADA-система, оцінка ризиків, кількісний аналіз ризиків, захищеність системи, CySeMoL, EAAT, вектори атаки, система безпеки

SCADA system, risk assessment, quantitative risk analysis, system security, CySeMoL, EAAT, attack vectors, security system

Системи SCADA збирають дані з датчиків на заводі або інфраструктурному підприємстві й можуть вносити зміни віддалено для оптимізації процесу на основі отриманих даних. Ці системи контролюють низку фізичних параметрів, таких як швидкість конвеєрної стрічки, температура й тиск у резервуарі, або будь-який процес, який можна контролювати без безпосереднього втручання людини.

Детальний аналіз архітектури систем SCADA дозволяє визначити передумови виникнення загроз для систем та причину їх недостатньої захищеності. Здебільшого вони полягають у стрімкому збільшенні вимог до функціональності, надійності та вартості, тоді як захищеність таких систем, або не є пріоритетною для власників, або її надзвичайно важко забезпечити через особливості цих систем.

Розглянемо вразливості систем SCADA. Людський фактор (недостатній рівень компетентності, або свідоме нехтування захищеністю систем заради розв'язання технологічних проблем). Уразливості операційних систем (часто у роботі використовують версії операційно системи з широко відомими вразливостями, задля забезпечення безперебійної роботи SCADA-систем). Слабка автентифікація. Віддалений доступ. Зовнішні мережеві підключення (хоча для систем SCADA вкрай нерекомендовані зовнішні підключення, у інформаційному звіті CyberX стверджується, що близько 40% АСУ ТП мають пряме підключення до інтернету). Засоби захисту та моніторингу (використання IDS і антивірусів не є поширеною). Бездротові мережі. Дистанційні процесори. Програмне забезпечення (ча-

сто містить значну кількість архітектурних недоліків). Фізична безпека (обладнання може перебувати за межами контрольованої зони).

Результати використання цих вразливостей можуть носити різний характер. Успішна атака може спричинити збій в роботі SCADA-системи, пошкодження промислового устаткування, порушення процесу виробництва продукції, зниження її якості, нанесення шкоди здоров'ю людей, флорі та фауні, порушення екологічної безпеки та охорони праці.

Інструменти оцінки захищеності. Ефективним для оцінювання захищеності SCADA-системи є інструмент для системного аналізу EAAT разом з P^2CySeMoL. Вони можуть створити модель архітектури системи й оцінити рівень кібербезпеки — ймовірність того, що зловмисник отримає доступ до захищених ресурсів. Для компаній, що пропонують продукти для управління технологічним процесом, де цілісність системи дуже важлива, допомога такого інструменту є надзвичайно корисною. Це б дозволило їм створювати й перевіряти рівень кібербезпеки, властивий архітектурі системи, до її впровадження й тестування на проникнення. Так недоліки можуть бути легко виявлені і виправлені на етапі проектування системи. Ще одна особливість інструменту полягає в тому, що він дозволяє спрогнозувати можливі наслідки конкретної архітектури системи.

Для виконання аналізу використовується імовірнісна модель відносин, яка визначає спосіб побудови баєсової мережі з об'єктної моделі. Баєсова мережа включає в себе заздалегідь заданий набір випадкових величин, де відносини між ними встановлюються наперед. Тому баєсові мережі часто не можуть представляти складні і великі системи. Тобто системи, де конфігурація об'єктів або їх кількість варіюється. Це пов'язано з тим, що такі мережі не здатні обробляти концепцію об'єктів. Іншими словами, вони не можуть представляти кілька схожих об'єктів у декількох умовах із загальними принципами. Модель імовірнісних відносин (PRM) розширює баєсову мережу. Вона вводить об'єкти, відносини між ними та їх властивості. Це дозволяє баєсовій мережі обробляти складні і великі системи.

Для проведення аналізу кібербезпеки системи, потрібно моделювати її архітектуру. Це включає визначення об'єктів в архітектурі системи, таких як операційні системи, сервери та персонал. Вони позначаються як активи (Assets) в CySeMoL. Також необхідно визначити наступні атрибути для кожного об'єкта: можливі способи компрометації активу (AttackSteps) та захист активу (Defence attributes). Приклади активів та їхні атрибути можна побачити на рисунку 1.1.

Створення моделі для CySeMoL складається з двох етапів. Першим кроком є визначення якісної структури, тобто які активи повинні бути включені, їх захист і шляхи атаки. Другим кроком буде додавання кількісних даних у цю якісну структуру, які визначають, наскільки ймовірно, що атака буде успішною, з урахуванням зазначених захистів.

Використання літератури, а також матеріалів від експертів у предметній області послужило основою для визначення того, які типи захисту й атаки повинні бути включені в CySeMoL. Залежно від змодельованої архітектури системи, CySeMoL обчислює умовні ймовірності для успіху атаки. Однак важливо визнати, що підсумкові розрахунки слід розглядати як опорні факти, а не жорсткі статистичні дані. Це пов'язано з низкою причин. По-перше, умовні ймовірності, створені CySeMoL, потребують оновлення, оскільки дані про захисників і нападників змінюються з часом. По-друге, CySeMoL більше орієнтований на жорсткі технічні аспекти безпеки, ніж на більш м'які, такі як соціальна інженерія або фізичні атаки, які є досить базовими в системах SCADA. Зловмисник діє суб'єктивно й піддається великим відхиленням. Тому важко зробити висновок, що розрахунки можна представити для різних типів зловмисників, наприклад, для досвідченого зловмисника та новачка.

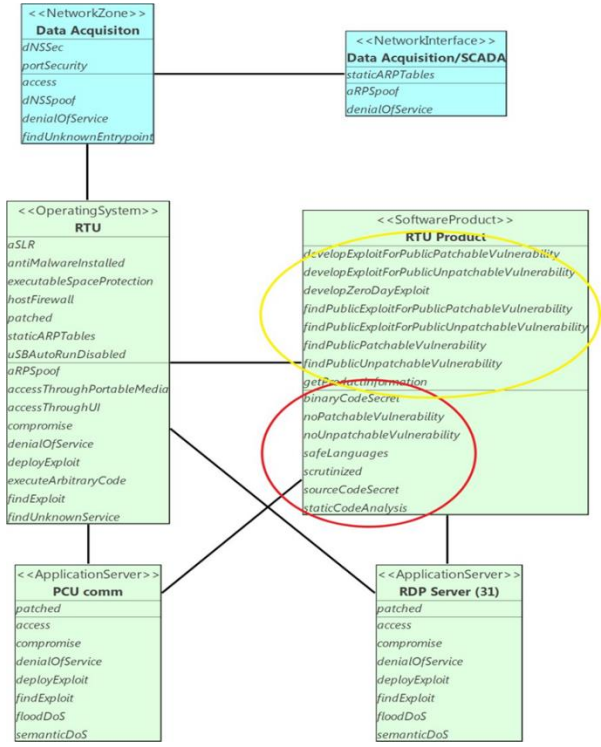


Рисунок 1.1 – Модель CySeMoL. Верхній жовтий овал позначає кроки атак, а нижній червоний – захисні атрибути

Література:

1. Supervisory Control and Data Acquisition (SCADA) System [Електронний ресурс] // Office of the Manager National Communications System. – 2004. – Режим доступу до ресурсу: https://scadahacker.com/library/Documents/ICS_Basics/SCADA%20Basics%20-%20NCS%20TIB%2004-1.pdf.

2. "Security Through Obscurity" Ain't What They Think It Is [Електронний ресурс] // Jay Beale, Lead Developer, Bastille Linux Project. – 2001. – Режим доступу до ресурсу: https://web.archive.org/web/20070202151534/http:/www.bastille-linux.org/jay/obscurity-revisited.html.

3. D5.4 – CockpitCI System Factory Trials Report [Електронний ресурс] / [R. Pietro, G. Antonio, D. Federico та ін.] // Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures. – 2014. – Режим доступу до ресурсу: https://cockpitci.itrust.lu/wp-content/uploads/2015/04/CockpitCI-D5.4-CockpitCI-System-Factory-Trials-Report.pdf.

4. ISA-99.00.01 Security for industrial automation and control systems—part 1: terminology, concepts, and models // American National Standard, Research Triangle Park. – 2007. – 95 с.

5. Sadowsky G. Information Technology Security Handbook / G. Sadowsky, J. Dempsey, A. Greenberg. – Washington: Global Information And Communication Technologies Department, 2003. – 392 с.

6. Guide to Industrial Control Systems (ICS) Security / [K. Stouffer, V. Pillitteri, S. Lightman та ін.]. // NIST Special Publication. – 2015. – №800. – С. 135.

7. Винокурова О. А. Безопасность промышленных информационных систем, виды угроз и общие принципы защиты информации / О. А. Винокурова, Е. В. Шибарова. // ВЕСТНИК МГУП ИМЕНИ ИВАНА ФЕДОРОВА. – 2016. – С. 4.

8. GLOBAL ICS & IIOT RISK REPORT [Електронний ресурс] // CYBERX. – 2019. – Режим доступу до ресурсу: https://cyberx-labs.com/resources/risk-report-2019/.

9. K. D. Wall. The Kaplan and Garrick Definition of Risk and its Application to Managerial Decision Problems [Електронний ресурс] / K. D. Wall. – 2011. – Режим доступу до ресурсу: https://my.nps.edu/documents/103424423/106950799/DRMI+Working+Paper+2011-3.pdf/bad99104-b54b-4646-9d92-45e16c2f80d8.

10. CySeMoL: A tool for cyber security analysis of enterprises [Електронний ресурс] / Hannes Holm, Teodor Sommestad. – 2013. – Режим доступу до ресурсу: http://www.sommestad.com/teodor/Filer/Ekstedt%20et%20al.%20-%202013%20-%20CySeMoL%20A%20tool%20for%20cyber%20security%20analysis%20of%20enterprises.pdf.

УДК 004.056

ПРОЦЕСОР НА ПЛІС ДЛЯ СТИСНЕННЯ ВІДЕО ПОТОКУ ДЛЯ СИСТЕМИ ЗБОРУ НАУКОВОЇ ІНФОРМАЦІЇ МІКРОСУПУТНИКА

Сіренко Н.О., Малець І.О.
Львівський державний університет безпеки життєдіяльності, Львів

Роботу присвячено актуальні проблемі проектування спеціалізованих апаратних засобів на базі ПЛІС для стиснення зображень без втрат методом JPEG-LS у середовищі.

Проблема стиснення зображень є актуальною у наш час, адже якість зображень та відео постійно зростає, а з ними і потреба в місці для їх зберігання в пам'яті та швидкості пересилання. На даний момент найбільш поширеним методом стиснення є JPEG. Це метод стиснення з втратами якості, що, натомість, не зменшує спектр його застосування та постійний процес модифікацій. Проте в сферах, де необхідна висока швидкість при великих об'ємах пересилання зображень та їх висока якість при мінімальних затратах пам'яті для збереження, необхідне застосування методу стиснення без втрат якості. Особливе значення це має для сфери медицини та космічних досліджень, де важливий не візуальний вигляд зображення, а інформація, що знаходиться в кожному пікселі для її подальшої обробки комп'ютерними засобами. Процесор для стиснення відеопотоку призначений для роботи на системі збору інформації мікросупутника. Він оброблятиме зображення формату pgm, що надходитимуть неперервним відеопотоком зі швидкістю 3 Гбіт/с. Зображення буде надходити неперервним відеопотоком з шириною рядків 18 тис. пікселів (16 біт/піксель). Для такого потоку даних необхідний простий, але ефективний метод стиснення, який можна буде реалізувати на обмежених ресурсах супутника.

Одним з таких методів є одна з розробок Групи експертів в області фотографії (Joint Photographic Experts Group) – метод JPEG-LS [1]. Він дозволяє зберігати оригінальну якість зображень та достатньо простий в реалізації. Його було розроблено на основі алгоритму LOCO-I [2, 3] в HP лабораторії ще в 1990 році та реалізовано в програмі JLSEncoder. Вихідні коди програми знаходяться в вільному доступі і використовуються в багатьох реалізаціях стиснення зображень. В методу Jpeg-ls також є багато апаратних реалізацій, зокрема – Lancero JPEG-LS Lossless Image Encoder IP Core фірми Microtronix [5] або ядро компанії Alma Technologies [4].

Для створення власної апаратної реалізації методу JPEG-LS на ПЛІС буде використовуватись САПР Vivado HLS, яка дозволяє використовувати існуючі програмні коди C/C++ та отримати з них коди мовами VHDL/Verilog/SystemC, які використовуються для створення топології ПЛІС.

Метою дослідження є проектування спеціалізованих апаратних засобів на базі ПЛІС для стиснення зображень без втрат методом JPEG-LS у середовищі Vivado. Для досягнення поставленої мети слід вирішити такі задачі:

- провести системний аналіз сучасного стану теорії, методів та засобів проектування цифрових засобів на ПЛІС;
- провести аналіз найбільш ефективних та відкритих алгоритмів стиснень зображень без втрат;
- провести дослідження роботи програмної реалізації методу JPEG-LS та визначити характеристики програми jpeg-ls v2.2. Визначити умови та параметри найбільш ефективного стиснення;
- розвинути метод проектування цифрових засобів на ПЛІС з використанням можливостей пакету Vivado з метою застосувати його при проектуванні;
- визначити основні архітектурні принципи побудови спеціалізованих апаратних засобів на базі ПЛІС, їхню структуровану модель та структурні алгоритми їх роботи;
- провести експериментальні дослідження розроблених моделей вузлів апаратного стиснення зображень без втрат.

При проектуванні апаратних засобів для стиснення зображень без втрат методом JPEG-LS на базі ПЛІС враховувалися висновки теорії обчислювальних машин, теорії обчислювальних систем, теорії комп'ютерних систем. Для реалізації елементів апаратних засобів для стиснення зображень без втрат методом JPEG-LS на ПЛІС використовувалися висновки теорії проектування НВІС, для визначення методів декомпозиції системи були задіяні теорія алгоритмів, теорія цифрових автоматів. Перевірка отриманих результатів здійснювалась відповідно до теорії випробувань шляхом моделювання.

У проведених дослідженнях широко використовується математичний апарат теорії алгоритмів, а також засоби моделювання цифрових схем.

Проведеними дослідженнями досягнуто поставлену мету та задачі, а саме проектування спеціалізованої системи збору наукової інформації для мікросупутника на базі ПЛІС для стиснення зображень без втрат методом JPEG-LS у середовищі Vivado. Джерелом інформації виступає бортовий сканер земної поверхні, що видає інформацію у вигляді неперервного відеопотоку швидкістю надходження - 3 Гбіт/с, формату – pgm (16 біт/піксель) та розміру зображень – 18 тис. пікселів на рядок. Для апаратної реалізації було вибрано ПЛІС фірми Xilinx – Spartan6. У ході дослідження було:

– проведено системний аналіз сучасного стану теорії, методів та засобів проектування цифрових засобів на ПЛІС;

– проведено аналіз найбільш ефективних та відкритих алгоритмів стиснень зображень без втрат;

– проведено дослідження роботи програмної реалізації методу JPEG-LS та визначено характеристики програми jpeg-ls v2.2. Визначено умови та параметри найбільш ефективного стиснення;

– розвинуто метод проектування цифрових засобів на ПЛІС з використанням можливостей пакету Vivado з метою застосувати його при проектуванні;

– визначено основні архітектурні принципи побудови спеціалізованих апаратних засобів на базі ПЛІС, їхню структуровану модель та структурні алгоритми їх роботи;

– проведено експериментальні дослідження та впровадження розроблених апаратних засобів в методи вирішення проблеми стиснення зображень без втрат.

– розроблено та перевірено ряд рекомендацій з перетворення існуючих С-кодів програм у вигляд, що придатний для сприйняття пакетом Vivado;

– розв'язано важливу науково-прикладну задачу – закладено основи технології створення спеціалізованих апаратних засобів на базі ПЛІС для стиснення зображень без втрат методом JPEG-LS у середовищі Vivado.

Література:

1. Алгоритмы сжатия и компрессии. Основи метода JPEG-LS [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – Режим доступу http://www.compression-pointers.ru/compress_82.html (дата звернення 18.05.2017) – Назва з екрана.

2. Глухов В.С., Мельник А.О. "Реалізація перетворення у реальному масштабі часу цифрових кодів кольору зображення у вигляді ядра ПЛІС ф. Xilinx" ("The real-time digital color converter core for Xilinx FPGA"). Матеріали конференції CADSM2001. Славське, 2001.

3. Дискретная математика: алгоритмы. JPEG, JPEG2000, JPEG-LS. Сжатие изображений с потерями и без [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – Режим доступу http://rain.ifmo.ru/cat/view.php/theory/data-compression/jpeg-2006 (дата звернення 17.03.2017) – Назва з екрана.

4. 7 Series FPGAs Data Sheet: Overview DS180 (v2.2) December 15, 2016.

5. ITU-T T-series recommendations terminals for telematic services «Information technology – Lossless and near-lossless compression of continuous-tone still images – Baseline» Posted 1999.08.11.

ТЕЛЕМЕТРІЯ ЧИ КІБЕРШПИГУНСТВО?

Смерека Б.А., Косиєв О.А.
Львівський державний університет безпеки життєдіяльності

В сучасному інформаційному просторі використання електронних пристроїв займає більшість нашого часу, інколи становлять суть нашої роботи та розваг. І, якщо раніше ми спостерігали у фантастичних фільмах, як людям вживляли чіпи для того, щоб спостерігати за ними, збирати інформацію та врешті керувати бажаннями та волею людей, то зараз зрозуміло, що все ж людство придумало куди більш гуманний спосіб, аніж хірургічний – ґаджети.

Мобільний телефон (смартфон), персональний комп'ютер, планшет, розумні годинники, телевізори і вже навіть будинки – всі ці речі мають систему збору, обробки, збереження та передачі інформації, і цю інформацію вводить не тільки сам користувач, але пристрої збирають її самостійно, аналізують, уособлюють та передають розробникам пристроїв чи програмного забезпечення. Слід одразу зрозуміти, для чого це відбувається.

Збір інформації про користувача, встановлені додатки, запити в мережі тощо власники ґаджетів, програмного та апаратного забезпечення здійснюють з метою покращення маркетингової діяльності. До прикладу, якщо ви намагались знайти якусь річ чи квитки, з часом ви помітите, що таргетована реклама почне вам пропонувати саме те, що ви шукали, або його аналоги. Також бували випадки, коли розумні годинники, збираючи інформацію про стан організму свого власника завдяки центру телеметрії та аналізу попереджав його про патологічні зміни в організмі, що могли призвести до проблем із здоров'ям, та навіть рятував життя. Проте, не завжди телеметрія є хорошим додатком до ваших персональних пристроїв. Особливо насторожує факт запиту дозволу до файлової системи, пошти, геолокації, мікрофону та списку дзвінків щойно встановленого калькулятора. Такі невиправдані запити на доступ – гіперболізований варіант прихованого відслідковування персональних даних. Даний факт незначний в інформаційній масі, тому про цей феномен зовсім рідко згадуються в засобах масової інформації і практично не згадується в літературі, що прекрасно приховує тотальний шпіонаж зі сторони деяких виробників та дрібних розробників. Так яку ж інформацію може ваш кишеньковий ґаджет передати про вас? Правильна відповідь: всю. Ваш телефон слідкує за вашим переміщенням, тим, що говорите, шукаєте, бачите, купляєте, за тим що вам подобається і що вам відразливо, з ким контактуєте та багато іншої інформації. Звісно, спочатку це звучить як черговий міф про змову, але попробуйте при увімкненому телефоні в розмові згадати щось незвичайне, що в розмові ви не згадували, але нібито хотіли б придбати, до прикладу – авто визначеної марки, та прослідкуйте за рекламою у Instagram чи Facebook, результат вас вразить.

Так чи інакше, електронні пристрої нас оточують постійно і завжди, то ж невже немає можливості захистити себе від витоку персональних даних та слідкуванням за своєю персоною? Якщо аскетизм – не вихід, то, на жаль, ні. Проте можна мінімізувати фактори витоку інформації з ґаджету шляхом:

1. обмеження доступу самих додатків в мережу інтернет, якщо його функціонал не залежить від мережі;

2. встановлення виключно перевірених додатків для спілкування та інтернет-серфінгу;

3. видалення стандартних програм, які ви не використовуєте;

4. регулярна чистка кешу та логів на пристрої;

Ці кроки є абсолютно прості для досвідченого користувача, проте навіть людина, що не надто розбирається в техніці просто стримуючи себе від встановлення великої кількості невідомих та непотрібних додатків, що запитують невиправдані потребами дозволи доступу до вашого телефону, вже частково себе забезпечує від того, щоб інформація з ґаджету не потрапила не в ті руки.

Проте не тільки кінцевий споживач персональної інформації може бути зацікавлений в ній, але й людина, яка зможе перехопити цю інформацію на стадії транспортування, що є куди небезпечнішим фактором ніж звичайний збір та обробка зі сторони розробників. Зловмисник, якому все ж вдалось перехопити та розшифрувати дані, отримує всю інкапсульовану в повідомленні інформацію. І все ж, якщо це вдалось один раз, то декілька повторних атак з перехопленням, систематизація отриманої інформації та комплексного аналізу дасть можливість створити цілісний образ про користувача.

Повертаючись до початку, слід підкреслити, що телеметрію слід чітко розмежовувати із кібершпіонажем. Достатньо знати, що збір необхідної інформації для маркетингу не вимагає її персоналізації чи присвоєння особистого ідентифікатора користувача.

Література:

1. Internet privacy and security course [Електронний ресурс] // [веб-сайт]- https://book.cyberyozh.com/(дата доступу 20.10.2019)

2. Кібершпигунство [Електронний ресурс] // [веб-сайт] - https://uk.wikipedia.org/wiki/ (дата доступу 21.10.2019)

3. Телеметрія [Електронний ресурс] // [веб-сайт] - https://uk.wikipedia.org/wiki/ (дата доступу 21.10.2019)

4. Нова функція у Facebook нагадуватиме користувачам піклуватися про здоров'я [Електронний ресурс] // [веб-сайт] – https://hromadske.ua/ (дата доступу 26.10.2019)

5. Цифрова лялька вуду від Google [Електронний ресурс] // [веб-сайт] - https://igate.com.ua/ (дата доступу 29.10.2019)

ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Требко А.О.
Національна академія Служби безпеки України, м. Київ

Інтенсивне впровадження новітніх інформаційних технологій, проникнення їх в усі сфери життєво важливих інтересів держави та суспільства зумовили появу низки суттєвих проблемних питань. Посилюється небезпека несанкціонованого втручання в роботу комп'ютерних, інформаційних і телекомунікаційних систем. Тому створення розвиненого і захищеного середовища є неодмінною умовою розвитку держави, в основі якого мають бути найновіші автоматизовані технічні засоби захисту.

Ключові слова: інформаційно-комунікаційні системи, інформаційна безпека, загрози безпеки інформаційним ресурсам, принципи захисту інформації, державна політика забезпечення інформаційної безпеки.

Розвиток сучасних інформаційних технологій, загальна комп'ютеризація та відчутне збільшення кількості інформаційно-комунікаційних систем (далі – ІКС) призвели до того, що інформаційна безпека стала не тільки обов'язковою їх складовою, а також являється однією з характеристик інформаційних систем.

Проблеми інформаційної безпеки України в сучасних умовах, принципи забезпечення захисту інформації є надзвичайно актуальними і вимагають поглибленого вивчення. Сьогодні точиться дискусія навколо цього питання, зокрема навколо оцінки критеріїв інформаційної безпеки, характеристик імовірних небезпек та їх структури, а також принципів побудови надійної системи захисту національних інтересів саме в інформаційній сфері від зовнішніх та внутрішніх загроз як для самої держави (суспільства), так і для конкретної людини.

Метою захисту інформації в ІКС є процес протидії негативному впливу на інформаціні ресурси, який здійснюється для порушення конфіденційності, цілісності та доступності шляхом знищення, викрадення, зниження ефективності функціонування або несанкціонованого доступу.

Побудова надійного та ефективного захисту інформаційної системи неможлива без знання можливих загроз безпеки [4] інформаційним ресурсам.

Під загрозою безпеки інформаційним ресурсам розуміють дії, які можуть призвести до спотворення, несанкціонованого використання або навіть до руйнування інформаційних ресурсів керованої системи, а також програмних і апаратних засобів [1-3].

Зважаючи на проведений аналіз наявних загроз інформаційним ресурсам, їх можна класифікувати за наступними критеріями:

1. інформаційній безпеці (загрози конфіденційності даних і програм; загрози цілісності даних, програм, апаратури; загрози доступності даних; загрози відмови від виконання операцій), впливають на безпеку інформаційних ресурсів і призводять до порушення основних властивостей інформації, яка зберігається і обробляється в інформаційній системі; по компонентам інформаційних систем, на які загрози націлені (інформаційні ресурси, персональні дані, програмні засоби, апаратні засоби, програмно-апаратні засоби);

2. за способами здійснення (*випадкові* – вихід з ладу апаратних чи програмних засобів, помилкові дії працівників або її користувачів, ненавмисні помилки в програмному та програмно-апаратному забезпеченні й т.п.; *навмисні* – мають на меті завдання збитків інформаційній системі або користувачам та можуть бути реалізовані шляхом довготривалої масованої атаки несанкціонованими запитами або вірусами, тощо, їх наслідки призведуть до руйнування (втрати) інформації, модифікації (зміни інформації на помилкову, яка коректна за формою і змістом, але має інший сенс), ознайомлення з нею сторонніх осіб, дії природного та техногенного характеру) [2,3];

3. за розташуванням джерела загроз (внутрішні та зовнішні).

З метою створення ефективної системи безпеки інформації, розроблення та вдосконалення існуючих методів її захисту, не можна не вказати на актуальні загрози безпеці, спрямовані проти інформаційних ресурсів у сучасних інформаційно-комунікаційних системах, а саме:

- протиправне збирання і використання інформації;
- порушення технології обробки інформації;
- впровадження в апаратні й програмні вироби компонентів, які реалізують функції, не передбачені документацією на такі вироби;
- розробка і поширення програм, які порушують нормальне функціонування інформаційних та інформаційно-телекомунікаційних систем, у тому числі систем захисту інформації;
- радіоелектронний вплив з метою виведення з ладу, пошкодження чи руйнування засобів і систем обробки інформації, телекомунікації зв'язку;
- вплив на парольно-ключові системи захисту автоматизованих систем обробки і передачі інформації;
- витік інформації технічними каналами;
- впровадження електронних пристроїв для перехоплення інформації в технічні засоби обробки, зберігання і передачі інформації з каналів зв'язку, а також у службові приміщення органів державної влади, підприємств, установ та організацій усіх форм власності;

- знищення, пошкодження, руйнування чи розкрадання машинних та інших носіїв інформації;
- перехоплення інформації в мережах передачі даних та лініях зв'язку, дешифрування цієї інформації і нав'язування хибної інформації;
- використання не сертифікованих віітчизняних і закордонних інформаційних технологій, засобів захисту інформації, засобів інформатизації, телекомунікації зв'язку при створенні і розвитку інформаційної інфраструктури України;
- несанкціонований доступ до інформації, яка знаходиться в банках і базах даних;
- порушення законних обмежень на поширення інформації.

При організації ефективного та надійного захисту необхідно керуватися системою принципів, яка дозволяє ефективно організувати роботу із захисту інформації. Під принципами захисту інформації розуміють основні ідеї й найважливіші рекомендації з питань організації та здійснення робіт для ефективного захисту інформаційних ресурсів ІКС.

Їх можна віднести до двох основних груп [4, 6]:

1) правові принципи (правове регулювання захисту інформації) базуються на положеннях основних конституційних норм, закріплюють інформаційні права і свободи, а також гарантують їх здійснення; ґрунтуються на особливостях і юридичних властивостях інформації як повноцінного об'єкту правовідносин.

До правових принципів захисту інформації відносяться: легітимність (законність); пріоритет міжнародного права над внутрішньодержавним; економічна доцільність [4].

2) організаційні принципи (роль організаційного захисту інформації в системі заходів безпеки визначається своєчасністю та правильністю прийнятих управлінських рішень, способів і методів захисту інформації на основі діючих нормативно-методичних документів).

Організаційні методи захисту передбачають проведення організаційно-технічних та організаційно-правових заходів, які включають в себе наступні принципи захисту інформації: науковий підхід до організації захисту інформаації; планування захисту; керування системою захисту; безперервність процесу захисту інформації; мінімальна достатність організації захисту; системний підхід до організації та проектування систем та методів захисту інформації; комплексний підхід до організації захисту інформації; відповідність рівня захисту цінності інформації; гнучкість захисту; багатозональність захисту, що передбачає розміщення джерел інформації в зонах з контрольованим рівнем її безпеки; багаторубіжність захисту інформації; обмеження числа осіб, які допускаються до захищеної інформації; особиста відповідальність персоналу за збереження довіреної інформації [4, 6].

Державна політика забезпечення інформаційної безпеки визначає головні напрями діяльності органів державної влади України, закріплює права та обов'язки щодо захисту інтересів країни, які ґрунтуються на дотриманні Конституції, законодавчих актів України, загальновизнаних принципів і норм міжнародного права при здійсненні діяльності із забезпечення інформаційної безпеки України; відкритості у реалізації функцій органів державної влади України і суспільних об'єднань; досягненні балансу інтересів громадян, суспільства й держави в інформаційній сфері.

Література:

1. Левин В.К., Гайкович В.Ю., Дорошкевич П.В. и др. Информационная безопасность компьютерных сетей.// Технологии электронных коммуникаций. – М. 1993. т.5. –128 с.

2. Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах: Учеб. пособие. – М.: Горячая линия – Телеком, 2005. –147 с.

3. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних: Підручник. – К.: Вид-во ТОВ «НВП» ІНТЕРСЕРВІС», 2009. – 716 с.

4. www.rusnauka.com/16 ADEN 2010/Informatica/68642.doc.htm

5. https://www.skrippy.com/61398__119284_Принципи організації захисту інформації

6. https://sites.google.com/site/infobezosob/osnovni-principi-zabezpecenna-zahistu-informaciie

Напрям 2

Захист інформації в комп'ютерних мережах

PROTECTION OF INFORMATION IN NETWORKS

Yuliya Hrynyk, Bozhena Vysochanska, Roman Golovatyi
Lviv State University of Life Safety

Останнім часом все більш актуальною стає проблема захисту інформації. Чим більше комп'ютеризуються різні сфери нашого життя, тим більше стає областей можливого проникнення зловмисників, конкурентів і просто комп'ютерних хуліганів. Для протидії зовнішнім атакам необхідно не тільки мати засоби захисту інформації, а й розуміти принципи їх функціонування, вміти правильно їх налаштувати, розуміти слабкі місця операційних систем.
Ключові слова: захист інформації, комп'ютерні мережі.

Recently, the problem of information security has become increasingly relevant. The more computerized different areas of our lives, the more areas of possible intrusion of intruders, competitors, and just computer bullies. To counteract external attacks, it is necessary not only to have information security tools, but also to understand the principles of their functioning, to be able to configure them correctly, to understand the weaknesses of operating systems.
Keywords: protection of information in networks

As general observations computers become better understood and more economical, every day brings new applications. Many of these new applications involve both storing information and simultaneous use by several individuals. The key concern in this paper is multiple use [1, 2].

For those applications in which all users should not have identical authority, some scheme is needed to ensure that the computer system implements the desired authority structure.

There are a variety of specialized techniques and types of network security you will want to roll out. Cisco, a networking infrastructure company, uses the following schema to break down the different types of network security, and while some of it is informed by their product categories, it's a useful way to think about the different ways to secure a network. Here they are [3]:

– Access control: You should be able to block unauthorized users and devices from accessing your network. Users that are permitted network access should only be able to work with the limited set of resources for which they've been authorized.

– Anti-malware: Viruses, worms, and trojans by definition attempt to spread across a network, and can lurk dormant on infected machines for days or weeks. Your security effort should do its best to prevent initial infection and also root out malware that does make its way onto your network.

– Application security: Insecure applications are often the vectors by which attackers get access to your network. You need to employ hardware, software, and security processes to lock those apps down.

– Behavioral analytics: You should know what normal network behavior looks like so that you can spot anomalies or breaches as they happen.

– Data loss prevention: Human beings are inevitably the weakest security link. You need to implement technologies and processes to ensure that staffers don't deliberately or inadvertently send sensitive data outside the network.

– Firewalls: Perhaps the granddaddy of the network security world, they follow the rules you define to permit or deny traffic at the border between your network and the internet, establishing a barrier between your trusted zone and the wild west outside. They don't preclude the need for a defense-in-depth strategy, but they're still a must-have.

– VPN: A tool (typically based on IPsec or SSL) that authenticates the communication between a device and a secure network, creating a secure, encrypted "tunnel" across the open internet.

– Web security: You need to be able to control internal staff's web use in order to block web-based threats from using browsers as a vector to infect your network. And others network security methods.

In reviewing the extent to which protection mechanisms are systematically understood (which is not a large extent) and the current state of the art [4, 5]. As in the case of all programming systems, it will be necessary for protection systems to be used and analyzed and for their users to propose different, better views of the necessary and sufficient semantics to support information protection.

Finally, one may wish to extend dynamically the range of objects protected [6]. Such a goal might be reached by making the type field large enough to contain an additional unique identifier, and allowing for software interpretation of the access to typed objects. This observation brings us to the subject of user-programmed controls on sharing and the implementation of protected objects and protected subsystems. We shall not attempt to examine this topic in depth, but rather only enough to learn what problems are encountered.

Reference:

1. Fruhlinger J. What is network security? Definition, methods, jobs & salaries [Електронний ресурс] / Josh Fruhlinger // CSOonline. – 2018. – Режим доступу до ресурсу: https://www.csoonline.com/article/3285651/what-is-network-security-definition-methods-jobs-and-salaries.html.

2. Зачко О. Б. Імітаційне моделювання потоку відвідувачів торговорозважального центру / О. Б. Зачко, Р. Р. Головатий // Управління проектами: стан та перспективи: матер. XII міжнар. наук.-прак. конф. – Миколаїв: МНУК, 2016 – С. 96 – 98.

3. Jerome S. the protection of information in computer systems [Електронний ресурс] / Saltzer Jerome. – 1975. – Режим доступу до ресурсу: http://web.cs.wpi.edu/~guttman/cs557_website/papers/saltzer1975.pdf.

4. Зачко О. Б. Управління безпекою на стадії планування проектів з масовим перебуванням людей з врахуванням категорії складності / О. Б. Зачко, Д. С. Кобилкін, Р. Р. Головатий // Вісник НТУ «ХПІ». Серія: Стратегічне управління, управління портфелями, програмами та проектами. – Х. : НТУ «ХПІ», 2018. – № 2 (1278). – С. 53–58. – Бібліогр.: 17 назв. – ISSN 2311–4738.

5. Купчак М. І., Смотр О. О., Купчак М. Я. Тенденції та проблеми впровадження інформаційних технологій в управління підрозділами університету. Вісник Львівського державного університету безпеки життєдіяльності. 2013. № 7. С. 28–32.

6. Рак Ю. П. Формування проектів методом візуалізації інформації для підвищення стану безпеки торгово-розважальних центрів / 123 Ю. П. Рак, Р. Р. Головатий // Управління проектами у розвитку суспільства: зб. тез доповідей XII Міжнар. конф. – Київ: КНУБА, 2015. – С. 226 – 228

СКАНЕРИ ВРАЗЛИВОСТІ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Балацька В.С., Шабатура М.М.
Львівський державний університет безпеки життєдіяльності

Summary. The increasing volume of attacks on the Internet has increased the demand for sophisticated tools for vulnerability analysis, intrusion detection, forensic investigations, and possible responses. Current hacker tools and technologies warrant reengineering to address cyber crime and homeland security. The creation of network scanners is necessary to secure the information infrastructure by gathering network topology, intelligence, internal/external vulnerability analysis, and penetration testing.

Keywords: vulnerability scanner, security, cyber crime, "back door", network scanners.

Сканери вразливості – це комплексні рішення, які можуть являти собою як апаратні, так і програмні засоби, призначені для постійного сканування стану комп'ютерної мережі, на предмет дії вірусів або підозрілих процесів. Їх основним завданням є оцінка безпеки процесів і пошук вразливостей та їх усунення.

Vulnerability scanner або сканер вразливості, дає адміністратору можливість пошуку існуючих в мережі «дірок» або «бекдор», за допомогою яких, хакери і шахраї можуть отримати доступ до мережі компанії і конфіденційних даних. Крім цього, до складу сканерів входять засоби для сканування запущених служб і процесорів, а також сканери портів.

Виходячи з цього, можна виділити такі функції сканерів вразливостей:

- пошук вразливостей і їх аналіз;
- перевірка всіх ресурсів у мережі, пристроїв, операційної системи, портів, додатків, процесів і т.п.;
- створення звітів, у яких вказується вразливість, шлях її поширення і характер.

В основі сканера лежать два механізми [1]. Перший механізм називається – зондування. Даний механізм є не дуже швидкий, але найбільш ефективний інструмент активного аналізу. Суть його полягає у тому, що він сам запускає атаки, і стежить за тим, де ці атаки можуть пройти. Під час зондування, підтверджуються можливі припущення і можливості проходження атак на певних напрямках.

Інший механізм – сканування. У цьому випадку інструмент працює швидко, але виробляється тільки поверхневий аналіз мережі, по найчастішим і можливим «діркам» в безпеці мережі. Відмінність другого способу в тому, що він не підтверджує наявність уразливості, а тільки повідомляє адміністратора про її можливості, ґрунтуючись на непрямих ознаках. Наприклад, відбувається сканування портів, визначаються їх заголовки і потім вони порівнюються з еталонними таблицями і правилами. У разі розбіжності значень, сканер повідомляє про знаходження потенційної уразливості, які адміністратор повинен перевірити більш надійними способами.

Основні принципи роботи сканерів вразливостей:

- збір всієї інформації в мережі, ідентифікація всіх служб, пристроїв і процесів;
- пошук потенційних вразливостей;
- використання спеціалізованих методів і моделювання атак, для підтвердження уразливості (існує не у всіх мережевих сканерах).

На сьогоднішній день найбільш поширеними є такі сканери: Xspider, Nessus, Shadow Security Scanner.

Xspider. Як заявляється розробник, їх рішення здатне виявити третину всіх можливих вразливостей, так званих «zero day». Основною перевагою даного сканера, є можливість виявлення максимального числа «дірок» в системі безпеки, до того, як їх зможуть виявити хакери. Даний сканер не вимагає додаткового програмного забезпечення. Після проведення аналізу, він формує повний звіт зі знайденими уразливими і можливими способами їх усунення. XSpider [2] створювався в першу чергу експертами з інформаційної безпеки, яким був необхідний професійний інструмент найвищої якості. Відрізняється безкомпромісною якістю роботи, без якого користь від застосування сканера безпеки стає сумнівною, незалежно від наявності інших плюсів. Характеризується розумною ціною і легкістю володіння, оскільки інформаційна безпека покликана запобігати втратам, а не збільшувати їх. Однаково зручний у використанні для компанії будь-якого масштабу (від одиниць до десятків тисяч обслуговуючих вузлів з'єднання). Універсальність XSpider є те, що він хоч і працює під управлінням Microsoft Windows, також він перевіряє всі можливі вразливості незалежно від програмної і апаратної платформи вузлів: починаючи від робочих станцій під Windows і закінчуючи мережевими пристроями Cisco (не виключаючи, звичайно, *nix, Solaris, Novell, AS400 і т.п.).

Nessus. Даний сканер почав свою роботу, ще з 1998 року, компанія Tenable Network Security, почала займатися розробкою свого сканера враз-

ливостей, завдяки чому має великий досвід і далеко попереду в своїй сфері. Багато років їх сканер є комерційним ПЗ. Ключовою особливістю сканера Nessus [3], є можливість розширювати функціонал за допомогою різноманітних плагінів. Таким чином, потужні тести, а саме тести на проникнення або інші, не встановлюються разом з головним модулем, а при необхідності підключаються окремо. Всі плагіни можна розділити на 42 категорії. Це означає, що, наприклад, для проведення пінтеста (тесту на проникнення), не обов'язково запускати повну перевірку, а можна виділити тільки тести з певної категорії або вибрати режим тестування вручну. Крім цього, Nessus має свою спеціальну скриптову мова, так що, адміністратори можуть самі писати необхідні їм тести.

Shadow Security Scanner. Сканер мережевої безпеки який завдяки унікальним методам дозволить надійно перевірити сайт або мережу на наявність дір і дозволить надійно захистити мережу від проникнення хакерів. При скануванні системи, програма робить аналіз даних, виявляє уразливі місця, можливі помилки у налаштуванні сервера і запропонує можливі шляхи виправлення недоліків та вразливих місць у системі, підкаже, звідки можна завантажити патч або оновлене програмне забезпечення. Вміє автоматично (Fix-It) виправляти знайдені помилки у безпеці одним натисканням на кнопку в меню Fix-It.

Shadow Security Scanner [4] сканує не тільки машини на яких стоять операційні системи Windows, але так само різні операційні системи Unix (Linux, * BSD, Solaris, etc) роутери, файрволи та системні пристрої. У нього входить аудит таких модулів як TCP / IP, UDP, FTP, DNS, SMTP, POP3, HTTP, CGI, NetBIOS, Registry, Users accounts, Password checks, Services, LDAP, DoS атаки, і багато іншого.

Висновок: використовувати такого роду засоби треба. Але хочу зауважити, що не варто вважати їх панацеєю від усіх бід. Вони ні в якому разі не замінюють фахівців в області безпеки. Вони всього лише автоматизують їх роботу, допомагаючи швидко перевірити сотні вузлів, в т.ч. і знаходяться на інших територіях. Вони допоможуть виявити практично всі відомі уразливості і порекомендувати заходи, їх усувають, автоматизують цей процес, а з урахуванням можливості опису своїх власних перевірок, допоможуть ефективно застосовувати їх в мережі будь-якої організації, з огляду на саме специфіку роботи.

Література:

1. Як працює сканер безпеки [Електронний ресурс] – Режим доступу: http://citforum.ru/internet/securities/scaner.shtml, вільний;

2. Сканер уязвимостей XSpider 7 [Електронний ресурс] – Режим доступу: http://www.ixbt.com/soft/xspider7.shtml#int, вільний;

3. NESSUS vulnerability assessment [Електронний ресурс] – Режим доступу: https://www.tenable.com/products/nessus, вільний;

4. Shadow Security Scanner [Електронний ресурс] – Режим доступу: http://www.safety-lab.com/en/products/securityscanner.htm, вільний.

КЛАСИФІКАЦІЯ МЕРЕЖЕВИХ АТАК ТА МЕТОДИ ПРОТИДІЇ І ЗАХИСТУ

Назар Болехівський, Орест Полотай
Львівський державний університет безпеки життєдіяльності

Приведено класифікацію основних мережевих атак. Кожну мережеву атаку розглянуто з точки зору її реалізації та захисту від неї.
Ключові слова: комп'ютерна мережа, мережева атака, захист мережі.

The classification of major network attacks is given. Each network attack is considered in terms of its implementation and protection against it.
Keywords: the computer network, network attack, network protection.

В реаліях розвитку інформаційного суспільства все більше розвиваються IT технології. Комп'ютерні мережі виступають одним з напрямів розвитку суспільства, в якому основним ресурсом виступає інформація. Однак, паралельно з розвитком технологій передачі даних, розвиваються і технології викрадення даних, в тому числі і з комп'ютерної мережі.

Сьогодні існують такі типи мережевих атак:

1. Сніффер пакетів – прикладна програма, яка використовує мережеву карту, що працює в невпорядкованому режимі (в цьому режимі всі пакети, отримані по фізичних каналах, мережевий адаптер відправляє додатком для обробки). При цьому перехоплюють всі IP-пакети, які передаються через певний сегмент.

Пом'якшити загрозу сніффінга пакетів можна за допомогою таких засобів:

Аутентифікація. Сильні засоби аутентифікації є першим способом захисту від сніффінга пакетів. Прикладом є одноразові паролі (OTP - One-Time Passwords). OTP - це технологія двофакторної аутентифікації, при якій відбувається поєднання того, що у вас є, з тим, що ви знаєте. Типовим прикладом двофакторної аутентифікації є робота звичайного банкомату, який пізнає вас, по-перше, по вашій пластиковій картці і, по-друге, по вашому ПІН-коду. Для аутентифікації в системі OTP також потрібно ПІН-код і ваша особиста картка [1].

Комутована інфраструктура. Ще одним способом боротьби зі сніффінгом пакетів у вашому мережевому середовищі є створення комутованої інфраструктури. Якщо, наприклад, у всій організації використовується комутований Ethernet, хакери можуть отримати доступ тільки до трафіку, що надходить на той порт, до якого вони підключені (результат микросегментации виробленої комутатором) [1].

Анти-сніфери. Третій спосіб боротьби зі сніффінгом полягає в установці апаратних або програмних засобів, які розпізнають сніфери, що пра-

цюють у вашій мережі. Ці засоби не можуть повністю ліквідувати загрозу, але, як і багато інших засобів мережевої безпеки, вони включаються в загальну систему захисту.

Криптографія – найефективніший спосіб боротьби зі сніффінгом пакетів. Вона робить роботу сніфферів марною.

2. IP-спуфінг відбувається, коли хакер, що знаходиться всередині корпорації або поза нею, видає себе за санкціонованого користувача. Це можна зробити двома способами. По-перше, хакер може скористатися IP-адресою, що знаходиться в межах діапазону санкціонованих IP-адрес, або вповноваженою зовнішньою адресою, якому дозволяється доступ до певних мережевих ресурсів.

Загрозу спуфінга можна послабити (але не усунути) за допомогою таких заходів:

Контроль доступу – найпростіший спосіб запобігання IP-спуфінга. Він полягає в правильному підборі управління доступом. Щоб знизити ефективність IP-спуфінга, необхідно відсікти будь-який трафік, що надходить із зовнішньої мережі.

Фільтрація RFC 2827. Можна припинити спроби спуфінга чужих мереж користувачами нашої мережі (і стати добропорядним «мережевим громадянином»). Для цього необхідно блокувати будь-який вихідний трафік, адреса джерела якого не є однією з IP-адрес нашої організації.

Аутентифікація. IP-спуфинг може функціонувати тільки за умови, якщо аутентифікація відбувається на базі IP-адрес. Тому впровадження додаткових методів аутентифікації робить цей вид атак марним.

3. Парольні атаки. Хакери можуть проводити парольні атаки за допомогою цілого ряду методів, таких як простий перебір (brute force attack), «троянський кінь», IP-спуфінг і сніффінг пакетів.

Парольних атак можна уникнути, якщо не користуватися паролями в текстовій формі. Одноразові паролі і / або криптографічна аутентифікація можуть практично звести нанівець загрозу таких атак.

З точки зору адміністратора, існує кілька методів боротьби з підбором паролів. Один з них полягає у використанні засоби L0phtCrack, яке часто застосовують хакери для підбору паролів в середовищі Windows NT. Це засіб швидко покаже вам, чи легко підібрати пароль, вибраний користувачем [2].

4. Атаки на рівні додатків можуть проводитися кількома способами. Найпоширеніший з них полягає у використанні добре відомих слабкостей серверного програмного забезпечення (sendmail, HTTP, FTP). Використовуючи їх, хакери можуть отримати доступ до комп'ютера від імені користувача, що працює з додатком. Відомості про атаки на рівні додатків широко публікуються, щоб дати можливість адміністраторам виправити проблему за допомогою корекційних модулів (патчів). На жаль, багато хакерів також мають доступ до цих відомостей, що дозволяє їм вчитися [3].

5. Мережевою розвідкою називається збір інформації про мережу за допомогою загальнодоступних даних і додатків. При підготовці атаки проти будь-якої мережі хакер, як правило, намагається отримати про неї якомога більше інформації. Мережева розвідка проводиться у формі запитів DNS, ехо-тестування (ping sweep) і сканування портів. Запити DNS допомагають зрозуміти, хто володіє тим чи іншим доменом і які адреси цього домену привласнені. Ехо-тестування (ping sweep) адрес, розкритих за допомогою DNS, дозволяє побачити, які хости реально працюють в даному середовищі. Отримавши список хостів, хакер використовує засоби сканування портів, щоб скласти повний список послуг, що надаються цими хостами. І, нарешті, хакер аналізує характеристики додатків, що працюють на хостах. В результаті видобувається інформація, яку можна використовувати для злому.

Повністю позбавитися від мережевої розвідки неможливо.

6. Соціальна інженерія. Часто, проектуючи мережеву безпеку, забувають захиститися від одного з найпростіших і в той же час дієвих способів злому – соціальної інженерії. Вона заснована на роботі зі службовцями компанії, їх підкуп або введення в оману. Наприклад, хакер може зателефонувати службовцю і, видавши себе за мережевого адміністратора, попросити назвати свій пароль для виконання будь-яких дій.

Протидія таким методам може здійснюватися лише через навчання і підготовку персоналу, закріплення в політиці безпеки правил поведінки.

Це далеко не повний вид мережевих атак, що розвинулись за останні декілька років. Аналітику безпеки чи системному адміністратору необхідно володіти всіма способами захисту від приведених вище атак ат вміти їх ефективно застосовувати на практиці.

Література:

1. Веб-сайт beasthackerz. [Електронний ресурс]. Режим доступу з beasthackerz.ru/uk/kompyuter/vidy-atak-identifikac...irovanie-portov.html

2. Грайворонський М. В. Безпека інформаційно-комунікаційних систем: підруч. для студ. вищ. навч. закл., які навчаються за напрямами "Безпека інформаційних і комунікаційних систем", "Системи технічного захисту інформації", "Управління інформаційною безпекою" / М. В. Грайворонський, О. М. Новіков. – К. : Вид-во BHV, 2009. – 608 с.

3. Петров В.А. Інформаційна безпека. Захист інформації від несанкціонованого доступу в автоматизованих системах / Петров В.А., Піскарьов С.А., Шеїн А.В. – М. : Изд-во Ореан, 1998. – 534 с.

УДК 654:316.774.323.28

ЗАХИСТ ІНФОРМАЦІЇ ПРИ КОРИСТУВАННІ СОЦІАЛЬНИМИ МЕРЕЖАМИ

Бужанська М., Подолець Р., Палійчук Р.
Львівський торговельно-економічний університет,

Анотація: У статті досліджуються особливості спілкування у соціальних мережах. Проведено аналіз переваг і недоліків різних методів захисту інформації. Проаналізовано метод визначення стратегії розповсюдження інформації в соціальній мережі. Авторами висвітлено актуальні питання обробки та захисту персональних даних в соціальних мережах, здійснено аналіз проблемних аспектів забезпечення приватності в соціальних мережах. Розглянуто, яким чином можна захистити свою інформацію та убезпечити себе від її витоку, користуючись соціальними мережами.

Ключові слова: Інформація, інформаційна безпека, соціальні мережі.

Summary: In this article explore specific communication in the social networks. The advantages and disadvantages of different methods of information protection are analyzed. The authors covered topical issues of processing and protection of personal data in social networks, analyzed the problematic aspects of provaiding privacy in social network. Consider how you can protect your information and protect yourself from its stealing, using social networks.

Keywords: Information, information security, social networks.

Об’єктивною реальністю сьогодення є широке впровадження в усі сфери життєдіяльності особи, суспільства та держави сучасних інформаційних технологій, розгортання на їх основі локальних і глобальних інформаційних систем та мереж, призначених для прискорення обміну інформацією та доступу до різноманітних інформаційних ресурсів. Людина отримала можливість обмінюватися інформацією в межах всієї планети, не залежно від кордонів і відстаней. [1]. Особиста інформація ще ніколи не була такою доступною, як сьогодні. Ситуація загострюється ще й через те, що більшість користувачів не знає елементарних правил безпеки онлайнового спілкування і використання. Саме тому пропонуємо вам ознайомитися з варіантами найпоширеніших небезпек та способів захисту від неправильного користування соціальними мережами. На етапі реєстрації в певній соціальній мережі користувачеві, власники змушують надати їм добровільно і найчастіше досить широку інформацію про користувачів. Іноді така інформація може суперечити основним положенням закону України «Про захист персональних даних» [2]. Розглянемо, яким чином захистити свою інформацію та убезпечити себе від її витоку, користуючись соціальними мережами.

Геолокація. За цими даними зловмисники точно можуть дізнатись де ви перебуваєте, коли відсутні у дома. Якщо ви практикуєте такі публікації досить часто, то з легкістю можна буде скласти ваш розпорядок дня, аби скористатись цим і можливо пограбувати вас. Радимо не прикріплювати постійно помітки про місце перебування, та відключити режим GPS.

Метадані. Ваші дані записуються в вигляді EXIF файлу - даних про медіа файл. Який включає в собі : ім'я та тип пристрою, дату і час зйомки, географічні координати, інформацію про автора та інше. В деяких випадках ця інформація може допомогти знайти загублений цифровий пристрій, якщо з нього фотографуватимуть і публікуватимуть медіа, а у інших "взламати" ваш електронний пристрій чи аккаунти у соц-мережах.

Публікація фотографій кредитних карток і важливих документів . Фото нещодавно отриманого водійського посвідчення, чи інших документів, аби похизуватись перед друзями, яке ви опублікували, можуть використати злочинці. Щоб отримати доступ до вашого банківського або електронного рахунку. Фото таких речей категорично не слід публікувати, краще поділитись досягненням в письмовому варіанті публікацій.

Створення надійного паролю. Багато людей досі використовують при створенні паролю, зв'язку імена близьких, чи кличку домашнього улюбленця та дату народження. Для створення надійного паролю необхідно обов'язково використовувати : великі букви , маленькі букви та цифри. Довжина паролів повинна бути не менш як 8 символів. Можна додатково вмикати функцію двоетапної перевірки, це функція котра вимагає ввести не тільки логін та пароль, а й код котрий надходить по sms[3].

Оновлення програмного забезпечення. Бувають випадки коли протидіяти певним ситуаціям антивіруси не можуть. Наприклад, перейшовши за посиланням в одній із соціальних мереж, з'явились певні види реклами, які закрити неможливо. Допомогти може оновлення вебпереглядача, або спеціального додатку для певної соціальної мережі, оскільки розробники цих застосунків у першу чергу дбають аби користувачі були задоволені при користуванні їхніми ресурсами.

Вибір антивіруса. Окрім функцій, які надають антивіруси споживачам, відомі випадки злочинів, таких як керування приватними даними на комп'ютерах користувачів. Встановлюючи антивірусне програмне забезпечення, користувачі самі надають програмі для її функціонування дозволи на керування даними аби боротись з вічно прогресуючими комп'ютерними вірусами. Тому слід обирати якісний продукт, а не безкоштовні піратські копії. Одним із найкращих варіантів є, користування стандартним антивірусним застосунком який йде в комплекті із операційною системою.

Спілкування в інтернеті. Розповсюдженим типом шахрайства є фішинг. Основна його мета - заволодіти персональними даними і отримати доступ до рахунку в банку чи інтернет-гаманця користувача. Таким спосо-

бом є : листи для підтвердження входу чи реєстрації та введення логіну з паролем, створення сайтів, які візуально подібні до оригіналу і коли користувач спробує увійти його пароль та логін викрадуть. Також дружнє знайомство і подальше надсилання вам зараженого вірусом файлу (наприклад документ Word), котрий надасть повний доступ до керування вашим комп'ютером і зловмисник зможе не тільки отримати ваші кошти, а й шантажувати вас. Наразі у всіх сучасних браузерах існує система антифішингу, яка повідомляє користувачеві, що цей сайт може належати зловмисникам[4].

Мобільні додатки для соціальних мереж. На відміну від браузерних версій соціальних мереж, додатки для мобільних пристроїв при встановленні, як і антивіруси, теж запитують доступ до ваших приватних даних, посилаючись на правила конфіденційності. Іноді вимагають доступ до файлів абсолютно не потрібних для роботи, визначеної задачі додатку. Досвідчені користувачі знають, як у сучасних операційних системах відключити різні дозволи доступу до даних для додатків на смартфоні.

Отож, для безпечного користування соціальними мережами необхідно, по-перше, думати яку інформацію про себе та своїх близьких людей, розміщати, не вказувати свої персональні дані, по-друге, використовувати антивірусне програмне забезпечення, по-третє, не заповняти всі поля, які пропонує соціальна мережа(адреси навчання, роботи, проживання і т.д.). Однак, ряд проблем можна вирішити тільки в результаті створення національної системи технічного захисту інформації. Розвиток і становлення такої системи можна реалізувати об'єднавши зусиля різних державних установ, підприємств, а також зусиль провідних вчених та інженерів.

Література:

1. Концепція розвитку Інтернет в Україні / Державний комітет зв'язку та інформатизації України. [Електрон. ресурс]. – Спосіб доступу: URL: http://www.stc.gov.ua/_info/concep_rozv.html.

2. Україна. Закон «Про захист персональних даних» / №2297 від 01.06.2010 р. [Електрон. ресурс]. – Спосіб доступу: URL: http://search.ligazakon.ua/l_doc2.nsf/link1/ed_2010_06_01/T102297.html

3. Деркаченко А. Я. Соціальні мережі, як середовище для технологій маніпулятивного впливу [Електронний ресурс] / А. Я. Деркаченко. – 2016. – Режим доступу до ресурсу: http://journals.dut.edu.ua/index.php/dataprotect/article/view/531/493.

4. Карманний Є. В. Підходи до захисту інформації при користуванні соціальними мережами [Електронний ресурс] / Є. В. Карманний, С. О. Ковжога. – 2015. – Режим доступу до ресурсу: http://dspace.nlu.edu.ua/bitstream/ 123456789/8420/1/Karmannuy_Kovgoa.pdf.

БЕЗПЕКА КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ДАНИХ: РЕАЛІЇ СЬОГОДЕННЯ

Градищук С.
ВПНУБПУ «Ірпінський економічний коледж»

Анотація. Важливість інформаційної безпеки в сьогоденні є важливою складовою досконалого захисту даних користувачів в комп'ютерних мережах чи мережах електрозв'язку. Загалом захист інформації та даних залежить від програмного забезпечення та територіального розміщення.
Ключові слова: Інформаційна безпека, дані, комп'ютерні мережі, ступінь захисту, інформація.

Abstract. The importance of information security today is an important component of the perfect protection of user data on computer or telecommunication networks. In general, the protection of information and data depends on the software and territorial location.
Keywords: Information security, data, computer networks, security level, information.

Комп'ютеризація стала невід'ємною частиною нашого буття, що призводить до дій злочинців в результаті яких відбувається: викрадення комп'ютерних даних, їх перекручення, блокування, маніпуляції, порушенні її маршрутизації чи знищення такої. Зазначені злочинні дії осіб в кінцевому результаті спричиняють небажаних, а також шкідливих наслідків (збитків): витоків ЕОМ (комп'ютерної) інформації; приведення її у непридатний стан; послаблення, виснаження та завдання матеріальної шкоди її законним власникам.

Існуючі системи захисту збереження комп'ютерної інформації, технологічно в цілому не можуть охопити весь спектр контролю за доступом до операційних програмних систем, комп'ютерних мереж чи мереж електрозв'язку. Як свідчить зарубіжна практика, провідні державні та приватні установи щорічно витрачають від 20 до 40 % чистого прибутку на придбання оновлених систем захисту програмних продуктів від їх викрадення [4, с.23-25]. Хоч загально відомо, що не існує єдиного досконалого програмного забезпечення, яке на 100% змогло б гарантувати безпечність витоків комп'ютерної інформації.

Перш за все потрібно сказати, що безпека інформаційних даних, які обробляються у ЕОМ (комп'ютерних) системах, та комп'ютерних мережах і мережах електрозв'язку розглядається через дві складові: висока ступінь захисту програмних продуктів та низька.

1. Висока – включає в себе ширше поняття, бо охоплює не лише безпеку програмного забезпечення, а й місце територіального розташування будівель, приміщень, кімнат, в яких знаходяться комп'ютерні устаткування. Зокрема здійснює такі заходи:

- постійну охорону території і споруд за допомогою технічних засобів безпеки та відповідного персоналу;
- спеціальне облаштування, екранування приміщень;
- введення адміністратора служби захисту інформації;
- систему доступу, допуску та контролю роботи за операційною системою [3, с. 10 - 12].

Як свідчить зарубіжна практика введення в штатний розпис адміністратора по захисту інформаційних даних у кілька разів знижує ймовірність скоєння комп'ютерних злочинів. Така особа або окремий відділ – це є спеціально підготовлені кадри, професіонали вищого гатунку, які пройшли стажування у відповідних установах, центрах.

2. Низький ступінь захисту – це більш вузько направлений напрямок безпеки витоків комп'ютерної інформації. Він визначається наявністю простого алгоритму обмеження доступу до програмного забезпечення, системи та комп'ютерної мережі чи мережі електрозв'язку. Тобто, застосуванні аутентифікації (перевірка оригіналу) через паролі та коди, ідентифікації (встановлення тотожності особи), системи реєстрації та сертифікації, допуску та протоколювання, проведення аудиту та інше [2, с. 64 - 68]. Наявність істинного добросовісного користувача конфіденційної інформації підтверджується знанням зазначеного у системі допуску пароля, криптографічного ключа, особистого ідентифікаційного номера. Можливого використання особистої магнітної карточки або іншого технічного облаштування аналогічного типу. Ідентифікування за біометричними параметрами людини (за голосом, сітчаткою очей, відпечатками папілярних візерунків пальців рук та ін.).

Спосіб криптографії вважається найбільш потужним засобом конфіденційності комп'ютерної інформації, як у самому комп'ютері, так і при передачі на інші магнітні носії [1, с.45- 47].

Підсумовуючи викладене, доходимо висновку, що захист інформації у сфері з використанням ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку перебуває у своєму потенційному розвитку і знаходить своє практичне застосування там, де використовуються комп'ютерні технології.

Література

1. Авторский коллектив под редакцией проф. Н.С.Полевого. Правовая информатика и кибернетика. Учебник для высших уч.заведений. М. "Юридическая литература", 1993. – 264 с.

2. Азаров Д. Особливості механізму вчинення злочинів у сфері комп'ютерної інформації // Юридична Україна. – 2004. – № 7 (19). – С. 64 – 68

3. Колесник В.А. Розслідування комп'ютерних злочинів. Наук.-метод. посіб. – К.: Вид-во НА СБУ, 2003. – 124 с.

4. Романец Ю.В., Тимофеев А.А., Шаньгин В.Ф.. Защита информации в компьютерных системах и сетях. М., 1999. . – 117 с.

ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Димкар В.М., Фірман І.В.
Львівський національний університет імені Івана Франка
Департамент політики Міністра МВС України

Судячи по зростаючій кількості публікацій і компаній, які професійно займаються захистом інформації в комп'ютерних системах, вирішенню цієї задачі надається велике значення. Однією із найбільш очевидних причин порушення системи захисту є навмисний несанкціонований доступ (НСД) до конфіденційної інформації з боку нелегальних користувачів і наступні небажані маніпуляції із цією інформацією.

Захист інформації — це діяльність щодо запобігання витоку, розкрадання, втрати, модифікації (підробки), несанкціонованих і ненавмисних) впливів на захищену інформацію. З суто технічних і ненавмисних причин, під це визначення підпадає також діяльність, пов'язана з підвищенням надійності сервера через відмови або збоїв у роботі вінчестерів, недоліків у використовуваному програмному забезпеченні та інше.

Шляхи несанкціонованого доступу

Несанкціонований доступ до інформації, що знаходиться в локальних мережах буває:

непрямим — без фізичного доступу до елементів локальних мереж;

прямим — з фізичним доступом до елементів локальних мереж.

В даний час існують наступні шляхи несанкціонованого отримання інформації (канали витоку інформації):

1. застосування підслуховуючих пристроїв;
2. дистанційне фотографування;
3. перехоплення електромагнітних випромінювань;
4. розкрадання носіїв інформації і виробничих відходів;
5. зчитування даних у масивах інших користувачів;
6. копіювання носіїв інформації;
7. несанкціоноване використання терміналів;
8. маскування під зареєстрованого користувача за допомогою розкрадання паролів та інших реквізитів розмежування доступу;
9. використання програмних пасток;
10. отримання даних, що захищаються за допомогою серії дозволених запитів;
11. використання недоліків мов програмування і операційних систем;
12. умисне включення в бібліотеки програм спеціальних блоків типу «троянських коней»;
13. незаконне підключення до апаратури або ліній зв'язку обчислювальної системи;
14. зловмисним виведення з ладу механізмів захисту.

Засоби захисту інформації

Для вирішення проблеми захисту інформації, основними засобами, використовуваними для створення механізмів захисту, прийнято вважати:

Технічні засоби

Технічні засоби — електричні, електромеханічні, електронні і ін. типу пристрою. *Переваги* технічних засобів пов'язані з їх надійністю, незалежністю від суб'єктивних факторів, високою стійкістю до модифікації. *Слабкі сторони* — недостатня гнучкість, відносно великі обсяг і маса, висока вартість. Технічні засоби поділяються на:

- апаратні пристрої, що вбудовуються безпосередньо в апаратуру, або пристрої, що сполучаються з апаратурою локальних мереж по стандартному інтерфейсу (схеми контролю інформації з парності, схеми захисту полів пам'яті по ключу, спеціальні регістри);
- фізичні — реалізуються у вигляді автономних пристроїв та систем (електронно-механічне обладнання охоронної сигналізації та спостереження. Замки на дверях, грати на вікнах).

Програмні засоби

Програмні засоби — програми, спеціально призначені для виконання функцій, пов'язаних з захистом інформації. А саме програми для ідентифікації користувачів, контролю доступу, шифрування інформації, видалення залишкової (робочої) інформації типу тимчасових файлів, тестового контролю системи захисту та ін. *Переваги програмних засобів* — універсальність, гнучкість, надійність, простота установки, здатність до модифікації і розвитку.

Недоліки — обмежена функціональність мережі, використання частини ресурсів файл-сервера і робочих станцій, висока чутливість до випадкових або навмисних змін, можлива залежність від типів комп'ютерів (їх апаратних засобів).

Змішані апаратно-програмні засоби

Змішані апаратно-програмні засоби, які реалізують ті ж функції, що й апаратні та програмні засоби окремо, і мають проміжні властивості.

Організаційні засоби

Організаційні засоби складаються з організаційно-технічних (підготовка приміщень з комп'ютерами, прокладка кабельної системи з урахуванням вимог обмеження доступу до неї та ін) і організаційно-правових (національні законодавства і правила роботи, що встановлюються керівництвом конкретного підприємства). *Переваги* організаційних засобів полягають у тому, що вони дозволяють вирішувати безліч різнорідних проблем, прості в реалізації, швидко реагують на небажані дії в мережі, мають необмежені можливості модифікації та розвитку. *Недоліки* — висока залежність від суб'єктивних чинників, у тому числі від спільної організації роботи в конкретному підрозділі.

У ході розвитку концепції захисту інформації фахівці прийшли до висновку, що використання якого-небудь з вище зазначених способів

захисту, не забезпечує надійного збереження інформації. Необхідний комплексний підхід до використання та розвитку всіх засобів і способів захисту інформації.

Програмні засоби захисту інформації

За ступенем поширення і доступності на першому місці стоять *програмні засоби*, тому далі вони розглядаються більш докладно. Інші засоби застосовуються в тих випадках, коли потрібно забезпечити додатковий рівень захисту інформації.

Серед програмних засобів захисту інформації в локальних мережах можна виділити і детальніше розглянути такі:

4. *засоби архівації даних* — засоби, що здійснюють злиття декількох файлів і навіть каталогів в єдиний файл — архів, одночасно зі скороченням загального обсягу вихідних файлів шляхом усунення надмірності, але без втрат інформації, тобто, з можливістю точного відновлення вихідних файлів.;

5. *антивірусні програми* — програми розроблені для захисту інформації від вірусів;

6. *криптографічні засоби* включають способи забезпечення конфіденційності інформації, у тому числі за допомогою шифрування і аутентифікації;

засоби ідентифікації і аутентифікації користувачів — аутентифікацією (встановлення достовірності) називається перевірка належності суб'єкта доступу пред'явленого ним ідентифікатора та підтвердження його достовірності. Іншими словами, аутентифікація полягає в перевірці: чи є суб'єкт, який підключається тим, за кого він себе видає. А ідентифікація забезпечує виконання функцій встановлення автентичності та визначення повноважень суб'єкта при його допуску в систему, контролювання встановлених повноважень в процесі сеансу роботи, реєстрації дій та ін.

7. *засоби керування доступом* — засоби, що мають метою обмеження та реєстрацію входу-виходу об'єктів на заданій території через «точки проходу»;

8. *протоколювання і аудит* — протоколювання забезпечує збір та накопичення інформації про події, що відбуваються в інформаційній системі. *Аудит* — це процес аналізу накопиченої інформації. Метою комп'ютерного аудиту є контроль відповідності системи або мережі необхідним правилам безпеки, принципам або індустріальним стандартам. Аудит забезпечує аналіз усього, що може ставитися до проблем безпеки, або все, що може призвести до проблем захисту.

Вбудовані

Вбудовані засоби захисту інформації в мережевих ОС доступні, але не завжди, як уже зазначалося, можуть повністю вирішити виникаючі на практиці проблеми. Наприклад, мережні ОС NetWare 3.x, 4.x дозволяють здійснити надійний «ешелонований захист" даних від апаратних збоїв та

пошкоджень. Система SFT (System Fault Tolerance — система стійкості до відмов) компанії Novell включає три основні рівня:

1. SFT Level I передбачає, зокрема, створення додаткових копій FAT і Directory Entries Tables, негайну верифікацію кожного знову записаного на файловий сервер блоку даних, а також резервування на кожному жорсткому диску близько 2 % від обсягу диска. При виявленні збою дані перенаправляються в зарезервовану область диска, а збійний блок позначається як «поганий» і в подальшому не використовується.

2. SFT Level II містить додаткові можливості створення «дзеркальних дисків", а також дублювання дискових контролерів, джерел живлення й інтерфейсних кабелів.

3. SFT Level III дозволяє застосовувати в локальній мережі дубльовані сервери, один з яких є «головним», а другий, що містить копію всієї інформації, вступає в роботу в разі виходу головного сервера з ладу[1].

Система контролю та обмеження прав доступу в мережах NetWare (захист від несанкціонованого доступу) також містить кілька рівнів:

- рівень початкового доступу (включає ім'я та пароль користувача, систему облікових обмежень: таких як, явний дозвіл або заборону роботи, допустимий час роботи у мережі місце на жорсткому диску, займане особистими файлами даного користувача, і т. д.);
- рівень прав користувачів (обмеження на виконання окремих операцій та/або на роботу даного користувача, як члена підрозділу, в певних частинах файлової системи мережі);
- рівень атрибутів каталогів і файлів (обмеження на виконання окремих операцій, у тому числі видалення, редагування або створення, що йдуть з боку файлової системи і стосуються всіх користувачів, що намагаються працювати з даними каталогами або файлами);
- рівень консолі файл-сервера (блокування клавіатури файл-сервера на час відсутності мережевого адміністратора до введення ним спеціального пароля).

Спеціалізовані

Спеціалізовані програмні засоби захисту інформації від несанкціонованого доступу володіють в цілому кращими можливостями і характеристиками, ніж вбудовані засоби мережевих ОС. Крім програм шифрування і криптографічних систем, існує багато інших доступних зовнішніх засобів захисту інформації. З найбільш часто згадуваних рішень, слід відзначити наступні дві системи, що дозволяють обмежити і контролювати інформаційні потоки.

– *Firewalls* — брандмауерів (firewall — вогняна стіна). Між локальною і глобальною мережами створюються спеціальні проміжні сервери, які інспектують і фільтрують весь трафік мережевого/транспортного рівнів, що проходить через них . Це дозволяє різко знизити загрозу несанкціонованого доступу ззовні в корпоративні мережі, але не усуває цю небезпеку повністю. Більш захищений різновид

методу — це спосіб маскараду (masquerading), коли весь вихідний з локальної мережі трафік надсилається від імені firewall-сервера, роблячи локальну мережу практично невидимою.

– *Proxy-сервери* (proxy — довіреність, довірена особа). Весь трафік мережевого/транспортного рівнів між локальною і глобальною мережами забороняється повністю — маршрутизація як така відсутня, а звернення з локальної мережі в глобальну відбуваються через спеціальні сервери-посередники. Очевидно, що при цьому звернення з глобальної мережі в локальну стають неможливими в принципі. Цей метод не дає достатнього захисту проти атак на більш високих рівнях — наприклад, на рівні програми (віруси, код Java і JavaScript).

Література:

1. Герасименко В. А. Захист інформації в автоматизованих системах обробки даних: розвиток, підсумки, перспективи. Зарубіжна радіоелектроніка, 2003 № 3.

2. Закер К. Комп'ютерні мережі. Модернізація і пошук несправностей. СПб .: БХВ-Петербург, 2001.

3. Галицький А. В., Рябко С. Д., Шаньгина В. Ф. Захист інформації в мережі – аналіз технологій і синтез рішень. М .: ДМК Пресс, 2004. – 616 с.

ІНТЕГРАЦІЯ ОБЧИСЛЕННЯ ІНФОРМАЦІЙНОЇ ЕНТРОПІЇ ДЛЯ ВИЯВЛЕННЯ АТАК, ЯКІ ВИКОРИСТОВУЮТЬ ПРОТОКОЛ DNS В ЕКОСИСТЕМІ SPLUNK

Журавчак Д., Устиянович Т. , Дудикевич В.
Національний університет «Львівська політехніка»

DNS – це основний протокол, який дозволяє таким програмам, як веббраузери, функціонувати на основі доменних імен. DNS не призначений для використання в якості команди управління та управління або каналу витоку даних. Однак було розроблено декілька утиліт, щоб дозволити таку діяльність через DNS. Оскільки він не призначений для загальної передачі даних, DNS часто приділяє менше уваги щодо моніторингу безпеки, ніж інші протоколи, такі як веб-трафік. Якщо напад, який використовує DNS, не виявиться, це становить значний ризик для організації. У цьому документі розглядається атаки, які використовують утиліти DNS, та розглядаються практичні методи виявлення тунелів DNS та інших векторів атак, які використовують DNS. Розглянуто дві категорії виявлення – аналіз корисної навантаження та аналіз трафіку. Методи виявлення корисної навантаження використовуються для успішного виявлення конкретних утиліт DNS. Метод на основі аналізу трафіку може використовуватися для універсального виявлення атак, які використовують DNS. За допомогою цих методів виявлення реалізовані організації можуть знизити ризик, пов'язаний з атаками, які використовують DNS.

Ключові слова: Інформаційна ентропія, ДНС, ДНС тунелювання, кібербезпека, Великі дані, Splunk.

DNS is a foundational protocol that enables applications such as web browsers to function based on domain names. DNS is not intended to be used as a command and control or data exfiltration channel. However, several utilities have been developed to enable such activities over DNS. Because it is not intended for general data transfer, DNS often has less attention in terms of security monitoring than other protocols such as web traffic. If the attack that uses DNS goes undetected, it represents a significant risk to an organization. This paper reviews attacks, that use DNS utilities and discusses practical techniques for detecting DNS tunnels and other attack vectors, that use DNS. Two categories of detection considered are payload analysis and traffic analysis. he payload detection techniques have been used to detect successfully specific DNS malware utilities. The traffic analysis-based technique can be used to universally detect attacks that use DNS. With these detection techniques, implemented organizations can reduce the risk associated with attacks, that use DNS.

Keywords: Entropy, DNS, DNS tunneling, Cybersecurity, Big Data, Splunk

Вступ. Кількість джерел інформації в сучасному середовищі мережі Інтернет продовжує зростати експоненціальними темпами. Таким чином, є дуже багато різних атак, такі як DNS тунелі, які використовують протоколи системи доменних імен. Ці атаки створюють великий ризик для корпоративної безпеки, здатні завдати витокам конфіденційних даних тощо. Мета дослідження є використання підрахунку ентропії доменних імен для пошуку вразливих доменів із застосуванням універсального програмного забезпечення Splunk для проведення аналітики, а також виявлення вразливостей серед існуючих доменів глобальної мережі Інтернет.

Дане рішення допоможе фахівцям у галузі захисту інформації, а також корпораціям, науковим установам, які містять велику кількість чутливих даних швидше детектувати злив даних та уникнути його наслідків. Для проведення даного дослідження було використано засіб призначений для опрацювання великих даних; файлів та інформації, які генеруються машинами, різноманітними девайсами; лог-файлів тощо, Splunk. Його особливість полягає у забезпеченні real-time моніторингу, аналітики масивів інформації, автоматизації певних security processes. Крім того, перевага у використанні Splunk як основний фреймворк, засіб для виявлення DNS атак, тунелювань є від великої кількості надбудов, які дозволяють автоматизувати певні процеси data ingestion and processing, customize visualization and improve its capabilities, таким чином дозволяючи здобути більше знань та інформації від потоків даних у режимі реального часу.

Аналіз літератури. Використання візуалізації кореневої DNS із застосування технологій 2D та 3D рендерінгу для швидкої та якісної інтерпретації взаємодії з великою кількістю мережевого трафіку було досліджено у працях Еріка Крокоса та інших [1]. Побудова міцних асоціаційних зв'язків між різноманітними DNS використовуючи аналіз графів серед даних кіберпростору дозволило дослідникам Кхалі Ісса, Тінк Ю та Бей Хуан удосконалити точність роботи системи призначеної для знаходження потенційно небезпечних доменних імен до 95%. Аналіз вже існуючих розробок на основі певних паттернів та здійснено їх класифікацію у наукових працях цих же дослідників [2]. пропонують метод на основі аналізу поведінки користувачів мережі Інтернет, який дозволяє не тільки виявити тунелювання DNS, але й також класифікувати діяльність, щоб зафіксувати та заблокувати зловмисний тунельний трафік. Запропонований спосіб може досягти масштабів виявлення в великих масивах DNS-інформації за допомогою технологій опрацювання масивів великих даних в режимі реального часу [3]. Детальний опис проблем кіберпезпеки з DNS тунелюванням, характеристику на аналіз існуючих методів боротьби з цим явищем, а також перелік програмного забезпечення для перешкоджання зловмисним DNS, зокрема застосування статистичних методів, здійснив Ґреґ Фарнхам [4]. Виявлення небезпечних DNS тунелів у режимі реального часу із застосуванням біграм з метою боротьби з нелегальними сервісами, конвертування та трансфером конфіденційної інформації та забезпечення ефективності захисту інформації досліджено та розроблено у науковій праці Ченг К'ю та інших [5].

Основна частина. Інформаційна ентропія є компоненом, що відповідає за показники мінливості та ненадійсності у випадкових величинах [6]. Для її вимірювання використовують формулу Клода Шеннона, наведену нижче.

$$H = -\sum p(x)\log p(x)$$

У сфері кіберпезпеки випадковою величиною є доменне ім'я, на основі вмісту якого обчислюються ентропія. Що вища випадковість комбінацій у доменному імені, то більшим є показник ентропії. Аномально високі значення

інформаційної ентропії на змінної, що складається з імені домену, можуть свідчити про підозріле та / або небезпечне програмне забезпечння, шкідкливого вмісту веб-сторінки, які містяться під певним доменом або субдоменном, що був створений використовуючи алгоритму генерації домену.

Для того, щоб здійснювати обчислення ентропії в середовищі Splunk, було використано такі надбудови як Splunk Stream та Splunk URL Toolbox. Перша надбудова використовується для пасивного збору та аналітики мережевого трафіку, виявлення DNS запитів тощо, тоді як URL Toolbox – це засіб для поділу URL-адреси або запиту DNS на частини та обчислення ентропії Шеннона на відповідних полі даних у Splunk. Після здійсненння своєрідного поділу на частини доменного імені та обчислення ентропії, визначається своєрідний поріг, за умови перевищення якого відбуватиметься додавання міток до набору даних про те, що певне домененне ім'я є підозрілим. Наступним кроком, можливе додавання його у чорний список та при спробі переходу на його адресу видаватиметься попередження і тому подібне. Використовуючи Splunk, всі обчислення є простими у використанні та автоматизованими, що суттєво дозволяє забезпечувати швидке опрацювання машинних даних та відображати дані мережевого трафіку в режимі реального часу, запобігати витокам конфіденційної інформації, використанню небезпечних доменів.

Висновки

Домени та субдомени з відносно високою ентропією – це показники, які свідчать про шкідливу та доволі підозрілу поведінку у мережі Інтернет. Встановивши відповідний поріг ентропії дозволить класифікувати домени на безпечні та небезпечні, а також забезпечити корпоративну безпеку на високому рівні, зменшити витоки даних, наявність інформаційних загроз.

Література

1. Krokos, Eric, Alexander Rowden, Kirsten Whitley, and Amitabh Varshney. "Visual Analytics for Root DNS Data." In 2018 IEEE Symposium on Visualization for Cyber Security (VizSec), pp. 1-8. IEEE, 2018.

2. Khalil, Issa, Ting Yu, and Bei Guan. "Discovering malicious domains through passive DNS data graph analysis." In Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, pp. 663-674. ACM, 2016.

3. Yu, Bin, Les Smith, Mark Threefoot, and Femi G. Olumofin. "Behavior Analysis based DNS Tunneling Detection and Classification with Big Data Technologies." In IoTBD, pp. 284-290. 2016.

4. Farnham, Greg, and A. Atlasis. "Detecting DNS tunneling." *SANS Institute InfoSec Reading Room* 9 (2013): 1-32.

5. Qi, Cheng, Xiaojun Chen, Cui Xu, Jinqiao Shi, and Peipeng Liu. "A bigram based real time DNS tunnel detection approach." *Procedia Computer Science* 17 (2013): 852-860.

6. Jayasree, N., and P. P. Amritha. "A Model for the Effective Steganalysis of VoIP." *Advances in Intelligent Systems and Computing Artificial Intelligence and Evolutionary Algorithms in Engineering Systems,* 2014, 379-87.

АНАЛІЗ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ СУЧАСНОГО ХОСТИНГУ ПРИ ТЕСТУВАННІ НА ПРОНИКНЕННЯ

Лагун А., Рудик А., Рудик Ю.
Львівський державний університет безпеки життєдіяльності, Львів

Summary. The levels of cloud computing and cyber security are considered. Approaches to information security of cloud hosting are given. Their essence is based on principle: the security of the cloud – is the responsibility of the provider, the security in the cloud – is the responsibility of the client. Therefore, the issue of improving the safety of cloud services and hosting requires a variety of attention.
Keywords: hosting, cyber security, vulnerability, cloud computing, safety, quality.

Анотація. Розглядаються рівні хмарних обчислень та кібербезпеки. Наведено підходи до інформаційної безпеки хмарного хостингу. Їх суть заснована на принципі: безпека хмари - це відповідальність провайдера, безпека в хмарі - це відповідальність клієнта. Тому питання підвищення безпеки хмарних сервісів та хостингу потребує різноманітної уваги.
Ключові слова: хостинг, кібербезпека, вразливість, хмарні обчислення, безпека, якість.

Враховуючи ріст потреби присутності в мережі інтернет більшості галузей людської діяльності все більше підприємців звертаються до послуг хостинг провайдерів. Адже вони дають можливість розмістити свій веб-ресурс на середовищі яке часто можна шкалювати в залежності від потреби споживача, що значно заощадить останнім кошти [1].

Але при цьому користувач хостингу розміщує свої особисті дані на апаратурі яка може знаходитись на іншому континенті, лише з надією на те що надавач хостингових послуг вбереже їх від потенційної небезпеки. При цьому користувач хостингу на своєму веб ресурсі може зберігати і дані своїх клієнтів, втрата яких може завдати чималої шкоди.

Надавачі послуг хостингу впевнені в безпеки своїх серверів з технічного боку, і наразі чималі зусилля прикладаються щоб закрити прогалину яку по собі лишає так званий людський фактор. При цьому кошти на ліцензоване ПЗ для захисту від вірусів, фаєрволи, ОС економляться за рахунок безкоштовних прогам з відкритим кодом.

Метою дослідження є проведення аналізу вразливостей які можна виявити у системах які користуються попитом у численної кількості хостинг провайдерів: cPanel на CentOS. Попри надзвичайну гнучкість та простоту у використанні, це ПЗ потребує постійних оновлень оскільки виявляються все нові вразливості в коді, що ставить під загрозу інформацію яка зберігається на таких системах.

Таким чином, виникає потреба у надійному та якісному обміні даними та застосуванні методів та інструментів програмного забезпечення. Це підвищить ефективність роботи пожежно-рятувальних підрозділів, якість взаємодії, обміну даними та оцінку результатів. Економічний ефект виправданий скороченням часу реагування та усуненням наслідків надзвичайних ситуацій, зменшенням залежності від апаратного старіння обладнання, гнучкості застосування веб-програмного забезпечення та незалежності платформи [2].

Методи дослідження. У роботі використовується комплексний метод дослідження, який включає: аналіз та узагальнення наукових досягнень у галузі інформаційних технологій, застосування статистики хостингу.

SQL – це тип вразливості безпеки веб-додатків, при якому зловмисник намагається використовувати код програми для доступу чи пошкодження вмісту бази даних. Якщо це вдасться, це дозволяє зловмиснику маніпулювати даними, які зберігаються в бек-енд-базі, будь-яким чином їм подобається. Інжекція SQL – це один з найпоширеніших типів уразливості безпеки веб-додатків [3].

Неправильна конфігурація безпеки охоплює кілька типів уразливості, все зосереджено на недостатньому обслуговуванні або недостатній увазі до налаштування сервера. Потрібно визначити та розгорнути безпечну конфігурацію для програми, рамок, сервера додатків, веб-сервера, сервера баз даних та платформи. Неправильні налаштування безпеки надають хакерам доступ до приватних даних або функцій і можуть призвести до повного системного компромісу. Оскільки ресурси на хостинговому сервері розтягуються, деякі хостинг-провайдери часто скорочують кути в своїх конфігураціях, щоб менше ресурсів витрачалося, коли служби безпеки виконують заплановані перевірки / завдання. Це, безумовно, ставить власників веб-сайтів у важке місце, часто вибираючи між ціною добре захищеного сервера або більш дешевою, менш безпечною альтернативою.

Завдяки програмному забезпеченню, що охоплює потенційний шкідливий код, вони часто заважатимуть роботі фактичного власника. Це так звані "помилково-позитивні" тригери, які зупинятимуть показ оновлень завдяки тому, що містять ключові слова, які потенційно можуть бути використані шкідливим чином. У цих випадках користувачі виберуть зручність користування перед безпекою шляхом дозволу цих ключових слів, відкривши вікно можливостей для тих, хто має наміри проникнення.

Безпека як складова є важливим елементом загальної якості обслуговування PQoS - це оцінка якості інформаційного обслуговування з точки зору сприйняття користувача як споживача цієї послуги.

Буде створена віртуальна лабораторія, що максимально близько імітуватиме середовище хостингу. Саме тестування на проникнення буде реалізовуватись за допомогою інструментарію який пропонується системою Kali Linux та іншим відповідним ПЗ.

Нарешті, у кожному заході цифрової безпеки завжди існує людський фактор, оскільки соціальні інженери намагатимуться ввести власників хостингу чи постачальників послуг хостингу в обмін даними входу на ресурси, інакше недоступні для них. Цей спосіб злому не вимагає поглиблених технічних знань і складних сценаріїв, тому жоден брандмауер не може захистити його. Люди, що працюють в галузі IT, повинні бути пильними щодо того, якими деталями вони діляться та кому. Провівши серію з тестувань на проникнення, можна зробити висновки щодо обґрунтованості виходу безпеки з точки зору ПЗ на другий план на фоні фокусу щодо зменшення витрат та зосередження на навчанні персоналу безпечної поведінки.

Також буде можливість співставити рівень опору тестуванню на проникнення з можливими затратами на ліцензійне ПЗ на прикладі Cloud-Linux та ConfigServer eXploit Scanner, що дасть можливість користувачам послуг хостингу підібрати надавача послуг таким чином, щоб впевненість в безпеці їхніх даних була непохитною.

Література

1. Maksymiv O, Rak T, Menshikova O, Deep convolutional network for detecting probable emergency situations, Data Stream Mining & Processing (DSMP), IEEE First International Conference, 2016.

2. Рак Т., Рудик Ю., Рудик А. Засоби оперативного управління діяльністю підрозділів ДСНС з використанням IT-технологій на базі геоінформаційного комплексу, Львів, АСВ, 2015– С. 267-270.

3. Most common web security vulnerabilities [online source] https://www.commonplaces.com/blog/6-common-website-security-vulnerabilities/

БЕЗПЕКА КОМП'ЮТЕРНИХ СИСТЕМ ТА ОСНОВНІ МЕРЕЖЕВІ АТАКИ

Лукомська А., Мирошниченко В.
Дніпропетровський державний університет внутрішніх справ

Анотація. В роботі розглянуто проблеми безпеки комп`ютерної системи та основні мережеві атаки різних типів вірусів.

Ключові слова: правова інформатика, компп'ютерна система, порушення конфіденційності, черв'як.

Summary. The paper deals with computer system security issues and major network attacks of various types of viruses.

Keywords: legal informatics , computer system, breach of privacy , Worm computer.

Провідну роль у процесах інформатизації правоохоронної діяльності повинна відігравати правова наука. Ось чому проблеми розроблення та впровадження інформаційних технологій у правоохоронну діяльність і процеси управління нею розглядається в межах досить молодого наукового напряму, що визначається сьогодні як "Правова інформатика" - "комплексна міждисциплінарна галузь знань про закономірності, умови й особливості використання ідей, методів і технічних засобів інформатики з метою оптимізації та підвищення ефективності інформаційних процесів при вирішенні конкретних завдань соціального управління, правових завдань, а також функціонування інформаційних систем правового змісту і управління ними" [1, с.156].

Безпека комп'ютерної системи є вирішальним завданням. Це процес забезпечення конфіденційності та цілісності. Кажуть, що система є безпечною, якщо її ресурси використовуються та отримують доступ за призначенням за будь-яких обставин, але жодна система не може гарантувати абсолютну безпеку від кількох різних шкідливих загроз та несанкціонованого доступу. Безпеці системи можна загрожувати через два порушення:

– ***Загроза***: програма, яка може завдати серйозної шкоди системі.

– ***Атака:*** спроба зламати безпеку та несанкціоновано використовувати актив.

Порушення безпеки, що впливають на систему, можна кваліфікувати як злісні та випадкові. Зловмисні загрози, як випливає з назви, є своєрідним шкідливим комп'ютерним кодом, розробленим для створення вразливості системи, що призводить до порушень безпеки. З іншого боку, від випадкової загрози порівняно простіше захиститися.

Безпека може бути порушена через будь-яке зі згаданих порушень:

1. Порушення конфіденційності: цей тип порушення передбачає несанкціонований доступ до даних.

2. Порушення доступності: передбачає несанкціоноване знищення даних або несанкціоновану модифікацію даних.

3. Крадіжка служби: являє собою несанкціоноване використання ресурсів.

4. Відмова в обслуговуванні: вміщує недопущення законного використання системи.

Як згадувалося раніше, такі напади можуть мати випадковий характер.

Основною метою інформаційної безпеки є забезпечення:

Цілісності: до об'єктів у системі повинен бути доступ будь-якого санкціонованого користувача, а будь-який користувач, який не має достатніх прав, не повинен мати можливості змінювати важливі системні файли та ресурси. Системні об'єкти повинні бути доступними лише обмеженій кількості авторизованих користувачів. Не всі повинні мати можливість перегляду системних файлів.

Наявності: усі системні ресурси повинні бути доступні всім авторизованим користувачам, тобто лише один користувач не повинен мати права використовувати всі системні ресурси. Якщо трапиться така ситуація, може статися відмова в наданні послуги. У такій ситуації зловмисне програмне забезпечення може приєднати ресурси до себе і тим самим не допустити до законних процесів доступу до системних ресурсів.

Іще однією розповсюдженою загрозою є комп'ютерний хробак. Це програма зараження, яка поширюється через мережі. На відміну від традиційного вірусу, вона націлена переважно на локальні мережі. Комп'ютер, постраждалий від хробака, атакує цільову систему і записує на неї невелику програму – «гачок». Цей гачок далі використовується для копіювання хробака на цільовий комп'ютер. Цей процес повторюється рекурсивно, і незабаром будуть зачеплені всі системи локальної мережі. Він використовує механізм нересту для дублювання себе. Черв'як породжує копії себе, використовуючи більшість системних ресурсів, а також блокуючи всі інші процеси. Основна функціональність хробака може бути представлена у вигляді сканування портів: це засіб, за допомогою якого зломщик визначає вразливість системи для атаки. Це автоматизований процес, який включає створення TCP / IP-з'єднання до певного порту. Щоб захистити особу зловмисника, атаки сканування портів запускаються від Zombie Systems, тобто систем, які раніше були незалежними системами, які також обслуговували своїх власників. Такі атаки не спрямовані на збір інформації або знищення системних файлів. Швидше, вони використовуються для порушення законного використання інформаційної системи. Ці атаки, як правило, застосовуються на комп'ютерні мережі. Вони поділяються на дві категорії:

– напади першої категорії використовують стільки системних ресурсів, що ніякої корисної роботи неможливо виконати. Наприклад, завантаження файлу з веб-сайту, який продовжує використовувати весь доступний час процесора;

– напади другої категорії передбачають зрив мережі об’єкта. Ці атаки є наслідком зловживання деякими основними принципами функціональних можливостей TCP / IP.

Для захисту комп’ютерної системи заходи безпеки можуть бути вжиті на таких рівнях:

- *на фізичному рівні:* об’єкти, що містять комп'ютерні системи, повинні бути фізично захищені від зловмисників. Робочі станції повинні бути ретельно захищені. Тільки відповідні користувачі повинні мати дозвіл на доступ до системи. Необхідно уникати фішингу (збирати конфіденційну інформацію) та дайвінгу (збирати основну інформацію для отримання несанкціонованого доступу).
- *на рівні операційної системи*: система повинна захищати себе від випадкових або цілеспрямованих порушень безпеки.
- *на мережевому рівні*: майже вся інформація поділяється між різними системами через мережу. Перехоплення даних у мережі може бути таким же шкідливим, як і вторгнення в комп'ютер, мережа повинна бути належним чином захищена від таких атак. Зазвичай програми Anti Malware використовуються для періодичного виявлення та видалення таких вірусів та загроз. Крім того, для захисту системи від мережевих загроз використовується також брандмауер.

Висновок

Безпека комп'ютерних мереж – це складне питання, яке включає багато аспектів комп'ютерних технологій, мереж управління, використання мережі та їх обслуговування. Щоб підвищити безпеку комп’ютерної мережі необхідно розробити ефективні рішення безпеки, заходи щодо покращення безпеки комп'ютерних мереж. Треба пройти дуже довгий та нелегкий шлях, щоб забезпечити нормальну роботу широкомасштабної мережевої комп’ютерної системи.

Література:

1. Беляков К. И. Управление и право в период информатизаций: Монография – К., КВШ, 2001. – 252 с.

ВИКОРИСТАННЯ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ТА СИСТЕМИ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЇХ ЗАХИЩЕНОСТІ

Лучечко Ю.В., Косиєв.О.А.
Львівський державний університет безпеки життєдіяльності

Питання захисту інформації є надзвичайно важливими та актуальними сьогодні, оскільки вже давно вийшли на одне з перших місць серед інших завдань, що вирішуються у процесі проектування, створення та використання сучасних інформаційних систем. Надзвичайно актуальним сьогодні є використання вільного та відкритого ПЗ (ВВПЗ) для потреб підвищення рівня захищеності комп'ютерних мереж і систем.

Ефективна політика безпеки повинна бути проактивною, щоб забезпечити достатній захист від різних відомих і невідомих атак і випадків. Дуже часто це хибно розуміють як підтримку в актуальному стані програмного та апаратного забезпечень. Регулярні оновлення необхідні, звичайно, проте вони ніяк не вирішують питання людських помилок – неправильної конфігурації чи підходів, що робить всю мережу вразливою для атак. Тому метою статті є висвітлення методики тестування на проникнення як засобу забезпечення всебічного рівня безпеки.

Тестування на проникнення (PENTEST) – це важлива складова заходів захист об'єктів критичної інфраструктури технічного та організаційного характеру, що призначена для виявлення проблем в системі захисту об'єктів та, як наслідок, превентивного попередження кібернетичних атак в майбутньому. Тестування на проникнення здійснюється шляхом імітування кібератаки на об'єкти захисту.

Етичність тестування безпеки повинна базуватись на правилах застосування (rules of engagement), яких повинен дотримуватися аудитор, котрого наймає організація для проведення тестування на проникнення до її інформаційних ресурсів, зокрема: як слід проводити тестування; визначення масштабів тестування; підготовка плану тестування; перебіг процесу тестування; забезпечення конфіденційної звітності по проведеній роботі тощо.

Відомі є ряд різних методик з відкритим кодом, покликані задовольнити потреби оцінки безпеки. За допомогою цих методик оцінки, можна легко скоротити час на проведення важливих і складних завдань оцінки системи безпеки в залежності від його розміру та складності. Деякі з цих методик зосереджуються на технічному аспекті тестування безпеки, в той час як інші націлені на управлінські критерії. Основна ідея формалізації цих методологій полягає у виконанні різних видів випробувань крок за кроком, що дасть змогу судити про безпеку системи більш точно. Зокрема, такими відомими методиками оцінки безпеки мережевого та прикладного рівнів є: Open Source Security Testing Methodology Manual (OSSTMM), Information Systems Security Assessment Framework (ISSAF), Open Web Application Security Project (OWASP) Top Ten, Web Application Security Consortium Threat Classification (WASC-TC).

Наведені методики покликані допомогти фахівцям з безпеки вибрати кращу стратегію, яка могла б вписатися у вимоги клієнтів, і кваліфікувати підходящий прототип тестування. Перші дві методики забезпечують загальні принципи і методи, забезпечуючи тестування безпеки для практично будь-яких інформаційних активів, останні два – відповідно в основному стосуються оцінки безпеки на прикладному рівні. Визначення правильної стратегії оцінки залежить від декількох факторів, у тому числі, технічних деталей, наданих про цільову систему, наявність ресурсів, знань аудитора і нормативних питань.

Література:

1. Assuring Security by Penetration Testing. Master the art of penetration testing with BackTrack// Packt Publishing Ltd. – Birmingham, 2011. 373 pp.

2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 року № 2163-VIII// Відомості Верховної Ради. – 2017. – № 45. – Ст. 403.

3. Конвенція про кіберзлочинність // Офіційний вісник України – 2007. – № 65. – Ст. 2535. – С. 107.

ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Охват М.С., Рябоконь Н.В.
ВП НУБіП «Ірпінський економічний коледж», м. Ірпінь

У наші дні використання інформаційних технологій не має меж. Віртуальний простір переймає від реального все підряд, у тому числі й злочинність у її нових формах і проявах.

Кіберзлочинність, захист інформації, комп'ютерні мережі, поради,як зберігти власні дані.

Today the use of information technology has no limits. Virtual space takes over everything from the real world, including crime in its new forms and manifestations.

Cybercrime, protection of information, computer networks, tips on how to save your own data.

Термін «кіберзлочинність» часто вживається поряд з терміном «комп`ютерна злочинність», причому нерідко ці поняття використовуються як синоніми.

Поняття «кіберзлочинність» (в англомовному варіанті - cybercrime) ширше, ніж «комп`ютерна злочинність» (computer crime), і більш точно відображає природу такого явища, як злочинність в інформаційному просторі. Так, Оксфордський тлумачний словник визначає приставку «cyber - » як компонент складного слова. Її значення – що відноситься до інформаційних технологій, мережі Інтернет, віртуальної реальності. Практично таке ж визначення дає Кембриджський словник

Таким чином, «cybercrime» – це злочинність, пов`язана як з використанням комп`ютерів, так і з використанням інформаційних технологій і глобальних мереж. У той же час термін «computer crime» в основному відноситься до злочинів, скоюваних проти комп`ютерів або комп`ютерних даних.

Об'єктом кіберзлочинів є персональні дані, банківські рахунки, паролі та інша особиста інформація як фізичних осіб, так і бізнесу та державного сектору. Кіберзлочинність є загрозою не тільки на національному, а й на глобальному рівні.

Найпоширенішими видами таких злочинів є:

Кардинг – використання в операціях реквізитів платіжних карт, отриманих зі зламаних серверів інтернет-магазинів, платіжних і розрахункових систем, а також із персональних комп'ютерів (або безпосередньо, або через програми віддаленого доступу, «трояни», «боти»).

Фішинг – вид шахрайства, відповідно до якого клієнтам платіжних систем надсилають повідомлення електронною поштою нібито від адміністрації або служби безпеки цієї системи з проханням вказати свої рахунки та паролі.

Вішинг – вид кіберзлочинів, у якому в повідомленнях міститься прохання зателефонувати на певний міський номер, а при розмові запитуються конфіденційні дані власника картки.

Онлайн-шахрайство – несправжні інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку.

Як вберегтися від кібершахраїв?

Банальні поради: не надавати нікому персональні дані, паролі і коди-підтвердження з смс для операцій з картками, не довіряти повідомленням про виграші в лотереях, перевіряти інформацію за офіційним номером банку, не скачувати в інтернеті сумнівні файли, користуватись ліцензійним програмним забезпеченням тощо.

Більшість людей знають всі ці речі, але все одно потрапляють у пастки кіберзлочинців.

Небанальні. Сумнівний номер телефону чи картки можна перевірити на сайті кіберполіції, а також звернутися до спеціалістів із запитом.

Кіберполіція радить, як не стати жертвою вірусу-вимагача, як виявити, що злочинці втручаються в систему вашого онлайн-банкінгу, або як захиститися від телефонних шахраїв.

Дуже часто до кіберполіції звертаються із заявами про викрадення криптовалюти. Існують шахрайські схеми, коли власник електронного гаманця надає доступ шахраям до своїх акаунтів і вони переводять десятки тисяч доларів на інший гаманець.

Чому часто кажуть, що безкоштовний Wi-Fi у кафе може бути пасткою?

Wi-Fi – це сервіс, який має слабкі сторони, і за допомогою Wi-Fi можна отримати доступ до будь-якого пристрою, підключитися та скористатися інформацією в злочинний цілях. Такі ситуації мають місце в Україні.

До будь-якого Wi-Fi підключатися не можна, варто звертати увагу на репутацію закладу і на його офіційну реєстрацію як юридичної особи. Тоді в разі чого можна буде пред'явити претензії.

Література:

1. https://ukrainepravo.com/legal_publications/essay-on-it-law/it_law_prytula_cybercrime/
2. https://www.gurt.org.ua/articles/34602/
3. https://www.radiosvoboda.org/a/details/29031166.html

АНАЛІЗ КРИТИЧНИХ РЕСУРСІВ І ПОТЕНЦІЙНИХ ЗАГРОЗ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Самсон В., Полотай О.
Львівський державний університет безпеки життєдіяльності

Описано ресурси комп'ютерної мережі, які вважаються критичними і потребують особливого захисту. Також наведено перелік усіх потенційних загроз комп'ютерної мережі.
Ключові слова: комп'ютерна мережа, ресурси мережі, загрози мережі.

Describes computer network resources that are considered critical and require special protection. It also lists all the potential threats to your computer network.
Keywords: the computer network, network resources, network threats.

На сьогоднішній день існує безліч цілей забезпечення мережевої безпеки, але найбільшої уваги заслуговують три основні: конфіденційність, доступність і цілісність інформації.

Цілісність даних гарантує збереження як в разі зловмисних дій, помилок, так і випадковостей. Одне з найскладніших завдань мережевої безпеки - це забезпечення цілісності даних.

Забезпечення конфіденційності даних – це одна з основних цілей побудови інформаційної безпеки. До конфіденційної інформації можна віднести наступні дані:

- особиста інформація користувачів;
- облікові записи (імена і паролі);
- бухгалтерська інформація;
- дані про розробки і різні внутрішні документи;
- дані банківських карт.

Доступність – це одна з важливих цілей, адже, якщо користувач не може працювати з даними, який сенс говорити про їх захист. До ресурсів, які використовуються в локальній мережі відносяться:

- сервери;
- робочі пристрої;
- пристрої для забезпечення діяльності;
- дані користувачів;
- будь-які критичні дані, необхідні для роботи.

Для побудови безпеки комп'ютерної мережі потрібно розглянути загрози і перешкоди. Їх можна розділити на дві великі групи: технічні загрози і людський фактор [1].

Технічні загрози:

- комп'ютерні віруси;
- помилки в програмному забезпеченні;
- різні DoS- і DDoS-атаки;
- технічні засоби знімання інформації;
- аналізатори протоколів і прослуховують програми

Комп'ютерні віруси – це одна з найстаріших категорій небезпек, яка в чистому вигляді практично не зустрічається. Через активне застосування мережевих технологій для передачі даних, віруси все тісніше інтегруються з троянськими компонентами і мережними хробаками. На даний момент комп'ютерні віруси використовують для свого поширення чи уразливості в програмному забезпеченні, або електронну пошту.

Помилки в програмному забезпеченні полягають у тому, що через те, що програмне забезпечення для таких пристроїв як: сервери, маршрутизатори, робочі станції і т.д. написано розробниками, тобто людьми, воно не може не містити помилки. Це робить програмне забезпечення одним з найбільш вузьких місцем будь-якої мережі. Чим вище складність програмного забезпечення, тим більша ймовірність присутності в ньому помилок і вразливостей. Для усунення даного виду вразливостей виробники програмного забезпечення регулярно випускають пакети оновлень. І необхідною умовою безпеки мережі є своєчасна установка цих оновлень.

DOS- і DDOS-атаки – DOS (Denial Of Service або відмову в обслуговуванні) – це особливий тип атак, який спрямований на виведення мережі або сегмента мережі з робочого стану. При атаках даного типу можуть використовуватися помилки в ПЗ, але в великих масштабах. Новий тип атак DDoS (Distributed Denial Of Service або розподілена атака типу відмова в обслуговуванні) – перевантажує канал трафіком і заважає проходженню інформації по каналах зв'язку, а часто і повністю блокує передачу по ним корисної інформації [3].

Технічні засоби знімання інформації – такі пристрої, як камери, клавіатурні жучки, реєстратори віброакустичних коливань і т.д. Дана категорія використовується не так часто, так як для установки пристроїв знімання інформації потрібен доступ в приміщення, де знаходяться складові мережі.

Аналізатори протоколів і «сніфери» – засоби перехоплення переданих в мережі даних. Зазвичай дані в мережі передаються у відкритому вигляді, це і дозволяє всередині локальної мережі перехопити їх зловмисникові. Деякі протоколи роботи з мережею не використовують шифрування паролів, в наслідок цього у зловмисника з'являється можливість перехопити їх для подальшого використання. Найбільш гостро ця проблема постає при передачі інформації з глобальних мереж [3].

Людський фактор:

– недбалість;
– низька кваліфікація;
– звільнені або незадоволені співробітники;
– промислове шпигунство.

Недбалість – одна з найпоширеніших категорій зловживань, таких як: недотримання інструкцій при роботі з секретною інформацією, використання несанкціонованих пристроїв для обміну інформацією в мережі і т.п. Підсумком недбалості є можливість зловмисників отримати безперешкодний доступ до ресурсів мережі.

Низька кваліфікація користувачів впливає на їх нерозуміння реальної загрози витоку інформації і т.п., а також не може визначити яку саме інформацію можна розголошувати, а яка є конфіденційною.

Звільнені і незадоволені співробітники можуть вкрасти будь-які дані для того, щоб потім продати цю інформацію або шантажувати керівництво. В особливу групу хотілося б виділити системних адміністраторів, які при звільненні або при незадоволенні умовами роботи можуть використовувати ресурси мережі в своїх цілях, в тому числі для своєї матеріальної вигоди.

Промислове шпигунство – найскладніша категорія, так як при прийомі на роботу керівництво не знає, чи є ця людина підставною особою з іншої організації, і влаштовується ця людина на роботу з метою передачі конфіденційної інформації організації, що найняла його [2].

Отже, для стабільної та ефективної роботи комп'ютерної мережі, системні адміністратори повинні враховувати всі перераховані загрози щодо найбільш важливих ресурсів мережі.

Література:

1. Галатенко В.А. Основы информационной безопасности / Под ред. члена-корреспондента РАН В.Б. Бетелина – М.: ИНТУИТ.РУ «Интернет-Университет Информационных Технологий», 2003.

2. Грайворонський М. В. Безпека інформаційно-комунікаційних систем: підруч. для студ. вищ. навч. закл., які навчаються за напрямами "Безпека інформаційних і комунікаційних систем", "Системи технічного захисту інформації", "Управління інформаційною безпекою" / М. В. Грайворонський, О. М. Новіков. – К. : Вид-во BHV, 2009. – 608 с.

3. Студопедія. [Електронний ресурс]. Режим доступу з studopedia.org/4-122974.html

ВИБІР ОБЛАДНАННЯ CISCO ДЛЯ РОЗГОРТАННЯ КОРПОРАТИВНОЇ VPN-МЕРЕЖІ

Тлумак О., Полотай О.
Львівський державний університет безпеки життєдіяльності

Описано основне апаратне забезпечення компанії Cisco, яке використовується для побудови корпоративної VPN мережі.

Ключові слова: комп'ютерна мережа, Cisco.

The basic hardware for Cisco that is used to build a corporate VPN network is described.

Keywords: the computer network, Cisco.

На сьогоднішній день корпоративні мережі – це невід'ємна частина бізнесу, адже з їх допомогою можна забезпечити безпечну і оперативну передачу даних між різними підрозділами підприємства, при чому вони можуть бути розташовані за сотні кілометрів один від одного.

В результаті потреби в можливості підключення до корпоративної мережі віддалених підрозділів і виникла технологія VPN [2], яка вирішує цю проблему, так як в її основі лежить глобальна мережа WAN, яка охоплює мільйони пристроїв по всьому світу. VPN-пристрій розташовується між внутрішньою мережею і Інтернет на кожному кінці з'єднання. Коли дані передаються через VPN, вони зникають «з поверхні» в точці відправлення та знову з'являються тільки в точці призначення. Цей процес прийнято називати «тунелюванням». Це означає створення логічного тунелю в мережі Інтернет, який з'єднує дві крайні точки. Завдяки тунелюванню приватна інформація стає невидимою для інших користувачів Інтернету.

Для побудови корпоративної мережі можна використовувати декілька видів інструментів, як програмного так і апаратного характеру. Якщо пріоритет надавати апаратній побудові VPN-мереж, то найкраще використовувати обладнання, яке пропонує потужна компанія Cisco.

Виходячи з специфіки корпоративної мережі, у якій її складові поділені на окремі підмережі, то найбільш оптимальною є структура мережі, яка повинна включати в себе: маршрутизатор, комутатора рівня ядра/розподілу, а також комутатор рівня доступу.

Серія маршрутизаторів 2900 компанії Cisco призначена для бізнесу малих і середніх розмірів, ці маршрутизатори задовольняють всім сучасним вимогам і забезпечують стабільне високошвидкісне з'єднання з мережею WAN. Цю серію і розглянемо для вибору маршрутизатора потрібної нам конфігурації.

На вибір компанія Cisco пропонує 4 моделі маршрутизаторів 2900 серії, з різною кількістю доступних інтерфейсів і модулів.

Наочне порівняння кількості інтерфейсів і модулів маршрутизаторів серії Cisco G2 2900 представлено в таблиці 1.

Таблиця 1 – Порівняння кількості інтерфейсів серії 2900

Модель	Доступні порти 10/100/1000 Мбіт/с, RJ45	Доступні порти 10/100/1000 Мбіт/с, SFP*	Порти SM	Порти double SM	Порти ISM
2901	2	0	0	0	1
2911	3	0	1	0	1
2921	3	1	1	1	1
2951	3	1	2	1	1

Найбільш відповідною є друга модель з лінійки з номером 2911, так як вона має 3 RJ45 роз'єму 10/100/1000 Мбіт / с і один порт SM і ISM.

Що стосується комутаторів, то компанія Cisco пропонує наступні типи комутаторів для корпоративних мереж відповідно до класифікації, [1]:

- Комутатори для кампусних мереж (Campus LAN Switches).
- Комутатори з хмарним керуванням (Cloud-Managed Switches).
- Комутатори для ЦОД (Data Center Switches).
- Комутатори для постачальників послуг (Service Provider Switches).
- Віртуальні мережі (Virtual Networking).

Виходячи цього, комутатор ядра доцільно вибирати з наступних моделей: 3560, 3750, 4500, 6500.

В таблиці 2 показано зведену інформацію про ці типи комутаторів.

Таблиця 2 – Порівняння комутаторів

Модель комутатора	Характеристика 1	Характеристика 2	Характеристика 3
3560	Пропускна здатність до 3 Тбіт/с	Підтримка технології Eas Virtual Network, а також 150 Гбіт/с Ethernet	Підтримка всіх існуючих протоколів безпеки
3750	Орієнтований на мережі невеликого розміру	Підтримка технологій StackWese Plus і StackPower	
4500	Орієнтований на мережі середнього розміру	Можливість гарячого оновлення ПЗ	
6500	Підтримка технологій Quality of Service	Підтримка швидкісної IP-маршрутизації	Підтримка Access Control List

Для рівня ядра корпоративної мережі середнього розміру досить комутатора серії 3560, що володіє швидкісними параметрами 100/1000 Мбіт/с.

Для вибору комутатора рівня доступу доцільно вибирати комутатори серії 2960, оскільки пристрої цієї серії мають володіють: можливістю розстановки пріоритетів при передачі інформації, підтримкою бездротового голосового зв'язку, а також швидкісної передачі файлів, швидким налаштуванням, підтримкою безліччю протоколів захисту. Найбільш популярний комутатор, який володіє усіма необхідними параметрами, є простим у налаштуванні та надійним у роботі, це комутатор Cisco 2960-24.

Отже, вибір даного обладнання, дасть змогу організувати корпоративну VPN мережу, та забезпечить надійну її роботу.

Література

1. Грайворонський М. В. Безпека інформаційно-комунікаційних систем: підруч. для студ. вищ. навч. закл., які навчаються за напрямами "Безпека інформаційних і комунікаційних систем", "Системи технічного захисту інформації", "Управління інформаційною безпекою" / М. В. Грайворонський, О. М. Новіков. – К. : Вид-во BHV, 2009. – 608 с.

2. Конев И. Р., Беляев А.В. Информационная безопасность предприятия – СПб: БХВ – Петербург 2007. – 752с.

DOS(DDOS)-АТАКИ

Тихолаз Д., Шабатура М.
Національний університет «Львівська політехніка»,
Львівський державний університет безпеки життєдіяльності

The development of information technology and the expansion of information space have a great impact on all areas of human activity related to the accumulation and processing of data. Currently, there is a huge variety of databases and other resources hosted on the Internet that contain information about various fields of scientific, educational and economic activity. At this stage, there is the question of protecting servers, networks and individual parts of the network from DDoS attacks and understanding the structure of such attacks.

Keywords: Dos-attacks, open-source servers, flood attack, HTTP flood, firewall, traffic analysis system, IP-addresses.

Атака на відмову в обслуговуванні або розподілена атака на відмову в обслуговуванні (англ. DoS attack, DDoS attack, (Distributed) Denial-of-service attack) – напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена [1].

Одним із найпоширеніших методів нападу є насичення атакованого комп'ютера або мережевого устаткування великою кількістю зовнішніх запитів (часто безглуздих або неправильно сформульованих) таким чином атаковане устаткування не може відповісти користувачам, або відповідає настільки повільно, що стає фактично недоступним. Причинами атак можуть бути особисті мотиви, розваги, політичні протести, вимагання, недобросовісна конкуренції. Взагалі відмова сервісу здійснюється:

- примусом атакованого устаткування до зупинки роботи програмного забезпечення/устаткування або до витрат наявних ресурсів, внаслідок чого устаткування не може продовжувати роботу;
- заняттям комунікаційних каналів між користувачами і атакованим устаткуванням, внаслідок чого якість сполучення перестає відповідати вимогам.

DoS-атак почали свою історію ще з 1997 році, зробивши «день мовчання» на web-сайт компанії Microsoft. І навіть у наші дні у 2018 році було зафіксовано дві надпотужні DDoS атаки з піковою потужністю 1,3 Тб/с проти Github та 1,7 Тб/с проти веб-ресурсу в США. Тоді, зловмисники скористались особливістю протоколу системи Memcached для мультиплікації UDP-трафіку. Відсутність автентифікації в системі memcached надала змогу зловмисникам використовувати «відкриті» сервери спочатку для завантаження власних даних, а потім надсилаючи запити на їхнє отримання із підробленою (так званий спуфінг) IP-адресою скеровувати відповіді на адресу жертви [2].

Якщо атака відбувається одночасно з великої кількості IP-адрес, то її називають розподіленою (англ. Distributed Denial-of-Service — DDoS) [3].

Організувати DDoS атаки можна шляхом зараження певного числа комп'ютерів програмами, які в певний момент починають здійснювати запити до атакованого сервера (ботнет) чи з домовленістю великого числа користувачів інтернету почати здійснювати певні типи запитів до атакованого сервера (флешмоб).

Існує три класи DDoS атак [1-4]:

- Атаки, направлені на переповнення каналу (flood attack);
- Атаки, що використовують вразливості стеку мережевих протоколів (Ping of death);
- Атаки на рівень додатку (HTTP флуд, атака фрагментованими HTTP пакетами, атака повільними сесіями (SlowLoris).

Небезпека більшості DDoS-атак – в їх абсолютній прозорості і «нормальності». Адже якщо помилка в ПЗ завжди може бути виправлена, то повна витрата ресурсів – явище майже буденне. З ними стикаються багато адміністраторів, коли ресурсів машини стає недостатньо, або web-сайт піддається слешдот-ефекту. І, якщо різати трафік і ресурси для всіх підряд, то можна врятуватися від DDoS, у той же час, втративши велику частину клієнтів. Виходу з цієї ситуації фактично немає, проте наслідки DDoS-атак і їх ефективність можна істотно понизити за рахунок правильного налаштування маршрутизатора, брандмауера і постійного аналізу аномалій в мережевому трафіку.

Є кілька методів боротьби проти DDoS-атак, один із них полягає використання фільтрувальної мережі. Мережа приймає трафік на себе, фільтрує його і до цільового сервера доходить тільки перевірений і якісний трафік від реальних користувачів [5].

Наведемо декілька рекомендацій, щоб уникнути виникнення цієї атаки:

– Всі сервери, які мають прямий доступ в зовнішню мережу, мають бути підготовлені до простої і швидкої віддаленої роботи. Перевагою буде наявність другого, адміністративного, мережевого інтерфейсу, через який можна отримати доступ до сервера при зайнятому основному каналі;

– Програмне забезпечення, використовуване на сервері, завжди повинно знаходитися в актуальному стані. Всі дірки — пропатчені, оновлення встановлені – це захистить вас від DoS-атак, багів у сервісах;

– Всі слухаючі мережеві сервіси, призначені для адміністративного використання, мають бути заховані брандмаузером від всіх, хто не повинен мати до них доступу. Тоді той, що атакує не зможе використовувати їх для проведення DoS-атаки або брутфорса;

– На підходах до сервера (найближчому маршрутизаторі) має бути встановлена система аналізу трафіку (Netflow в допомогу), яка дозволить своєчасно дізнатися про атаку, що починається, і вчасно виконати заходи з її запобігання.

Висновок: Підсумовуючи, можна зазначити, що такого роду атаки є дуже поширеними в наш час. Сфера кіберзлочинності стрімко розвивається , багато людей постраждали від такого роду атак через свою необізнаність та легкість реалізації самої DoS-атаки. Проте , можна захистити себе дотримуючись спеціальних налаштувань та наявності актуального програмного забезпечення.

Література:

1. What is a DDoS Attack? [Електронний ресурс] – Режим доступу: https://www.digitalattackmap.com/understanding-ddos/

2. What is a DDoS Attack? Електронний ресурс] – Режим доступу: https://ddos-guard.net/ru/terminology/attacks/ddos-ataka

3. Denial-of-service attack [Електронний ресурс] – Режим доступу: https://en.wikipedia.org/wiki/Denial-of-service_attack

4. DDoS attack protection [Електронний ресурс] – Режим доступу: https://www.cloudflare.com/lp/ddos-x/?_bt=396751245091&_bk=ddos%20attack&_bm=p&_bn=g&_bg=70618747359&_placement=&_target=&_loc=1012859&_dv=c&gclid=Cj0KCQiA5dPuBRCrARIsAJL7oegS2ApZkfhVNwimDbXI4-1hROllGtiI5c9JjHF2BZ8NW68LR6jHgssaAo5pEALw_wcB

5. Дослідження вразливостей Web–сайтів та методи їх усунення http://phone.kpi.ua/wp-content/uploads/2014/06/4.pdf

ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Фрідріхсон Н.
Ірпінський економічний коледж, м. Ірпінь

В статті розглядаються важливі питання інформаційної безпеки громадян та організацій. Розглянуті основні «трюки» хакерів та правила техніки безпеки поводження в мережі.

Кібербезпека, кіберзлочин, мережа, системні програмісти, комп'ютерні віруси, хакерські атаки, загроза.

The important problems of information safety of the citizens and organizations considered in the article. The main hacker attacks and accident prevention rules to behave in the networks were considered.

Cyberwarfare, cyberattack, network, system program, computer virus, hacker attacks, distress.

Комп'ютерна безпека — це сукупність проблем у галузі телекомунікацій та інформатики, пов'язаних з оцінкою і контролюванням ризиків, що виникають при користуванні комп'ютерами та комп'ютерними мережами і розглядуваних з точки зору конфіденційності, цілісності і доступності.

Створення безпечних комп'ютерних систем і додатків є метою діяльності мережевих інженерів і програмістів, а також предметом теоретичного дослідження як у галузі телекомунікацій та інформатики. У зв'язку із складністю і трудомісткістю більшості процесів і методів захисту цифрового обладнання, інформації та комп'ютерних систем від ненавмисного чи несанкціонованого доступу вразливості комп'ютерних систем становлять значну проблему для їхніх користувачів.

Кібербезпека – це безпека ІТ систем (обладнання та програм). Кібербезпека є частиною інформаційної безпеки будь-якої організації.

З 1 жовтня у всіх країнах ЄС розпочався місяць кібернетичної безпеки, присвячений підвищенню обізнаності громадян щодо кіберзагроз, а також обміну досвідом у цій сфері. Про це інформує Єврокомісія.

Як уточнюється, місяць кібербезпеки присвячений розвитку базових навичок перестороги, котрі мають стати частиною повсякденної поведінки кожної людини при контактах з високотехнологічними пристроями.

Загальна мета акції – донести до європейців знання про онлайн-загрози та дати їм належні інструменти, аби громадяни стали впевненими убезпеченими користувачами.

В епоху інформаційних технологій неможливо почуватися захищеним у кіберпросторі. З розвитком технологій стрімко зростає кількість злочинів у цій сфері, а тому з впевненістю можна стверджувати, що саме «кіберзлочини» у XXI столітті будуть одними з найчисельніших. Щодня у людей та компаній крадуть персональні дані, кошти з рахунків, збирають

безліч конфіденційної та комерційної інформації, блокують діяльність тощо. Проте успішність запобігання таким злочинам, їх викриття та притягнення винних осіб до відповідальності наразі є достатньо рідкісним явищем, якщо порівнювати з кількістю таких правопорушень.

Сьогодні кібератаки шкодять не лише фізичним та юридичним особам, але й державам. Щорічно у світі проводяться сотні заходів різних рівнів щодо обговорення актуальних проблем кібербезпеки. Кібербезпека та боротьба з кіберзлочинністю у XXI столітті – це одні з найбільш важливих питань, які потребують глибокого аналізу, розробок та впровадження високотехнологічних рішень з метою запобігання та викриття кіберзагроз.

Щороку кіберзлочинність завдає державам та приватним особам дуже великої шкоди. На 73-й сесії Генеральної асамблеї ООН генеральний секретар Антоніу Гуттереш оцінив щорічні збитки від кіберзлочинності у світі в розмірі 1,5 трлн доларів. На жаль, прогнози експертів з кібербезпеки невтішні. В майбутньому кількість злочинів та збитків від кібератак лише зростатиме, адже зазвичай правопорушники йдуть щонайменше на крок попереду механізмів, які мають державні органи та приватні особи щодо запобігання і розкриття таких злочинів.

Сьогодні можна виділити такі основні (найпопулярніші) способи злочинних цілей хакерів:

1.Фішинг –підробка адреси відомого сайту або його дизайну. Шахрай видає свій сайт за справжню відому компанію. Мета фішингу – отримання доступу до конфіденційних даних користувачів (паролів, логінів, даних особових рахунків і банківських карт).

2.Вірусні програми, які встановлюється без відома та проти волі користувача на його комп'ютер або інший пристрій. Часто вірус буває вбудований у завантажену з інтернету програму, яка «випускає» вірус на волю, після того як «жертва» її встановлює.

3.Соціальна інженерія – це підхід до злому, який не залежить від технологій і полягає у застосуванні шахраями тактики, завдяки якій вони переконують «жертву» розкрити конфіденційну інформацію.

4.Шкідливе ПЗ (Malware) – до таких програм належать так звані «трояни», програми-шпигуни чи рекламне ПЗ. Достатньо часто вони встановлюються разом з іншою, корисною програмою, яку вирішила завантажити «жертва».

5.Злом – це умисна дія, спрямована на несанкціоноване проникнення у ПЗ або систему шляхом обходу механізму безпеки, з метою отримання несанкціонованого доступу до певного ПЗ або системи.

6.За допомогою вказаних вище способів у 2018 р. були здійснені найбільш гучні кібератаки. В минулому році хакери зламали сервери компанії T-Mobile та вкрали особисті дані більше ніж 2 млн їхніх клієнтів. Інші хакери зламали базу даних мережі готелів Marriott та викрали данні близь-

ко 500 млн клієнтів. Повністю захистися від кібератак неможливо. Проте виконання хоча б мінімальних правил техніки безпеки поводження в мережі значно підвищить шанси, що вас не зламають. Отже, пропоную ознайомитися з основними правилами:

– користуватися виключно офіційним ПЗ і вчасно його оновлювати;
– не завантажувати програмне забезпечення з ненадійних джерел;
– використовувати антивіруси для роботи з комп'ютерами;
– нікому не передавати особисті персональні дані (пін-коди карток, CVV коди, паролі до акаунтів тощо);
– створювати складні паролі;
– не здійснювати платіжних операцій у відкритій, незахищеній мережі Wi-Fi;
– не відкривати файли та листи від підозрілих джерел;
– не переходити на підозрілі посилання та за спливаючими вікнами;
– не заходити на ненадійні сайти та не завантажувати з них жодного ПЗ;
– не вставляти у свій комп'ютер флешки та зовнішні диски, якщо не довіряєте повністю їх джерелу;
– періодично здійснювати резервне копіювання важливої інформації.

Виконання зазначених засобів безпеки дозволить лише мінімізувати можливість випадкового несанкціонованого проникнення у ваші пристрої та системи. Однак неможливо надати повної гарантії уникнення зламу. Для максимальної мінімізації таких ризиків компаніям рекомендовано користуватися послугами спеціалістів у сфері кібербезпеки з чітким виконанням всіх інструкцій, які вони зазначають.

Література:

1. Косинський В.І., Швець О.Ф. Сучасні інформаційні технології. Навчальний посібник. – К.: «Знання», 2012. – 318 с.

2. Швиденко М.З., Ткаченко О.М., Глазунова О.Г., Мокрієв М.В., Попов О.Є. Інформатика і комп'ютерна техніка. Навчальний посібник. – К.: Освіта України, 2012. – 489 с.

СОЦІАЛЬНІ ІННОВАЦІЇ І БЕЗПЕКА З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ БЛОКЧЕЙНУ І СМАРТ-КОНТРАКТІВ

Чаплінська С.
Національний Університет «Львівська політехніка»

Анотація: Проведено дослідження технологій блокчейну і смарт-контрактів, методів гарантування їх безпеки та можливостей їх використання при впровадженні соціальних інновацій.
Ключові слова: блокчейн, смарт контракт, хеш, алгорим консенсусу

Summary: The research of blockchain and smart contract technologies, methods of guaranteeing their security and the possibilities of their use in the implementation of social innovations are conducted.
Keywords: blockchain, smart contract, hash, consensus algorithm

Вступ. ‘Під впливом глобалізації та інновацій у сфері інформаційних і комунікаційних технологій швидкий розвиток та популярність отримали технології блокчейну та смарт-контрактів. Як показують дослідження, вони, окрім застосування у криптовалютах, мають цілий спектр інших можливостей. Зокрема, їх можна застосовувати при впровадженні соціальних інновацій, про що свідчить поява тих чи інших інформаційних систем на базі технології блокчейну, що мають виражене соціальне призначення. Під поняттям соціальних інновацій будемо розуміти “нові рішення”, які задовільняють соціальні потреби та забезпечують нові можливості. Метою висвітленого у даній доповіді дослідження є опрацювання сучасного стану технологій блокчейну і смарт-контрактів та дослідження можливості їх застосування у соціальній сфері.

1. Огляд технологій блокчейну і смарт-контрактів

Блокчейн – це технологія упорядкування в зростаючий список записів, які називають блоками, що пов'язані між собою з використанням методів криптографії [1, с.24]. Коли ми говоримо слова "блок" і "ланцюг" (англ. *chain*) у цьому контексті, ми фактично говоримо про цифрову інформацію ("блок"), що зберігається в зв’язаній публічній базі даних (“ланцюжок”). Кожен користувач системи може додавати нові записи до бази даних, але не може їх змінювати. У блоці міститься інформація (тіло блоку) та обчислений дайджест (хеш-функція) цього і попереднього блоків. Інформація, яка міститься всередині, залежить від типу блокчейну [2, с. 51-66]. Для прикладу, інформація всередині криптовалюти *bitcoin* - це деталі транзакції (відправник, кількість монет) та хеш цього і попереднього блоків.

Хеш ідентифікує блок. Розміщення хешу попереднього блоку в наступному утворює з блоків ланцюжок і робить блокчейн безпечним,

надаючи йому криптографічного захисту. Кожен з вузлів верифікує блок і перевіряє, чи не був він сфальшованим. Якщо перевірка проходить успішно, кожен користувач додає його у свій власний блокчейн. Окрім хешу, в основі безпеки блокчейну є алгоритми консенсусу. Ці алгоритми призначені для забезпечення достовірності транзакцій через перевірку точності проведених дій в мережі. Існує кілька типів алгоритмів консенсусу. Найпоширенішими є PoW і PoS. [1, с.52-66]. *Proof-of-work* - це алгоритм уповільнення процесу створення нових блоків. Він робить підробку блоків надзвичайно складною, тому що якщо підробляється один блок, необхідно змінити *proof-of-work* для усіх інших. *Proof-of-Stake* — це альтернатива PoW, при використанні цього алгоритм*у* тривалість формування блоку не залежить від потужності використовуваного обладнання.

Одним з недавніх оновлень технології блокчейну стало застосування смарт-контрактів. Смарт-контракти реалізують як програми, що зберігаються в блокчейні і можуть бути використані для контролю і надання інформації про володіння об'єктом. Після створення їх неможливо змінити і вони є розподіленими, тобто вихідні дані контракту підтверджені усіма користувачами мережі. Вони дозволяють здійснювати транзакції без посередника.

Є різні типи блокчейну, що підтримують смарт-контракти; з них найбільший - *Ethereum*. Для розробки смарт контрактів використовують спеціальну мову - *Solidity*. Вона була створена для *Ethereum* і за синтаксисом нагадує *Javascript*. *Bitcoin* теж підтримує смарт-контракти.

2. Приклади застосування технологій блокчейну та смарт-контрактів для соціальних інновацій

• Цифрове голосування

Існуючі системи проведення голосувань недостатньо надійні та легко піддаються фальсифікаціям. Системи голосування на основі блокчейну будуть прозорими і максимально надійними, так як «голоси» будуть пов'язані в ланцюжок, що робить фальсифікацію надзвичайно складною.

• Захист особистих даних.

Використовуючи смарт-контракти, можливо захистити власні дані, упорядкувавши їх у блокчейн.

Наприклад, можна запровадити зберігання медичних даних у блокчейні і надати доступ до цих даних лише лікарям та лише за умови, що ми підтверджуємо доступ за допомогою цифрового підпису.

• Збереження ідентифікаційних даних.

Так само можна зберігати свої ідентифікаційні дані і вибирати, яку інформацію ми хочемо розкрити.

• Харчова індустрія

Приклад можливого використання: відстежування харчових продуктів з моменту їх збору/виготовлення до моменту потрапляння до покупця. Це надасть можливість створити цифровий сертифікат для кожної одиниці продукції, що підтверджуватиме її походження. У разі знаходження будь-якого роду порушення можливо відслідкувати його походження і миттєво вжити заходів та повідомити інших покупців.

• Автомобільна техніка

Наведемо приклад: злочини з одометром. Відомою практикою є зміна показників одометра і продаж автомобілів по ціні більшій, аніж мала б бути насправді.

У деяких країнах практикують фіксувати кілометраж автомобіля під час інспекцій, але, очевидно, що цього недостатньо. Вирішенням проблеми може стати заміна звичайних одометрів на розумні, що будуть підключені до мережі інтернет і записуватимуть пробіг автомобіля у блокчейн. Це дасть можливість створити електронний сертифікат для кожного автомобіля і відповідно кожен клієнт отримає доступ до історії автомобілів, що підключені до цієї системи.

• Страхові компанії.

Можуть використовувати смарт контракти для підтвердження запитів та розрахунку виплат.

Висновок

Технології блокчейну та смарт-контрактів можуть успішно використовуватись при впровадженні соціальних інновацій для захисту ідентифікаційних та особистих даних, при створенні систем обробки та зберігання даних та ін. Завдяки використанні функцій хешування, алгоритму консенсусу та децентралізації, блокчейн є надійною технологією, що гарантує безпечне зберігання даних у ньому.

Література:

1. Michael Casey and Paul Vigna. The truth machine: the blockchain and the future of everything. Picador, 2019, 336p.

2. Anthony Lewis. The basics of bitcoins and blockchains. Mango, 2018, 408p.

Напрям 3

Технічний захист інформації

ПРОГРАМНО-ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ ОХОРОННОЇ СИСТЕМИ

Бойко К., Полотай О.
Національний університет «Львівська політехніка»

Описано основні засоби і методи захисту інформації від несанкціонованого і таємного добування. Показано як можна захистити приміщення від зловмисників за допомогою охоронної системи. Описано криптографічний метод захисту інформації.
Ключові слова: захист інформації, охоронна система, крипто-захист.

The basic means and methods of protecting information from unauthorized and secret extraction is described. Shown how you can protect premises using the security system from intruders. The cryptographic method of information security is described.
Keywords: protection of information, security system, crypto-protection.

Захист інформації в сучасних умовах стає все більш складною проблемою, що обумовлено рядом обставин, основні з яких: масове розповсюдження засобів електронної обчислювальної техніки; ускладнення шифрувальних технологій; необхідність захисту не тільки державної і військової таємниці, але і промислової, комерційної і фінансової таємниць; збільшення можливостей несанкціонованих дій над інформацією.

Крім того, в даний час набули широкого поширення засоби і методи несанкціонованого і таємного добування інформації. Вони все більше застосовуються не тільки в діяльності державних правоохоронних органів, але і в діяльності різного роду злочинних угруповань.

Недобросовісна конкуренція, активізація дій терористів примушують суспільство звертати увагу на проблеми забезпечення безпеки, одним з найважливіших аспектів якої є інформаційна безпека.

Основні надії фахівці пов'язують з впровадженням інтегральних підходів і технологій. Необхідною умовою реалізації інтегрального підходу є блокування всіх технічних каналів витоку і несанкціонованого доступу до інформації, тому для створення ефективних систем безпеки, в першу чергу, необхідно досліджувати можливі канали витоку і їх характеристики.

Необхідно пам'ятати, що природні канали витоку інформації утворюються спонтанно, через специфічні обставини, що склалися на об'єкті захисту.

Що стосується штучних каналів просочування інформації, то вони створюються навмисно із застосуванням активних методів і способів отримання інформації. Активні способи припускають навмисне створення технічного каналу витоку інформації з використанням спеціальних технічних засобів. До них можна віднести незаконне підключення до каналів, проводів і ліній зв'язку, високочастотне наведення і опромінення, установка в технічних засобах і приміщеннях мікрофонів і телефонних закладних пристроїв, а також несанкціонований доступ до інформації, що обробляється в автоматизованих системах (АС) і т.д.

Тому особливу роль і місце в діяльності із захисту інформації займають заходи зі створення комплексного захисту, що враховують загрози національної і міжнародної безпеки і стабільності, зокрема суспільству, особі, державі, демократичним цінностям і суспільним інститутам, суверенітету, економіці, фінансовим установам, розвитку держави.

Здавалося б, на перший погляд, нічого нового в цьому немає. Потрібні лише відомі зусилля відповідних органів, сил і засобів, а також їх відповідне забезпечення всім необхідним.

Разом з тим, проблемних питань із захисту інформації багато, їх вирішення залежить від об'єктивних і суб'єктивних чинників, у тому числі і дефіциту можливостей.

Таким чином, проблема захисту інформації і забезпечення конфіденційності набуває актуальності.

Захистити приміщення від зловмисників можна шляхом встановлення охоронної системи.

Охоронна система – автоматизований комплекс для охорони різних об'єктів майна (будівель, включаючи прилеглу до них територію, окремих приміщень, автомобілів, водного транспорту, сейфів та ін.) Термін є узагальнюючим для декількох типів систем. Основне призначення – попередити, по можливості запобігти або сприяти запобіганню ситуацій, в яких буде завдано шкоду людям або матеріальним і не матеріальним цінностям, пов'язаних насамперед з діями інших осіб.

Дієвим способом програмно-технічного захисту інформації, є крипто-захист, тобто системи, що дозволяють шифрувати та дешифрувати інформаційні потоки. Традиційна криптографія виходила з того, що для шифрування та дешифрування використовується один і той же секретний ключ, який мав мати відправник повідомлення і отримувач. Одним з поширених, сьогодні, методів шифрування є алгоритм RSA, в основі якого кожен учасник процесу має власний таємний ключ та відкритий ключ, що не є секретним з допомогою якого проводиться обмін повідомленнями. Електронний цифровий підпис (ЕЦП) – це аналог власного підпису посадової особи в електронному вигляді.

Криптографічні методи захисту інформації широко використовуються в автоматизованих банківських системах і реалізуються у вигляді апаратних, програмних чи програмно-апаратних методів захисту. Використовуючи шифрування повідомлень в поєднанні з правильною установкою комунікаційних засобів, належними процедурами ідентифікації користувача, можна добитися високого рівня захисту інформаційного обміну.

Отже, надійно захистити приміщення ми зможемо за допомогою охоронної системи. Крім того, захист інформації в сучасних умовах стає великою проблемою, яку важко вирішити. Ми виявили, що криптографія є одним з найкращих засобів забезпечення конфіденційності і контролю цілісності інформації, також займає центральне місце серед програмно-технічних регулювальників безпеки.

Література:

1. Засоби і методи захисту інформації [Електронний ресурс]. – Режим доступу: http://kiev-security.org.ua/
2. Охоронна система [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Охоронна_система
3. Крипто-захист [Електронний ресурс]. – Режим доступу: https://buklib.net/books/28625/

ЕЛЕМЕНТИ БЕЗПЕКИ ТЕХНОЛОГІЇ SMART GRID

Гапонюк С.
Національний університет «Львівська політехніка», Львів, Україна

Анотація: Розглянуті основні напрямки Smart Grid та елементи забезпечення безпеки концепції.
Ключові слова: Smart Grid, інтегровані комунікації, SCADA-система, відновлювальні джерела енергії.

Summary: The basic directions of smart grid technology and elements of ensuring their safety are considered.
Keywords: Smart Grid, integrated communications, SCADA-system, renewable energy sources.

Актуальність: Процеси інтелектуалізації сьогодні в Україні розгортаються на рівні концепції Smart Grid(рис.1). З появою кіберзлочинності також з'явилось занепокоєння щодо безпеки інфраструктури, в основному тієї, що використовує комунікаційні технології. Є ризик, що можливості, сконструйовані для взаємодії між виробниками, лічильниками у домогосподарствах і виробництві у реальному часі, також можуть бути використані для злочинів або терористичних атак.

Основні напрямки технології Smart Grid: інтегровані комунікації, давачі та вимірювачі, високотехнологічні компоненти, інтелектуальне керування, інтерфейси та прийняття управлінських рішень.

Згідно з основними напрямками технології Smart Grid виникають загрози: на рівні комунікаційних технологій (меш-мережі), кібератаки на ланки взаємодії між виробником та отримувачем електроенергії, віддалений несанкціонований доступ до енергопостачання, використання шкідливого програмного забезпечення для SCADA-систем.

Рис.1. Характеристика Smart Grid

Безпека елементів: Серед комунікаційних технологій, що використовуються в розумних енергосистемах – стандарт ZigBee, який функціонує на рівні високорівневих протоколів зв'язку. Для ZigBee характерні загрози: використання помилок і вразливостей реалізації, використовуваних в системі протоколів і мережевих сервісних служб; можливості виникнення та прояви недокументованих властивостей мережевого обладнання при його функціонуванні на навантаженнях близьких до граничних; крадіжка фізичного пристрою; глушіння координатора. Технологіями забезпечення безпеки ZigBee відповідно до названих загроз є: застосування механізмів захисту мережевих протоколів; контроль за роботою апаратури мережі; керування доступом та захист від зчитування коду; обмеження і контроль доступу, що забезпечує конфіденційність, цілісність і доступність інформації.

Серед інтегрованих комунікацій - система SCADA призначена для: забезпечення функціонування систем збору, обробки, відображення, архівування інформації про об'єкт моніторингу/управління. Імовірними загрозами для SCADA-системи є: збої техніки (компонентів системи); атаки на людинно-машинний інтерфейс SCADA- системи; атаки на клієнтське програмне забезпечення SCADA-систем. Технологіями забезпечення безпеки SCADA-системи є: застосування автономних джерел живлення; застосування ефективної системи автентифікації та ідентифікації; постійне оновлення програмного забезпечення, що комплексно забезпечує конфіденційність, цілісність і доступність інформації.

АНАЛІЗ ТЕХНОЛОГІЙ ЕНЕРГЕТИЧНОГО ПРИХОВУВАННЯ СИГНАЛІВ

Клим О.
Національний університет "Львівська політехніка", м.Львів

Анотація: розглянуто технології енергетичного приховування, їх актуальність та принципи дії.
Ключові слова: глушіння, звукопоглинання, звукоізоляція.

Summary: technologies of energy signal concealment.
Keywords: signal silencing, sound absorption and isolation.

Актуальність енергетичного приховування сигналів. Енергетичне приховування сигналів вважається одним з найбільш актуальних та ефективних технологій захисту інформації в предметних сферах суспільства. Приховування забезпечується шляхом застосування способів та методів, які зменшують енергію носія або збільшують енергію перешкод. Для отримання максимального результату використовують комплекс методів і засобів приховування сигналів. Розглянемо деякі з них.

Методи енергетичного приховування сигналів. Для створення безпечного простору зберігання, оброблення та передавання інформації використовують основні види технологій приховування сигналів: звукопоглинання, звукоізоляція, глушіння, зашумлення [1].

Глушіння акустичних сигналів. Глушіння використовують для створення перешкод в процесі передавання сигналу у безпровідних системах зв'язку. Засобами глушіння є генератори електромагнітних перешкод у відповідному частотному діапазоні технологій зв'язку (рис. 1).

Рис. 1. Схематичне зображення принципу роботи глушіння за допомогою генератора перешкод

Звукопоглинання та звукоізоляція. Дані технології приховування спрямовані на ослаблення акустичного сигналу з метою унеможливлення його виділення на фоні природніх шумів. Використовуючи названі методи досягають співвідношення сигнал/шум до значення, що виключає можливість добування інформації зловмисниками за межами контрольованої зони. Оскільки середній рівень розмови в приміщенні становить 50 – 60 дБ, тому звукоізоляція, залежно від категорії, повинна бути не менша припустимих норм (табл.1).

Табл.1.

Припустимі норми звукоізоляції

Частота , Гц	**Звукоізоляція, дБ**
500	53
4000	55

Зашумлення, генератори шумів. В ряді випадків, незважаючи на застосування пасивних методів захисту, на межі контрольованої зони відношення сигнал/шум перевищує допустимі значення. У цьому випадку використовуються активні заходи захисту, до яких і відноситься зашумлення, основним засобом для реалізації якого є генератор шуму. Генератори шуму в мовному діапазоні використовуються для захисту від несанкціонованого видобування акустичної інформації шляхом маскування безпосередньо корисного звукового сигналу. Розглянемо один з них. Даний комплекс віброакустичного захисту під назвою «Барон», призначений для захисту об’єктів інформатизації 1 категорії та протидії технічним засобам перехопленням мовної інформації (рис.2).

Рис 2. Комплекс віброакустичного захисту «Барон»

«Барон» має чотири канали формування перешкод, до кожного з яких можуть підключатися віброперетворювачі п’єзоелектричного або електромагнітного типу, а також акустичні системи, що забезпечують перетворення електричного сигналу, який формується приладом, в механічні коливання в

огороджувальних конструкціях, а також в акустичні коливання повітря. Робочий діапазон частот даного комплексу становить від 60 до 16000 Гц, які розбиваються на менші частотні піддіапазони. Здатний генерувати різні види перешкод для забезпечення максимального рівня безпеки В даний час в основному застосовуються системи просторового зашумлення, які використовують перешкоди типу "білий шум", тобто випромінюють широкосмуговий шумовий сигнал (як правило, з рівномірно розподіленим енергетичним спектром у всьому робочому діапазоні частот), що істотно перевищує рівні побічних електромагнітних випромінювань (рис.3).

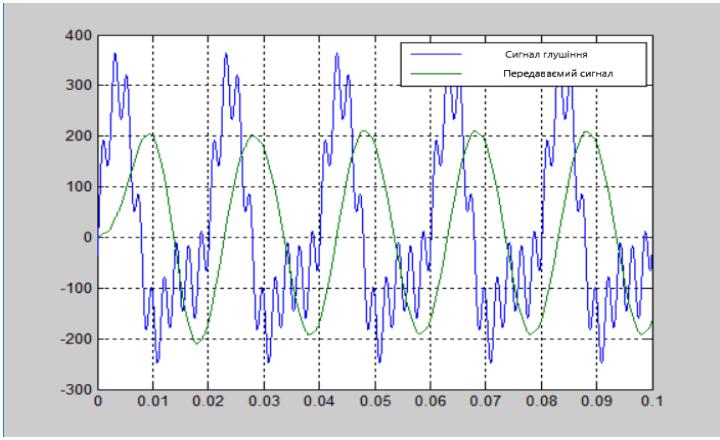


Рис. 3. Принцип накладання шуму на акустичний сигнал

Висновок: Проаналізовано деякі технології енергетичного приховування акустичних сигналів.

Література:

1) Um.co.ua [Електронний ресурс] : [Веб-сайт]. – Способи та засоби енергетичного приховування акустичного сигналу. – режим доступа : http://um.co.ua/6/6-6/6-65546.html (дата звернення 09.11.2019). – Назва з екрана.

АНТЕНИ ДЛЯ РАДІОСИГНАЛІВ: КЛАСИФІКАЦІЯ, ХАРАКТЕРИСТИКИ

Наконечний В., Кравець В.
Національний університет "Львівська політехніка"

Антени у сучасному світі використовуються більшістю приладів які працюють безпровідникового від домофонів до космічних шатлів. Антени були потрібні є і будуть використовуватись у майбутньому оскільки безпровідникові апарати використовуються все більше.

Антена – радіотехнічний пристрій для передавання/приймання електромагнітних хвиль. Принцип дії антен ґрунтується на дипольному випромінюванні. Сигнал передається від високочастотного генератора у простір. При прийманні сигналу електромагнітні хвилі наводять в приймальній антені струми, які за необхідності підсилюються і демодулюються приймачами.

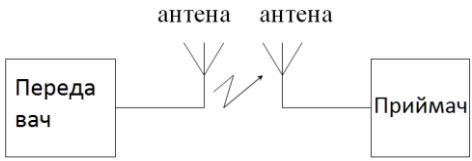


Рис.1. Структурна схема принципу дії антени

Антени класифікуються за : 1) за функціональним призначенням які поділяються на приймальні, передавальні, зв'язкові, телевізійні, радіолокаційні, бортові; 2) за конструкторсько-технологічними ознаками це - рупорні, спіральні, друковані, дзеркальні, щілинні, лінзові, вібраторні; 3) за електродинамічними або електричними властивостями та параметрами і за способом формування випромінюваного поля які в свою чергу поділяються на класи: (випромінювачі невеликих розмірів $l \leq \lambda$ для діапазонних частот 10кГц – 1ГГц; антени біжучої хвилі розмірами від λ до 10 λ для діапазонних частот 3МГц – 10ГГц.; антенні решітки розмірами від λ до 100 λ для частот 3Мгц – 30ГГц.; апертурні антени розмірами від λ до 1000 λ для діапазонних частот 100МГц – 100ГГц та вище.).Також можливі і класифікації: 1)за діапазоном довжин хвиль це антени ДХ (довгих), СХ (середніх), КХ (коротких), УКХ (ультракоротких), НВХ (наддовгих); 2) за відносною шириною смуги пропускання – широкосмугові, над-широкосмугові, діапазонні, вузькосмугові, резонансні; 3) за поляризаційною ознакою: антени кругової, еліптичної, лінійної, вертикальної, горизонтальної поляризації і антени можуть розрізнятися своїми спрямованими властивостями (спрямовані, слабкоспрямовані, ненаправлені);

Кожна антена характеризується як пасивний лінійний пристрій який може працювати в режимах передавання і прийому. В обох режимах антена характеризується спрямованими, поляризаційними, фазовими властивостями і вхідним опором. До основних характеристик і параметрів, що описує ці властивості, відносяться: Діаграма спрямованості передавальної (приймальної) антени характеризує інтенсивність випромінювання (прийому) антеною в різних напрямках. Для передавальної антени використовують ДН по напруженості поля в електричної складової електромагнітного поля або за рівнем його потужності. Коефіцієнт спрямованої дії антени - визначається як відношення щільності потужності випромінювання, що створюється антеною в даному напрямку на даному відстані, до щільності потужності випромінювання, що створюється на тій же відстані і в тому ж напрямку деякої стандартної антеною, за умови, що випромінюються обома антенами потужності однакові. Як стандарт антени використовують ізотропний випромінювач, або в деяких випадках, ідеальний півхвильовий диполь або ідеальний чотирьохвильовий штир. Поляризація - взаємне зміщення векторів магнітного та електричного поля електромагнітної хвилі при її поширенні у вільному просторі

Для прикладу класифікацій антен розглянемо 3G/4G GSM і телеком-антену.

3G/4G GSM. за функціональним значенням антена приймальна її діапазон частоти 1,700 - 2,170 ГГц, за конструкторсько - технологічними ознаками – вібраторна і за відносною шириною вузькосмугова антена Властиві спрямовані властивості за поляризаційною ознакою – вертикальна за способом формування випромінювального поля – належить до антен біжучої хвиліРекомендується використовувати в радіусі до 20 км від передавальної базової станції в зонах, де рівень сигналу дорівнює 0 або нестабільний.

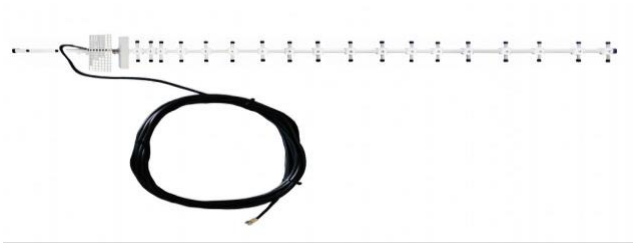


Рис. 3. 3G/4G GSM антена

Телеком-антена. за функціональним значенням антена телевізійна і її максимальний діапазон довжини хвилі 30 км. За конструкторсько - технологічними ознаками – антена вібраторна, за відносною шириною це діапазонна антена їй властиві діапазонні властивості ,за поляризаційною озна-

кою – еліптична і за способом формування випромінювального поля – антена решітка. Ця антена складається з адаптúвної антéнної решíтки (ААР) - тип антенної решітки, в якій динамічна зміна параметрів і характеристик здійснюється адаптивно до впливів зовнішніх або внутрішніх факторів. Як правило, таким чинником є наявність активних завад, за присутності яких можливість адаптації підвищує якість прийому сигналів.

Рис.4. Телеком-антена

Висновки: Антени на сьогодні використовуються майже у всіх приладах які мають беспровідникове підключення,тому від їх захисту залежать ваша безпека

Література:

1. Міжнародний научно-інформаційний портал “ Studopedia ” Основні характеристики та параметри антен. – [Электронный ресурс]. – Режим доступа: http://www.hydrogen.ru/ifsseht2000/projects/1580censor.html

ПОНЯТТЯ, СУТНІСТЬ ТА ЦІЛІ ЗАХИСТУ ІНФОРМАЦІЇ

Шевцова Л., Мирошниченко В.
Дніпропетровський державний університет внутрішніх справ

Анотація. В роботі розглянуті напрями, технології і засоби забезпечення інформаційної безпеки, методи реалізації безперервного процесу захисту інформації.
Ключові слова: виявлення загроз, механізми захисту інформації, рівень захищеності, умови виникнення загроз.

Summary. The directions, technologies and means of providing information security, methods of realization of continuous process of information protection are considered in the work.
Keywords: detection of threats, mechanisms of information protection, security level, conditions of occurrence of threats.

Сутність захисту інформації полягає у виявленні, усуненні або нейтралізації джерел негативних впливів, причин і умов впливу на інформацію. Ці джерела становлять загрозу безпеки інформації. Мета й методи захисту інформації відображають її сутність.

Захист інформації забезпечується за наступними напрямами:

- ідентифікація загроз;
- виявлення загроз, тобто реальних загроз і конкретних злочинних дій;
- попередження загроз шляхом впровадження превентивних заходів для забезпечення інформаційної безпеки спрямованих на уникнення умов їх виникнення;
- нейтралізація загроз завдяки застосуванню корегуючих заходів та засобів;
- локалізація загроз що передбачає виключення можливості поширення загроз за межі певної припустимої області;
- ліквідація загрози або конкретних злочинних дій;
- ліквідація наслідків загроз та злочинних дій і відновлення попереднього стану.

Враховуючи викладене, захист інформації можна визначити як діяльність із застосуванням певної сукупності методів, засобів і заходів, що спрямовані на забезпечення інформаційної безпеки держави, суспільства й особи у всіх областях їх життєво важливих інтересів.

Основними цілями захисту інформації є унеможливлення або мінімізації ризиків реалізації загроз безпеки особи, суспільства та держави внаслідок:

- витоку, розкрадання, втрати, викривлення, модифікації, підробки інформації;
- несанкціонованих дій по знищенню, викривленню, копіюванню, блокуванню інформації у комп'ютерних системах;
- порушення прав суб'єктів інформаційних процесів при розробці, виробництві й застосуванні інформаційних систем, технологій і засобів їх забезпечення.

З аналізу загроз безпеки інформації, цілей і завдань її захисту випливає, що досягти необхідного рівня захищеності можна тільки за рахунок певних принципів захисту інформації, до яких належіть комплексне використання існуючих методів і засобів захисту, безперервну реалізацію заходів із захисту інформації, необхідність та достатність комплексу засобів та заходів, адекватність витрат на захист вартості можливої шкоди внаслідок реалізації загроз [1].

Мета захисту інформації на об'єктах захисту може бути досягнута за умов проведення комплексу робіт з наступних напрямків:

- визначенню охоронюваних відомостей;
- виявленню можливих технічних каналів витоку інформації;
- аналізу можливостей і небезпеки несанкціонованого доступу до інформаційних об'єктів;
- аналізу небезпеки знищення або викривлення інформації за допомогою програмно-технічних впливів на об'єкти захисту;
- розробці й реалізації організаційних, технічних, програмних і інших засобів і методів захисту інформації від усіх можливих загроз;
- створенню комплексної системи захисту.

Процес захисту інформації повинен здійснюватися безупинно на всіх етапах. Реалізація безперервного процесу захисту інформації можлива тільки на основі систем концептуального підходу й промислового виробництва засобів захисту, впровадження надійних механізмів захисту й забезпечення їх сталого функціонування й високої ефективності, провадження відповідних робіт тільки фахівцями високої кваліфікації в області захисту інформації [2].

Список літератури:

1. Ленков С.В., Перегудов Д.А., Хорошко В.А., Методы и средства защиты информации/ под. ред. В.А.Хорошко. – К.: Арий, 2008. – Том I. Несанкционированное получение информации, – 464 с.

2. Ленков С.В., Перегудов Д.А., Хорошко В.А., Методы и средства защиты информации/ под. ред. В.А.Хорошко. – К.: Арий, 2008. – Том II. Информационная безопасность, – 344 с.

Напрям 4

Безпека інформації у хмарних сховищах

БЕЗПЕКА ІНФОРМАЦІЇ У ХМАРНИХ СХОВИЩАХ

Віблий В.М., Смотр О.О.
Львівський державний університет безпеки життєдіяльності, м. Львів

Роботу присвячено аналізу сучасних технологій зберігання даних з використанням засобів «хмарних сховищ» віртуальних серверів. Надано рекомендації щодо вибору кращого «хмарного сховища».
Ключові слова: інформаційні технології, сервер, зберігання інформації, хмарні технології, хмарне сховище.

The article is devoted to the analysis of modern technologies of data storage using the means of "cloud repositories" of virtual servers. Recommendations for choosing the best cloud storage are provided.
Key words: information technology, server, storage of information, cloud technologies, cloud storage service.

Хмарне сховище (англ. cloud storage) – модель схову даних, де цифрові дані зберігаються в логічні пули, а фізичне зберігання охоплює кілька серверів (і часто в різних місцях (локаціях)), фізичне середовище, як правило, належить хостинговим компаніям, вони ж керують цим середовищем [1].

Хмарні сховища, та їх сервіси стають все популярнішими, адже вони не лише забезпечують місце для зберігання великих об'ємів даних та постійний доступ до них із будь-якого розташування. Їх сервіси спрощують синхронізацію файлів, роботу через Інтернет і співпрацю над документами вважають. Однак, незважаючи на це, згідно з даними компанії Microsoft, понад 50 відсотків організацій вважають хмарне сховище найризикованішою категорією програм [2]. Адже досі не існує універсальної моделі, яка здатна забезпечити надійне збереження інформації. 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. До 2019 року ринок рішень безпеки для хмарних середовищ досягне 8,71 мільярда доларів США [2].

Щоб уникнути витоку даних багато компаній розробляють власні механізми захисту, які працюють за якимись конкретними принципах, оскільки загальних положень щодо цього не існувало. Згодом певні зведення правил почали з'являтися і за рахунок цього розроблені форми захисту стали чимось схожі між собою. Перш за все почали впроваджувати спеціальні стандарти безпеки, які доводиться дотримуватися всім власникам IT-структур. Мова йде про ISO/IEC 27017, який є стислим керівництвом щодо заходів безпеки даних в хмарних сервісах. Додатково треба звернути увагу на стандарт ISO/IEC 27018, який являє собою звід практик, щодо захисту персональних даних в ситуації, коли вона зберігається в публічних хмарах. Дотримуючись міжнародних стандартів можна довести систему захисту до досконалості і при цьому сертифікувати її (отримавши підтвердження її функціональності і надійності). В результаті відповідні органи не зможуть пред'явити претензії і вимагати негайного припинення зберігання персональних даних або їх надання. Однак, далеко не всі постачальники хмарних сховищ надають однаково якісні послуги, зокрема якщо це стосується захисту.

Розглянемо та проаналізуємо ряд найпопулярніших на сьогодні хмарних сховищ:

– Google Диск – безумовний лідер серед хмарних сховищ. До його переваг можна зарахувати: – 15 Гб простору безкоштовно, однак слід зауважити, що ці 15 Гб є загальними для усіх служб Google (Gmail, Google+ і т.п.); – вбудований офісний пакет Googel Docs; –– наявність розширень, які можуть забезпечити здійснення всіх необхідних операцій з файлами: офісну роботу, прослуховування музики, перегляд відео, роботу з архівами, безпосередньо в хмарному сховищі, з браузера, без необхідності завантаження файлів на пристрій.

– Dropbox – одне з найстаріших хмарних сховищ. На безкоштовній основі виділяє лише 2 Гб вільного простору, однак постійно проходять акції з безкоштовного збільшення обсягу зберігання. Для прикладу, ще 19 ГБ безкоштовного простору можна отримати шляхом запрошення друзів.

– Яндекс.Диск – заручився підтримкою Microsoft Office Online, що забезпечує його користувачам можливість працювати з офісними документами прямо в браузері. Надає 10 Гб безкоштовного простору, максимальний розмір файлу 3 ГБ.

– Box – до переваг можна віднести: 10 Гб безкоштовного простору; шифрування даних; вбудований записник; стабільність. Як недолік, дане сховище більше зорієнтоване на бізнес сегмент, для безкоштовних користувачів, є ряд обмежень: обмеження розміру файлів до 250Мб; обмеження швидкості завантаження тощо.

– Copy – сховище Copy радує своєю стабільністю. Воно просто дає 15 Гб вільного простору і працює стабільно. Ніяких перебоїв і ніяких інших проблем. Воно просто синхронізує всі ваші дані, а саме це є головним критерієм для будь-якого хмарного сховища. Однак бракує цьому сховищу екосистеми, зв'язку з іншими сервісами та додатками і можливості відкри-

ти хоч якісь типи файлів прямо в хмарі, без необхідності завантаження їх (зараз мова йде про веб-версію).

– OneDrive – хмарне сховище від Microsoft, яке прийшло на зміну закритому SkyDrive. Висока швидкість роботи, 5 Гб безкоштовного простору і інтеграція з Microsoft Office Online (надає можливість працювати з документами Microsoft Office в режимі реального часу з іншими користувачами) підтримує завантаження знімків із смартфона.

– SpiderOak – переваги: - високий рівень захищеності, вважається одним з найбезпечніших сховищ даних; - кросплатформенність (додатки під велику кількість операційних систем). Недоліки - безкоштовно дається тільки 2 Гб вільного місця; втрачений пароль до зашифрованих даних неможливо відновити, відсутність авторизації у веб-інтерфейсі.

– iCloud – зберігає настройки, дані користувачів пристроїв від Apple, через нього відбувається синхронізація величезної кількості файлів і багато іншого. Однак, навіть на операційних системах від Apple при роботі з iCloud може виникнути проблема, з Windows версією все ще гірше, а на інших системах і зовсім немає даного сховища.

– MEGA – дає 50 Гб безкоштовного простору, зручний інтерфейс, задекларованне забезпечення конфіденційність і всебічне шифрування. До недоліків можна зарахувати - відносно невисоку швидкість доступу, ліміти на трафік.

Підсумовуючи вищенаведене можна зауважити, що ідеального хмарного сховища на всі випадки життя не існує. Кожен користувач повинен сам визначити, що для нього його пріоритетним: безпека, об'єм наданого простору, вартість тощо. Якщо Вашим пріоритетом є об'єм інформації, яку можна розмістити, то зверніть увагу на такі хмарні середовища, як Box або Mega. Якщо на першому місці у Вас стабільність, мабуть варта обрати Google Drive, адже стабільність, підключення до інших сервісів Google, 15 Гб пам'яті і вбудований пакет Google Docs забезпечують стабільність. Однак саме безпека має бути першою в списку пріоритетів і, говорячи про неї, обов'язково слід звернути увагу на такі аспекти, як наявність у хмарного середовища: протоколу підтримки HTTPS та інших протоколів безпеки; надійного положення про конфіденційність; чітких формулювань в угоді про обслуговування та солідної репутації.

Література:

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

2. Офіційний сайт Microsoft [Електронний ресурс] – Режим доступу до ресурсу: https://www.microsoft.com/uk-ua/microsoft-365/growth-center/resources/6-security-red-flags-when-identifying-the-perfect-cloud-storage-solution?SilentAuth=1&f=255&MSPPError=-2147217396.

ІНФОРМАЦІЙНА БЕЗПЕКА ХМАРНИХ СЕРВІСІВ

Градищук М.
Ірпінський економічний коледж»

Анотація. Інформаційна безпека хмарних сервісів є невід'ємною частиною безпечного користування та захисту даних користувачів. Загалом процедура захисту даних потребує найжорсткіших вимог інформаційної безпеки.
Ключові слова: Хмарні сервіси, хмарні обчислення, хмари, інформаційна безпека, дані.

Abstract. Information security cloud services are an integral part of safe use and the protection of user data. In general, the data protection procedure requires the most stringent information security requirements.
Keywords: Cloud services, cloud computing, clouds, information security, data.

Сучасні підприємства знаходяться під постійним впливом факторів, пов'язаних із розвитком технологій, які, з одного боку, спрощують роботу з великими обсягами інформації, проте, з іншого – зумовлюють проблеми, пов'язані насамперед з інформаційною безпекою. Однією із таких технологій є хмарні сервіси (хмарні обчислення), що з'явилися в 2006 році, коли Amazon's Elastic Computing Cloud побудували свої дата-центри. Нині завершується ранній етап розвитку хмарних технологій, які характеризуються новаторськими експериментами, нестійкістю бізнес-моделей, невирішеними питаннями їх інформаційної безпеки [1, с. 75-80].

Поява хмарних технологій спровокувала розгортання великомасштабних розподілених систем для постачальників програмного забезпечення. Хмарні системи забезпечують просту й уніфіковану взаємодію між постачальником і користувачем і включають програмне забезпечення, тобто сервісну підсистему, та базу даних із багаторазовим доступом. Ці системи динамічно розподіляють обчислювальні ресурси у відповідь на запити про резервування ресурсу користувачем і, відповідно, до певних стандартів якості обслуговування користувачів [2, с. 104-108].

Загалом процедура захисту даних побудована на конфіденційності, цілісності та доступності. Конфіденційність належить до так званої прихованої функції фактичних даних або інформації і є однією із найжорсткіших вимог інформаційної безпеки. У випадку хмарних обчислень дані накопичуються в центрах обробки даних, де безпека та конфіденційність даних ще важливіші. Цілісність даних у будь-якому вигляді не відіграє значної ролі для гарантії несанкціонованого видалення, зміни або пошкодження. Доступність даних означає, що користувачі можуть використовувати дані за рахунок використання потенціальних можливостей хмарних технологій.

Також для захисту даних використовується тришарова захисна структура системи, кожен шар якої виконує свої власні завдання для забезпечення захисту даних на всіх рівнях «хмари».

Перший шар відповідає за аутентифікацію користувачів цифрових сертифікатів, виданих відповідними органами; управляє кодами доступу користувачів.

Другий шар відповідальний за шифрування даних користувача, а також захист конфіденційності користувачів у певний спосіб.

Третій шар – використання даних користувача для швидкого відновлення.

Захист усієї системи – це останній рівень даних користувача. За допомогою трирівневої структури аутентифікація користувача використовується для забезпечення цілісності даних. Якщо в системі аутентифікації користувача відбулося нелегальне втручання і небезпечний користувач входить в систему, шифрування файлів і захист конфіденційності можуть забезпечити цей рівень захисту. На цьому рівні дані користувача зашифровуються у випадку, якщо ключ доступу був введений нелегально. Через функцію захисту конфіденційності небезпечний користувач не зможе отримати повного доступу до інформації, що дуже важливо для захисту комерційних таємниць ділових користувачів у середовищі хмарних обчислень [3].

Загалом ідея доступних комп'ютерних послуг стає реальністю. Можливості «хмар» дозволяють розв'язувати завдання бізнесу та надавати користувачам сервіси в коротші терміни. Центри обробки даних отримують можливість надавати свої послуги більшій кількості користувачів. Розробники можуть думати про нові генерації своїх продуктів. Програмні застосування майбутнього матимуть частину, що працює на комп'ютері користувача, та частину, що працює у «хмарі». Мають бути розроблені системи керування енергетичним забезпеченням, щоб зробити можливим переведення у режим енергозбереження сервери разом з усією пам'яттю та мережею. І це також є одним з елементів інформаційної безпеки. Питання інформаційної безпеки технології хмарних сервісів потребують значного вдосконалення, а в багатьох аспектах – першочергових розробок і напрацювань.

Література:

1. Бондар Є. С. Хмарні обчислення та їх застосування / Є. С. Бондар, М. М. Глибовець, С. С. Гороховський // Вісник КНУ ім. Т. Шевченка. – Вип. № 1. – К.: КНУ, 2011. – С. 74–82.

2. Гудзовата О. О. Хмарні сервіси: можливості, безпека, перспективи: колективна монографія: у 4 т. / О. О. Гудзовата // Теоретичні та прикладні аспекти підвищення конкурентоспроможності підприємств. – Дніпропетровськ: «Герда», 2013. – Т. 1 – 352 с. (Розділ 1.12). – С. 102–110.

3. Сороківська О. А. Інформаційна безпека підприємства: нові загрози та перспективи / О. А. Сороківська, В. Л. Гевко. [Електронний ресурс]. – Режим доступу: http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf

БЕЗПЕКА ПЕРЕДАЧІ ДАНИХ МІЖ ПРИСТРОЯМИ В БЕЗПРОВІДНИХ СЕНСОРНИХ МЕРЕЖАХ ІОТ

Гузела Н., Белей Н.
Національний університет «Львівська Політехніка»

Розглянуто основні проблеми безпеки пов'язані з тим, що існуючі методи та засоби захисту спочатку були розроблені для настільних комп'ютерів і не враховували особливостей та обмежень Інтернету речей.
Ключові слова: Інтернет речей, підключення до мережі, система безпеки, стандартизація, автентифікація, контроль доступу.

The main security issues are related to the fact that the existing security methods and remedies were originally designed for desktops and did not take into account the particularities and limitations of the Internet of Things.
Keywords: Internet of things, network connectivity, security system, standardization, authentication, access control.

З огляду на особливості вимірювальних пристроїв, а також їх різну природу вимірювань, питання безпеки мережевої взаємодії потребують розгляду нових аспектів. Більшість виявлених загроз безпеки стосувалися незашифрованих даних, збору персональних даних, вразливого користувальницького інтерфейсу та небезпечних зв'язків. Сьогодні, поряд з адаптацією існуючих технологій безпеки, важливе значення мають питання стандартизації в галузі Інтернету речей [1].

Підходи до побудови системи безпеки повинні враховувати кожен із структурних елементів і все ж вирішувати проблеми, що виникають при поєднанні декількох пристроїв та створенні мережі. Пропозиції щодо захисту інформації в Інтернеті речей спрямовані на підвищення безпеки пристроїв, мереж та даних [2].

Безпека повинна забезпечуватися як протягом усього періоду функціонування виробу, так і після його виведення з експлуатації. Криптографічні ключі не повинні зберігатися у енергонезалежній пам'яті пристрою у відкритому вигляді. Крім того, може бути передбачено утилізацію виведених з експлуатації пристроїв.

Особливості Інтернету речей накладають обмеження на побудову системи безпеки в такій мережі. Звичайних методів захисту інформації в бездротових мережах може бути недостатньо, або вони можуть бути непридатними через обмеження, накладені Інтернетом речей.

Пропонований протокол забезпечує роботу в сценаріях з потенційно нестабільним з'єднанням від керуючого центру до системи користувача, а також у випадку можливості встановлення прямих з'єднань між делегованим пристроєм та автентифікацією різних користувачів .

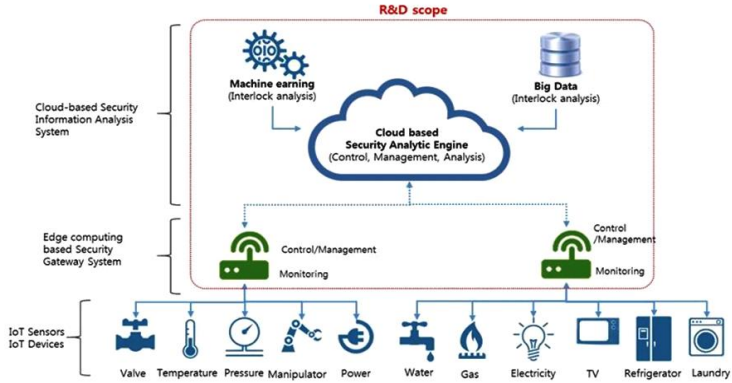


Рис. 1. Схема покрокової реалізації захисту передачі даних у безпровідних сенсорних мережах IoT.

Протокол автентифікації для делегування прав на використання електронних пристроїв складається з певних оперативних етапів (етапів): (1) початкове об'єднання нового пристрою; (2) передача пристрою протягом певного періоду часу; (3) повернення пристрою у користування власником; (4) дисоціація пристрою.

Під час роботи протоколу вводиться ключ MC, який асоціюється з користувачем Alice. Цей ключ дозволяє забезпечити симетричне шифрування даних, що передаються та зберігаються на DED, а також служить додатковим захистом від витоку конфіденційної інформації користувача Alice, що зберігається на окремому DED. Подальші кроки протоколу позначені відповідними номерами на рис. 2.

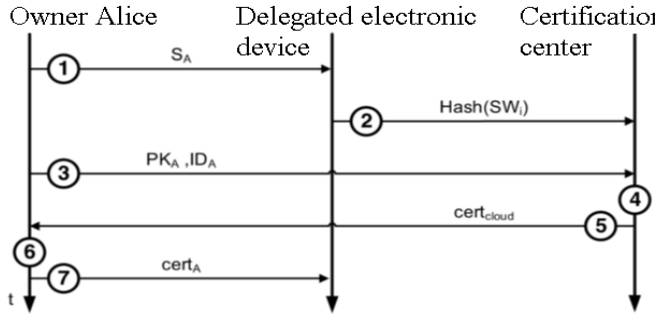


Рис. 2. Схема реалізації передачі даних від вимірювального пристрою до користувача даних в безпровідній сенсорній мережі.

1. Користувач Alice генерує секретний ключ MC для нового DED wi та передає його по захищеному каналу.

2. DED w_i передає результат виконання хеш-функції від власного програмного забезпечення до MC за допомогою захищеного каналу (*(hash (SW$_i$))*

3. Користувач Аліса передає свій відкритий ключ PKA та IDA до США.

4. MC генерує сертифікат США для Alice. Сертифікат має вигляд $cert_A = sign_{cloud}(w_i, ID_A, hash(SW_i))$. Цей крок виконується з метою забезпечення цілісності системних даних.

5. MC, використовуючи захищений канал, передає сертифікат користувачеві Alice.

6. Користувач Аліси підписує сертифікат, отриманий від MS, своїм знаком $cert_A = sign_A(cert_{cloud})$.

7. Користувач Alice подає сертифікат до DED

Представлений протокол автентифікації для моніторингу електронних пристроїв, розроблений для використання в умовах нестабільного зв'язку з центром сертифікації. Алгоритми, що реалізують етапи функціонування запропонованого протоколу, можуть бути реалізовані як у вигляді програмного забезпечення для універсального комп'ютера будь-якої архітектури, так і у вигляді апаратного забезпечення для спеціалізованого комп'ютера будь-якої архітектури. Протокол можна використовувати в місцях з відсутністю інфраструктури, оскільки для здійснення делегування не потрібно постійного з'єднання з центром сертифікації.

Література:

1. O. Belej, N. Nestor, O. Polotai and J. Sadeckii. Features of Application of Data Transmission Protocols in Wireless Networks of Sensors // *3rd International Conference on Advanced Information and Communications Technologies (AICT).* – IEEE, Lviv, Ukraine, 2019. – pp. 317-322.

2. O. Belej, N. Nestor and O. Polotai. Developing a Local Positioning Algorithm Based on the Identification of Objects in a Wi-Fi Network of the Mall // *IEEE XVth International Conference on the Perspective Technologies and Methods in MEMS Design (MEMSTECH).* – IEEE, Lviv, Polyana, Ukraine, 2019. – pp. 32-36.

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ЗАХИСТ ПЕСОНАЛЬНИХ ДАНИХ В ХМАРНИХ СЕРВІСАХ

Дулова О.
Ірпінський економічний коледж

Анотація: Дедалі популярнішими в сфері інформаційних технологій стають хмари, разом з цим змінюються і потреби в забезпеченні безпеки даних. Слід за хмарними сервісами для бізнесу з'явилися хмарні сервіси для інформаційної безпеки, або безпеку як послуга. Розглянуто питання інформаційної безпеки у хмарних сервісах, описано рішення безпеки як послуги - Security as a Service (SecaaS), в якій сервіс-провайдер послуг безпеки інтегрує свої сервіси в корпоративну інфраструктуру замовника.
Ключові слова: безпека, захист персональних даних, хмарні сервіси, технології, безпека як послуга

Abstract: Clouds are becoming increasingly popular in the field of information technology, and so are the needs for data security. Following on from cloud services for business, cloud services have emerged for information security, or security as a service. Information security issues in cloud services are discussed, security solutions as a service are described - Security as a Service (SecaaS), in which a security service provider integrates its services into the customer's corporate infrastructure.
Keywords: security, protection of personal data, cloud services, technologies, security as a service

В сучасному світі, поряд із шаленим розвитком інформаційного суспільства, важливу роль відіграє питання його захисту, захисту інформаційної безпеки.

Для розвитку інформаційного суспільства притаманне поєднання глобальних інформаційно-комунікаційних систем, впровадження баз даних та знань, зростання спектру послуг і сервісів, різке збільшення клієнтського навантаження на серверний простір. Результатом еволюційного розвитку інформаційних технологій стали «хмарні технології». За їх допомогою стає можливим вирішення виниклого протиріччя – невідповідності між зростанням обсягів інформаційних потоків і мережевих сервісів та сучасним технічним станом програмно-апаратного забезпечення мережевої інфраструктури інформаційних систем [2]. Під час використання хмарних технологій програмне та технічне забезпечення надається користувачеві як Інтернет-сервіс; він має доступ лише до власних даних, а не до інфраструктури, операційної системи і програмного забезпечення, з якими працює. “Хмара” – це Інтернет, який приховує усі технічні деталі.

Стрімке опанування хмарних технологій ІТ-компаніями, застосування у малому та середньому бізнесі, у навчальному процесі, для управ-

ління підприємствами – все це свідчить про черговий якісний стрибок у сфері інформаційних технологій. З іншого боку, «важливе рішення щодо використання хмарних технологій несе в собі реальні загрози безпеки бізнесам, якими вони керують, і це може розглядатися, як новий технологічний, економічний, фінансовий виклик XXI ст.» [1] .

Насправді, застереження з боку власників підприємств, які використовують у своїй роботі хмарні сервіси були завжди. Справа в тому, що досі не існує універсальної моделі, яка могла б забезпечити надійне збереження інформації. Якщо дані потрапляють до зовнішньої 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. Щоб уникнути витоку даних компанії розробляють власні механізми захисту, які працюють запевними принципами, оскільки загальних положень щодо цього не існувало [4].

Безпека як послуга, або Security as a Service (SecaaS) - це бізнес-модель, в якій сервіс-провайдер послуг безпеки впроваджує свої сервіси в корпоративну інфраструктуру замовника. При цьому сукупна вартість володіння для компанії знижується за рахунок хмарної архітектури рішень, оплати сервісів за підпискою і відсутності капітальних витрат для замовника. Деякі категорії SecaaS вже звичні - антивірусна і антиспам-фільтрація електронної пошти в хмарі, сервіси захисту від DDoS-атак. Все більше підсистем безпеки йдуть в хмару, так як це дозволяє захищати дані в нових IT-системах і пристосовуватися до мінливої IT-інфраструктури. SecaaS-рішення, що базуються на хмарних технологіях, на відміну від традиційних засобів захисту, архітектурно краще підходять для захисту даних в новій IT-інфраструктурі, до якої відносяться:

– Мобільні співробітники з ноутбуками, смартфонами і планшетами. Приклад – традиційні засоби контролю веб-доступу і URL-фільтрації, що встановлюються всередині периметра компанії, не здатні захищати доступ віддалених співробітників з їх різноманітних пристроїв.

– Динамічна і масштабована інфраструктура веб-додатків. Приклад: традиційний «коробковий» Web Application Firewall, що встановлюється всередині периметра, не зможе захистити веб-додаток, динамічно розгорнуте в декількох дата-центрах. Хмарний Web Application Firewall, що надається по SaaS-моделі, здатний економічно ефективно впоратися із завданням захисту веб-додатків в сучасних інфраструктурах.

– Хмарні сервери, інфраструктура як сервіс (IaaS), гібридні хмари. Для прикладу візьмемо базові підсистеми безпеки - міжмережеве екранування і виявлення вторгнень. У традиційній корпоративної інфраструктурі ці підсистеми безпеки реалізуються на апаратних платформах. Але для серверів в публічній або гібридної IaaS-інфраструктурі необхідні більш гнучкі рішення – так на сцену вийшли host-based кошти мережевої безпеки.

Найбільшу цінність і зручність керування надають SecaaS-рішення, які інтегруються з інтерфейсами управління IaaS-платформи.

Не тільки вигоди SaaS застосовні до SecaaS, але і ризики. Перед запуском SecaaS, як у випадку з іншими хмарними рішеннями, необхідно провести оцінку ризиків, пов'язаних з передачею своїх даних і систем третій стороні і з потенційною доступністю цих даних через інтернет. До слова, більшість SecaaS-вендорів серйозніше інших виробників SaaS відносяться до інформаційної безпеки та захищеності своїх сервісів. Розробники SecaaS-рішень часто відкрито заявляють про застосовувані заходи захисту, які використовуються процесах безпеки, аудити третьою стороною [3]. Не рідкість серед SecaaS-провайдерів сертифікація по ISO27001, PCI DSS, обчислювальні потужності провайдерів розміщуються в сертифікованих дата-центрах. Також потенційному замовнику особливу увагу слід звертати на SLA SecaaS-провайдера.

Література:

1. Яковицький І. Технологія хмарних обчислень як інструмент створення інформаційної інфраструктури управління // Комунальне господарство міст. – 2012. – № 102. – С. 320-327

2. Комiссар Д.О., Луппол Є.Ю. Хмарні технології безпеки. // Вісник східноукраїнського національного університету імені Володимира Даля. – 2013. – Ч. 1.– № 15(204). – С. 83-87.

3. Mell P. The NIST Definition of Cloud Computing (Special Publication 800-145) : Recommendations of the National Institute of Standards and Technology / Peter Mell, Timothy Grance / National Institute of Standards and Technology, U.S. Department of Commerce.– September 2011. – 7 P.

4. Інформаційна безпека та захист персональних даних в хмарних сервісах. На що звернути увагу при виборі постачальника послуг. – [Електронний ресурс] – Режим доступу до ресурсу: https://ua.ikmj.com/information-security-and-personal-data-protection-in-cloud/

ПРОБЛЕМИ БЕЗПЕКИ ІНФОРМАЦІЇ У ХМАРНИХ СХОВИЩАХ

Масляк О. І., Григлевич М. О., Фірман В.М.
Львівський національний університет імені Івана Франка

Сьогодні швидко набирають популярності хмарні середовища, які є по-своєму надійними та зручними. Зручні тарифні плани дозволяють позбавити користувача зайвих витрат на диски та інші види фізичних сховищ та дозволяють використання тих самих файлів на всіх пристроях, які мають доступ до хмарного сховища.

Хмарне сховище даних (англ. cloud storage) – модель онлайн-сховища, в якому дані зберігаються на численних розподілених в мережі серверах, що надаються в користування клієнтам, в основному третьою стороною-постачальником. На відміну від моделі зберігання даних на власних виділених серверах, придбаних або орендованих спеціально для подібних цілей, кількість або будь-яка внутрішня структура серверів в загальному випадку, не відома клієнту. Дані зберігаються і обробляються в так званій «хмарі», яка представляє собою, з точки зору клієнта, один великий віртуальний сервер. Фізично ж такі сервери можуть розташовуватися віддалено один від одного. Постачальники хмарних систем зберігання даних відповідають за зберігання наявної інформації і доступ до неї, та за роботу фізичного середовища. Користувачі купують у постачальників послуг хмарного сховища змогу зберігати там дані. [1] [2]

Хмарне сховище ґрунтується на основі високоступеневої віртуалізованої інфраструктури є широко-доступним з погляду інших інтерфейсів, також сюди можна додати гнучкість, масштабованість, наявність мульти-оренд і функцій виміру ресурсів. Хмарне сховище може бути використане або за межами підприємства (Amazon S3) або на підприємстві (VION Місткість послуг).

Послуги хмарного сховища можуть бути доступні через інтерфейс програмного веб-сервісу (API) або додатки, які використовують API.

Хмарне сховище:

- Зроблене з багатьох розподілених ресурсів, але виступає як одне ціле – часто називають хмарним зберіганням, або федеративним;
- Висока відмовостійкість унаслідок резервування й розподілу даних;
- Висока міцність шляхом створення версій, копій [2].

Проблеми хмарних середовищ та їх вирішення.

Основна вразливість інтернет-сервісів полягає в використанні практично виключно парольної аутентифікації і застосуванні не цілком надійних способів відновлення забутих аутентифікаційних даних - логінів і паролів (перш за все – через електронну пошту). Якщо користувач не довіряє надавачу хмарного сервісу або хоче забезпечити додатковий захист інформації в хмарі, то він може застосувати шифрування даних в хмарі. Такий спосіб захисту можливий, якщо користувач не планує обробляти інформацію в хмарі (наприклад, редагувати фото або текст), а тільки зберігати і передавати дані в початковому вигляді. [1]

Так яке ж хмарне сховище варто використовувати якщо користувач все-таки зважився завантажити туди свої дані? Для прикладу можна виділити кілька популярних хмарних сховищ, таких як: DropBox чи iCloud. Як і більша частина конкурентів, Dropbox шифрує дані клієнтів на стороні сервера, однак відмовляється від шифрування в клієнтській частини програми. Також потокова передача файлів з серверів компанії не завжди зашифрована. Таким чином стає можливою компрометація даних в ході завантаження і вивантаження файлів на сервери. Крім того, у Dropbox значна історія інцидентів пов'язаних з безпекою.

Для користувачів техніки Apple існує хмарне сховище iCloud drive. З цим сервісом пов'язаний, напевно, найбільший скандал в історії хмарних сховищ, коли в 2014 році відбувся масова атака на акаунти iCloud, в результаті якої в мережу потрапило безліч персональних даних користувачів. Після інциденту Apple серйозно взялись за покращення безпеки сервісу - зараз дані в iCloud Drive шифруються і при передачі, і на сервері, пароль перевіряється на надійність, присутній двофакторна аутентифікація. З урахуванням вищезгаданого хмарне сховище від Apple на даному етапі є вкрай надійним.

На підставі вищевикладених даних можна виділити основні проблеми хмарних сховищ:

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

– Надійність, своєчасність отримання і доступність даних в «хмарі» дуже сильно залежить від багатьох проміжних параметрів, таких як: канали передачі даних на шляху від клієнта до «хмари», якість роботи інтернет-провайдера клієнта, доступність самої «хмари» в даний момент часу. Якщо ж сама компанія, що надає онлайн сховище, буде ліквідована, клієнт може втратити всі свої дані;

– Загальна продуктивність при роботі з даними в «хмарі» може бути нижче, ніж при роботі з локальними копіями даних;

– Абонентська плата за додаткові можливості (збільшений обсяг зберігання даних, передача великих файлів і т. д.).

Хмарні сховища мають безліч недоліків, але в той же час і не менша кількість переваг. Чи довіряти свої персональні дані «хмарам» - це особисте питання для кожного користувача. Компанії, що надають дані послуги, з кожним роком намагаються збільшити безпеку своїх сховищ. Вони зацікавлені в нових користувачах, а ті в свою чергу потребують конфіденційності, тому ступінь захисту персональних даних буде тільки збільшуватись.

Література:

1. Дроздова И. И. Жилин В. В. / Безопасность облачных хранилищ
2. Michael J. Kavis / Architecting the Cloud: Design Decisions for Cloud Computing Service

БЕЗПЕКА ІНФОРМАЦІЇ У ХМАРНИХ СХОВИЩАХ

Романчук Д.А.
ВП НУБІП України "Ірпінський економічний коледж"

Хмарні технології з кожним роком все більше використовуються для задоволення різних потреб населення. І,якщо раніше, хмарні технології використовувалися вузьким колом ІТ-спеціалістів, то сьогодні дана технологія єдоступною для кожного користувача. Використання безкоштовного поштового сервісу gmail компанії Google,Hotmail компанії Microsoft, використання віртуальних дискових просторів, додатків для спільної роботи віддалених користувачів та інші сервіси, що стали звичними для людства. Широке використання хмарних технологій призвелодо появи специфічних для кіберпростору технологій загроз безпеки інформації. Тому досить актуальним є розробканових інформаційних технологій захисту інформації в кіберпросторі та безпеки хмарних обчислень. Хмарні обчислення (cloud computing) – це технологія розподіленої обробки даних в якій комп'ютерні ресурси і потужності надаються користувачеві як Інтернет-сервіс, тобто робочий майданчик на віддаленому сервері. Сучасні програмні продукти характеризуються збільшенням вимог до технічних характеристик комп'ютерів, навіть операційні системи все більше вимагаються ресурсів. Тому багато підприємств задаються питанням щододоцільності закупки нового обладнання та розглядають як альтернативний варіант закупки лише тонких клієнтів, а в ролі термінального сервера використовувати сервер «хмари». Проведемо аналіз сервісів хмарних технологій. Все,що стосується Cloud computing (далі СС), зазвичай прийнято називати aaS – «as a Service», тобто «як сервіс», або «увигляді сервісу». На даний час концепція передбачає надання наступних типів послуг своїм користувачам:

– Storage-as-a-Service («зберігання як сервіс»). Найпростіший з СС-сервісів, що представляє собою дисковийпростір на вимогу користувача та дає можливість зберігати дані в зовнішньому сховищі, в «хмарі», у виглядідодаткового логічного диску або папці. Даний сервіс є базовим для інших, оскільки входить до складу практичнокожного з них.

– Database-as-a-Service («база даних як сервіс»). Послуга надає можливість працювати з базами даних, подібно до СУБД, що встановлено на локальному ресурсі.

– Information-as-a-Service («інформація як сервіс»). Даний сервіс надає можливість віддалено використовувати будь-які види інформації, яка динамічно може змінюватися.

– Process-as-a-Service («управління процесом як сервіс»). Віддалений ресурс, який може зв'язати воєдино кілька ресурсів для створення єдиного бізнес-процесу.

– Application-as-a-Service («додаток як сервіс»). Також називається, Software-as-a-Service («ПЗ як сервіс»). Позиціонується як «програмне забезпечення на вимогу», яке розгорнуто на віддалених серверах і кожен користувач може отримувати до нього доступ за допомогою Інтернету, причому всі питання оновлення та ліцензій на дане забезпечення регулюється постачальником даної послуги.

– Platform-as-a-Service («платформа як сервіс»). Користувачеві надається комп'ютерна платформа з встановленою операційною системою і певним програмним забезпеченням.

– Integration-as-a-Service («інтеграція як сервіс»). Це можливість отримувати з «хмари» повний інтеграційний пакет, включаючи програмні інтерфейси між додатками і управління їх алгоритмами.

– Security-as-a-Service («безпека як сервіс»). Даний вид послуги надає можливість користувачам швидко розгортати продукти, що вимагають безпечного використання веб-технологій, електронного листування, локальної мережі. Користувачі даного сервісу мають змогу економити на розгортанні та підтримці своєї власної системи безпеки.

– Management / Governace-as-a-Service («адміністрування та управління як сервіс»). Дає можливість керувати і задавати параметри роботи одного або багатьох «хмарних» сервісів. Це в основному такі параметри, як топологія, використання ресурсів, віртуалізація.

– Infrastructure-as-a-Service («інфраструктура як сервіс»). Користувачеві надається комп'ютерна інфраструктура, зазвичай віртуальні платформи (комп'ютери), пов'язані в мережу, які він самостійно налаштовує під власні цілі.

– Testing-as-a-Service («тестування як сервіс»). Дає можливість тестування локальних або «хмарних» систем з використанням тестового програмного забезпечення з «хмари» (при цьому жодного устаткування або забезпечення на підприємстві, не потрібно)

Як зробити хмари надійними? Очевидно, ризики в хмарах існують. Але не слід думати, що тільки провайдер відповідає за безпеку. Найбільші гравці ринку, такі як Amazon, Microsoft і Google, гарантують в першу чергу фізичну безпеку дата-центрів і збереження даних клієнтів від руйнування. Клієнти ж відповідають за те, що відбувається на їх віртуального ділянці хмари. Само собою, і провайдери, і незалежні постачальники систем безпеки Предоставляютя цілий арсенал для цифрового захисту, але їх використання - прерогатива IT-відділів компаній і вимагає додаткового кваліфікованого персоналу і відповідних бюджетів.

У CSA підкреслюють, що перший крок до організації безпеки хмари – дослідження можливих загроз. Там також називають кілька ключових рішень для посилення хмарної безпеки. Серед них - шифрування даних, а також їх захист при передачі. Зашифрована інформація під час передачі повинна бути доступна тільки після аутентифікації користувача з достатніми правами.

Крім традиційного пароля рекомендується використовувати додаткові кошти аутентифікації, такі як токени і сертифікати. Також фахівці радять організувати максимально прозоре і безпечне взаємодія провайдера з системами авторизації компанії - такими як LDAP (Lightweight Directory Access Protocol) і SAML (Security Assertion Markup Language). Варто пам'ятати і про важливість ізоляції користувачів в хмарному середовищі - найчастіше через можливих помилок в налаштуваннях або в коді програмного забезпечення, один користувач може Отримати доступ до НЕ належить йому даними.

БЕЗПЕКА ЗБЕРІГАННЯ ІНФОРМАЦІЇ В ХМАРНИХ СХОВИЩАХ

Тютченко С.М., Воробець Х.О.
Дніпропетровський державний університет внутрішніх справ

Анотація: Сучасні підприємства знаходяться під постійним впливом факторів, пов'язаних із розвитком технологій. Широке використання хмарних технологій призвело до появи специфічних для кіберпростору технологій загроз безпеки інформації. Тому досить актуальною є розробка нових інформаційних технологій захисту інформації в кіберпросторі та безпеки хмарних обчислень. Застосування спеціалізованого програмного забезпечення для віртуального середовища вимагає значної зміни у підходах до забезпечення інформаційної безпеки хмарних систем .

Ключові слова: інформація, хмарні технології, інформаційна безпека, кіберпростір, провайдер.

Abstract: Modern businesses are constantly influenced by technology-related factors. The widespread use of cloud technologies has led to cyberspace-specific information security threats. Therefore, the development of new information technologies for information security in cyberspace and security of cloud computing is quite relevant. The application of specialized software for the virtual environment requires a significant change in approaches to ensuring information security of cloud systems.

Keywords: information, cloud technologies, information security, cyberspace, provider.

Розповсюдження мереж з високою потужністю, низька вартість комп'ютерів і пристроїв зберігання даних, а також широке впровадження віртуалізації привели до величезного зростання хмарних обчислень. Кінцеві користувачі мають доступ до власних даних і можуть не перейматися роботою обладнання технологічної інфраструктури (а в залежності від моделі обслуговування і програмним забезпеченням) "хмари", яка їх підтримує. Проте в цьому проявляється головний недолік хмари – приватна інформація користувача фактично стає доступна третій стороні – провайдеру. Крім цього, дані можуть стати вразливими під час їх передачі по каналам зв'язку [1].

Хмарні технології з кожним роком все більше використовуються для задоволення різних потреб населення. І, якщо раніше, хмарні технології використовувалися вузьким колом IT-спеціалістів, то сьогодні дана технологія є доступною для кожного користувача. Широке використання хмарних технологій призвело до появи специфічних для кіберпростору технологій загроз безпеки інформації. Тому досить актуальним є розробка нових інформаційних технологій захисту інформації в кіберпросторі та безпеки хмарних обчислень [2].

Концепція хмарних технологій полягає в наданні користувачам віддаленого динамічного доступу до послуг, обчислювальних ресурсів і додатків,

включаючи операційні системи та інфраструктуру через різні канали доступу, в тому числі і через Інтернет. Така великомасштабна інфраструктура має підвищені ризики і досить обмежену можливість контролю над її ресурсами. У цьому і полягає актуальність проблем хмарних обчислень – захист інформації та довірливе ставлення користувачів до хмарних провайдерів.

Сучасні підприємства знаходяться під постійним впливом факторів, пов'язаних із розвитком технологій, які, з одного боку, спрощують роботу з великими обсягами інформації, проте, з іншого – зумовлюють проблеми, пов'язані насамперед з інформаційною безпекою.

Одним з головних джерел загрози безпеки є сервер централізованого управління віртуальної інфраструктури, отримавши контроль над яким, зловмисник отримує повний доступ до всіх віртуальних машин, хостів віртуалізації, віртуальних мереж і сховищ даних. Тому необхідно, в першу чергу, ретельно захищати сам сервер управління, звертати посилену увагу на засоби аутентифікації і розмежування прав доступу, для чого має сенс використовувати додаткове програмне забезпечення, що розроблене спеціально для віртуальних інфраструктур. Доступ до сервера віртуалізації повинен здійснюватися за безпечними протоколами, а доступ адміністраторів повинен бути обмежений за IP-адресами.

Для забезпечення захисту даних у хмарі, які розміщені за межами сфери фізичного доступу клієнта, здійснюють шифрування віртуальних жорстких дисків. При зчитуванні з диска дані розшифровуються і при записі на диск зашифровуються. При цьому ключі зберігаються на окремому сервері управління ключами, який спочатку перевіряє ідентифікаційні дані і цілісність хмарного сервера, який направив запит.

Застосування спеціалізованого програмного забезпечення для віртуального середовища вимагає значної зміни у підходах до забезпечення інформаційної безпеки хмарних систем [3]. Рішення задач забезпечення безпеки об'єднує в собі традиційні та специфічні рішення з особливостями, які в процесі виконання задач повинні оптимізовуватись для економії продуктивності віртуального середовища із забезпеченням захисту інформації і хмарних ресурсів.

У разі позитивного відгуку надається ключ і хмарний сервер отримує доступ до інформації, що зберігається і ресурсів хмари. Більш потужний варіант безпеки даних являє собою комбінування технологій шифрування даних і захищеної передачі. Для підвищення безпечного використання хмарних технологій доцільно використовувати системи виявлення вторгнень і міжмережевого екранування з контролем зовнішніх підключень до середовища віртуалізації за допомогою апаратних рішень, а внутрішніх - за допомогою програмних рішень, реалізуючи, таким чином, комбінований підхід [4].

Під час використання хмарних технологій програмне та технічне забезпечення надається користувачеві як Інтернет-сервіс. Користувач має доступ до власних даних, але не може управляти і не повинен піклуватися про інфраструктуру, операційну систему і програмне забезпечення, з якими він працює.

Уся процедура захисту даних побудована на конфіденційності, цілісності та доступності. Конфіденційність належить до так званої прихованої функції фактичних даних або інформації і є однією із найжорсткіших вимог інформаційної безпеки. У випадку хмарних обчислень дані накопичуються в центрах обробки даних, де безпека та конфіденційність даних ще важливіші.

Вірно підібрані рішення безпеки дозволяють отримати уявлення про рівень використовуваних ресурсів і своєчасно виявити атаки, які націлені на різні хмарні об'єкти. Для зниження операційних витрат, пов'язаних із засобами захисту систем віртуалізації, рекомендується використовувати спеціально розроблене програмне забезпечення, що адаптоване для хмарних обчислень. Але все ж ще залишаються проблеми адаптації захисту віртуалізації в хмарі, які вимагають подальшого аналізу і вдосконаленого рішення.

Література:

1. Котяшичев И. А. Защита информации в «Облачных технологиях» как предмет национальной безопасности / И. А. Котяшичев, Е. А. Бырылова // Молодой ученый. — 2015. — №6.4. — С. 30-34.

2. Ладигіна О.А. Перспективи захисту інформації в хмарних обчисленнях від атак на засоби віртуалізації // Збірник тез доповідей науково-практичної конференції «Інформаційні технології та комп'ютерна інженерія». – Кіровоград: КНТУ, 2014. -164 с

3. Google Engineer Spied on Chats [Електронний ресурс] / Gawker. – Режим доступу: http://gawker.com/5637234/gcreep-google-engineer-stalked-teens-spied-on-chats

4. Dropbox Core API [Електронний ресурс]: Dropbox Core API // Dropbox – Dropbox. – Режим доступу: https://www.dropbox.com/developers/core/.

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ AMAZON WEB SERVICES

Шуцман Р. П., Дудикевич В.Б.
Національний університет «Львівська політехніка»

Безпека даних завжди була головною проблемою в інформаційних технологіях. У середовищі хмарних обчислень вона стає особливо серйозною, оскільки дані знаходяться в різних місцях по всьому світу. AWS прагне допомогти вам досягти найвищого рівня безпеки в хмарі. В даній роботі буде розглянуто методи захисту які використовуються у середовищі AWS.

Ключові слова: хмарні обчислення, безпека даних, інформаційні технології, методи захисту, AWS, відмова в обслуговуванні, порушення даних, криптовалюта.

Data security has consistently been a major issue in information technology. In the cloud computing environment, it becomes particularly serious because the data is located in different places even in all the globe. AWS is committed to helping you achieve the highest levels of security in the cloud. This paper will look at the security methods used in the AWS environment.

Keywords: cloud computing, data security, information technology, security methods, AWS, DoS, data breach, crytopjacking.

I. Вступ

В даний час питання захисту даних має величезну важливість. Важливість обґрунтовується постійно зростаючою кількістю інформації, яку потрібно зберегти. Оскільки за останні декілька років було досягнуто великого прогресу у хмарних обчисленнях. Збільшуючи кількість компаній, які використовують ресурси в хмарі, існує необхідність захистити дані різних користувачів, що використовують централізовані ресурси. Деякі серйозні проблеми, з якими стикаються хмарні обчислення - захищати та обробляти дані, що є власністю користувача. Метою роботи є дослідження та аналіз сучасних методів та засобів що використовуються для забезпечення захисту в хмарних технологіях сервісами AWS.

II. Загрози в хмарних обчисленнях

Використання хмари для розміщення даних, додатків та інших активів вашого бізнесу пропонує ряд переваг щодо управління, доступу та масштабованості. Але хмара також представляє певні ризики для безпеки. Традиційно ці ризики зосереджені на таких сферах, як відмова в обслуговуванні, втрата даних, зловмисне програмне забезпечення та вразливості системи.[2]

Коли бізнес розглядає хмарні обчислення, однією з головних переваг, яку часто цитують, є той факт, що він може зробити ваш бізнес більш безпечним. Насправді, в останні роки багато підприємств вирішили перейти до хмари спеціально для переваг безпеки. Отже, вас може здивувати,

дізнавшись, що існує ряд загроз кібербезпеки, які можуть спричинити всілякі проблеми хмарних систем. Тоді важливо точно зрозуміти, де ваша система може опинитися під загрозою, і що ви можете щодо цього зробити. У цій статті ми розглянемо сім ключових загроз кібербезпеки, які можуть вплинути на ваші послуги хмарних обчислень:[3]

- Порушення даних
- Втрата даних
- Відмова в обслуговуванні (DoS)
- Криптовалюта
- Викрадення облікових записів
- Небезпечні програми
- Інсайдерські загрози

III. Методи захисту за допомогою AWS.

Веб-сервіси Amazon (AWS) надають декілька служб безпеки, щоб допомогти своїм клієнтам захистити їх хмарні дані на основі даних від втрат, корупції чи викривлення. Ці сервіси є основними складовими будь-якої стратегії захисту даних, наприклад, керування доступом на основі ролей, автентифікація користувачів, моніторинг подій та трафіку, журнали та сповіщення тощо. Далі буде описано розширені служби безпеки AWS та те, як вони забезпечують рівень безпеки даних та додатків при стратегічному використанні із будівельними блоками безпеки AWS.[4]

– Захист додатків: AWS WAF та AWS Firewall Manager - AWS WAF з метою задоволення потреб у безпеці сьогодні широко розповсюджених додатків, брандмауер веб-додатків AWS (AWS WAF) відстежує запити HTTP / HTTPS на всіх відповідних вхідних інтерфейсах. Ці інтерфейси включають шлюз API Amazon, Amazon CloudFront (мережа доставки вмісту) та балансир завантаження програм.[5]

– Атака DDoS: AWS Shield – це безкоштовна послуга захисту від розподіленої відмови у наданні (DDoS) для всіх програм, що використовують послуги AWS. Він захищає веб-сайти та програми від найчастіших DDoS-атак. [5]

– Інтелектуальне виявлення загроз: Amazon GuardDuty – застосовує всі новітні технології виявлення загроз – машинне навчання, штучний інтелект, аналітику поведінки та багато іншого – оскільки він постійно здійснює моніторинг облікових записів AWS та навантажень для зловмисної діяльності та аномальної поведінки. [5]

– Автоматизована безпека даних: Amazon Macie – це повністю керована інтелектуальна служба захисту даних. Вона автоматично виявляє, класифікує та захищає конфіденційні дані, такі як особиста інформація або інтелектуальна власність. [5]

Висновки

Використання хмарних обчислень зросло за останні кілька років, і таке зростання безумовно сприяло посиленню загроз безпеки, оскільки хакери продовжують експериментувати з новими способами атаки. Як наслідок, загроза безпеці стає повсякденним явищем. Саме тому в даній роботі було досліджено які види загроз можуть бути у хмарних технологіях, а також запропоновано програмні засоби сервісу AWS, які використовуються для захисту даних користувачів.

Література

1. https://www.techrepublic.com/article/how-to-prevent-the-top-11-threats-in-cloud-computing/
2. https://cloudacademy.com/blog/key-cybersecurity-threats-to-cloud-computing/
3. https://easternpeak.com/blog/the-top-cloud-security-threats-for-your-business-in-2019-and-how-to-avoid-them/
4. https://aws.amazon.com/security/
5. https://mediatemple.net/blog/tips/aws-security-services/

Напрям 5

Криптографічні та стеганографічні засоби захисту інформації

КРИПТОГРАФІЧНІ ТА СТЕГАНОГРАФІЧНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

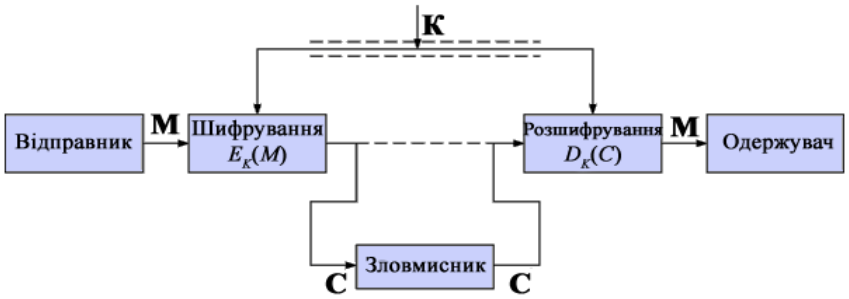
Кіріченко Станіслав
Львівський національний університет імені Івана Франка

Криптографія — це сукупність методів перетворення даних, спрямованих на приховання їх інформаційного змісту.

Криптографічна система захисту інформації — це сукупність криптографічних алгоритмів, протоколів і процедур формування, розподілу, передачі й використання криптографічних ключів.

Припустимо, що відправник хоче послати повідомлення одержувачеві. Більш того, цей відправник хоче послати своє повідомлення безпечно: він хоче бути впевнений, що в разі перехоплення повідомлення зловмисник не зможе довідатися про зміст повідомлення. У цьому разі відправникові доцільніше використати криптографічні перетворення.

Саме повідомлення називається відкритим текстом. Зміна виду повідомлення з метою приховати його суть називається шифруванням. Шифроване повідомлення називається шифротекстом. Процес перетворення шифротексту у відкритий текст називається розшифруванням. Узагальнену схему криптографічної системи, що забезпечує шифрування переданої інформації, показано на рис. 1.



Криптографія застосовується в наш час майже всюди від логування у месенджери та на будь-які сайти, і до шифрування нашої інформації при проведенні платежів за допомогою додатків на телефоні або у термінала і банкоматах.

Найпопулярнішими на сьогодні є функції хешування MD5, SHA-512, HMAC-SHA-256.

Стеганографія (steganos – секрет, таємниця; graphy – запис) відома ще з стародавніх часів, на тепер – це, по-перше, метод приховування певного повідомлення в іншому (яке є свідомо великим), таким чином, що неможливо побачити присутність або сенс прихованого повідомлення; по-друге, цифрова стратегія приховування файлу в мультимедійному форматі (наприклад: картинка, звуковий файл – WAV, MP3 або відео файл).

Стеганографічні методи також спрямовані на протидію системам моніторингу та управління мережевими ресурсами промислового шпигунства, дозволяють протистояти спробам контролю над інформаційним простором при проходженні інформації через сервери керування локальних і глобальних обчислювальних мереж. Для корпорацій та державних відомств, що зберігають важливі масиви даних, це одна із неоціненних функції стеганографії.

Іншим важливим завданням стеганографії є камуфлювання програмного забезпечення (ПЗ). У тих випадках, коли використання ПЗ незареєстрованими користувачами є небажаним, воно може бути закамуфльовано під стандартні універсальні програмні продукти (наприклад, текстові редактори) або приховано в файлах мультимедіа (наприклад, у звуковому супроводі комп'ютерних ігор).

Прикладом використання стеганографії у захисті авторського права від піратства є нанесення спеціальної мітки на комп'ютерні графічні зображення. Мітка залишається невидимою для очей людини, але розпізнається спеціальним ПЗ, яке вже використовується в комп'ютерних версіях деяких журналів. Даний напрямок стеганографії призначений не тільки для обробки зображень, але і для файлів з аудіо– та відеоі– нформацією й забезпечює захист інтелектуальної власності.

Важливим і перспективним є кожне із названих завдань стеганографії. Розуміння проблем захисту інформації та її безпеки полягає у подальшому розвитку питань і шляхів їх вирішення, які може запропонувати стеганографія.

Існуючі способи вирішення технічної проблеми. Для приховування інформації у цифровому вигляді за допомогою стеганографії існують спеціальні алгоритми. Внесення нової інформації у вже наявні файли (наприклад, мультимедійні) призводить до спотворенньь, які перебувають нижче порогу чутливості людини, тому це не викликає помітних змін у сприйнятті вхідних файлів.

Література:

1. Барсуков В.С., Романцов А.П. Компьютерная стеганография вчера, сегодня, завтра [Электронный ресурс]. – Режим доступа: http://www.bnti.ru/showart.asp?aid=330&lvl=03.07.06 (дата звернення 18.05.2017)

2. Бабаш, А. В. Криптография [Текст]: учеб. пособие / А. В. Бабаш, Г. П. Шанкин. – М.: СОЛОН-Р, 2002. – 511 с.

РОЗРОБКА ПРОГРАМНОГО КОМПЛЕКСУ ДЛЯ ПРИХОВУВАННЯ У ПСЕВДОВИПАДКОВО ОБРАНИХ БІТАХ РАСТРОВОГО ЗОБРАЖЕННЯ ЗАШИФРОВАНОГО ЗА ДОПОМОГОЮ ШИФРУ RC4 ПОВІДОМЛЕННЯ

Кордунова Ю., Кухарська Н.
Львівський державний університет безпеки життєдіяльності, м. Львів

У роботі описано процес розроблення програмного комплексу для створення криптостеганографічної системи захисту інформації.
Ключові слова: криптографія, стеганографія, шифр RC4, метод псевдовипадкової перестановки.

The article describes the process of developing a software complex of creating a crypto-steganographic information security system.
Keywords: cryptography, steganography, RC4 cipher, method of pseudorandom restructuring

Одним із найцінніших предметів сучасного життя є інформація. З появою комп'ютерних мереж одержання доступу до неї стало надзвичайно простим. Переваги подання та передачі даних у цифровому вигляді значно полегшують роботу користувачам, проте можуть бути перекреслені з такою ж легкістю, як і можливі їх викрадення й модифікація. Саме тому, питання захисту інформації особливо гостро постають в наш час.

У даній роботі було описано процес розроблення програмного комплексу на основі криптостеганографічного підходу захисту інформації.

Криптостеганографічною називають систему передачі інформації у відкритих каналах зв'язку, що базується на одночасному використанні криптографічних і стеганографічних алгоритмів.

Криптографічний захист – послідовність перетворень інформації з метою зробити її незрозумілою для непосвячених, приховання змісту повідомлень за рахунок шифрування [2].

У даній роботі повідомлення шифрувалося з допомогою потокового шифру RC4. Цей алгоритм працює з n-бітовими словами. Всі обчислення проводяться за модулем 2^n (остача $x \bmod 2^n$ обчислюється дуже швидко шляхом виділення n молодших біт в x з допомогою логічної операції «і»). Як відомо, RC4 використовує L-слівний ключ $K=K_0 K_1 \dots K_{L-1}$ і генерує послідовність слів $\bar{z}=z_1 z_2 z_3 \dots$, конкретний вигляд якої визначається ключем K. Стан генератора задається таблицею S (вектор ініціалізації) з 2^n слів і двома змінними i та j. У кожен момент часу таблиця S містить всі можливі *n*-бітові числа в перемішаному вигляді. Оскільки кожен елемент таблиці приймає значення в проміжку $[0, 2^n - 1]$, то його можна трактувати двояко: або як число, або як номер іншого елемента в таблиці [3].

Криптографічний захист не вирішує згадану вище проблему захисту інформації повністю, позаяк наявність шифрованого повідомлення привертає увагу зловмисника. Саме тому було прийнято рішення використати ще один метод захисту інформації – стеганографічний. Даний метод полягає у приховуванні ж самого факту існування секретних даних при їх передачі, зберіганні чи обробці.

Відповідно, у розробленому програмному комплексі реалізовано процес приховування зашифрованого тексту у растровому зображенні удосконаленим методом заміни найменш значу-щого біта. Молодший значущий біт зображення несе в собі найменше інформації, людина не здатна помітити зміни його значення [1]. Цим і пояснюється його використання для стеганогра-фічних цілей. Молодший біт замінюють бітами секретного повідомлення. У цій роботі дані вбудовуються не у всі пікселі растрового зображення, а лише в обрані псевдовипадково способом.

Можна зробити висновок: стеганографія займаючи свою нішу в інформаційній безпеці, не замінює, а доповнює криптографію, а у комплексі ці дві науки дають змогу здійснити надійний захист важливої інформації.

Література:

1. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. Киев : МК-Пресс, 2006. 288 с.

2. Хорошко В. А. Чекатков. А. А. Методы и средства защиты информации. Киев : ЮНИОР, 2003. 504 с

3. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии. Москва : Горячая линия-Телеком, 2002. 175 с.

ВИКОРИСТАННЯ КРИПТОГРАФІЧНИХ ТА СТЕНОГРАФІЧНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ БЕЗПЕКИ ЖИТТЄДІЯЛЬОСТІ

Онишко Т., Фірман Л.
Львівський національний університет імені Івана Франка

В наш час інформація перетворюється на найдорожчий ресурс. Оперативне отримання інформації дає перевагу над конкурентами, які її не мають, конфіденційна інформація про вас та вашу діяльність, що потрапила до зловмисників може серйозно вам нашкодити. Тому, у літературі виділяють різні способи захисту інформації, серед яких найбільш ефективні - криптографічні та стенографічні.

Криптографічний захист – це вид захисту, який реалізується за допомогою перетворень інформації з використанням спеціальних (ключових) даних з метою приховування змісту інформації, підтвердження її справжності, цілісності, авторства тощо. Криптографічний метод захисту, безумовно, самий надійний метод захисту, так як охороняється безпосередньо сама інформація, а не доступ до неї (наприклад, зашифрований файл не можна прочитати навіть у випадку крадіжки носія). То ж навіть якщо файли і потраплять до зловмисників, імовірність їхнього використання зводиться до нуля.[3] Даний метод захисту реалізується у вигляді програм або пакетів програм.

Сучасна криптографія включає в себе чотири великих розділи:

- симетричні криптосистеми;
- криптосистеми з відкритим ключем;
- електронний підпис;
- управління ключами; [2]

У симетричних криптосистемах і для шифрування, і для дешифрування використовується один і той самий ключ. У системах з відкритим ключем використовуються два ключі - відкритий і закритий, які математично пов'язані один з одним. Інформація шифрується за допомогою відкритого ключа, який доступний всім бажаючим, а розшифровується за допомогою закритого ключа, відомого тільки одержувачу повідомлення. Криптографічні системи з відкритим ключем використовують так звані незворотні або односторонні функції, які мають наступну властивість: при заданому значенні x відносно просто обчислити значення F(x), однак якщо y = F(x), то немає простого шляху для обчислення значеннях. Безліч класів незворотних функцій і породжує все розмаїття систем з відкритим ключем. Системою електронного підпису називається його криптографічне перетворення, що приєднуються до тексту і дозволяє при отриманні його іншим користувачем перевірити авторство і достовірність повідомлення. [1]

Для сучасних криптографічних систем захисту інформації сформульовані наступні загальноприйняті вимоги:

– Зашифроване повідомлення повинне піддаватися читанню тільки при наявності ключа;

– Число операції, необхідних для визначення використаного ключа шифрування по фрагменту шифрованого повідомлення й відповідного йому відкритого тексту, повинне бути не менше загального числа можливих ключів;

– Число операцій, необхідних для розшифровування інформації шляхом перебору всіляких ключів, повинне мати строгу нижню оцінку й виходити за межі можливостей сучасних комп'ютерів (з урахуванням можливості використання мережних обчислень) або вимагати неприйнятно високих витрат на ці обчислення;

– Знання алгоритму шифрування не повинне впливати на надійність захисту;

– Незначна зміна ключа повинна приводити до істотної зміни виду зашифрованого повідомлення навіть при шифруванні того самого вихідного тексту; [2]

Одними із найбільш поширених криптографічних методів шифрування є метод Віженера, алгоритм перестановки, шифр Вернама, RSA-алгоритм, криптографічний стандарт DES.

Стеганографія – це метод організації зв'язку, який власне приховує сама наявність зв'язку. На відміну від криптографії, де ворог точно може визначити чи є передане повідомлення зашифрованим текстом, методи стеганографії дозволяють вбудовувати секретні повідомлення в нешкідливі послання так, щоб неможливо було запідозрити існування вбудованого таємного послання. Стеганографія займає свою нішу в забезпеченні безпеки: вона не замінює, а доповнює криптографію. Приховування повідомлення методами стеганографії значно знижує ймовірність виявлення самого факту надіслати повідомлення. А якщо це повідомлення до того ж зашифровано, то воно має ще один, додатковий, рівень захисту. В стенографії будь-яку інформацію, призначену для приховування таємних повідомлень прийнято називати контейнером.

Будь-яка стегосистема повинна відповідати наступним вимогам:

– Властивості контейнера повинні бути модифіковані, щоб зміни неможливо було виявити при візуальному контролі. Ця вимога визначає якість приховування впроваджуваного повідомлення: для забезпечення безперешкодного проходження повідомлення по каналу зв'язку, воно жодним чином не повинно привернути увагу атакуючого.

– Повідомлення повинно бути стійко до спотворень, в тому числі і зловмисних. У процесі передачі зображення (звук або інший контейнер)

може зазнавати різні трансформації: зменшуватися або збільшуватися, перетворюватися в інший формат і т. д. Крім того, воно може бути стислим, в тому числі і з використанням алгоритмів стиснення з втратою даних.

– Для збереження цілісності вбудованого повідомлення необхідне використання коду з виправленням помилок.

– Для підвищення надійності вбудоване повідомлення має бути продубльоване. [4]

Також у галузі захисту інформації має місце комп'ютерна стенографія, у якій більшість досліджень пов'язана власне із цифровою обробкою сигналів, що дозволяє говорити про цифрову стенографію. У цьому випадку секретні повідомлення вбудовуються у цифрові дані, які, як правило, мають аналогову природу (мова, зображення, аудіо- і відеозаписи) [5]

В даний час найбільш поширеним, але найменш стійким є метод заміни найменших значущих бітів або LSB-метод. Він полягає у використанні похибки дискретизації, яка завжди існує в оцифрованих зображеннях або аудіо і відеофайлах. Дана похибка дорівнює найменшому значущому розряду числа, що визначає величину колірної складової елемента зображення (пікселя).

Література:

1. Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Грайворонський, О. М. Новіков. – К. : Видавнича група BHV, 2009.

2. Ємець В. Сучасна криптографія. Основні поняття / В. Ємець, А. Мельник, Р. Попович. – Львів : Бак, 2003.

3. Кузнецов О. О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011.

4. О. В. Генне журнал "Захист інформації. Конфідент", № 3, 2000

5. Пузиренко, Олександр (2006). Комп'ютерна стеганографія. Теорія і практика

ОСОБЛИВОСТІ НЕЗБАЛАНСОВАНОЇ МЕРЕЖІ ФЕЙСТЕЛЯ

Петлеванна І., Зайва А.
Одеський національний політехнічний університет, м. Одеса

В роботі виконано порівняння незбалансованої та збалансованої мереж Фейстеля. Показані переваги незбалансованої системи перед збалансованою: її більш доказову безпеку. Також приведені алгоритми де використовується незбалансована мережа Фейстеля.

Ключові слова: незбалансована мережа Фейстеля, збалансована мережа Фейстеля, порівняння.

The paper compares the unbalanced and balanced Feistel networks. The advantages of an unbalanced system over a balanced one are shown: its more demonstrable security. Algorithms for using the unbalanced Feistel network are also given.

Keywords: unbalanced Feistel network, balanced Feistel network, comparison.

Мережа Фейстеля — це загальний підхід перетворення будь-якої функції (яку часто називають F-функцією) в перестановку. Він був винайдений Хорстом Фейстелем, коли він працював у IBM, в його проекті Люцифера і з тих пір використовувався в багатьох конструкціях блочних шифрів: DES, FEAL, Хуфу і Хафре [1].

Сучасні блокові шифри — все складові, але вони розділені на два класи. Шифри в першому класі використовують і оборотні, і необоротні компоненти. Ці шифри називають шифри Фейстеля. Шифри в другому класі застосовують тільки оборотні компоненти. Їх називають "не-Фейстеля», через відсутність іншої назви [2].

Головним блоком мережі Фейстеля є F-функція: залежне від ключа відображення вхідного рядка у вихідний рядок. F-функція завжди нелінійна і майже завжди є незворотною [3].

Шифр Фейстеля містить в блоках усі незворотні елементи і використовує один і той же модуль в алгоритмах шифрування і дешифрування. Фейстель показав, що вони можуть бути збалансовані [4]. Алгоритми "основних кроків криптоперетворень" для шифрів, подібних ГОСТ, побудовані ідентичним чином, і ця архітектура називається збалансована мережу Фейстеля (Balanced Feistel Network)

Проблема збалансованої мережі Фейстеля в тому, що складно створити блоковий шифр з великим розміром введення / виведення. Тобто, коли блоковий шифр може обробляти великий обсяг даних за один раз, вхідний розмір раундової функції, що використана у мережі Фейстеля також збільшується. Слід зазначити що, вартість реалізації раундової функції пропорційна розміру введення цієї функції [5]. Отже попередня (збалансована) структура мережі Фейстеля недоречна при побудові блочного шифру з великим розміром введення / виведення.

Одним із засобів вирішення цієї проблеми є використання незбалансованої структури мережі Фейстеля.

Незбалансована мережа Фейстеля (UFN) — це мережа Фейстеля, де «ліва половина» і «права половина» не мають однакового розміру. Зняття

цього обмеження в мережах Фейстеля має наслідки для розробки шифрів, захищених від лінійних і диференціальних атак [6].

Раундова функція в незбалансованій мережі Фейстеля може бути реалізована з меншими витратами, ніж в збалансованій, так як можна контролювати розмір вхідних даних. Коли можливості комп'ютера з обробки інформації збільшуються, блоковий шифр з великим розміром введення/виведення, який здатний обробляти велику кількість інформації стає необхідним інструментом для шифрування і дешифрування інформації.

Переваги незбалансованої мережі Фейстеля перед збалансованою:

1. Побудови блокових шифрів з великим розміром введення / виведення.

2. Збалансована мережа Фейстеля гарантує безпеку приблизно для $2^{\frac{n}{4}}$ змагальних запитів (при більшій кількості раундів можна наблизитися до межі $2^{\frac{n}{2}}$). Незбалансована мережа Фейстеля ж гарантує безпеку при достатній кількості раундів приблизно для 2^n змагальних запитів.

Приклади використання незбалансованої мережі [7]. 1. Texas Instruments – американська компанія, виробник напівпровідникових приладів, мікросхем, електроніки і виробів на їх основі. Вона використовує власні незбалансовані мережі Фейстеля для виконання аутентифікації запит-відповідь при передачі цифрових підписів.

2. Thorp shuffle – це крайній випадок незбалансованої мережі Фейстеля, в якому одна сторона є один біт. Це забезпечує кращу доказову безпеку, ніж збалансований шифр Фейстеля, але вимагає більшої кількості раундів.

3. XXTEA – криптографічний алгоритм, який реалізує блочне шифрування і представляє собою мережу Фейстеля. Є розширення алгоритму Block TEA. Він буде більш ефективним, ніж XTEA, для більш довгих повідомлень.

Література

1. Viet Tung Hoang, Phillip Rogaway, “On Generalized Feistel Networks”.

2. Прикладная криптология: методы шифрования : учебное пособие / Б. С. Ахметов, А. Г. Корченко, В. П. Сиденко и др. – Алматы : КазНИТУ имени К. И. Сатпаева, 2015. – 496 с.: ил

3. Jacques Patarin, “Security of balanced and unbalanced Feistel Schemes with Linear Non Equalities”;

4. Горбенко І.Д. Захист інформації в інформаційно-телекомунікаційних системах : Навч. посіб. для студ. Ч. 1. Криптографічний захист інформації / І. Д. Горбенко, Т. О. Гріненко. – Х. : Харк. нац. ун-т радіоелектрон., 2004. – 368 с.

5. Bruce Schneier, John Kelsey, “Unbalanced Feistel Networks and Block Cipher Design”;

6. Математичні основи криптоаналізу : Навч. посіб. / С.О. Сушко, .В. Кузнецов, Л.Я. Фомичова, А.В. Корабльов. – Д. : Національний гірничий університет, 2010. – 465 с.

7. Colin Boyd, “Information Security and Privacy: 14th Australasian Conference, ACISP 2009”.

АНАЛІЗ ВБУДОВУВАННЯ ІНФОРМАЦІЇ У ЗОБРАЖЕННЯ ЗА ДОПОМОГОЮ ВЕЙВЛЕТ ПЕРЕТВОРЮВАНЬ

Тарабаєва Д.Д., Шпінарева І.М.
Університет ім. І.І.Мечнікова, кафедра МЗКС, Одеса

Вейвлет-перетворення є одним з визнаних методів для виконання частотного тимчасового перетворення сигналу або зображення. ДВП вважаються більш стійкими до компресії мультимедійних даних. В роботі проаналізовано вплив рівнів розкладання контейнера зображення на якість приховування інформації за допомогою вейвлетів з різними базисами: Хаара, Добеші, симлети. Наведені базиси відрізняються різними значеннями вейвлет-коефіцієнтів та підходами до формування спектрів.

Ключові слова: вейвлет-перетворення, Хаар, Добеши, симлет, середньоквадратична похибка, шум.

Wavelet conversion is one of the recognized methods for performing frequency temporal signal or image conversion. DVPs are considered more resistant to compression of multimedia data. The influence of levels of decomposition of the image container on the quality of information hiding by means of wavelets with different bases loke Haara, Dobeshi, Simlets is analyzed in the work. The presented bases differ in different values of wavelet coefficients and approaches to the formation of spectra.

Keywords: wavelet transform, Haar, Dobeshi, simlet, root mean square error, noise.

В останні десятиліття функції типу маленької хвилі (сплески, або вейвлети) знайшли широкі застосування в обробці сигналів і зображень. Ці додатки стимулювали потужне розвиток теорії вейвлетів. Теорія вейвлетів є альтернативою аналізу Фур'є і дає більш гнучку техніку обробки сигналів. Одне з основних переваг вейвлет-аналізу полягає в тому, що він дозволяє помітити добре локалізовані зміни сигналу, тоді як аналіз Фур'є цього не дає – в коефіцієнтах Фур'є відбивається поведінка сигналу за весь час його існування.

У даній роботі розглянути алгоритми вбудовування повідомлення у відеофайл формату MPEG за допомогою ДВП і порівняні три види вейвлетів: Добеши, Хаара та симлети.

Вейвлет Хаара – один з перших і найбільш простих вейвлетів. Вейвлети Хаара ортогональні, добре локалізовані в просторі, але не є гладкими. Перетворення Хаара використовується для стиснення вхідних сигналів, компресії зображень, в основному кольорових і чорно-білих з плавними переходами. Ідеальний для картинок типу рентгенівських знімків.

Двовимірне перетворення Хаара – це не що інше, як композиція одновимірних перетворень Хаара. Нехай двовимірний вхідний сигнал являє собою таблицю S. Після застосування одновимірного перетворення Хаара до кожного рядка матриці S виходять дві нові матриці, рядки яких містять

апроксимуючі і деталізуючи частини рядків вхідної матриці. Аналогічно, до кожної колонки отриманих матриць застосовують одномірне перетворення Хаара і на виході отримують чотири матриці, одна з яких є апроксимуючої складової вихідного сигналу, а три містять деталізує інформацію – вертикальну, горизонтальну і діагональну.

Вейвлети Добеші являють собою сімейство ортогональних вейвлетів, що визначають дискретне вейвлет-перетворення і характеризується максимальною кількістю зникаючих моментів для деякого заданого носія функції. З кожним вейвлетом є функція масштабування, яка генерує прямокутний кратномасштабний аналіз. У загальному випадку, вибирають вейвлети Добеші, щоб мати найвище число зникаючих моментів A, (це не означає кращу плавність) для заданої ширини носія функції 2^{A-1}.[1] Використовують дві схеми іменування, DN з використанням довжини, або кількості відводів та dbA з посиланням на число зникаючих моментів. Таким чином, D4 і db2 такі ж вейвлет-перетворення. Серед 2^{A-1} можливих рішень рівнянь, обирається рішення, у якого масштабуючий фільтр має екстремальну фазу.

Сімлет-вейвлети – вейвлети Добеши з найменшою асиметрією і компактним носієм.

Для порівняння обраних вейвлетів проаналізуємо стегозображення. Для вбудовування інформації використовуємо алгоритм [2] і будемо вбудовувати на другий и третій рівні. Якість приховування інформації у зображенні визначається за допомогою пікового відношення сигнал/шум (PSNR) (рис.1) та середньоквадратичною похибкою MSE (рис.2).

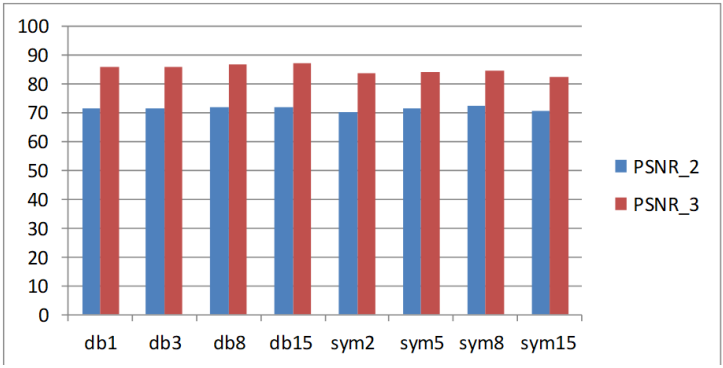


Рисунок 1 – Аналіз стегозображення з використанням різних вейвлетів за допомогою PSNR

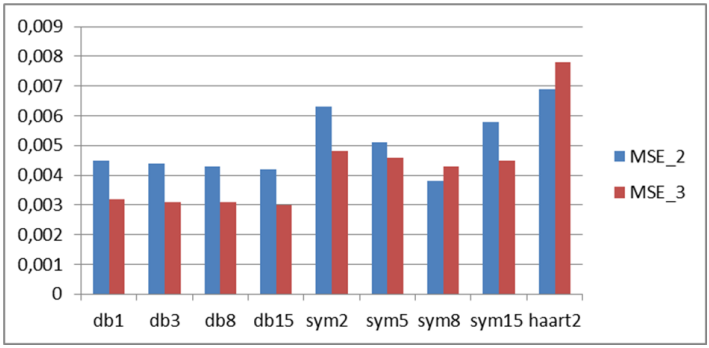


Рисунок 2 – Аналіз стегозображення з використанням різних вейвлетів за допомогою MSE.

Як можна побачити при використанні для приховування повідомлення «Тестування вейвлетів» вейвлетів Добеші у файл розміром 14Мб, якість стегозображення збільшується із збільшенням порядкового номеру вейвлета Добеші, що пояснюється більшою кількістю коефіцієнтів у випадку db15, які формують спектр зображення. Проте ці зміни досить незначні, тобто використовувати можна будь який з них. Симлети в свою чергу демонструють кращу якість зображення із вбудованим повідомленням, найкраща з яких sym8. Крім того, результати демонструють, що вбудовування на третій рівень даю суттєво кращі результати.

Література

1. Захаров В. Г. Вейвлет-анализ: теория и приложения. Часть 1: Непрерывное вейвлет-преобразование. – Пермь: ПГУб, 2003. – 100 с.

2. Тарабаєва Д.Д., Шпінарева І.М. Вейвлет перетворення дял приховування інформації в відеофайлах. VIII Міжнародна науково-практична конференція «Інформаційні управляючі системи та технології – Одеса – 2019 – 82 с.

СИСТЕМА ЕЛЕКТРОННОГО ГОЛОСУВАННЯ З ЗАСТОСУВАННЯМ ТЕХНОЛОГІЇ БЛОКЧЕЙН

Тарасов А.І., Шпінарева І.М.
Одеський національний університет ім.І.І Мечникова

Розглянуто можливість використання технології блокчейн в системі електронного голосування. Приведені переваги та доцільність створення системи електронного голосування з застосуванням технології блокчейн.

Ключові слова: система електронного голосування, технологія блокчейн, алгоритм консенсусу, хеш.

The possibility of using blockchain technology in the electronic voting system is considered. The advantages and expediency of creating an electronic voting system based on blockchain technology are presented.

Keywords: electronic voting system, blockchain technology, consensus algorithm, hash.

Розвиток інформаційних систем створює умови для розробки і впровадження сучасних інформаційних засобів, що дозволяють автоматизувати, і, тим самим, більш ефективно реалізовувати процеси управління. Одним з процесів, що необхідно автоматизувати є процес голосування з урахуванням усіх вимог.

Системи голосування, які не виробляють фізичної записи, такі як системи електронного голосування, створюють додаткові предмети для суперечок і підозр. Зникає прозоре підтвердження вибору, виборець повинен довіряти, що система функціонує вірно. З появою технології блокчейн ці проблеми є не актуальні.

Блокчейн – журнал записів, які є зв'язані один з одним та розміщенні у хронологічному порядку, що зберігаються в розподіленій базі даних. Кожен охочий може мати копію записів на своєму пристрої. Кожен запис у цьому журналі є блоком транзакцій, що містить у собі заголовок блоку, в якому зберігається хеш попереднього блоку, дата і час створення блоку та деяка системна інформація, та список транзакцій. Перший блок розглядається як окремий випадок, так як немає попереднього блока.

Для того, щоб додати новий блок у блокчейн необхідно вирішити складну математичну задачу. Такі алгоритми називаються алгоритми консенсусу. Прикладом таких алгоритмів є Proof of Work, Proof of Stake. Основною задачею цих алгоритмів є усунення можливості подвійної трати, DoS-атак та спаму [1]. Найпоширенішим є Proof of Work, принцип якого є вирішити задачу з підрахунком хеша заданої складності. Процес вирішення даної задачі називається майнингом.

Для реалізації системи електронного голосування на основі технології блокчейн необхідно використати централізовану базу даних на сервері виборчої комісії, що буде зберігати виборців, а також розподілену базу даних для голосування, що буде зберігатися на пристроях виборців. Під

час голосування авторизованому користувачу – виборцю надається одноразовий токен для голосування. Для того, щоб проголосувати, виборцю необхідно «замайнити» блок транзакцій, в якому знаходиться його токен з адресою гаманця обраного кандидата. Після цього блок добавляється до розподіленої бази. Кожна транзакція має підпис приватним ключем виборця. Якщо зловмисник змінить яку-небудь інформацію в блоці, йому буде необхідно перерахувати усі наступні блоки в блокчейні, тобто перерахувати усі хеші з заданою складністю, а це неможливо. Таким чином, кожен може відстежити свій голос та перевірити блокчейн на правильність даних.

Впровадження блокчейна дозволяє виконати всі зазначені вимоги щодо системи електронного голосування [2] і є шлях для створення безпрецедентно високого рівня проведення виборів.

Література

1. Proof of Work vs Proof of Stake: Basic Mining Guide. [Електронний ресурс] – Режим доступу: https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/

2. Тарасов А. И., Шпинарева И. М. Обзор методов электронного голосования. Шістнадцята всеукраїнська конференція студентів і молодих науковців «Інформатика, інформаційні системи та технології» – Одеса, 2019 –198с.

ПОБУДОВА КРИПТОСТЕГАНОСИСТЕМИ НА ОСНОВІ ВИКОРИСТАННЯ ШИФРУ AES ТА МЕТОДУ БЛОКОВОГО ПРИХОВУВАННЯ ІНФОРМАЦІЇ

Хомич І., Кухарська Н.
Львівський державний університет безпеки життєдіяльності, м. Львів

У роботі описано процес розробки алгоритмічного та програмного забезпечення, в якому поєднано криптографічні та стеганографічні принципи захисту інформації у комп'ютерних мережах.

Ключові слова: криптостеганосистема, стеганографія, криптографія, шифр AES, метод блокового приховування.

This paper describes the process of developing algorithmic and software software that combines cryptographic and steganographic principles for protecting information on computer networks.

Key words: cryptosystem, steganography, cryptography, AES code, block concealment method.

Питання захисту інформації від несанкціонованого доступу в останні роки стало як ніколи актуальним. Перспективним напрямком програмного захисту інформації є об'єднання методів криптографії та комп'ютерної стеганографії, яке дає змогу позбутися слабких сторін відомих методів захисту інформації та розробити більш ефективні нові нетрадиційні методи забезпечення інформаційної безпеки.

Мета цієї роботи – розробити криптостеганосистему на основі використання шифру AES та методу блокового приховування інформації.

Для побудови криптостеганосистеми інформацію спочатку потрібно зашифрувати, а потім приховати. Опишемо процес шифрування за допомогою шифру AES. Для шифрування використо-вуємо ключ розміром 128 біт, який представимо у вигляді матриці 4x4. На початку процесу шифрування, вхідне повідомлення розбиваємо на блоки (*state*) розміром 16 байт або 128 біт. Кожен блок згідно AES-алгоритму шифрується незалежно один від одного за декілька етапів – раундів.

Схема криптоперетворень виглядає наступним чином. Спочатку розширюємо ключ шифрування для того, щоб мати набір даних для раундових ключів та сумуємо раундовий ключ з основним. Далі реалізовуємо наступні чотири кроки. Замінюємо байти *state* відповідно до таблиці замін, циклічно зсовуємо рядки, після чого здійснюємо перестановку стовпців та знову підсумовуємо з раундовим ключем. Ці операції повторюємо під час кожного з дев'яти раундів. Після цього реалізовуємо десятий завершальний раунд, який включає в себе наступні три кроки. Здійснюється заміна байтів *state* відповідно до таблиці замін, циклічно зсовуються рядки та виконуються сумування з раундовим ключем [2].

Зашифроване вище описаним способом повідомлення вбудовуємо в аудіоконтейнер методом блокового приховування інформації. ASCII-коди символів подаємо у вигляді вектора бітів. Послідовність звукових амплітуд файла контейнера розбиваємо на n блоків, де n – кількість біт повідомлення. Приховуючи i-ий біт повідомлення, виконуємо наступні дії. В i-ому блоці аудіо-файла сумуємо за модулем 2 найменші значущі біти (НЗБ) усіх його елементів. Отриману суму порівнюємо із значенням біта повідомлення. Якщо вони не дорівнюють один одному, інвертуємо НЗБ будь-якого, обраного випадковим чином, елемента блоку. У підсумку отримаємо, що у кожному блоці аудіо-сигналу буде "зашито" по одному бітові повідомлення. Під час процедури видобування отримуємо їх, додаючи за модулем 2 НЗБ елементів блоків [1, 3].

Розроблені нами комплекси програм дають змогу зашифрувати записані в TXT-файлах дані та приховати їх в аудіофайлах формату WAVE будь-якої частоти дискретизації та бітності.

Література:

1. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. Киев : МК-Пресс, 2006. 288 с.

2. Ako Muhamad Abdullah Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data. *Cryptography and Network Security*. URL: https://www.researchgate.net/publication/317615794.

3. Хомич І. В., Кухарська Н. П. Реалізація методу блокового приховування текстового повідомлення у звукових файлах *Проблеми та перспективи системи безпеки життєдіяльності* : зб. наук. праць XIII Міжнар. наук.-практ. конф. молодих вчених, курсантів та студентів, (м. Львів, 22-23 берез. 2018 р.). Львів, 2018. С. 253-254.

Напрям 6

Інформаційні війни

УДК 004.62

ІНФОРМАЦІЙНА ВІЙНА ЯК ЗАГРОЗА БЕЗПЕЦІ ДЕРЖАВИ

Бойко В.С., Бурак Н.Є.
Львівський державний університет безпеки життєдіяльності

У роботі здійснено огляд сучасних загроз інформаційній сфері діяльності громадян України. Проведено аналіз поточного стану безпеки інформації та шляхи виникнення загроз.
Ключові слова: інформаційна війна, захист, інформаційна безпека, загрози, кібератака.

In this paper were reviewed the current threats to the information sphere of Ukrainian citizens. Also were analyzed the current state of information security and the ways of threats emerged.
Keywords: information war, protection, information security, threats, cyberattack.

У сучасних умовах глобальної інформатизації, інформація є першочерговим та необхідним ресурсом для прийняття рішень з важливих питань у різних сферах діяльності людини. Тому, володіння даними в поєднанні з контролем інформаційного простору, управлінням його потоками та захистом є надзвичайно важливою та серйозною проблему. Причиною цього є те, що за інформацію, як ресурс, яким можна користуватись та здійснювати вплив на інших, розгортається боротьба на всіх рівнях сучасних суспільних відносин.

Сьогодні виділяють наступні три рівня забезпечення інформаційної безпеки суспільства:

- рівень особи;
- суспільний рівень;
- державний рівень.

Вплив поширення кібератак призвів до виникнення нового методу боротьби –інформаційних війн, до яких на міжнародній арені цифрового простору особливий інтерес. По-перше, це пояснюється високим рівнем глобалізації та “ущільнення” простору існування націй і держав, а по-друге – з бажанням звести до мінімального можливий фізичний вплив, а також з метою запобігання застосуванню військової сили у сучасних міжнародних відносинах, оскільки технологічний розвиток ІТ постійно відкриває нові та

більші можливості по збору, обробці, зберіганню та розповсюдженню інформації, є основним знаряддям кібератак.

Поточний стан національної безпеки нашої держави свідчить, що інформаційні війни, які ведуться проти України призводять до появи наступного ряду загроз:

- військові дії на сході країни здійснюються у супроводі масових кібер та інформаційно-психологічних операцій;
- латентні (приховані, мережеві) заходи противника;
- неправомірні інформаційно-пропагандистські підпільні організації, розташовані в середині країни;
- низький рівень застосування заходів протидії, а саме: більшість внутрішніх загроз виникають на фоні сформованого у радянський період світогляду та успадкованої бюрократичної системи, яка сьогодні не відповідає вимогам сьогодення;
- високий рівень поширення кібератак, і як результат – ріст масштабів кібервійни.

Основною метою інформаційної війни – є послаблення моральної і матеріальної сили противника або ж конкурента, в той же час зміцнивши власні, застосувавши елементи пропагандистського впливу на свідомість людини в сферах її життєдіяльності та розвитку.

На основі аналізу даних сайту StopFake.org, який було засновано у 2014 році з метою перевірки та спростування пропагандистської неправдивої інформації у електронних сервісах, у період з березня 2014 р. по червень 2017 р командою даного сайту було опрацювала більше 800 новин/повідомлень, які містили фіктивні дані та інформацію про Україну загалом та окремі сфери діяльності зокрема. Усі статті, які вони опрацювали можна класифікувати на чотири категорії: російські ЗМІ, ЗМІ інших країн, українські ЗМІ, та ЗМІ невизнаних ЛНР та ДНР (див. Рис. 1). Частка російських засобів масової інформації, які поширюють неправдиву інформацію сягає 47 %, що підтверджує значний вплив на суспільство України проросійських ЗМІ. За останніх два роки (2018–2019 роки) команда сайту StopFake.org здійснила аналіз 1101 різних статей (див. рис. 2.).

Рисунок 1 – Розподіл опрацьованих статей за джерелами

Рисунок 2 – Кількість опрацьованих статей за 2018-2019 року

Результати досліджень дають зрозуміти, що використання засобів масової інформації є важливою зброєю в інформаційній війні, які дають змогу маніпулювати суспільством та розхитувати ситуацію в середині країни, провокуючи там самим виникнення заворушень та протестів. Наслідки таких діянь можуть бути катастрофічні – знищення інфраструктури та падіння економіки країни через припинення роботи підприємств і державних установ. Однак основною зброєю в таких війнах є кібератаки.

Україна веде активну політику щодо протидії інформаційній війні та застосовує жорсткі методи боротьби з кібератаками. Результатами цього є забезпечення належної безпеки громадян, їх захист, блокування неправдивої інформації, що сприяє поширенню достовірних новин про події в державі, а це є основним фактором формування суспільної думки та підтримання безпечних умов життєдіяльності.

На сьогоднішній день для досягнення захисту здійснено багато, зроблено важливі кроки на «світовій шахматній дошці», отримано підтримку світових лідерів та організацій, однак до стану повної безпеки ще далеко. Значка кількість завдань ще повинна бути виконана, комбінації дій ґрунтовно продумані, і тоді результати не заставлять на себе чекати.

Література

1. Фейки, спростовані проектом StopFake в 2014-2017 роках: наративи та джерела. [Електронний ресурс]. – Режим доступу: https://www.stopfake.org/uk/fejky-sprostovani-proektom-stopfake-v-2014-2017-rokah-narratyvy-ta-dzherela/

2. Brzhevska, Z., Dovzhenko, N., Kyrychok, R., Gaidur, G., & Anosov, A. (2019). ІНФОРМАЦІЙНІ ВІЙНИ: ПРОБЛЕМИ, ЗАГРОЗИ ТА ПРОТИДІЯ. Кібербезпека: освіта, наука, техніка, 3(3), 88-96. https://doi.org/10.28925/2663-4023.2019.3.8896

3. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення / Ю. О. Горбань // Вісник Національної академії державного управління при Президентові України. – 2015. – № 1. – С. 136-141. – Режим доступу: http://nbuv.gov.ua/UJRN/Vnadu_2015_1_21.

4. Бурак Н.Є. Управління проектом підготовки і навчання кіберрятувальника: компетентнісний підхід / Н.Є. Бурак, Ю.П. Рак // Вісник Львівського державного університету безпеки життєдіяльності. – Львів, 2013. – №8. – С. 55-60

5. Головатий Р. Р. Управління безпекою на стадії планування проектів створення об’єктів з масовим перебуванням людей : автореф. дис. канд. техн. наук: 05.13.22; Держ. служба України з надзвичайн. ситуацій, Львів. держ. ун-т безпеки життєдіяльності. Львів, 2018. 24 с.

ІНФОРМАЦІЙНА ВІЙНА ЯК СЬОГОДЕННА РЕАЛЬНІСТЬ

І.В. Бородін, А.Б. Тарнавський
Львівський державний університет безпеки життєдіяльності, м. Львів

Анотація: Розглянута проблема інформаційних війн у сучасному суспільстві, вплив та наслідки, які утворюються з цієї проблеми. Вказана роль України у сучасній інформаційній війні.
Ключові слова: мережа “Інтернет”, інформаційна війна, соціальні мережі, медіа-простір.

Summary: The problem of information wars in the modern society, the impact and consequences that arise from this problem are considered. The role of Ukraine in the modern information war is indicated.
Keywords: network "Internet", information war, social networks, media-space.

На сьогодні усі високо розвинуті країни мають доступ до необмеженої кількості інформації, якою люди можуть користуватись у суспільних, економічних, політичних, соціальних та інших сферах життя. За останні тридцять років відбувся інформаційний бум, який дав можливість людству розвиватися усе швидше, і це, неодмінно, – позитивна сторона. Але існує ще й негативна сторона у вигляді інформаційного сміття, підривання ідеалів і духовності людства та великого шансу на інформаційні катастрофи, у тому числі й інформаційні війни.

Може здаватись, що інформаційні війни з’явились нещодавно, – після початку розвитку мережі “Інтернет”, але насправді це не так. Подібного роду інформаційні війни існували ще задовго до винаходу Інтернету, телета радіомовлення. У Біблії і існують згадки про Гедеона, який маючи невелике військо, зміг перемогти ворога залякавши його настільки, що той вдарив по своїх же військах. Крім того, є згадки в історії древнього Риму як інформація та дезінформація допомагали у веденні війн та врегулюванні громадських конфліктів.

Але у сучасному XXI сторіччі існує найкраще середовище для ведення інформаційної війни – мережа “Інтернет”. Кожна людина, яка має доступ до цієї мережі може розпочати війну просто сидячи за домашнім комп’ютером або смартфоном. Невеличкий викид дезінформації може перетворитись у “сніжний ком”, який все більше набирає масу та тягне все за собою. Саме цим і користуються корпорації з різним масштабом впливу. Але не тільки люди та корпорації користуються можливістю використання та управління інформацією, а й країни, які використовують ресурси заради набуття конкурентоздатної переваги над противником.

Вплив інформаційної війни дуже сильно відчула на собі Україна за останні шість років. Як було наведено вище – невідомо коли така війна починається, але наслідки цієї війни ми побачили ще в кінці 2013 року, коли люди почали обурюватись щодо рішення зупинки підготовки до підписання Угоди про асоціацію між Україною та ЄС. Саме тоді було зрозуміло, що тодішній Президент та частина Верховної Ради під впливом російської сторони робили усе можливе для надання Росії можливості контролю над Україною.

Наступним прикладом є подія, яка сколихнула увесь світ – проведення у Криму незаконного референдуму щодо приєднання півострову до території Росії. Російська сторона робила усе можливе для того, що б показати на весь світ, що жителі Криму бажають бути росіянами, і що вони всі до одного – росіяни. Після цього такий самий прийом провели по відношенню до Донбасу. Facebook, Twitter та інші соціальні мережі вибухали від постів та коментарів російських ботів на захист ідеї референдуму, ідей того, що в Україні живуть окремо “западеньці” і окремо жителі Донбасу, а кожен регіон та кожна область живуть окремо, а також в Україні немає єдності. Кожна з цих ідей багато разів “обсмоктувалась” ботами у соціальних мережах та на кожному російському телеканалі.

Література

1. История информационных войн. Часть 1 / Н. Л. Волковский. – СПб.: ООО Издательство “Полигон”, 2003. – 510 с. – (Военно-историческая библиотека).

УДК 654:316.774.323.28

ВИДИ ІНФОРМАЦІЙНИХ ВІЙН

Бужанська М., Манич Т.
Львівський торговельно-економічний університет

Анотація: У публікації досліджується проблема інформаційної безпеки країни та захисту національного інформаційного простору від негативних інформаційних впливів. Розкрито поняття інформаційної війни, форми і види інформаційних війн. На конкретних прикладах висвітлено дію інформації та пропаганди на різні сфери та верстви суспільства, протидію їх наступу. Показана роль інформаційної війни у системі сучасних економічних, політичних та військових протистоянь.

Ключові слова: інформаційна безпека, інформаційна війна, інформація, пропаганда, гібридна війна, Україна.

Summary: The publication explores the problem of information security of Ukraine and the protection of the national information space from negative influences. We considered the question of information war, form and kind of information wars. On specific examples of the highest information about and dissemination in various fields and loyalty of people, neutralization of their activity. Shown results of information war in today's economic, political and military confrontations.

Keywords: information security, information war, information, propaganda, hybrid war, Ukraine.

Поняття інформаційної війни сьогодні є одним із найзагрозливіших для безпеки країни. Поняття «інформаційна війна» ввів у науковий обіг американський дослідник М. Маклюен, який проголосив тезу : «Істинно тотальна війна – це війна за допомогою інформації». Інформаційна війна — це маніпулювання інформацією, якій довіряє об'єкт, без відома об'єкта, щоб об'єкт приймав рішення проти своїх інтересів, але в інтересах того, хто веде інформаційну війну. Як наслідок, незрозуміло, коли починається інформаційна війна, наскільки вона сильна або руйнівна і коли закінчується [1].

За всю історію ведення інформаційних війн, можна виділити такі їх різновиди:

1. Інформаційна війна в мирний час. Головна зброя в такій війні – інформація, яка впливає на масову свідомість. Цей вплив діє на громадську думку та змушує населення чинити в інтересах зацікавленої сторони. Як правило це інформація, яка не відповідає правді; зміна пріоритетності інформації; зміна процесу подачі інформації. Найчастіше подібний різновид війни можна побачити під час виборчої кампанії.

2. Інформаційна війна у воєнний час. У цьому контексті інформаційна війна – допоміжний механізм реальної війни. Інформаційний вплив у воєнний час може допомагати виконувати військові функції або замінювати їх.

3. Інформаційна операція при вирішенні миротворчих проблем. Така операція виконує такі завдання: підтримка нової влади, вироблення єдиної думки щодо певної ситуації, введення пропагандистських повідомлень щодо опонентів тощо. При цьому завдання такої операції одне – сформувати нову модель поведінки громадськості. Міжнародні миротворчі сили не раз уже відігравали головну роль у відновленні нормального життя в тих чи інших країнах або у гасінні міждержавних збройних конфліктів. На загал, сьогодні складається враження, що більшість політиків й експертів вважає введення міжнародних миротворчих сил на окуповану територію Донбасу ледь не панацеєю, яка приведе до встановлення в регіоні миру та його наступної інтеграції до України. Мовляв, спершу стане фактом підтримання дійсного «режиму тиші» на так званій «лінії розмежування» українських військ і формувань протилежної сторони, потім буде встановлений міжнародний контроль за тією ділянкою українсько-російського кордону, яка сьогодні перебуває в руках окупантів, затим будуть забезпечені умови для проведення в ОРДЛО демократичних виборів і, нарешті, після виборів почнеться процес мирного повернення «особливих районів» до Української держави. Що ж стосується миротворчих сил на теренах ОРДЛО, то їх, як виглядає, не будуть озброювати важкою технікою та надавати їм потужне авіаційне прикриття. Бронетранспортери, автомобілі, легка стрілецька зброя – і значно менша чисельність, ніж у двох «армійських корпусів» «ЛДНР», які безпосередньо перебувають під російським командуванням, не рахуючи численних «козаків» й «ополченців». Причому танків у цих військ більше, ніж, скажімо, у Великої Британії. За таких обставин миротворці думатимуть радше про власну безпеку, ніж не про забезпечення порядку та контроль за діями російських і проросійських формувань. А 5 тисяч поліцейських аж ніяк не зможуть забезпечити цілодобове дотримання порядку на всій території ОРДЛО, де і в мирні часи вистачало правопорушень різного ґатунку.

4. Інформаційна операція при вирішенні соціальних проблем. Найчастіше інформаційне повідомлення може втручатися в масову свідомість, диктуючи стиль поведінки та дій. У виняткових випадках суспільство може протистояти такому впливу, і відбувається його розпад.

5. Інформаційна війна пропагандистського та суто інформаційного характеру. Інформаційна війна виступає як допоміжний механізм збройної війни. Під впливом ЗМІ видимий світ перестає бути реальністю, перетворившись у віртуальний, цілком сконструйований світ вимислу, який створено професійними технологами. Так, за часів Першої світової війни вперше почали використовувати метод пропаганди. Але на той момент вона мала інформаційний характер, джерело повідомлення не приховували. Проте вже під час Другої світової війни почали використовувати “чорну пропаганду”: джерело повідомлення приховували, інформацію подавали не в повному обсязі або не зовсім точно, пропаганда була багатофункціонального характеру. У післявоєнний радянський період були створені досить

великі інформаційні кампанії, пропаганда заповнила майже весь офіційний інформаційний простір. Після цього відбувається перехід до інформаційного суспільства й створюється основа для ведення війни нового типу – суто інформаційної (як окремої стратегії впливу), в якій здійснюється вплив на суспільну свідомість. Одне із завдань цієї війни полягає в тому, щоб відірвати суспільну свідомість від реальності, змусити людей діяти в чужих інтересах.

6. Інформаційна війна з використанням Інтернету. Сьогодні інформаційна війна йде не тільки через офіційні канали ЗМІ, а й у просторах Інтернету. Інформаційних потоків стає все більше, створюються події, яких не було насправді, користувачам не просто відрізнити правду від вигадки. Соціальні мережі помітно впливають на взаємодію державної влади і суспільства. Вони все частіше стають своєрідними посередниками між владою та громадянами через офіційні сторінки політиків та центральних органів, на яких активно пропагуються основні позиції влади. Саме представленість політиків у мережі позитивно впливає на створення їхнього іміджу в очах виборців, адже «ближчі до народу», вони видаються більш чесними та людяними. Проте читаючи новини та повідомлення від представників владних структур, слід враховувати те, що більшість повідомлень спрямовані не поінформувати користувача, а вплинути на нього.

Як бачимо, спектр засобів впливу на думку особи та суспільства доволі широкий – від кібератак до організації акцій протесту, терористичних актів та організованого збройного опору. Інформаційно-психологічні операції є сьогодні невід'ємною частиною систем управління військами, політичними та економічними процесами. У зв'язку з активною віртуалізацією людства, такі конфлікти переносяться у інтернет-простір і набувають формату мережевих он-лайн протистоянь. У системі сучасних економічних, політичних та військових протистоянь інформаційні війни в соціальних он-лайн мережах займають важливу роль, як один з ключових супроводжувальних процесів. Інформаційна зброя такого типу здатна знищувати чи, як мінімум, блокувати системи координації, поширення інформації та інші відповідні управлінські процеси, а також перешкоджати роботі певних центрів керування.

Література:

1. *М. А. Ожеван, О. В. Шевченко*. Війна інформаційна // Українська дипломатична енциклопедія: У 2-х т./Редкол.:Л. В. Губерський (голова) та ін. — К: Знання України, 2004 — Т.1 — 760с. ISBN 966-316-039-Х

2. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи [Електронний ресурс] / В. Петрик. – Режим доступу: http://www.justinian.com.ua/article.php?id=3222 14. Почепцов Г. Сучасні інформаційні війни / Г. Почепцов. – К. : Вид.дім "Києво-Могилянська академія", 2015. – 497 с.

УДК 654:316.774.323.28

ІНФОРМАЦІЙНА БЕЗПЕКА ВАЖЛИВА СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Бужанська М., Мацега В.
Львівський торговельно-економічний університет

Анотація: У публікації досліджується проблема інформаційної безпеки України та захисту національного інформаційного простору від негативних інформаційних впливів. Авторами визначено загрози інформаційній безпеці країни. Проаналізовані шляхи вирішення проблем інформаційної безпеки. Авторами висвітлено актуальні питання інформаційної безпеки країни. Розглянуті шляхи та методи забезпечення інформаційної безпеки в Україні.
Ключові слова: Інформація, інформаційна безпека, національна безпека.

Summary: The publication explores the problem of information security of Ukraine and the protection of the national information space from negative influences. The authors identified dangers to the country's information security. The ways of solving information security problems are analyzed. The authors cover topical issues of information security of the country. Ways and methods of providing information security in Ukraine.
Keywords: Information, information security, social networks.

Національний інформаційний простір України, на даний час, зазнає суттєвих загроз, та викликів, які становлять небезпеку функціонування держави, її політичного та економічного розвитку, інтеграції у європейські та євроатлантичні структури. Основними загрозами національній безпеці України в інформаційній сфері є – сукупність умов та чинників, які становлять небезпеку життєво важливим інтересам держави, суспільства і особи через можливість негативного інформаційного впливу на свідомість та поведінку громадян, а також на інформаційні ресурси та інформаційно-технічну інфраструктуру [1]. У Законі України “Про основи національної безпеки” зазначено, що однією з основних загроз інформаційній безпеці є “намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації” [2].

Поняття інформаційної загрози відкриває новий тип соціально політичного (переважно невоєнного), конфлікту, що характеризується застосуванням сторонами мережевих форм організації і відповідних їй доктрин, стратегій і технологій інформаційної епохи. Необхідно також пам’ятати, що система інформаційної безпеки держави є складовою частиною загальної системи національної безпеки країни і повинна базуватись на органах державної влади, які мають узгоджено здійснювати діяльність із забезпечення інформаційної безпеки на основі єдиних правових норм. Дану систему необхідно розбудовувати на основі розмежування повноважень органів законо-

давчої, виконавчої і судової влади в сфері інформаційної безпеки, а також органів державної влади. У Доктрині інформаційної безпеки України, визначено загрози інформаційній безпеці країни: поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України; зовнішні деструктивні інформаційні впливи на суспільну свідомість через ЗМІ, а також мережу Інтернет; деструктивні інформаційні впливи, які спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності та недоторканності України; прояви сепаратизму в ЗМІ, а також у мережі Інтернет за етнічною, мовною, релігійною та іншими ознаками [3].

Інформація стала чинником, який може призвести до військових конфліктів та поразок у них, дезорганізувати державне управління, фінансову систему, роботу наукових центрів. Як бачимо, чим вищий рівень інтелектуалізації та інформатизації суспільства, тим необхідніша надійна інформаційна безпека. Інформаційна безпека - стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Вирішення проблеми інформаційної безпеки повинно реалізовуватись шляхом: створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів; підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань; вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері; розгортання та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація. Сьогодні в Україні створено низку організаційних структур, спрямованих на вирішення проблем управління інформаційною безпекою держави, вдосконалено нормативно-правове забезпечення національної безпеки в інформаційній сфері, а також відновлюється система підготовки фахівців з інформаційної безпеки.

Політика забезпечення інформаційної безпеки в Україні базується на наступних засадах: обмеження доступу до інформаційного ресурсу є винятком із загального принципу відкритості інформації й реалізується тільки відповідно до чинного законодавства; суб'єкти, які збирають, накопичують і обробляють персональні дані й конфіденційну інформацію, несуть відпові-

дальність перед законом за збереження і використання; держава забезпечує захист суспільства від хибної, викривленої і недостовірної інформації, що надходить через засоби масової інформації; держава реалізує контроль за створенням і використанням засобів захисту інформації шляхом їхньої обов'язкової сертифікації та ліцензування діяльності в галузі захисту інформації; держава сприяє всебічному розвитку української мови як основного інструменту перетворення накопичених людством знань в інформаційний ресурс України [2].

Отже, інформаційна безпека суспільства, держави характеризується ступенем її захищеності, та, як наслідок, стійкістю головних сфер життєдіяльності у відношенні до небезпечних інформаційних впливів. Інформаційна безпека визначається здатністю нейтралізувати такі впливи. Основні акценти державної інформаційної політики повинні зосереджуватись на забезпеченні права на достовірну, повну та своєчасну інформацію, свободи слова та інформаційної діяльності в національному інформаційному просторі, недопущення втручання в зміст та внутрішню організацію інформаційних процесів, крім випадків, визначених законодавством відповідно до Конституції України; збереженні та вдосконаленні вітчизняного національного інформаційного продукту та технологій, національно-духовних та культурних цінностей України; забезпеченні інформаційної та національно-культурної ідентифікації України у світовому інформаційному просторі; гарантування державної підтримки та розвитку ресурсів науково-технічної продукції та інформаційних технологій.

Література

1. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи [Електронний ресурс] / В. Петрик. – Режим доступу: http://www.justinian.com.ua/article.php?id=3222 14. Почепцов Г. Сучасні інформаційні війни / Г. Почепцов. – К. : Вид.дім "Києво-Могилянська академія", 2015. – 497 с.

2. Про основи національної безпеки України : Закон України // Відомості Верховної Ради України. – 2003. – № 39. – Ст. 351. Із змінами, внесеними згідно із Законом № 3200-IV (3200-15) від 15.12.2005. ВВР. – 2006. – № 14. – Ст. 116.

3. Доктрина інформаційної безпеки України [Електронний ресурс]. – Режим доступу: http://www.zakon3.rada.gov.ua/laws/ show/514/2009 5.

ІНФОРМАЦІЙНА ВІЙНА ЯК СОЦІАЛЬНА НЕБЕЗПЕКА ДЛЯ ДЕРЖАВИ

Ільчишин Я., Марич В. Соловйов Д.
Львівський державний університет безпеки життєдіяльності

Проаналізовано та проведено аналіз інформаційних війн як соціальної небезпеки для держави. Розглянуто проблеми інформаційної війни на фоні конфлікту в Донбасі та анексії АР Крим. Виокремлено і проаналізовано інформаційні війни внутрішнього характеру, що відбуваються в середині країни переважно між політичними силами, та зовнішнього характеру – безпосередньо між державами.

Ключові слова: інформаційна війна, соціальна небезпека, агресія, інформація, інформаційна зброя, засоби масової інформації, методи інформаційної війни.

Information wars are analyzed and analyzed as a social danger for the state. The problems of information war against the background of the conflict in Donbass and annexation of the Autonomous Republic of Crimea are considered. Information wars of internal character, occurring in the middle of the country mainly between political forces, and external character, directly between the states, are separated and analyzed.

Keywords: information war, social danger, aggression, information, information weapons, mass media, methods of information war.

Війна інформації на сьогодні стала одним з найнебезпечніших видів зброї. Безпосередньо застосування цієї зброї, через анексію АР Крим та війну на Донбасі відчувають на собі громадяни України. Користуватися компроматами, виливанням бруду, підкиданням неправдивої інформації, намагання за допомогою інформації ввести в оману стало для агресора сенсом життя.

Інформація має вплив на маси, тобто за умови вдалого маніпулювання свідомістю мас можна досягти практично будь-якої мети: знищити опонента, прибрати з дороги конкурентів чи розпалити війну.

Не офіційно вважається, що засоби масової інформації в державі мають статус четвертої гілки влади. Журналісти тримають у руках зброю, тільки не завжди використовують її за призначенням. На тлі останніх подій, які відбуваються в Україні можна зрозуміти, що основна боротьба між політичними силами та з агресором відбувається за допомогою інформації, тобто в країні інформаційна війна набула нового статусу.

Інформаційна війна Росії проти України призвела до того, що більше половини опитаних росіян готові воювати з українцями. Вірусом ненависті насамперед заражені молоді люди, які ніколи не були в Україні і не мають контактів із її громадянами. Старших людей лякають “бандерівця-

ми-головорізами, які прийшли до влади". Це результат планомірної тотальної брехні, яка розробляється ідеологами Кремля та транслюється на їхньому телебаченні [1]. Щороку Росія витрачає проти України на інформаційну війну до чотирьох мільярдів доларів [2].

Інформаційна війна – циклічний або лінійний обмін інформацією, яка може/має спричинити певну шкоду отримувачу, а автору надати певну перевагу. Об'єктом інформаційної війни є як масова свідомість, так і індивідуальна [3].

Нав'язування чужих цілей – це те, що робить інформаційну війну війною і відрізняє її від звичайної реклами. Інформаційний вплив містить спотворення фактів або нав'язує аудиторії емоційне сприйняття, вигідне стороні агресора. Як правило, методами інформаційної війни є викид дезінформації, або подання інформації у вигідному для себе ключі. Дані методи дозволяють спотворювати оцінку того, що відбувається, деморалізувати громадян, і, в перспективі, забезпечити перехід на сторону інформаційного агресора [4].

Мета інформаційної війни – послабити моральні і матеріальні сили супротивника або конкурента та посилити власні. Вона передбачає заходи пропагандистського впливу на свідомість людини в ідеологічній та емоційній галузях.

Істотна залежність сучасної цивілізації від інформаційної складової зробила її набагато уразливішою. Швидкість інформаційного обігу й поширення інформаційних мереж багаторазово збільшили ефективність саме інформаційної зброї. Додатково ускладнює ситуацію «відкритість» сучасних суспільств. Основні методи інформаційної війни засновані на блокуванні або спотворенні інформаційних потоків та процесів прийняття рішень супротивника. Інформаційна війна розглядає інформацію як окремий об'єкт або як потенційну зброю та вигідну ціль. Інформаційну війну можна розглядати як новий вид бойових дій.

Війну інформації також розпочинають тоді, коли треба досягти якоїсь мети. Як приклад можна розглянути війну між США та Іраком. Експерти висувають різні версії, щодо справжньої мети нападу США на Ірак. Одною з версій конфлікту в Іраку було зовсім не наявність зброї масового знищення, а велика кількість нафти, яку прагнув взяти під свій контроль американський уряд. Тільки раніше приводу не було розпочати цю війну, треба було людству якось пояснити таку позицію, довелося провести цілу низку виливів інформації на маси. Конфлікт в Іраку триває, а зброю так і не знайшли.

В інформаційному суспільстві, на порозі якого перебуває все прогресивне людство, життєві стандарти не диктуються реальністю, а вміло пропагуються й поширюються за допомогою нових технологій. Основним об'єктом впливу є масова свідомість.

Зрозуміло, що інформаційні війни частіше використовуються на міжнародному рівні. Україна і Росія вже не один рік ведуть таку війну. Росія постійно провокує гучними заявами український уряд та й просто зневажливо ставиться до українців у своїх інформаційних матеріалах.

Інформаційні війни точаться не лише між країнами і охоплюють міжнародну аудиторію, а й на місцевому рівні, тобто в середині держави, регіону та колективу. Зокрема, українські політики, як ніколи, вивчили технологію ведення інформаційної війни. Останнім часом дедалі популярнішим серед українських політиків стає знищення опонента за допомогою так званих «інформаційних бомб».

Якщо розібратися в суспільних процесах можна зробити висновок, що інформаційна війна в світі вже давно розпочалася. Вона набагато страшніша, бо знищення відбувається завдяки інформації, що немає матеріального втілення і знищити інформацію яка є в суспільстві надзвичайно важко. І, якщо кулі і снаряди відомо звідки летять, то інформаційні бомби з'являються несподівано та у невідомому місці, іноді відбити таку атаку взагалі неможливо. Зважаючи на розвиток технологічного та інформаційного прогресів в суспільстві і маючи на руках таку інформаційну зброю та вміння впливати на аудиторію – можна завоювати світ.

Література:

1. Штогрін І. Називай агресію "захистом": принципи інформаційної війни проти Росії [Електронний ресурс] / Ірина Штогрін. – Режим доступу : www.radiosvoboda.org/cntent/article/25293307.html.;

2. Інформаційна війна коштує Росії 4$ мільярди [Електронний ресурс]. – Режим доступу : www.ukrinform.ua/ukr.news/2030605.;

3. Навчальний посібник сучасні інформаційні війни у мережевому он-лайн просторі Курбан О. В.;

4. Електронний ресурс: http://novosti.dn.ua/article/4889-informaciyna-skladova-gibrydnoi-viyny-poglyad-z-donbasu;

5. Електронний ресурс: https://www.pravda.com.ua/articles/2006/04/20/4399050/

МЕТОДИ ПРОТИДІЇ БУЛІНГУ У СОЦІАЛЬНИХ МЕРЕЖАХ

Ляшенко А., Герасимов А., Прокопов С.
Дніпропетровський державний університет внутрішніх справ

Анотація. Тези присвячені порівняльній характеристиці зарубіжних та вітчизняних методів боротьби з булінгом
Ключові слова: булінг, методи боротьби, цькування, інтернет, кодекс поведінки, батьківський контроль.

Abstract. Theses are devoted to the comparative characteristics of foreign and domestic bulling methods
Keywords: bulling, methods of struggle, harassment, internet, code of conduct, parental control.

Булінг – це одна з найголовніших проблем, з якою потрібно боротися на даний момент. Усі ми живемо у еру цифрових технологій, кожна мала чи доросла людина має сторінку у соціальних мережах, де найчастіше люди зустрічаються зі цькуванням. Головним чинником, через який цькування проходить саме у мережі інтернет, є елемент безпеки за те, що булер залишиться непокараним.

Розглянемо закордонні методи боротьби з булінгом:

Link crew (Команда зв'язку).

Ця система існує у північноамериканській практиці (США та Канаді) та вигадана Джоном Дьюи.

Створюється команда зв'язку, з самих позитивних, усміхнених , активних з лідерськими якостями учнів школи. Їх відбирають та спеціально готують (для цього їм на тиждень раніше потрібно повернутися з літніх канікул, але ніхто не скаржиться, це велика честь потрапити до Команди. Для чого їх готують? Стати "шефами" учнів молодше . Наприклад, учень одинадцятого класу курирує учнів дев'ятого. Проводячи співбесіди, особові розмови, переглядаючи коментарі на сторінках у соціальних мережах вони попереджають значну кількість випадків цькування серед однолітків **[1].**

По принципу дії мережі Facebook

У мережі Facebook існує алгоритм, який відслідковує небажану для перегляду користувачів інформацію, де скриває її від доступу до користувачів. Існує алгоритм, який допомагає фіксувати інформацію зі словами, які можуть бути пов'язані з цькуванням. Програма збирає посилання на публікації, які входять у зону булінгу. Користуючись інформацією, яка збирається програмою, та перевіряє її за допомогою підрозділів поліції. Це значно знижає рівень образ та цькування. Через це присутнє у свідомості людей розуміння того, що мережу контролюють органи поліції, та відсутній елемент безкарності.

"Дитячий режим" або Батьківський контроль.

Одним із варіантів, який існує, є створення окремого режиму у програмах для виходу в мережу Інтернет, під назвою "Дитячий режим". Цей додаток контролює дії дитини у мережі, та блокує доступ до посилань, на яких може знаходитись інформація небажана для перегляду дитиною. Встановлюється програма на комп'ютер чи мобільний пристрій, яка відслідковує дії дитини у мережі, пос-

тійно інформуючи батьків про підозрілу активність зі сторони дитини. Також до її функцій можна віднести фільтрування новин, реклами та іншої інформації, яка б могла нашкодити дитинні у мережі. Отримуючи повідомлення про активність, батьки матимуть змогу вирішити проблеми, з якими стикається їх дитина або звернутися за допомогою до психолога **[2]**.

Кодекс поведінки у мережі Інтернет

Повернемося до Сполучених Штатів. Вони надзвичайно продуктивно працюють над проблемою булінгу. Так, наприклад, у 20-ти штатах передбачена кримінальна відповідальність за інтернет-знущання. У кожному з них, крім Монтани, закон наділяє правом навчальні заклади ідентифікувати випадки булінгу та користуватися так званим кодексом безпеки (SafeSchoolPlan), який передбачає всі заходи та міри, які будуть використані навчальним закладом у випадку ідентифікації цькування. Ведення кодексів поведінки, які будуть навчати дітей ще з малечку поводженню у мережі. Встановлюватимуться інструкції як для осіб, які зіштовхнулися зі цькуванням, так і для тих, хто не мав зв'язку з булінгом. Інформуватимуть усіх про те, яке покарання їх чекає, тим самим, попереджаючи та запобігаючи прояву булінгу **[3].**

В Україні, як і у всьому світі, цькування в Інтернеті набрало такого розголосу, що ми не можемо не усвідомити те, що воно заполонило увесь простір. Такі соцмережі і месенджери як: Instagram, Facebook, Twitter, Telegram, Viber, WhatsApp не виняток. Через своє шифрування та конфіденційне збереження інформації, які нам гарантує розробник, влада країни не має права доступу до листування користувачів, що й захищає булерів у своїх протиправних діях. Ми пропонуємо розробити спеціальний додаток на смартфон, який допоможе інформувати підрозділи поліції для розкриття справ, пов'язаних з булінгом. Як це буде працювати? Наприклад, звичайний користувач в Інтернеті побачив пост з погрожуючим або принижуючим характером, він робить скріншот, який має інформацію щодо акаунту, з якого був відправлений запис, година, о котрій зроблено публікацію, а також, у деяких випадках, місце (геолокацію), з якого надіслано цю інформацію. Свідки – ті, хто побачив даний запис роблять фіксацію правопорушення скріншотом, заходять у додаток, де є спеціальна форма. Там вони можуть вибрати різні категорії: вид правопорушення (цькування, приниження гідності, погрози і навіть заклик до суїциду), метод булінгу (надіслання листів тестового/аудіо/фото/відео характеру), кіл-ть булерів (один/декілька), соц.мережа або месенджер (Instagram/Facebook/Twitter/ Telegram/Viber/WhatsApp), інформація щодо булера (логін у соц. мережі/стать/ вік), інша інформація щодо цього (як правило у текстовому характері з можливістю додавання фото, аудіо, відео доказів). А потім, заповнивши дану форму, вони можуть відправити цей запит операторам поліції, які будуть обробляти їх. Після фільтрування цих запитів вони будуть направлятися у спец. підрозділи кіберполіції по боротьбі з булінгом. І певна група фахівців вже буде досліджувати цей випадок, маючи інформацію щодо акаунту булера. За допомогою співпраці з підрозділом кіберполіції буде відбуватися наступне: адміністратори цих мереж і месенджерів за запитом поліцейських з доказами правопорушення будуть передавати інформацію щодо IP, місця реєстрації, провайдера, а також, як пов'язані

ці реєстраційні данні, з даними інших соц. мереж користувача. Тим самим «виходячи» на цю людину. Якщо будуть збіги, то за допомогою баз даних можна буде ідентифікувати особу. Якщо ж ні – то працювати треба буде методом пошуку місця реєстрації, останнього входу або ж методом «на живця», тобто, роблячи приманку з працівника поліції. Плюс цього додатку в тому, що за допомогою нього можна швидко зафіксувати факт скоєння правопорушення і доповісти про це підрозділам кіберполіції, бо чим раніше зафіксований акт, тим легше знайти булера фахівцям по гарячих слідах.

Ми могли б інтерпретувати у нашій практиці метод протидії булінгу – «Link Crew». Задіявши найпідготовленіших бажаючих для слідкування за учнями старших шкіл, закріплювати за кожним певний відсоток людей. Ці, так звані «шефи» виконуватимуть функції спілкування, моніторингу і вирішення проблем щодо цькування та приниження честі в мережі Інтернет. Користуючись цим методом, ми зможемо виявляти прояви булінгу у соц. мережах і вчасно реагувати на них. У Дніпропетровському державному університеті внутрішніх справ уже з'являються пропозиції щодо залучення курсантів для такого роду занять. За допомогою спілкування вони будуть знати про психічний стан і настрій учнів.

Отже, у еру колосальної швидкості розвитку інформаційних технологій і науки інформатики в цілому не має обмеження щодо нових систем і механізмів роботи у певних сферах. Тобто з кожним днем людство винаходить нові методи все більш ефективніші та легші для опрацювання іншими.

Це стосується і булінгу. Хоча ця проблема і зовсім нова (Виникла не так давно у інтернет мережі), але вона вже получила значного розголосу по всьому світу. З кожною годиною програмісти та інші спеціалісти у сфері інформаційних технологій намагаються придумати нові методи боротьби з булінгом. Деякі з найбільш популярних ми спробували Вам описати і розказати про їх принцип роботи. Це дійсно тема, яка потребує обговорення і неабиякої уваги. Зробивши акцент на цьому, ми заінтересуємо інші країни для майбутніх можливостей співпраці і взаємодопомоги у вирішенні цієї допомоги. Методи боротьби з булінгом потребують свого доповнення і, можливо, коректування. Кожний другий перегляд програми\додатку\системи дає змогу знайти мінуси у певних структурах цієї цілісності. Тобто можна зробити висновок, що тема боротьби з булінгом набирає все більшої зацікавленості. Наша країна не повинна залишатися позаду інших, бо вона має непогану базу і достатню кількість спеціалістів, які здатні працювати у цій сфері. Тож, зацікавленість влади повинна використовувати свою матеріальну базу для винаходу інших методів боротьби з булінгом.

Література:

1. Інформаційно-ресурсний центр «Дитинство без насильства». URL: https://rescentre.org.ua//bezpeka–ditei-v-interneti/...dytyni

2. Інформаційний портал «Нетикет». Що таке кібербулінг та як йому протистояти? URL: http://netiquette.in.ua/2018/03/04.

3. Інформаційний портал «Життя». Кібербулінг: захиститися можливо? URL: https://life.pravda.com/columns/2019/07

ДОСЛІДЖЕННЯ ВПЛИВУ ІНФОРМАЦІЙНОГО ТЕРОРИЗМУ НА БЕЗПЕКУ ЖИТТЄДІЯЛЬНОСТІ СУСПІЛЬСТВА

Марич В., Ільчишин Я., Грунт Р.
Львівський державний університет безпеки життєдіяльності, м. Львів

Досліджено вплив інформаційного тероризму на безпеку життєдіяльності суспільства. Наведена коротку характеристика інформаційного тероризму. Проаналізовано основні категорії інформаційного тероризму. Розглянуто та роз'яснено відмінності у поняттях «тероризм» та «інформаційний тероризм»
Ключові слова: інформаційний тероризм, інформаційна зброя, соціальні мережі, безпека життєдіяльності.

The influence of information terrorism on the security of society is investigated. A brief description of information terrorism is given. The main categories of information terrorism are analyzed. Differences in terms of "terrorism" and "information terrorism" are considered and explained
Keywords: information terrorism, information weapons, social networks, life safety.

У сучасному світі відбуваються кардинальні зміни у сфері безпеки життєдіяльності та забезпечення міжнародної безпеки суспільства. Безпека перестала розглядатись лише у військово-політичних категоріях. Пов'язано це з появою нових видів загроз як на глобальному, так і на регіональному рівнях. Слід зазначити, що серед всіх економічних, екологічних, політичних та інших проблем, які частіше за все мають характер міжнародних, на важливому місці стоїть проблема тероризму. Зокрема за останні десятиліття, внаслідок бурхливого розвитку суспільства, з'явилася нова соціальна небезпека – інформаційний тероризм. Така проблема несе у собі глобальне значення і велику небезпеку для міжнародного співтовариства. Якщо раніше тероризм обмежовувався кордонами тієї чи іншої країни, то нині ці межі стерті, і він набув характеру всесвітньої проблеми, з якою зіткнулися всі учасники міжнародних правовідносин.

Інформаційний тероризм - це, насамперед, форма негативного впливу на особистість, суспільство і державу усіма видами інформації. Його ціль – ослаблення і розхитування конституційного ладу. Він ведеться різноманітними силами і засобами – від агентури іноземних спецслужб до вітчизняних і закордонних засобів масової інформації. Інформаційний тероризм здійснюється в області, що охоплює політичні, філософські, правові, естетичні, релігійні й інші погляди й ідеї, тобто в духовній сфері, там, де ведеться боротьба ідей. Доступність інформаційних технологій значно підвищує його ризики, бо, чим інформатизованішим є суспільство, тим більш воно піддатливе до впливів масово-психологічного терору [1].

Інформаційний тероризм можна розділяють на дві основні категорії:

1. Інформаційно-психологічний тероризм (контроль над засобами масової інформації з метою поширення дезінформації, чуток, демонстрації могутності терористичних організацій): а) медіа-тероризм або „медіа-кілерство" зловживання інформаційними системами, мережами, та їхніми компонентами для здійснення терористичних дій та акцій;

2. Інформаційно-технічний тероризм (завдання збитків окремим елементам і всьому інформаційному середовищу супротивника в цілому: руйнування елементної бази, активне придушення ліній зв'язку, штучне перезавантаження вузлів комунікації тощо): а) кібер-тероризм – сукупність дій, що включають інформаційну атаку на комп'ютерну інформацію, обчислювальні системи, апаратуру передачі даних, інші складові інформаційної інфраструктури, яка здійснюється злочинними угрупованнями або окремими особами [2].

У рамках ООН розроблена конвенція про боротьбу з тероризмом, яка враховує наявні сьогодні Конвенції і відповідні Резолюції Генеральної Асамблеї. Проте, навіть цей міжнародний документ не став базою, яка прибрала прогалину визначення поняття «тероризму». Тероризм не є чимось безпричинним, оскільки це певне соціальне явище, яке виникло внаслідок конкретних дій чи подій та яке несе певну мету. Загалом тероризмом можна назвати спосіб досягнення певних політичних цілей шляхом диверсій і нагнітання страху у суспільстві.

На відміну від тероризму у звичайному його розумінні, інформаційний тероризм є менш страхітливим, оскільки немає вибухів, жертв. Проте, якщо поглянути на ситуацію з іншого боку, стає зрозуміло, що картина не настільки радісна як здавалось. Інформаційний тероризм – не лише кіберзлочин, це не коректні маніпуляції з інформацією, її підтасування, у деяких випадках подача свідомо помилкових фактів, наслідком чого і є залякування населення та впровадження параноїдальних думок. У сучасному світі інформаційні технології є у вільному доступі, що значно підвищує ризики негативних масово-психологічних впливів на свідомість людей.

Джерелами інформаційного тероризму стають засоби масової інформації. Саме через них у значній кількості випадків здійснюється психологічний вплив на осіб внаслідок легкості сприйняття такої інформації. Такий вид інформаційного тероризму прийнято називати інформаційно-психологічним.

Соціальні мережі (соц-мережі) – найбільш доступний і небезпечний засіб впливу на загальну масову думку людей. Соціальна мережа зараз є елементом масової культури [3].

Прикладом практичного інформаційного протиборства стала подія, коли в грудні 2016 року найбільші соціальні мережі, такі як facebook, twiter, youtube, за підтримки microsoft об'єдналися для боротьби з контентом екстремістського змісту, блокування певного виду матеріалів, що викликають підозру на вміст пропаганди до насилля, порнографії, терористичних дій тощо[4].

В наші дні інформаційний тероризм більше тисне на свідомість і психіку людей, ніж раніше. Таким чином можна вважати, що інформаційний тероризм являє собою принципово новий вид терористичної діяльності, що спрямований на використання сучасних інформаційних технологій з метою порушення або знищення державної інфраструктури та безпеки суспільства. Його особливістю є маніпуляції свідомістю людей шляхом активного використання психологічного впливу. Слід зазначити, що попри всю сукупність матеріалів досліджень, що проводились з цього питання, протидія даному виду злочинної діяльності значно відстає від потреб безпеки життєдіяльності суспільства. Кажучи точніше, вона знаходиться на стадії становлення і потребує наукового забезпечення особливо на рівні організаційно-безпечного аспекту. Саме тому існує досить яскрава перспектива подальшої розробки питання інформаційного тероризму та протидії йому на міжнародному рівні.

Література:

1. Електронний ресурс: http://www.aratta-ukraine.com/text_ua.php?id=149;
2. Бойченко О. В. Медіа-тероризм: особливості сучасних ознак інформаційній безпеці / О. В. Бойченко // Інтегровані інтелектуальні робото технічні комплекси (ПРТК-2009): Друга міжнародна наук.-практ. конф. (25–28 травня 2009 р.). – К.: НАУ, 2009. – С. 230–232.;
3. Електронний ресурс: https://uk.wikipedia.org;
4. Мітін В. І. «Інформаційний тероризм на сучасній міжнародній арені», Міжнародний науковий журнал «Інтернет наук».

ІНФОРМАЦІЙНІ ВІЙНИ

Проць Б. О., Кулик С. Ю., Бардін О. І.
Львівський національний університет імені Івана Франка

Аналіз інформаційної війни, її принципів і методів дозволяє зрозуміти суть цих впливів. На підставі вивчення літературних джерел та аналітичного матеріалу запропоновано окремі заходи протидії інформаційній війні та інформаційно-психологічному впливу. Також наведені приклади впливу ЗМІ на суспільство, що найбільш часто застосовуються [1].

Людство живе у, так звану, інформаційну епоху, тому одним з ефективних методів впливу на людей в сучасних умовах глобалізаційних процесів є інформаційна війна, яка впливає на інформаційні системи, маючи на меті введення в оману масової чи індивідуальної свідомості, виведення з ладу або десинхронізацію процесів управління суспільством та його складовими, передусім військовими.

Інформаційна війна – це спосіб маніпулювання людьми, за допомогою інформаційних технологій. Зокрема, інформаційна війна – це наявність боротьби між державами, або нав'язування думки в середині однієї держави(налаштування одного суспільства, діяти одне проти одного), за допомогою інформаційної зброї, тобто це відкриті та приховані цілеспрямовані інформаційні впливи систем (держав) одна на одну, з метою отримання переваги в матеріальній сфері, де інформаційні впливи – це впливи з допомогою таких засобів, використання яких дозволяє досягати задуманих цілей. В основному розрізняють чотири підходи до визначення даного поняттях [3].

– Перший підхід пояснює їх як сукупність політико-правових, соціально-економічних, психологічних дій, що передбачають захоплення інформаційного простору, витіснення ворога з інформаційного середовища, руйнування його комунікацій, ліквідація засобів передачі повідомлень.

– За другим підходом інформаційна війна – це найбільш гостра форма протистояння в інформаційному просторі, де першочергового значення набувають такі якості взаємодії, як безкомпромісність, висока інтенсивність суперечки та короткотривалість гострого суперництва;

– За третім підходом інформаційна війна представляється як форма забезпечення та ведення військових дій за допомогою сучасних електронних приладів(цифрових випромінювачів, супутникових передавачів та інших засобів, які застосовуються для виконання військових завдань);

– Четвертий підхід прирівнює інформаційні війни з кібернетичними війнами (протистояння між технічними системами).

Основним інструментом ведення інформаційної війни є інформаційна зброя. Такою зброєю можуть бути широко розповсюджені засоби, такі як: ЗМІ (Радіо, телебачення, преса), інтернет, мобільний зв'язок, наукова, художня або спеціальна література, кіно та мистецтво. Це може бути спеці-

ально підготовлена дезінформація, розрахована на емоційний вплив та на концентрацію сил і матеріального забезпечення на інше, свідомо неправильне русло. Таким чином, інформаційна зброя — це пристрої та засоби, які призначені для нанесення протидіючій стороні максимальної шкоди в ході інформаційної боротьби (шляхом небезпечних інформаційних впливів) [4].

Об'єктами впливу можуть бути: інформаційно-технічні системи, інформаційно-аналітичні системи, інформаційно-технічні системи, які включають людину, інформаційно-аналітичні системи, які включають людину, інформаційні ресурси, системи формування суспільної свідомості та думки, яка базується на засобах масової інформації та пропаганди, а також психіки людини.

Також до інформаційної зброї зараховують й сукупність спеціальних способів і засобів впливу на психіку суспільства та держави в цілому [5].

Для проведення будь-якої інформаційної компанії як в міжнародних відносинах, так і на внутрішньому інформаційному полі необхідно враховувати особливості конкретного інформаційного простору. Насамперед необхідно розшукати вразливі точки в інформаційному просторі і тільки потім переходити до рішучих дій.

В наш час можна спостерігати ефективне ведення інформаційної війни в мережі Інтернет. Її елементами можуть виступати так звані фейки – неправдиві сторінки, що містять, зокрема, інформацію з минулого, яку видають за новину дня. Фейк може бути і візуальним, для чого користуються графічними та відео редакторами. Головним об'єктом ураження залишається людина, прихований вплив на яку здійснюється через її нервову систему та психіку, здебільшого на підсвідомому рівні.

Як тоді протистояти інформаційній війні:

1. Розрізняти інтерес, який стоїть за пропагандою
2. Мислити самостійно – робити висновки самому, не приймаючи на віру інші думку
3. Шукати підтвердження інформації, вдаючись до двох і більше джерел
4. Обговорювати свої висновки з компетентними людьми, експертами, порівнюючи різні думки
5. Не робити висновки емоційно, не посилатися на одне джерело інформації.

Інформаційно-комп'ютерна революція відкриває широкі можливості для впливу на народи та владу, маніпулювання свідомістю та поведінкою людей навіть на віддалених просторах [6].

Отже, беручи до уваги процес глобалізації телекомунікаційних мереж, що відбувається в світі, можливо припустити, що саме інформаційним видам агресії буде відданий пріоритет у майбутньому. Потрібна серйозна увага до цього питання, щоб уникнути найбільш негативних наслідків інформаційного обману для всього людства.

Список літератури.

1. Богуш В.М. Інформаційна безпека держави [Текст] /В.М. Богуш, О.К. Юдін. –К.: МК-Прес, 2005.– 432 с. 2. Гуз А.М. Історія захисту інформації в Україні та провідних країнах світу: Навчальний посібник [Текст] / А.М. Гуз. – К.: КНТ, 2007 – 260 с.

2. Магда Є. Виклики гібридної війни: інформаційний вимір [Текст] / Євген Магда // Наукові записки Інституту законодавства Верховної Ради України . – 2014. – No 5. – С. 138-142.

3. Саприкін О. Інформаційна експансія, інформаційна війна та інформаційна атака у засобах масової інформації на прикладі Євро-2012 [Текст] / Олександр Саприкін // Вісник Книжкової палати. – 2013. – No 1. – С. 40-43.

4. Цуканова О.В. Інформаційні війни: вплив на суспільство [Електронний ресурс] / О.В. Цуканова. – Режим доступу: https://www.sworld.com.ua/konfer34/800.pdf – Назва з екрана.

5. Чирва Р. Інформаційна війна – зброя, страшніша за ядерну [Текст] / Раїса Чирва // Профспілкові вісті. – 2014. – No 13. – С. 8-9.

6. Шпига П.С. Основні технології та закономірності інформаційної війни [Текст] / П.С. Шпига, Р.М. Рудник // Проблеми міжнародних відносин . – 2014. – Вип. 8. – С. 326-339.

ІНФОРМАЦІЙНІ ВІЙНИ

Смолінська М.В., Малець І.О.
Львівський державний університет безпеки життєдіяльності

Найнебезпечнішим видом зброї на теперішній час були і залишаються інформаційні війни. Як не дивно, та користуватися компроматами, підкидати неправильну інформацію і ввести людство в оману є досить популярно в інформаційних технологіях сьогодення. Інформація має найбільший вплив на оточуючих, так як за умови вправного маніпулювання людством, можна прибрати з дороги конкурентів та знищити будь-якого опонента [1].

Відомий американський дослідник, філософ, а також дослідник впливу медіа, як засобів комунікації на аудиторію М. Маклюен запропонував досить цікаве твердження щодо ролі інформації в сучасному світі: «Істинно тотальна війна – це війна за допомогою інформації». Він став досить популярним, завдяки своїм дослідженням формування людини і суспільства, на яких впливають інформаційні технології. М. Маклюен був першим, хто оголосив про економічні зв'язки, які не приймають форму обміну товарами, а більше і більше приймають форму обміну знаннями. Таким чином, засоби масової інформації стали новими «природними ресурсами», які збагачують суспільство новими знаннями. Отож, можна визнати, що головним постає доступ до інформаційних ресурсів, знань, а це у свою чергу призводить до війн в інформаційному просторі за допомогою інформаційних видів озброєнь [2],[5] .

Перші згадки про термін «інформаційна війна» появилися в кінці 80-х років XX століття. Цей термін став поширеним після чітко представленої задачі по скасуванню СРСР тяжкої праці видатних теоретиків збройних сил США. Стрімко застосовуватися «інформаційна війна» почала в момент проведення воєнної компанії США в Іраку. Де уже в 1991 році уперше були представлені інформаційні технології.

Перш за все, коли ми починаємо говорити про війну, в тому числі інформаційну, то потрібно брати до уваги стан взаємин між конкурентами. В такому випадку термін «інформаційна війна» моє псевдонауковий характер і виникає з новітніх підходів застосування інформації в цілому [4].

Психологи провели дослідження і підтвердили досить небезпечну тенденцію, що молодь, яка з малечку перебуває в світі ЗМІ і телебачення, досить швидко звикає до глибокого занурення у віртуальний світ. Вона не усвідомлює, як об'єкти звичайної культури стають просто нереальними та незначними взагалі. Телебачення особливо здатне створити ефект заціпеніння і людина таким чином може втратити вміння аналізувати та прогнозувати. Людство не замислюється над тим, як стає слухняним об'єктом інформаційних технологій. Саме тому, молодь більш сприятливе покоління для маніпуляцій в цьому плані. Теоретиками інформаційних війн запропоновано схему інформаційного протиборства:

1. Розслабити суспільство — переконувати через ЗМІ, що стосовно нього не ведеться ніяких агресивних дій, йому бажають лише добра («остановіть АТО!», «свободу народу Донбаса!»).

2. Змусити суспільство слухати тільки противника, виключивши досвід будь-яких інших країн і народів («словянский союз», «православіє», «общєрускій язик»).

3. Змусити суспільство не розмірковувати над тим, що говорить супротивник, а для цього виключити зі ЗМІ серйозні аналітичні передачі, зробивши акцент на яскравих розважальних шоу («Голос країни», «Україна має талант» «Міняю жінку», «Я соромлюся свого тіла» та багато інших програм).

4. Зосередити увагу громадськості на якомусь окремому предметі, крім спрямованого маніпуляційного потоку (наприклад, «распятий хунтой мальчик», «снєгірі»), щоб підсистема захисту, відповідальна за обробку інформації, не виконувала свою функцію [3].

Та головним є те, що нові інформаційні технології здатні обернутися для людства тотальною катастрофою, якщо їх у свою чергу розглядати, як зброю. Інформаційна війна, як інструмент політики представляє існування одного суспільства ціною виключення іншого. Одним із прикладів є те, що в концепціях інформаційної війни, яку проти нас веде Росія є аморфна з геологічного погляду територія, на якій можуть плодитися лише так звані «народні республіки», а суверенної Української держави не існує взагалі [3].

Отже, на сам перед, інформаційна війна – це складова частина ідеологічної боротьби, а також політичної комунікації. Навіть руйнування, до яких призводять інформаційні війни в психології людини за своїми масштабами і значенням рівні наслідкам збройних війн. Трапляється і таке, що збройні війни сховаються за війни інформацією, адже їх створюють з метою послабити матеріальні та моральні сили противника [1].

Література:

1. Інформаційна війна – зброя масового знищення! [Електронний ресурс] // [веб-сайт]- https://www.pravda.com.ua/rus/articles/(дата доступу 18.10.2019)

2. Інформаційна війна [Електронний ресурс] // [веб-сайт] - https://uk.wikipedia.org/wiki/ (дата доступу 20.10.2019)

3. Інформаційні війни в українському контексті [Електронний ресурс] // [веб-сайт] - http://www.global-analityk.com/ (дата доступу 22.10.2019)

4. Поняття інформаційної війни [Електронний ресурс] // [веб-сайт] - http://politics.ellib.org.ua/pages-8282.html (дата доступу 26.10.2019)

5. Маршалл Маклуен [Електронний ресурс] // [веб-сайт] - https://uk.wikipedia.org/wiki/ (дата доступу 29.10.2019)

ВПЛИВ ІНФОРМАЦІЙНОЇ ВІЙНИ НА БЕЗПЕКУ УКРАЇНИ

Тютченко С. М., Дембицька Т. П.
Дніпропетровського державного університету внутрішніх справ

Анотація: Інформаційні війни давно зайняли належне місце у військовій парадигмі. За допомогою інформаційної зброї протиборчі сторони здатні вирішувати стратегічні завдання. В період інформаційної війни ворог може маніпулювати свідомістю для широкомасштабної експансії і загрожує національній безпеці України. Тому необхідна адекватна інформаційна протидія.

Ключові слова: інформаційне суспільство**,** інформатизація, інтернет-технології, інформаційні війни, національна безпека.

Annotation: Information technology has long taken the place of the business paradigm. For the additional information on the protection of the side of the strategic cooperation strategy. In the period of information technology, we can offer you a large-scale expansion and overseas national insurance in Ukraine. That is necessary adequate information protidiya.

Key words: information suspension, information technology, Internet technology, information technology, national security

На сьогодні людство живе в інформаційному суспільстві. Це новий тип суспільства, в якому володіння інформацією є рушійною силою його перетворень та розвитку, і де процвітає людська інтелектуальна творчість.

За допомогою інформаційної зброї протиборчі сторони здатні вирішувати стратегічні завдання, зокрема: завдавати серйозної шкоди національним інтересам, підривати основи державності; дискредитувати органи влади й ускладнювати прийняття ними важливих рішень, паралізувати управління країною в кризових ситуаціях тощо. Українські події змусили багатьох говорити про світову інформаційну війну.

З'явилася точка зору, що третя світова війна вже настала, просто вона ведеться переважно інформаційними засобами, тому ми не відчуваємо її масштабів. Безсилля державних інформаційних структур особливо виявилося сьогодні, у розпал інформаційної російсько-української війни. Інформаційні війни давно зайняли належне місце у військовій парадигмі. Існує інфраструктура відповідної підготовки спеціалістів та їх місце у військовій ієрархії. Все це трапилося на наших очах, коли прийшло нове бачення війни, що було підказане новим інструментарієм – інформаційним. Це також співпало зі зміною парадигми війни в цілому, що реалізувалася в переході військових і до нелегальних видів зброї, і до більш складної роботи з населенням. Інформаційні війни є інформаційними технологіями, що впливають на інформаційні системи, маючи на меті введення в оману масової чи індивідуальної свідомості, виведення з ладу процесів управління суспільством та його складовими, передусім військовими.

Відомо, що в інформаційній боротьбі перемагає та сторона, яка ефективніше використовує інформацію та канали впливу. При загостренні конфліктів інформаційна боротьба переростає в інформаційну війну. І тоді всі засоби прийнятні:

1) маніпулювання – дезінформація, приховування або перекручення інформації;

2) порушення інформаційного обміну – несанкціонований доступ або необгрунтоване обмеження доступу до ресурсів, протиправне збирання і використання інформації;

3) руйнування інформаційного простору країни або його використання з антидержавною метою;

4) інформаційний тероризм – поширення комп'ютерних «вірусів», встановлення програмних і апаратних закладних пристроїв, радіоелектронних приладів перехоплення в технічних засобах і приміщеннях, незаконне використання телекомунікаційних систем і ресурсів, нав'язування фальшивої інформації та ін.

Сьогодні чітко стало зрозумілим, що важливим компонентом для виграшу є не лише населення ворожої сторони, а й власне населення, бо війни можуть вигратися на полі боя, а програватися в свідомості людей [1].

Інформаційну війну, що є інформаційним забезпеченням агресії Російської Федерації проти України, відомий російський політик Борис Нємцов охарактеризував як війну нацистського режиму проти демократичної держави.

Підсумовуючи висловлене, можна стверджувати, що в період інформаційної війни ворог може маніпулювати свідомістю для широкомасштабної експансії і загрожує національній безпеці України. Тому необхідна адекватна інформаційна протидія [2]. Вважаємо, що задля запобігання масштабній інформаційній війні та збереження цілісності України потрібно дотримуватися таких рекомендацій:

1) не можна анонсувати воєнні операції;

2) необхідна більша кількість репортажів з місця подій;

3) потрібно постійно пояснювати, що це наша земля;

4) на форумах варто вести полеміку про те, що Україна – понад 20 років суверенна держава.

Література:

1. Веймер Д. Л. Аналіз політики: концепції і практика [Текст] / Веймер Девід Л., Вайнінг, Ейден Р.; пер. з англ. І. Дзюб. – К. : Основи., 2000. – 656 с.

2. Информационная война против Украины: сюжеты, методы, противоядие [Електронний ресурс]. – Режим доступу: http://news.liga.net/articles/politics/104 1096informatsionnaya_voyna_protiv_ukrainy_syuzhety_metody_protivoyadie.htm.

ІНФОРМАЦІЙНІ ВІЙНИ

Чепурний Б., Карабіневич А.
ВП НУБіП України «Ірпінський економічний коледж», м. Ірпінь

Інформаційна війна — використання і управління інформацією з метою набуття конкурентоздатної переваги над супротивником. Інформаційна війна — це маніпулювання інформацією, якій довіряє об'єкт, без відома об'єкта, щоб об'єкт приймав рішення проти своїх інтересів, але в інтересах того, хто веде інформаційну війну. Як наслідок, незрозуміло, коли починається інформаційна війна, наскільки вона сильна або руйнівна і коли закінчується.

ІВ, пропаганда, інформаційні ресурси, фейк, радіоелектронна боротьба, геббельсівська пропаганда.

Information warfare – the use and management of information to gain a competitive edge over an opponent. Information warfare is the manipulation of information trusted by an object, without the object's knowledge, for the object to make decisions against its own interests, but in the interests of the one waging the information war. As a consequence, it is unclear when the information war begins, how strong or destructive it is and when it ends.

IW, propaganda, information resources, fake, electronic warfare, Goebbels propaganda.

Інформаційні війни супроводжують всю історію людства. Спочатку вони були релігійними та ідеологічніми, причому для боротьби з носіями чужих поглядів застосовувалися всі види репресій. В далекому минулому інквізиція чи репресивні апарати тоталітарних держав двадцятого сторіччя вели активну боротьбу з носіями чужих ідей.

Найбільш вразливим місцем сучасних складних систем стають процеси прийняття рішень. Саме тому інформація як така поступово почала змінювати свій статус. Вона стала переходити від сили, що допомагала в бою, до сили основної, яка й вирішує результат війни.

Першим варіантом інформаційної війни можна визнати пропаганду. Вся холодна війна базувалася на механізмах пропаганди, бо механізми гарячої війни не застосовувалися. До речі, потреба пропаганди в холодній війні надала суттєвий поштовх розробці теорії комунікації, бо виникла велика кількість суто прикладних завдань у галузі комунікації.

Інформаційна війна може включати в себе:

- збір тактичної інформації;
- гарантування безпеки власних інформаційних ресурсів;
- поширення пропаганди або дезінформації, щоб деморалізувати військо та населення ворога;
- підрив якості інформації супротивника і попередження можливості збору інформації супротивником.

Часто ІВ ведеться в комплексі з кібер- та психологічною війнами з метою ширшого охоплення цілей, із залученням радіоелектронної боротьби та мережевих технологій.

Основним засобом ведення ІВ є інформаційна зброя, ведеться шляхом інформаційних операцій.

Вперше це поняття було закріплене в директиві Міністерства оборони США DOD S 3600.1 (від 21 грудня 1992 року), де воно вживалося у вузькому значенні і розглядалося як різновид радіоелектронної боротьби. В подальшому, в звіті американської корпорації «Ренд» MR-661-0SD «Strategic Information Warfare. A new face of War» (1996 р) вперше з'явився термін — «стратегічна інформаційна війна (інформаційне протиборство)». Вона визначалася як війна з використанням державного глобального інформаційного простору й інфраструктури для проведення стратегічних військових операцій і зміцнення впливу на власний інформаційний ресурс.

Прикладом ІВ на сучасному етапі може бути російсько-український конфлікт.

Від часу проголошення незалежності України Російська Федерація веде постійну інформаційну війну проти України. Особливо вона була посилена в роки правління проросійського режиму Януковича. На думку деяких оглядачів, від початку агресії Російської Федерації (лютий 2014) російська пропаганда набула форм геббельсівської пропаганди часів Другої світової війни.

Ще на початку збройного конфлікту, під час розгортання операції із захоплення та анексії Криму, дослідники Національного інституту стратегічних досліджень України підготували аналітичну записку, в якій зазначили, що: намагання Російської Федерації провести кампанію із введенням збройних сил до АР Крим супроводжувалось діями, які мали всі ознаки підготовленої та продуманої за цілями, заходами та наслідками інформаційно-психологічної спецоперації, скерованої в першу чергу на російську аудиторію, а з іншого боку на українську та західну аудиторію.

Ключовими завданнями цієї спецоперації було:

– Деморалізація населення України.

– Деморалізація особового складу збройних сил та силових відомств, а також спонукування їх до державної зради й переходу на бік супротивної сторони.

– Формування у громадян Росії та України викривленого «медіа бачення» подій, що відбуваються, а не їх дійсних причин та наслідків.

– Створення вигляду масової підтримки дій РФ з боку населення Південно-Східних регіонів.

– Психологічна підтримка українських прихильників радикального зближення регіонів Сходу й Півдня України з РФ.

Зазначені завдання реалізувались через майже повний спектр каналів комунікацій, до яких передусім слід віднести:

– Традиційні ЗМІ.

– Електронні ЗМІ (телебачення).
– Інтернет ЗМІ.
– Соціальні мережі.

При цьому використовувалися усі методи інформаційно-психологічної боротьби — від розміщення тенденційною інформації та напівправди до неприхованої неправди («фейку»).

Також прикладом ІВ може бути конфлікт в Іраку.

Приводом для бомбардування Багдаду Сполученими Штатами стала поширена через усі світові ЗМІ інформація, що режим Саддама Хусейна нібито має зброю масового знищення.

Війна в Іраку триває, а зброю так і не знайшли. Війну інформації також розпочинають тоді, коли треба досягти якоїсь мети.

Такі війни точаться не лише між країнами і охоплюють міжнародну аудиторію, такі війни починають вестися і на місцевому рівні. Зокрема, українські політики, як ніколи, вивчили технологію ведення інформаційної війни.

Останнім часом дедалі популярнішим серед українських політиків стає знищення опонента за допомогою інформаційних бомб.

Література:

1. https://uk.wikipedia.org/wiki/
2. https://ms.detector.media/ethics/manipulation/informatsiyni_viyni_tendentsii_ta_shlyakhi_rozvitku
3. https://www.pravda.com.ua/rus/articles/2006/04/20/4399050/

ЧИ МОЖНА ПЕРЕМОГТИ В ІНФОРМАЦІЙНІЙ ВІЙНІ?

Школик Валерій
Ірпінський економічний коледж», місто Ірпінь

Анотація: розглянеться питання про те чи можна перемогти в інформаційній війні?Аналіз інформаційної війни, її принципів і методів дозволяє зрозуміти суть цих впливів. Також в статті наведені та проаналізовані моделі впливу ЗМІ на суспільство, що найбільш часто застосовуються інформаційні впливи бувають як позитивні, так і негативні. Причому позитивна інформація виконує виховну функцію в суспільстві. Метою ж негативною інформації (пропаганди) є розпалювання соціальних конфліктів, загострення розбіжності в суспільстві. Проблеми інформаційної війни слід вирішувати за рахунок протидії маніпулятивним технологіям противника і удосконалення методів протидії.

Ключові слова: інформаційна війна, інформаційний вплив, інформаційна зброя, протидія.

Abstract: Consideration of whether it is possible to win the information war? Also in the article are presented and analyzed models of influence of the media on the society, the most commonly used information influences are both positive and negative. Moreover, positive information performs an educational function in

society. The purpose of negative information (propaganda) is to ignite social conflicts, exacerbate differences in society. The problems of information warfare should be solved by counteracting the manipulative technologies of the enemy and improving methods of counteraction.

Keywords: information war, information influence, information weapon, counteraction.

Безсумнівно, найважливішим є питання: як виграти в інформаційній війні, стратегії якої стають все більш витонченими і глобальними? Дуже поширена думка, що у війні переможе той, у кого виявляться кращими програмісти. Однак в інформаційній війні, яка ведеться за вміння і серця людей, технічні засоби при всій їх показній та зростаючій міці все ж таки є засобом, а не метою. Крім того, чим більше інформаційна система розосереджується в світі, розкидаючи свої мережі, тим більше вона стає технічно вразливою в будь-якій точці цієї мережі. Але не технічний колапс є метою інформаційних війн, їхня мета — глобальний контроль над простором шляхом контролю над умами людей. Легітимність будь-якої влади, в тому числі інформаційної, — проблема добровільного прийняття цієї влади більшістю[2].

Ще одназ поширених точок зору полягає в тому, що перемогу в інформаційній війні може здобути той, хто постійно атакує і підсилює тиск. Цей важливий висновок виник під впливом поразки СССР в холодній війні, однією з причин якої справедливо називають ідеологічний застій, коли штампи «розвиненого соціалізму як найпередовішого суспільного ладу» перестали концептуально оновлюватися і втратили ідеологічну гостроту. Якщо узяти сучасний російський ідеологічний концепт «рускій мір», то слід відзначити його значно меншу універсальність та більшу примітивність, порівняно з комуністичною ідеєю. Він не стане новим «марксизмом-ленінізмом» через низку причин, а передусім — через хронічний брак нових марксів та ленінів. Тому нівеляція міфу «руского міра» в очах росіян відбудеться досить швидко за історичними масштабами.

Досить ефективною відповіддю на виклик електронних ЗМІ може бути відновлення особистих контактів з аудиторією, що під час виборчих кампаній широко використовує ВО «Свобода». Не випадково інформаційна епоха, яка тиражує масову культуру, так високо цінує харизматичні пасіонарні особистості. Відомо, що під час політичних виборів виборці голосують за кандидата, а не за партію. Тому сьогодні особливо велика увага приділяється видатним особистостям та їх ролі в історії.

Найглибше до аналізу викликів інформаційної революції підійшов німецький соціальний філософ і психолог Еріх Фромм (1900-1980) в своїй фундаментальній праці «Анатомія людської деструктивності» (1973). Він звернув увагу на те, що людині, як істоті, важливо опертися на певну систему моральних координат — розділити добро і зло, щоб протистояти зовнішнім обставинам. Коли людина чітко ідентифікує себе з певним суспільством, бачить себе частиною певної групи або колективу, вона «обростає моральним корінням», оскільки суспільство пропонує їй певну систему ко-

ординат, яка допомагає всім колективно вижити в найскладніших ситуаціях [1].Адже недарма найменше піддаються маніпулюванню люди з чітко вираженою соціальною і політичною позицією, оскільки маніпулятивні дії обернено пропорційні соціокультурній ідентичності, освіченості, груповій солідарності, партійній приналежності. Саме тому у виробленні колективної контрсугестії особливе значення має система виховання і освіти, яка розвиває громадянські якості, патріотизм, любов до Батьківщини [3].

Особливу роль у розвитку колективної ідентичності відіграє національна ідея — система ціннісних установок суспільства, в яких виражається самосвідомість народу і задаються цілі особистого і національного розвитку в історичній перспективі. З цієї точки зору перемогти в інформаційній війні може та країна, яка збудує в інформаційному просторі та запропонує своїм громадянам яскравий символічний проект національної ідеї — систему національних пріоритетів, ідей і традицій, які для більшості виявляться більш значимими, ніж будь-які інформаційні впливи та спокуси ззовні.

Саме тому так актуальні сьогодні слова Маршалла Маклюена про переваги традиційних суспільств в інформаційній війні. Його алгоритм перемоги в інформаційному протиборстві залишається актуальним: щоб бути «агресивно ефективними в сучасному світі інформації», необхідно активізувати у свідомості людей національну систему пріоритетів, створити яскравий образ національної ідеї, адаптувати традиції до нових засобів комунікації [1].

Література:

1. Роман Кухаренко «Інститут інформаційних війн в українському контексті».[Електронний ресурс] – Режим доступу до ресурсу:http://www.global-analityk.com

2. Інформаційні війни: тенденції та шляхи розвитку. [Електронний ресурс] – Режим доступу до ресурсу: https://ms.detector.media/ethics/manipulation/informatsiyni_viyni_tendentsii_ta_shlyakhi_rozvitku/

3. Сучасні інформаційні війни у мережевому он-лайн просторі. Навчальний посібник. . [Електронний ресурс] – Режим доступу до ресурсу:http://www.mil.univ.kiev.ua/files/222_1044284240.pdf

4. Особливості застосування інформаційної зброї в умовах глобального інформаційного суспільства. [Електронний ресурс] – Режим доступу до ресурсу:http://www.dy.nayka.com.ua/?op=1&z=123

Секція 2
ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Напрям 7

Інформаційні технології управління проєктами

ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ ТА ARTIFICIAL INTELLIGENCE

Медяник Є. І.
Одеський національний політехнічний Університет

Анотація. Одним із найголовніших завдань перед людством є розробка штучного інтелекту.Таким чином, у зв'язку з швидким розвитком інформаційних технологій у двадцять першому сторіччі постає потреба у опрацюванні великої кількості інформації.Тому експерти з усього світу намагаються розробити найефективніші способи для вирішення цього питання.Метою цієї роботи є опис застосування штучного інтелекту і відповідно його складової – машинного навчання.

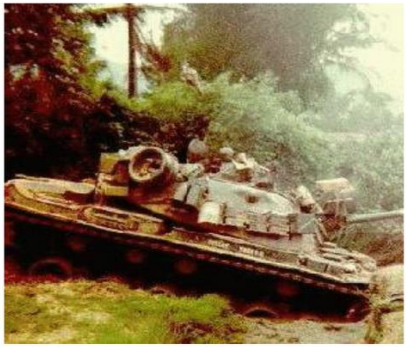
Ключові слова:штучний інтелект,машинне навчання,глубоке навчання,технології ,нейронна мережа.

Annotation. One of the most important task for humanity is developing artificial intelligence technology.Therefore,due to fast evolution of informational technology in twenty first century ,creating a demand in processing of big data.Therefore,experts all around the world are trying to develop the most effective solution for this task.Point of this article is to describe where artificial intelegence and his main component machine learning is using.

Keywords:artificial intelligence, machine learning, deep learning, technologies, neural network.

Аналіз даних і навчання машини дозволяють людям розвинути технології використання даних у порівнянні з попередніми роками,коли знання обмежували створення штучного інтелекту.Перші принципи роботи зі штучним інтелектом почали застосовуватися ще з середини двадцятого століття,такими вченими та експертами як Норберт Вайнер,Клаудія Шеннон, а також Алан Тьюринг.Вони поєднували стандартні принципів зчитування електричних сигналів та обчислювань.У 1943 році Уоренн Маккаллок та Уолтер Піттс розробили першу модель нейронної мережі.Проте багато років пройшло з того часу і попит на технології із застосуванням штучного інтелекту є неабияким затребуваним у найрізноманітніших сферах діяльності,здебільшого у сфері інформаційних технологій.

Наприклад за допомогою штучного інтелекту ми можемо контролювати та збільшувати швидкість трансферу даних між компонентами того чи іншого приладу.До таких приладів я можу віднести окуляри віртуальної реальності,швидкість обміну даними є неабияким важливим фактором роботи цього пристрою,адже будь-яка затримка під час обміну інформацією може призвести до втрати зв'язку з реальністю ,яка проектується на пристрій.




Ця технологія потребувала серйозних розробок та виправлень проблем,тому згодом було розроблено нову технологію яка отримала назву “Deep Learning”,або глибоке вивчення.

Машинне навчання безумовно є потужним компонентом ,який доповнює штучний інтелект,але “deep learning” виводить цю технологію на абсолютно новий рівень.”Deep learning”-це еволюція машинного навчання,що створює все більш складні ієрархічні структури та моделі,які створенні для імітування мисленнєвих процесів у мозку людини ніж просто стандартні моделі машиного навчання.Таким чином,”deep learning”-це технологія яка розширяє машинне навчання,при цьому залишаючись підмножиною як штучного інтелекту так і доповненням”machine learning”.

Однією із постійно триваючих проблем для експертів у сфері інформаційних систем є відокремлення інсайдерських погроз від помилкових тривог.На жаль, метод ”deep learning” ,як складова штучного інтелекту на даний момент менш ефективний,коли справа стосується визначених випадків та проблем,наприклад справжніх кібер атак,тому що спеціалісти просто не знають визначеного типу та обсягів даних які використовуються у атаках цього типу.

На мою думку,покращенню вже існуючих додатків MuseNet,Wordsmith,Amazon Alexa,Google Assistant,NomuraSecurities штучного інтелекту може сприяти інвестування великих компаній як Alluviate,Google,Cray,Intel,IB.

Література:

1. Understanding Machine Learning: From Theory to Algorithm/Shai Shalev-Shwartz,Shai Ben-David

2. Artificial Intelligence For Dummies /John Paul Mueller,Luca Massaron

3. Artificial Intelligence and Machine Learning 101/MicroFocus

4.The elements of statistical learning/Trevor Hastie,Robert Tibshirani,Jerome Friedman

УДК 614.843(075.32)

СТВОРЕННЯ ІНФОРМАЦІЙНИХ ЗАСОБІВ ДЛЯ АНАЛІЗУ БЕЗПЕКИ УКРИТТІВ

Тарапата Н. В., Шеремей В. С., Мартин Є.В.
Львівський державний університет безпеки життєдіяльності

Анотація. У роботі розглянуто проблеми створення інформаційних технологій щодо облаштування бомбосховищ, захисту людей від небезпечних факторів зброї масового ураження та наслідків стихійних лих. На основі попередньо заданих даних розроблене програмне забезпечення, яке дозволить суттєво полегшити витрату сил, засобів на розрахунки параметрів безпеки, а також вказати на умови, які варто покращити.

Ключові слова: програмне забезпечення, пожежна безпека бомбосховища, аналіз надзвичайних ситуацій у бомбосховищі.

Abstract. This paper deals with the problems of the construction of bomb shelters during emergencies, as well as analyzes the protection of people against dangerous factors of weapons of mass destruction and the effects of natural disasters. Based on the predefined data, we have developed software that will greatly facilitate the use of forces, tools for calculating security parameters, and indicate the conditions that should be improved.

Keywords: software, bomb shelter fire safety, bomb shelter emergency analysis.

Для визначення рівня безпеки необхідно виконати характеристику бомбосховища, моніторинг стану техногенної (пожежної) безпеки, в результаті якого вже встановлюється фактичний ступінь вогнестійкості приміщення та розрахунок сил, засобів для ліквідації надзвичайної ситуації (пожежі) на об'єкті [1]. На сьогодні практично досягнути нульового рівня ризику неможливо, проте можна до нього максимально наблизитись. Розроблене нами програмне забезпечення «Безпека бомбосховищ» дозволяє на основі попередньо заданих даних оцінити стан безпеки бомбосховища, а також аналізувати ймовірність того, чи вдасться врятувати усіх людей, присутніх у бомбосховищі [2]. На основі проведеного аналізу програма видає рекомендації, що вказують на те, які умови стали причиною погіршення ситуації і до чого варто придивитись уважніше в процесі облаштування бомбосховища. Для розробленого нами програмного забезпечення мову програмування було обрано із кількох значущих причин [3]. Спершу увага було звернута на те, що мова програмування для виконання даного проекту має реалізовувати принципи об’єктно-орієнтованого програмування (ООП). ООП як парадигма розглядає програму в якості зчисленої множини об’єктів, що взаємодіють між собою. Її основу складають чотири принципи: інкапсуляція, успадкування, поліморфізм та абстракція.

Наступним важливим чинником для нас стала кросплатформленість, тобто можливість виконання нашої програми на будь-якій платформі, для якої нами написана **java** - машина. Саме тому для розроблення програми «Безпека бомбосховищ» нами було використано сучасний редактор і компілятор **Intellij IDEA**, який завдяки багатозадачності найкраще зарекомендував себе серед подібних середовищ для створення програмного забезпечення [4]. Враховуючи специфіку навчального процесу пожежних-рятувальників, слід розуміти потреби та принципи, яким мусить задовольняти програмне забезпечення; тому розроблена програма «Безпека бомбосховищ» повинна відповідати наступним критеріям: інтерфейс повинен бути простим та зрозумілим для користувача, а також повинна постійно оновлюватись та покращуватись матеріальна база (рис.1).

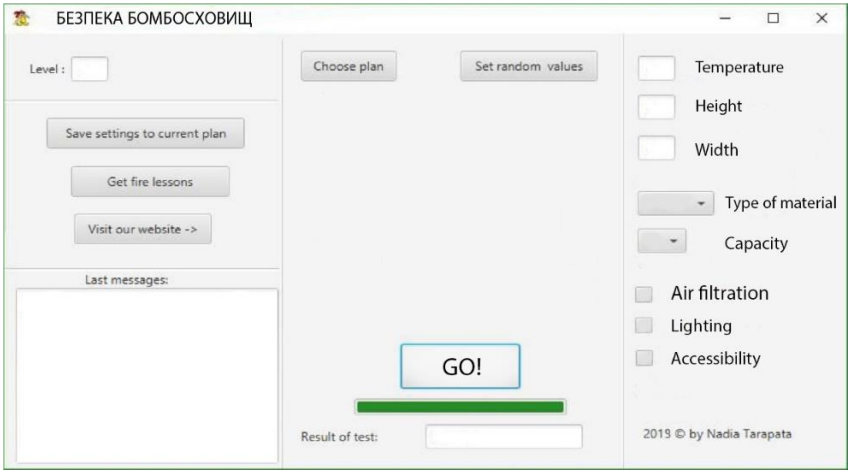


Рис. 1. Робочий простір програми «Безпека бомбосховищ»

Від стихійних лих та зброї масового ураження стається безліч нещасних випадків. Щоб правильно оцінити безпеку бомбосховища, потрібно знати та правильно ввести всі необхідні дані, які вказані у програмі [5]. Результатом даної роботи є те, щоб користувач міг завжди перевірити надійність заданого бомбосховища та оцінити свої шанси на виживання у випадках надзвичайних ситуацій [6]. Розроблене програмне забезпечення дозволяє досягнути мінімального рівня ризику та за короткий час та одержати усю необхідну інформацію.

Література:

1. Сховище цивільної оборони. [Електронний ресурс] – Доступний з https://uk.wikipedia.org/wiki/Сховище_цивільної_оборони

2. Державні будівельні норми України. [Електронний ресурс] - Доступний з kbu.org.ua/assets/app/documents/dbn2/14.1.%20ДБН%20360-92.pdf

3. Мови програмування [Електронний ресурс] – Доступний з http://kamzosh.at.ua/publ/2-1-0-6

4. Васильев А.П. Java с примерами и программами //А.П.Васильев. – М.: 2017. – 368 с.

5. Програмна система оцінювання та прогнозування надійності програмного забезпечення / Сенів М. М., Федасюк Д. В., Парфенюк Ю. І., Яковина В. С., Чабанюк Я. М. // Відбір і обробка інформації : міжвід. зб. наук. пр. / НАН України, Фіз.-мех. ін-т ім. Г.В. Карпенка. – Львів, 2010. – Вип. 33(109). – С. 123–129.

6. Пожежна безпека технологічних процесів [Електронний ресурс] - Доступний з http://res.in.ua/pojejna-bezpeka-tehnologichnih-procesiv-kategoriyi-primishene.html

РОЛЬ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В УПРАВЛІННІ ПРОЄКТАМИ

Ходирєва І., Мирошниченко В.
Дніпропетровський державний університет внутрішніх справ

Анотація. Тези присвячені визначенню ролі сучасних інформаційних технологій в управлінні проектами. Розглянуто основні переваги та недоліки застосування інформаційних технологій. Перелічені завдання та елементи системи управління проектами в розрізі автоматизованої системи.

Ключові слова: інформаційні системи, прогнозування, оптимізація, ресурси, економічний ефект, витрати, ризики.

Abstract. Theses are devoted to defining the role of modern information technologies in project management. The main advantages and disadvantages of the use of information technologies are considered. The tasks and elements of the project management system in the context of the automated system are listed.

Keywords: information systems, forecasting, optimization, resources, economic effect, costs, risks.

Сьогоднішній світ перейшов на новий етап життя, де головну роль виконує інформація, а також економіка, що будується на ній. Сучасний розвиток інформаційного суспільства безпосередньо пов'язаний з необхідністю збору, обробки і передачі величезних об'ємів інформації, перетворенням інформації у товар, як правило, значної вартості. Це стало причиною глобального переходу від індустріального суспільства до інформаційного. Поява всесвітньої мережі Інтернет спричинила масштабне зростання міжнародних спілкувань у різних сферах людського життя.

На сьогоднішній день інформаційні технології відіграють важливу роль, що здатні адаптуватися до сучасного світу шляхом зосередження своєї уваги на тенденції розвитку ринку, зниження та посилення конкуренції для отримання максимальної користі. Зараз реалізація інформаційних систем управління предметами збільшення можливості та шляхів управління даною системою, та покращення процесів керування організацією, що на кожному етапі управління зміцнюється впровадженням програмного забезпечення в сучасних ринкових умовах, є обставинами вдалого функціонування фірми в нинішніх умовах.

Виклад основного матеріалу.

З розвитком сучасних інформаційних технологій зростає прозорість світу, швидкість і обсяги передачі інформації між елементами світової системи, з'являється ще один інтегруючий світової фактор. Це означає, що роль місцевих традицій, що сприяють самодостатньому інерційному розвитку окремих елементів, слабшає. Одночасно посилюється реакція елементів на сигнали з позитивним зворотним зв'язком. Інтеграцію можна було б тільки вітати, якби її наслідком не ставало розмивання регіональних і культурно-історичних особливостей розвитку

Побережець О.В зазначає, економічне зростання передбачає стійкий розвиток підприємства, але сучасному суспільстві притаманне зростання економіки, що спричиняє зростання та розвиток підприємницьких структур. Зовнішнє оточення підприємства через зростаючу динаміку формує специфічний конкурентний простір. Прогрес будується на визначені фактичного теперішнього стану підприємства та прогнозування її майбутнього стану, враховуючи конкурентний простір [1, с. 500]. Сталий розвиток бере за основу уміння та досвід пов'язаності цих станів, а у стані проектів та програм розвитку віддзеркалюється процес переходу. При застосуванні сталого розвитку проект виглядає як якась ідея, сприйняття, перспективний стан або потребуючі предмети для його впровадження та реалізації. Основними ознаками проекту є новизна, концептуальність, неповторність, адаптивність, кількісна вимірюваність, лімітованість часу та інші. В управлінні проектами, проект тлумачиться як система пов'язаних процесів та отримання кінцевих запланованих результатів, що обмежуються ресурсами та часом.

При впровадженні інформаційних технологій, фірми мають змогу вдало керувати проектами, налагоджувати зв'язок між учасниками проекту, знаходити та оперативно реагувати на відхилення, складати звітність по всім етапам проекту та мати змогу швидко здійснювати контроль. На думку Башинської І.О. інформаційна технологія – це поєднання процедур, що реалізують функції збору, накопичення, зберігання, обробки і передачі даних на основі використання відібраного комплексу технічних засобів за участі управлінського персоналу. Саме тому існує тісний зв'язок із програмним та технічним оточенням інформаційної технології [2, с. 3].

Башинська І.О. зазначає інформаційні технології управління проектами дозволяють автоматизувати одну або декілька складових управління проектами: складання календарного плану робіт, управління ресурсами, витратами, ризиками, якістю тощо. Системи автоматизації управління проектами містять такі структурні елементи:

– засоби для календарного планування;
– засоби розв'язання окремих задач (серед них слід виділити допроектний аналіз, розробку бізнеспланів, аналіз ризиків, управління строками, управління витратами) ;
– засоби для організації комунікацій між виконавцями проекту.

В автоматизованій системі управління проектами зазвичай модель проекту будується на основі трьох елементів:

– структури робіт проекту;
– структури ресурсів;
– матриці призначення ресурсів на роботи проекту.

Структура робіт проекту – це перелік етапів і робіт проекту згідно з їхньою підпорядкованістю, взаємозв'язків між роботами, орієнтовної три-

валості виконання робіт. В автоматизованому режимі програма визначає дати початку і завершення окремих робіт і всього проекту, розраховує календарний графік проекту, резерви часу.

На думку Бродської А.О. в автоматизованих системах управління проектами існує одна важлива особливість планування – визначення їх структури, тривалість виконання та їх взаємозв'язок, а не зв'язок робіт до конкретних дат. Структура ресурсів проекту – це людські ресурси, обладнання, матеріали і кошти. Такі ознаки як кількість ресурсів, продуктивність та вартість можуть описуватись в електронних таблицях. Також у системах можна включати календарі використання ресурсів. До складу матриці призначень включається інформацію про застосовані ресурси і яким шляхом їх будуть використовувати по кожному етапу проекту. Також система зберігає дані про властивості ресурсів та їх потребу в роботі [4, с. 8]. По закінченню оформлення даних ресурсів за кожним етапом роботи проекту програма здійснює автоматичний перерахунок календарного плану з урахуванням лімітованості ресурсів. Нині розроблено кілька сотень систем, за допомгою яких можливо реалізувати функції календарного планування і контролю проектів. Серед яких – Microsoft Project, Open Plan Professional, Spider Project, Sure Trek Project Manager, Primavera Project Planner (P3), Time Line, CA Super Project, Project Scheduler, Turbo Project, Artemis Views.

Висновки. На нашу думку успішність від впровадження інформаційної системи та отримання максимальної вигоди та користі на підприємстві залежить від ефективності управління витратами протягом всього терміну роботи проекту. Також від використання інформаційних систем управління проектами має місце не тільки економічний ефект (якість організації складових підприємства, покращення фінансово-економічних показників), але й соціальний, тобто це такі показники як: збільшення рівня інвестиційної привабливості підприємства, чіткість та прозорість обліку та аналізу, адаптивність в результаті реструктуризації бізнесу, підвищення мобільності проекту.

Література:

1. Побережець О.В. Теоретико-методологічні та практичні засади дослідження системи управління результатами діяльності промислового підприємства: [моногр.] / О.В. Побережець. – Херсон: Видавництво: Грінь Д.С., 2016. – 500 с.

2. Башинська І.О. Управління ризиками в проектах / І.О. Башинська, Д.О. Макарець // Економіка, фінанси, право. Щомісячний інформаційно-аналітичний журнал. – К.: Аналітик, 2017. – №6 – С. 3-5.

3. Бродська А.О. Використання інформаційних технологій в управлінні проектами підприємств / А.О. Бродська // Управління розвитком складних систем. – 2013. – Вип. 13. – С. 8–11.

ІНФОРМАЙНІ ТЕХНОЛОГІЇ УПРАВЛІННЯ ПРОЕКТАМИ

Штерн Б.
ВП НУБІП України «Ірпінський економічний коледж»

Управління проектом – це складний процес, реалізація якого вимагає перед замовниками та учасниками високу ступінь відповідальності, контролю та організації взаємодії. Управління проектами підпорядковується правилам чіткої логіки, які зв'язують між собою різні області знань і процеси управління проектами та забезпечує високу надійність досягнення цілей проекту і скорочує витрати на його реалізацію

Управління проектами в області інформаційних технологій за останній час завоювало визнання як найкращий метод планування та управління реалізацією інвестиційних проектів.

За американськими оцінками застосування методології Управління Проектами забезпечує високу надійність досягнення цілей проекту і на 10-15% скорочує витрати на його реалізацію.

У світі накопичено величезний досвід застосування управління проектами в області інформаційних технологій. Зокрема, ця методологія застосовується у всіх великих IT компаніях світу. Програмні засоби для управління проектами встановлені на мільйонах комп'ютерах в усьому світі – тільки пакет Microsoft Project встановлений більш ніж на два мільйони комп'ютерів.

Асоціація управління проектами Project Management Institute (Інститут Управління Проектами) об'єднує близько 40 тисяч членів і має відділення майже на всіх континентах.

Розглянемо основні поняття і методи управління проектами.

Проект – це тимчасова організація, призначена для створення унікальних продуктів або послуг.

В даному контексті "Тимчасова" означає, що у кожного проекту є початок і неодмінно настає завершення, коли досягається поставлена мета, або приходить розуміння, що цілі не можуть бути досягнуті.

В даному контексті "Унікальних" означає, що створювані продукти або послуги відрізняються від інших аналогічних продуктів і послуг.

Приклади проектів: розробка нового обладнання, розробка або впровадження програмних засобів, наукові, технічні розробки і т.д.

Згідно PMBook, управління проектами - це застосування знань, досвіду, методів і засобів до робіт проекту для задоволення вимог, що пред'являються до проекту, і очікувань учасників проекту. Щоб задовольнити ці вимоги й очікування необхідно знайти оптимальне поєднання між всіма характеристиками проекту.

Управління проектами підпорядковується правилам чіткої логіки, які зв'язують між собою різні області знань і процеси управління проектами.

Кожен проект приводить до створення унікального продукту, послуги або результату.

Перш за все, у проекту обов'язково є одна або кілька цілей. Під цілями розуміється не тільки кінцеві результати проекту, а й обрані шляхи досягнення цих результатів (наприклад, застосовувані в проекті технології, система управління проектом).

Досягнення цілей проекту може бути реалізовано різними способами.

Для порівняння цих способів необхідні критерії успішності досягнення поставлених цілей. Зазвичай в число основних критеріїв оцінки різних варіантів виконання проекту входять терміни і вартість досягнення результатів. При цьому заплановані цілі і якість зазвичай служать основними обмеженнями при розгляді та оцінки різних варіантів. Звичайно, можливе використання і інших критеріїв, і обмежень - зокрема, ресурсних.

Для управління проектами необхідні важелі. Впливати на шляху досягнення результатів проекту, цілі, якість, терміни і вартість виконання робіт можна, вибираючи застосовуються технології, склад, характеристики і призначення ресурсів на виконання тих чи інших робіт. Таким чином, застосування технологій і ресурси проекту можна віднести до основних важелів управління проектами.

Крім цих основних існують і допоміжні засоби, призначені для управління основними. До таких допоміжним важелів управління можна віднести, наприклад, контракти, які дозволяють залучити потрібні ресурси в потрібний термін. Крім того, для управління ресурсами необхідно забезпечити ефективну організацію робіт. Це стосується структури управління проектом, організації інформаційної взаємодії учасників проекту, управління персоналом.

Інформація, яка використовується в управлінні проектами, зазвичай не буває стовідсотково достовірною. Облік невизначеності вихідної інформації необхідний і при плануванні проекту і для успішного укладання контрактів. Розгляд та облік невизначеностей дозволяє проаналізувати ризики проекту та ступінь його виконання.

Управління проектом здійснюється за допомогою належного застосування та інтеграції логічно згрупованих процесів, об'єднаних в 5 груп:

– Процеси ініціації – ухвалення рішення про початок виконання проекту.

– Процеси планування – визначення цілей і критеріїв успіху проекту і розробка робочих схем їх досягнення.

– Процеси виконання – координація людей і інших ресурсів для виконання плану.

– Процеси моніторингу і контролю – визначення відповідності плану і виконання проекту поставленим цілям і критеріям успіху, прийняття рішень про необхідність застосування коригувальних дій і визначення необхідних коригувальних впливів, їхнє узгодження, затвердження і застосування.

– Процеси закриття - формалізація виконання проекту і підведення його до впорядкованого фіналу.

Практично методологія управління проектами допомагає:

– обґрунтувати доцільність інвестицій;
– розробити оптимальну схему фінансування робіт;
– скласти план робіт, що включає терміни виконання етапів, використання ресурсів, необхідні витрати;
– оптимально організувати виконання робіт і взаємодію учасників проекту;
– здійснювати планування і управління якістю;
– здійснювати аналіз і управління проектними ризиками;
– оптимально планувати і управляти контрактами;
– аналізувати відхилення фактичного ходу виконання робіт від запланованого і прогнозувати наслідки відхилень, які виникають;
– формувати коригувальні дії на інформаційних моделях проектів і приймати обґрунтовані управлінські рішення;
– вести архіви проектів і аналізувати досвід їх реалізації, який може бути використаний в інших проектах.

Для забезпечення реалізації мети, процесів та методології управління проектом використовується повний спектр програмно-технічних заходів в сфері інформаційних технологій, таких як:

– розміщення та розподіл інформації в локальних, глобальних та віртуальних мережах;
– використання професійних галузевих програмно-технічних засобів та спеціалізованого програмного забезпечення для ведення повного обліку та аналізу проектів;
– створення комфортних умов для комунікації та документування для всіх учасників та зацікавлених сторін проектів без обмежень на відстань та мови спілкування;
– створення можливостей для безпечного спільного використання проектної інформації та забезпечення необхідного рівня захисту та конфіденційності для кожного з учасників проекту програмними та програмно-технічними засобами;
– використання спеціалізованих програм та мережених ресурсів для забезпечення збереження та варіативності кожного з етапів реалізації проекту.

УДК 658.512.2

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ПІДВИЩЕННЯ РІВНЯ БЕЗПЕКИ ВОДІЇВ

Яковчук В.С., Мартин Є. В.
Львівський державний університет безпеки життєдіяльності. Львів

Анотація. Запропонована інформаційна технологія, функціональне призначення якої полягає у забезпеченні вищого рівня безпеки водіїв та їх пасажирів у процесі керування авто на дорогах та у випадку дорожніх пригод (надзвичайних ситуацій). Принцип роботи програми базується на автоматичному використанні виклику до екстрених служб відразу ж після аварії [1]. Подібна програма входить до складу систем, розповсюджених у країнах Америки та Європи, а також вмонтована в автомобілях, вище 2015 року випуску [2]. Однак в Україні така система не використовується, проте її практичне використання надзвичайно актуальне.

Ключові слова: програмне забезпечення, безпека водіїв, аналіз надзвичайних ситуацій на дорогах.

Функціювання системи забезпечується за допомогою програми, яка встановлюється в бортовий комп'ютер автомобіля. Автоматизована програма фіксує швидкість автомобіля, число пасажирів, точне місце положення автомобіля, кількість подушок та ременів безпеки, котрі ще не активовані. Інтерфейс програми має наступний вигляд (рис.1).

Рис.1. Інтерфейс програми

Програмі присвоюється персональний номер, з котрого водій зможе зателефонувати до будь якої служби чи людини, використовуючи бортовий комп'ютер. Це дасть змогу екстреним службам встановити зв'язок з водієм після отримання повідомлення про аварію для перевірки наявності

пасажирів у салоні авто. Програма передбачає модуль «Геометрія», який вираховує траєкторію руху автомобіля і, відповідно, відхилення її від нормативної при обгоні (рис.2).

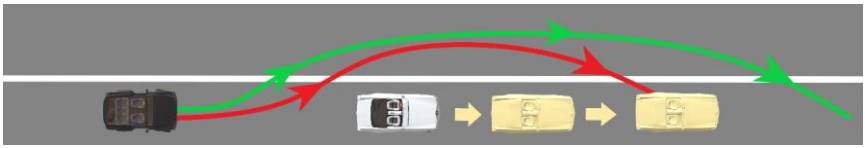


Рис. 2. Траєкторіі руху автомобілів

Встановлена програма призначена для роботи на бортовому комп'ютері. Робота програми передбачає залучення деяких вхідних даних; вона фіксує початок руху автомобіля, а саме місце, час та дату відправлення автомобіля. Програма контролює та фіксує швидкість автомобіля, число пасажирів, число працюючих подушок безпеки та ременів безпеки. При наявності несправностей програма подає знак тривоги. Основна функція автоматизованої програми полягає у передачі інформації екстреним службам (101,102,103) про аварію. Програма реагує на спрацювання подушок безпеки, надсилаючи повідомлення до екстрених служб, тобто до програми, котра встановлена на робочих комп'ютерах чергових екстрених служб. Передаючи інформацію про надзвичайну ситуацію, програма фіксує місце знаходження автомобіля, де сталася аварія, фіксовану швидкість авто до аварії, кількість спрацьованих подушок та ременів безпеки, фіксований час аварії та кількість пасажирів, присутніх в автомобілі. Автоматично передається номер, через котрий служба матиме можливість зв'язатися з постраждалими.

Програма передбачає наявність функції зв'язку з екстреними службами для одержання допомоги, або ж повідомлення про дорожньо — транспортну пригоду на дорозі.

Література

1. Джек Грінфілд, Кіт Шорт, Стів Кук, Стюарт Кент, Джон Крупи Фабрики розробки програм (Software Factories): потокова збірка типових додатків, моделювання, структури та інструменти = Software Factories: Assembling Applications with Patterns, Models, Frameworks, and Tools. — М.: «Діалектика», 2006. — С. 592. —ISBN 978-5-8459-1181-0.
2. Постанова №1306 Про Правила дорожнього руху – КМУ.

Напрям 8

Інформаційні технології в освіті

USE OF MODERN INFORMATION TECHNOLOGY IN EDUCATION

Tania Ben, Yuliia Onofriichuk, Roman Golovatyi
Lviv State University of Life Safety

Процеси глобалізації, які характеризують розвиток сучасного суспільства, запровадження цифрових технологій на всіх рівнях освіти суттєво змінюють вимоги до професійної підготовки майбутніх освітян. Формування компетентних фахівців, які вільно орієнтуються в інформаційному просторі сучасної освіти, на високому рівні володіють інформаційно-комунікаційними технологіями, використовують їх у навчанні, професійній діяльності, під час проведення науково досліджень, є одним із нагальних завдань вищої освіти.

Ключові слова: інформаційні технології, освітні технології.

The processes of globalization that characterize the development of modern society, the introduction of digital technologies at all levels of education are significantly changing the requirements for professional education of future educators. Formation of competent specialists, who are free to navigate in the information space of modern education, have a high level of information and communication technologies, use them in training, professional activity, during the conduct of scientific research, is one of the urgent tasks of higher education.

Keywords: information technologies, educational technologies.

The current state of the higher professional education is determined by the necessity of permanent modification of the education process of a higher educational institution with the purpose of, on the one hand, ensuring training of skilled employees in the circumstances of varying demands, and, on the other hand, adopting and adapting the successful experience of other educational institutions in their activity [1].

Undoubtedly, at the development of modern methods of education, it is necessary to take into account the rapid growth of the use of information technologies, which has been observed within the last decade, and also a large quantity of educational and technical innovations. One of such innovations is the use of the blended learning, the concept of which assumes that in the current state of the system of higher professional education, traditional education can be combined with the advantages of distant educational technologies . The idea is that a considerable part of the material is transformed into the distant form, allowing time at classes for various interactive forms, which would improve their efficiency . The "teacher-student" and "student- student" interactions can be also

implemented in the distant form using various educational elements of the learning management system [2, 4].

At teaching humanitarian students, the Moodle learning management system was used. Informational and educational functionality of the given system was added by the electronic library system, the reading room, and the Internet center of the university. Interaction of the given elements made it possible to build the current infrastructure of theinformational and educational environment of the university [3, 5] :

- the administrative unit (organization and control of the education process)
- the educational unit (educational interaction of the participants of the education process), which is subdivided into three elements:
- the informational element (the study process itself, use of electronic and printed versions of educational materials).

1. the social element (the direct or mediated dialog in the form of the "student-student" and "student-teacher" interactions, and also group interaction through forums, chats, etc.).

2. the creative element (using databases on the course subject, supplying content for glossaries, accomplishing creative works by means of the wiki-technology, etc.).

3. the program engineering block (hardware and software used for storing information and providing for interaction between the participants of the education process)

The main problem of implementation of the first approach was the organizational complexity, which was aggravated with the functionality of the hardware and software system. Therefore, the second approach was used more often: a student gained necessary methodical materials, fulfilled some tasks, and based on the studied material developed his own project. At that, the individual work (or in pairs or groups) on project development was organized using the Moodle learning management system. Methodical directions for accomplishment of laboratory works were provided in electronic form.

As a rule, they were combinations of text and some graphic information in the form of screenshots. In certain cases, this content was provided as videos. Videos represented the program work area and audios represented the teacher's comments concerning actions to be done for achieving certain effect. Experience showed that in that case it was easier to teach main principles of operation with the given means in the visual form. Thus, the possibility remains to work simultaneously with methodical stuff; one can pause the video at any time and make necessary actions.

The learning management system application was reduced to acquaintance with the questions for preparation for the respective form of the control and evaluation event and to fulfillment of training tests. Independent work of a student

consisted in single or group learning of the part of a discipline, which had been scheduled for distant learning.At implementation of the blended learning methodology, there was a probability of its rejection by some teachers and students. Therefore, among them regular polls were taken using the learning management system for the purpose of modification of the education process. It is necessary to mention the most popular suggestions: use of electronic mail for communication of a teacher with a student; refusal from the blended learning for the benefit of the traditional one; use of the learning management system just for delivery of the training stuff and cancellation of interactive forms.

To sum up, the education, which is compiled using the informational and educational environment with a similar infrastructure, has much in common with traditional education, but it allows using modern production technologies and experience in the circumstances of decreasing the share of intramural classes. At that, the education of students becomes more intensive due to the group work and the creative element of the education and more transparent due to the control through the learning management system and other elements, which together create the informational and educational environment, namely reading rooms, libraries, Internet centers, etc.

Reference:

1. Kumar, S. and R. Toteja, 2012. Print to digital: a study of students' psychosomatic cost in traditional and e-learning. Procedia – Social and Behavioral Sciences, 67: 553-560.

2. Рак Ю. П. Формування проектів методом візуалізації інформації для підвищення стану безпеки торгово-розважальних центрів / Ю. П. Рак, Р. Р. Головатий // Управління проектами у розвитку суспільства: зб. тез доповідей XII Міжнар. конф. – Київ: КНУБА, 2015. – С. 226 – 228.

3. Safranj, J., 2013. Using Information Technology in English Language Learning Procedure: Blended Learning. Procedia – Social and Behavioral Sciences, 83: 514-521.

4. Li, X. and F. Gao, 2012. Development-Driven E-learning Education Model and Application in Teaching Information Technology Original Research Article. IERI Procedia, 2: 854-858.

5. Зачко О. Б. Інновінг управління проектами створення об'єктів з масовим перебуванням людей засобами безпеко-орієнтованого підходу // О. Б. Зачко, Р. Р. Головатий // XIV Міжнародна науково-практична конференція «Управління проектами у розвитку суспільства». – Київ, 2017 – С.121-123.

6. Борзов Ю. Особливості застосування комп'ютерного моделювання для покращення навчального процесу / Ю. Борзов, Р. Головатий, Я. Магеровський. // Інформаційні технології розвитку змісту освіти. – 2019. – С. 80–81.

ВИКОРИСТАННЯ ГЕЙМІНГУ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ НАВЧАННЯ В ЗАКЛАДАХ ВИЩОЇ ОСВІТИ

Гаврись А., Гарасим'юк А.
Львівський державний університет безпеки життєдіяльності

В роботі проаналізовано позитивний вплив геймінгу на студентів при використанні його в навчальному процесі. Приведено його ефективне використання в розвитку певних навичок людини, які їй потрібні для виконання своєї професійної діяльності в майбутньому.

Ключові слова: відеоігри, когнітивний потенціал, навчальний процес.

In this paper the positive influence of students gaming during their educational process was analyzed. Effective use in the development of certain skills of the person, which they need to fulfill their professional activity in the future, was showed.

Keywords: video games, cognitive potential, learning process.

Геймінг– це гра у відеоігри. Засновником відеоігор вважається американський інженер і винахідник Ралф Бер. В 1996 році він випустив першу в історії відеогру під назвою «Chase», що і поклало початок індустрії відеоігор та кіберпростору загалом.

Відеоігри почали входити в повсякденне життя людей як вид розваг та заробітку.

Проте з розширенням кількості та типів відеоігор збільшуються можливості їх використання. Одна з таких можливостей - застосування відеоігор в навчанні та освіті. Це так звана концепція Game Based Learning (GBL) , тобто навчання, засноване на грі [1].

У 1978 році були проведені перші дослідження, які виявили мотиваційний ефект і когнітивний потенціал відеоігор. Згідно досліджень [2,3] відеоігри показали позитивний вплив на людину в певних аспектах її діяльності.

Позитивний вплив виявлено в наступному:

1. **Розвиток дрібної моторики.** Під час гри мозок безперервно дає рукам команди вчасно натискати потрібні кнопки і швидко міняти поєднання клавіш. Дрібна моторика - це, простіше кажучи, спритність рук, пальців. Зв'язок може здатися неочевидним, але в підсумку хороша дрібна моторика має великий вплив на загальний розвиток людини, в тому числі, зміцнює психіку, удосконалює мовну функцію, творчі здібності, мислення, пам'ять і логіку.

2. **Вибір рівня складності.** Серед важливих переваг навчання за допомогою відеоігор – можливість вибирати рівень складності. Це співвідноситься з звичайної навчальної ситуацією: всі студенти знаходяться на різному рівні освоєння матеріалу, здатності і особливості сприйняття теж у

всіх різні. І якщо навчати всіх на загальному усередненому рівні, то знання доходять з середньою успішністю і здібностями: при цьому відстаючі не встигають «підтягнутися», а випереджаючим нудно, вони не реалізовують потенціалу своїх здібностей. EL earning за допомогою ігор якраз вирішує цю проблему, студенти грають в одну і ту ж гру , але вдосконалюють і закріплюють навички на своєму рівні складності. Отже, вибір рівня дасть змогу, як оцінювати студентів за їхнім рівнем розвитку, так і самі студенти зможуть розвиватися відповідно того рівня з яким вони можуть справитись.

3. **Залучення.** Під час класичного уроку, коли викладач щось доносить до студента йому легко заплутатись у своїх думках. Особливо, якщо тема заняття не цікава або складна для сприйняття. Навчальні комп'ютерні ігри забезпечують надзвичайно високий рівень залучення в освітній процес і утримують увагу, тобто за допомогою ігор набагато простіше привернути увагу студента.

4. **Постановка цілей.** Відеоігри за своєю природою наділені чіткими цілями: там є сюжет, персонажі, їх відносини, цілі, до яких прагнуть персонажі. Навчаючись принципам вирішення проблем, стратегічного мислення і логіки прийняття рішень студенти зможуть краще продумувати свої дії для того щоб дістатись до своєї мети таким чином вони розвинуть в собі далекоглядність.

5. **Ігрове освоєння матеріалу.** Наприклад, ігровий бестселер 2005 року God of War для PlayStation базується на грецькій міфології. Її і за словником Іліади вивчати одне задоволення, а вже через гру – повний освітній захват. Що, зрозуміло, не скасовує необхідності книжкової теорії, але після гри вона піде куди веселіше і з більшим ентузіазмом. І це не єдина відеогра, яка може чогось навчити.

6. **Інтерактивність і симуляції ефект.** За допомогою відеоігор навчають не тільки школярів і студентів. Наприклад, симулятором Air Force тренують пілотів.

7. **Тренування комплексу життєвоважливих навичок.** Не зважаючи на жорстокість таких ігор як Call of Duty або серія про морських котиків Socom , вони тренують у гравців стратегічні і тактичні навички, а також концентрацію уваги. Багато дослідників говорять про високий освітній потенціал The Sims , оскільки ця гра симулює соціальні взаємодії. Швидкість реакції тренують не тільки шутери, але і музичні відеоігри (Guitar Hero, Rock Band). Покрокові стратегії з будівництвом і елементами виживання (Minecraft , Civilization), Квести та рольові ігри (DeusEx: Human Revolution) покращують просторове мислення, удосконалюють здатність до вирішення проблем.

Американський дослідник в області психолінгвістики, соціолінгвістики і білінгва-освіти, експерт зі світовим ім'ям в галузі освіти за допомо-

гою комп'ютерних ігор, член Національної Академії Освіти. В даний час викладає в університеті Арізони, США в своєму відео- зверненні зазначає [4], що «ми не зможемо змінити парадигму освіти і зробити її більш глибокою, вчити вирішувати проблеми та інновацій, поки не змінимо систему оцінювання і тестів» – і це, начебто, всім давно зрозуміло, але зміни в цьому напрямку дуже-дуже повільні.

Висновок. Отже, можна припустити таку теорію якщо ввести в навчальну програму ігри тоді навчання стане цікавішим. Оскільки сучасні діти змалку розвиваються в технологічній структурі і мало кому цікаво читати скучний текст з книжок, а тим більше його запам'ятати. А якщо навчання зробити в розважальній програмі у вигляді ігор, то студенти самі змушені відкрити той чи інший посібник, для того щоб дізнатися як пройти певний рівень. Також відеогра може бути як спосіб оцінювання тобто пройшовши певну гру і заробивши достатню кількість балів учень може отримати хорошу оцінку, яка буде враховуватися на заліку чи екзамені.

Література:

1. Гаврись А.П. Гейміфікація як інструмент підвищення ефективності навчання у віртуальному університеті / А.П. Гаврись, І.М. Гарасимюк // XIV Міжнародна науково-практична конференція молодих вчених, курсантів та студентів «Проблеми та перспективи розвитку системи безпеки життєдіяльності». – ЛДУ БЖД. - Львів. – 2019. – с. 428-429.

2. Adam C. Oei, Michael D. Patterson «Enhancing Cognition with Video Games: A Multiple Game Training Study» // PLoS One. 2013; 8(3): e58546. Published online 2013 Mar 13. doi: 10.1371/journal.pone.0058546. Access - https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3596277/

3. Sandro Franceschini,Simone Gori,Milena Ruffino,Simona Viola,Massimo Molteni,Andrea Facoetti «Action Video Games Make Dyslexic Children Read Better» // Current Biology Publisher: Elsevier Published: February 28, 2013. DOI:https://doi.org/10.1016/j.cub.2013.01.044. Access - https://www.cell.com/current-biology/fulltext/S0960-9822(13)00079-1

4. Відеозвернення Джеймса Пола Джі. Режим доступу – https://www.youtube.com/watch?v=qGd1URORsoE.

ЗАСТОСУВАННЯ ГРАФІЧНОГО МЕТОДУ АНАЛІЗУ ДАНИХ ПРИ ВИВЧЕННІ ЕКОНОМІЧНИХ ПОКАЗНИКІВ

Голуб Є.
ВП НУБіП України «Ірпінський економічний коледж»

Анотація. Швидкий і доступний спосіб обробки складних і великих обсягів даних завжди був актуальним для фахівців економічної сфери діяльності. Саме тому важливим є навчати студентів певних спеціальностей користуватись аналітичними застосунками, які пропонує сучасний ринок програмного забезпечення.
Ключові слова: прогнозування, ефективність, апроксимація, лінія тренду, величина достовірності, графічний метод дослідження.

Abstract. A fast and affordable way to handle complex and large amounts of data has always been relevant to economic professionals. That is why it is important to teach students of certain specialties to use the analytical applications offered by the modern software market.
Keywords: forecasting, efficiency, approximation, trend line, reliability, graphical research method.

В підготовці майбутніх фахівців фінансово-економічної сфери важливо враховувати, що специфіка їх роботи буде полягати в обробці великих обсягів даних, виконанні розрахунків різної складності та представленні результатів у візуально доступному форматі. Всі ці операції стають на багато легшими, якщо спеціаліст володіє певними вміннями і знаннями не тільки в рамках безпосередньо своєї спеціальності, але і навичками обробки даних за допомогою програмно-апаратної складової. Важливо зауважити, що спеціального програмного забезпечення для вказаних операцій, на етапі навчання встановлювати не потрібно, бо стандартний офісний пакет MS Office може задовольнити всі можливі примхи користувача по обробці даних.

Наведемо приклад розв'язання задачі економічного характеру на прогнозування.

Студентам пропонується таблиця зі статистичними даними по ВВП України за період у неповних 7 років (2008 – 2015 рр)[2], див. Табтлиця 1.

[2] Статистичні дані взяті на сторінці Національного Банку України за адресою: https://bank.gov.ua › files › BUD_u

Таблиця 1

Роки	Номінальні доходи (млн.грн.)	Номінальні видатки (млн.грн.)	Номінальне кредитування (млн.грн.)	Номінальні дефіцит (–), профіцит (+) (млн.грн.)
2008	1838516,45	1759370,33	8245,78	70900,35
2009	1728876,07	1868237,55	17224,18	-156585,36
2010	1909536,46	2231600,68	-2280,23	-319783,19
2011	2439150,53	2476703,01	23691,17	-61243,65
2012	2739920,58	2896729,04	26854,16	-183662,62
2013	2796660,47	3111377,72	5696,38	-320413,62
2014[3]	2900078,17	3176796,73	17717,07	-294435,62
2015[4]	2221797,88	2077658,45	6628,88	137510,55

За допомогою спеціального графічного інструменту MS Excel, який називається ***Лінія тренду***, майбутні фахівці, не вдаючись до громіздких розрахунків, наближено можуть оцінити поведінку статистичної вибірки. Для побудови ліній тренду використовуються формули, за допомогою яких можна розрахувати наближену до експериментальних точок криву – ***криву апроксимації***. Чим більша кількість значень для аналізу, тим точнішим буде прогнозування. При чом студенти мають можливість продовжити лінію тренду в обидва боки, налаштовуючи крок апроксимації.

Варто зауважити, що підбираючи різні види апроксимації (лінійна, поліноміальна, логарифмічна, експоненціальна, степенева), можна досягти максимального наближення лінії тренду до рельєфа діаграми. Степінь наближення характеризується ***величиною достовірності апроксимації***. Вона актуальна в діапазоні від 0 до 1, і, відповідно, чим ближче значення до одиниці, тим краще підходить функція і точніше апроксимація. Цей коефіцієнт в MS Excel розраховується автоматично, що дає можливість не відволікатись від безпосереднього аналізу отриманої при побудові лінії тренду інформації, і як найшвидше зробити певні висновки щодо характеру і тенденції вибірки значень.

На основі поданої таблиці значень і за допомогою вище згаданого інструмента студент має можливість швидко оцінити перспективи і стан економіки країни, за умови, що не буде ніяких змін в характері керування і організації у вказаній економічній сфері. Результатом побудови по першому стовбцю даних таблиці буде така апроксимаційна крива у вигляді крапочок на рисунку 1, з коефіцієнтом апроксимації 0.9756 (поліноміальна апроксимація 5-го степерня).

[3] Починаючи з 2014 року обчислення здійснені до ВВП розраховано без урахування тимчасово окупованої території Автономної Республіки Крим, м.Севастополя та частини зони проведення антитерористичної операції.

[4] Враховано неповний рік (тільки 3 квартала).

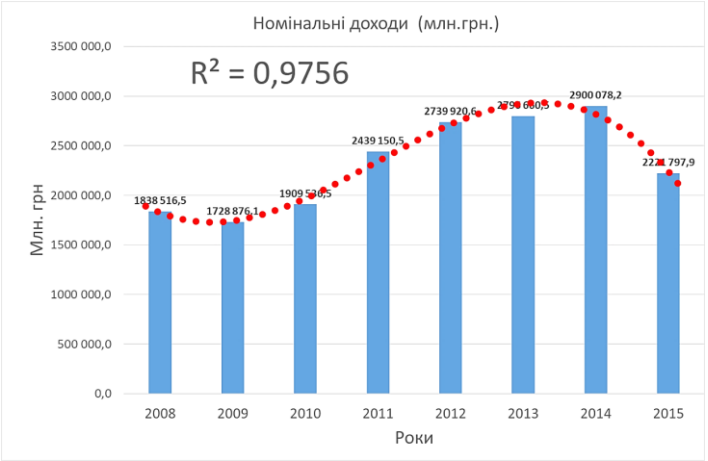


Рисунок 1 – Лінія тренду для ряду даних "Номінальні доходи (млн.грн.)"

На основі побудованої діаграми, очевидні зміни у ряді даних «Номінальні доходи», але за умови, що 2015 рік побудований по неповним даним, об'єктивної інформації на кінці кривої отримати неможливо. Проте тенденція більш-менш проглядається. Якщо ж читач зацікавиться такою можливістю прогнозування, то він завжди може скористатись наданою вище таблицею, та розглянути лінії тренду для ще трьох рядів даних, діаграми для яких, не надано навмисно.

Таким чином, майбутні фахівці, на основі вказаної вибірки даних, користуючись спеціальними можливостями MS Excel, навчаються швидко аналізувати досить великі обсяги даних, синтезувати нові підходи до представлення своїх висновків, подавати результати досліджень у зрозумілому і доступному форматі.

Література:

1. Офіційний сайт Національного Банку України. Режим доступу: https://bank.gov.ua › files › BUD_u

ЦЕНТРАЛІЗОВАНИЙ ПІДХІД ДО РОЗРОБКИ СИСТЕМИ УПРАВЛІННЯ ТЕМАТИЧНОЮ НАВЧАЛЬНОЮ КВЕСТ-КІМНАТОЮ THE HOT TEST ROOM

Жезло Н.В., Хлевной О.В.
Львівський державний університет безпеки життєдіяльності

Використання тематичних квестів в реальності при підготовці населення до дій в умовах пожежі є інноваційним підходом до набуття знань, вмінь і навиків безпечної поведінки та формування у майбутніх рятувальників психологічної готовності до оперативного та правильного реагування на небезпеку. The Hot Test Room – проект тематичної квест-кімнати для квесту в реальності, сюжет якого передбачає виконання комплесу завдань, пов'язаних із порятунком із приміщення, охопленого пожежею. Для забезпечення можливості повторної участі у грі передбачено поділ кімнати на комірок. Проведеними дослідженнями встановлено, що за співвідношенням ціни і максимальної кількості можливих варіантів, оптимальним є поділ на 6 комірок [1].

Для забезпечення функціонування квест-кімнати запропоновано проект системи управління, яка б давала змогу не тільки керувати усіма процесами, а й забезпечувати можливість виконання різних варіантів сценаріїв в залежності від дій гравців. Оптимальним варіантом є об'єднання усіх пристроїв у одну мережу і керування нею з головного комп'ютера.

При облаштуванні приміщень необхідно використати наступну периферію: управління GPIO (замки, світло, вентиляція, генератори диму), інформація з GPIO (датчики, кнопки), система відеоспостереження, монітори.

В якості керуючого пристрою доцільно застосовувати звичайний ПК з Unix-подібною операційною системою. Це дасть змогу запустити фонову програму (демон), яка і буде контролювати весь квест. Для об'єднання всіх пристроїв у мережу потрібно використовувати Ethernet і протокол UDP.

Зважаючи на різноманіття периферії, виділимо три типи пристроїв, які потрібно підключити в мережу. Це звичайний комп'ютер (з операційною системою Debian), Arduino Mega та Raspberry Pi.

Для програмування мікроконтролерів оптимально використовувати C ++ (компілятор avr-g ++), в якості утиліти для збірки – CMake. На відміну від Arduino IDE, це дозволить автоматизувати процес складання і домогтися більшої гнучкості.

В якості модуля Ethernet непоганим варіантом є недорогий Microchip ENC28J60 (близько 150 грн.). Як бібліотека використовується EtherCard. Вона звертається до arduino-style функцій, зокрема, pinMode. Замість того, щоб переписувати бібліотеку, можна взяти з коду Arduino реалізацію лише потрібних нам функцій, цим самим отримавши «міні-версію» ядра Arduino. CMake дозволяє легко підключити «міні-ядро» до проектів.

Дуже важливо забезпечити можливість віддаленої зміни прошивки контролера. Для цього потрібно використати проект avr-etherboot, трохи змінивши його для роботи з Mega 2560. Працює він у такий спосіб: файли .hex з прошивками зберігаються на центральному комп'ютері і доступні по протоколу TFTP. Avr-etherboot генерує bootloader, який прошивається по ISP в кожен контролер. При завантаженості контролера запускається bootloader, підключається до мережі і викачує по TFTP прошивку. Далі відбувається робота прошивок на кожному мікроконтролері. Написаний скрипт дозволяє згенерувати bootloader для кожного мікроконтролера та прошити його однією командою. Щоб мати змогу перепрошити усі мікроконтролери, необхідно застосовувати 8-канальне реле, через яке відбувається живлення усіх Ардуіно, крім однієї (призначена для управління цим реле і перепрошивається через USB з центрального комп'ютера).

Щоб реалізувати сценарій квесту, слід використовувати кілька процесів. Кожен процес має мати повний доступ до периферії. Також слід передбачити можливість взаємодії процесів між собою. В окремі процеси винесемо незалежні завдання і очікування подій. Коли подія настає, процеси будуть реагувати належним чином. При цьому основний сценарій – це окремий процес. Він передбачає очікування подій проходження кожної з комірок, а також надсилання команди периферії на виконання дій.

Взаємодія між процесами може бути забезпечена за допомогою іменованих каналів. Для того, щоб з одного UDP-сокета периферійні пристрої могли зчитувати кілька процесів, варто використати розгалужувачі (за кількістю процесів). Пакет, отриманий від певного пристрою, пересилається в усі ці канали. Використання додаткового TCP-сервера може дозволити керувати квест-кімнатою, створюючи події і показуючи лог. TCP-сервер дає можливість створити веб-інтерфейс, що дасть змогу контролювати квест з планшета [2].

Отже, реалізації подібної ідеї системи управління квест-кімнатою дає змогу легко міняти сценарії, завдання і налаштування пристроїв, керувати процесами через веб-інтерфейс і легко усувати несправності. Наявність зовнішнього IP дає можливість керувати кімнатою віддалено.

Література:

1. Хлевной О.В., Буряк Н.Є. Квести в реальності як засіб підготовки майбутніх рятувальників до дій в умовах пожежі. Розвиток цивільного захисту в сучасних безпекових умовах: матеріали 21 Всеукр. міжнар. наук.-практ. конф., − Електронне видання комбінованого використання. – Київ: ІДУЦЗ, 2019. – С. 287–289.

2. Умный квест в реальности: демоны и проводки. URL: https://habr.com/ru/company/technoworks/blog/258585/

ОСОБЛИВОСТІ ВПЛИВУ КОМП'ЮТЕРНИХ ТА НАВЧАЛЬНИХ КОМП'ЮТЕРНИХ ІГОР НА РОЗВИТОК ПІЗНАВАЛЬНОЇ ДІЯЛЬНОСТІ

Жолубак Л.І., Карабин О.О.
Львівський державний університет безпеки життєдіяльності, Львів

Розглянуто основні групи ком'ютерних ігор з точки зору їх впливу на розвиток основних пізнавальних здібностей людини таких як, увага, пам'ять, логчне мислення, орієнтація в просторі. Розумне використання комп'ютерних ігор сприяє зацікавленості та мотивації до навчальної і пізнавальної діяльності.

Ключові слова: комп'ютерна гра, навчальний процес, пізнавальна діяльність.

The main groups of computer games are considered in terms of their influence on the development of basic cognitive abilities of a person, such as attention, memory, logical thinking, space orientation. The smart use of computer games fosters interest and motivation for learning and learning.

Key words: computer game, educational process, cognitive activity.

Пізнавальні процеси: сприйняття, увага, уява, пам'ять, мислення, мова – виступають як найважливіші компоненти будь-якої людської діяльності. Всі ці компоненти людина розвиває в процесі навчання. Найбільш активно пізнавальна діяльність розвивається в дитячому і підлітковому віці, але для досягнення хороших результатів в навчальній і пізнавальній діяльності має бути мотивація, якої на жаль дуже мало в зазначеному віці. Пізнавальний та навчальний процес школярів та студентів буде тим більше ефективний, чим більше зацікавленими будуть школярі та студенти на заняттях [1]. Дитина вчиться пізнавати світ через гру. Тому виникає ідея, що саме гра внесе в навчальний процес момент зацікавленості. В сучасних умовах високих технологій використання компютерних ігор та тренажерів стає доступним в кожному навчальному закладі – від дитячого садочка до закладу вищої освіти.

Метою роботи є проаналізувати особливості основних груп ком'ютерних ігор та навчальних комп'ютерних ігор та можливості їх використання в навчальному процесі.

Необхідно чітко диференціювати навчальні комп'ютерні ігри від власне ком'ютерних ігор.

Комютерні ігри можна поділити на такі групи:

- стратегії;
- адвентурні;
- рольові;
- аркадні;
- логічні;

– симулятори;
– 3D -action.

Фахівці з Великобританії, що працюють за проектом освітніх програм Teachers Investigating Educational Multimedia, провели дослідження, спостерігаючи за навчанням і розвитком більш як 700 дітей на заняттях з використанням інформаційно-комунікаційних технологій, і виявили, що використання комп'ютерних ігор може потужно сприяти розвитку як логічного, так і інших видів мислення. Це стосується насамперед ігор, де потрібно будувати міста і створювати співтовариства людей, як, наприклад, в іграх SimCity, Championship Manager чи RollerCoaster Tycoon. У змістовній частині гри конструюються конфліктні ситуації, розраховані на певну вікову групу, де учасники цього процесу повинні не тільки досягти конкретного позитивного результату на рівні особистих навчальних цілей, але й своїми успіхами опосередковано впливати на інших дітей, що діють в аналогічних ситуаціях.

Адвентурні ігри (Counter-Strike) сприяють розвитку кмітливості і логічного мислення, розвивають орієнтацію в просторі, увагу і реакцію. Але ці ігри чинять велике навантаження на нервову систему. Якщо контролювати такі ігри за часом, то вони можуть бути корисними.

Ігри стратегії (Clash Royale, Clash of Clans) сприяють розвитку мислення, розвивають здатність до планування та посидючості.

Аркадні ігри (World of Tanks) розвивають увагу та швидкість реакції. Розвитку програмування, регуляції і контролю діяльності сприяють квести і стратегії.

Рольові ігри (Grand Theft Auto, Pokémon Go), сприяють розвитку аналітичного мислення, умінню використовувати властивості персонажів гри. Такі ігри вважають найбільш небезпечними з погляду формування стійкої психологічної залежності. Особливість рольової комп'ютерної гри в тому, що гравець ідентифікує себе з комп'ютерним персонажем, виступаючи в ролі героя. Комп'ютерна рольова гра побудована таким чином, щоб спровокувати гравця до "відмови" від навколишньої дійсності, у зв'язку з чим діти, у яких не сформовано самоконтроль, проводять за комп'ютером значну кількість часу, що може мати негативі наслідки, такі як порушення здоров'я і особистісна деформація.

Використання 3D-Action ігр, таких як Clash of Clans, – де використано тривимірну графіку і спецефекти, сприяє тільки частковому розвитку моторних функцій.

Розвитку логічного мислення сприяють ігри-головоломки, такі як King of Thieves. Під час проходження логічних ігор діти навчаються лічити, писати, читати.

Використання ігор-симуляторів (імітатори) різних засобів пересування (літаків, кораблів, автомобілів, космічних апаратів та ін.), для яких характерна реалістичність і дотримання найдрібніших технічних показни-

ків (Minecraft, The Sims, Toca Kitchen, Need For Speed) дає дитині можливість "приміряти" дорослі види діяльності. Насамперед слід відзначити взаємозв'язок з простором, а цього дуже не вистачає сучас ним дітям. Візуально-просторові функції включають орієнтування "право-ліво", "верх-низ", порівняння розмірів, оцінку розташування елементів у просторі.

Навчальних компютерних ігор, доступних в мережі Internet є не досить багато. Розглянемо деякі з них, які можна використати на заняттях з математики в початковій школі або в дошкільних навчальних закладах.

Гра на закріплення навичок лічби (Math Learning) пропонує порахувати приклади та вдосконалити майстерність лічби.

Гра на уважність (Фанатики математики) пропонує ребуси з розтановки чисел так, щоб їх сума, добуток, частка дорівнювали певному числу.

Ігри на розвиток логічного мислення пропонують встановити закономірності в наборах рисунків.

Ігри на швидкість реакції сприяють збільшенню швидкості лічби.

Висновок: Створення і використання в освітньому процесі навчальних комп'ютерних ігор, які спрямовані на гармонійний розвиток особистості – одна із актуальних проблем сьогодення, якою зацікавлені вітчизняні та зарубіжні педагоги. Універсальність комп'ютерних ігор визначається тим, що вони можуть бути застосовані не тільки як практичний посібник на заняттях, а і як засіб розширення можливостей навчально-виховного процесу всіх навчальних закладів від дитячого садка до вищого навчального закладу.

Література:

1. Тарапата Н. Комп'ютерна гра. Інструменти і методологія створення комп'ютерних ігор / Тарапата Н., Семьонова М., Смотр О., // Захист інформації в інформаційно-комунікаційних системах : зб. тез доповідей II Міжвуз. наук.-практ. конф. студ. і курсантів. – Львів : ЛДУ БЖД, 2017. – С. 55-56.

2. Конахович Г. Ф. Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, А. Ю. Пузыренко. – К. : Изд-во "МК-Пресс", 2006. – 288 с.

3. Закревська Є. С. Комп'ютерні ігри як засіб формування здорового способу життя школярів [Електронний ресурс] / Є. С. Закревська – Режим доступу до ресурсу: http://visnyk.chnpu.edu.ua/?wpfb_dl=3098.

ПОРТАЛ ДЛЯ ПОШИРЕННЯ УКРАЇНОМОВНИХ АУДІО КНИГ

Заяць А.Р., Пасічник Т.В.
Львівський Національний Університет імені Івана Франка, м. Львів

Ключові слова: фреймворк APS.NET Core 2.2 Web API; засоби EF Core; система керування базами даних MS SQL; засоби MS SQL; хмарна платформа Azure; платформа контролю версій Azure DevOps; клієнт фреймворк Angular; мова програмування C#; мова програмування TypeScript; бібліотека Angular material.

Keywords: APS.NET Core 2.2 Web API; EF Core; MS SQL; MS SQL; Azure; Azure DevOps; Angular; C#; TypeScript; Angular material.

Для чого потрібна звукова книга, якщо є звичайна. Існують дві причини появи звукових книг.

По-перше, для читання звичайної книги потрібні більш-менш комфортні умови, хороший зір, освітленість, а звукові книги можна слухати практично в будь-яких умовах: під час ранкової зарядки, сніданку, прогулянки по дорозі на роботу, в своєму автомобілі (особливо під час очікувань, в пробках, при поїздках на тривалі відстані).

По-друге, гарне виконання може донести такі нюанси книги, на які не звертається увага при читанні. Іноді процеси читання книги та її прослуховування, відрізняються так само, як читання нот від живого виконання твору музикантом.

Одна з найважливіших проблем це те, що більшість аудіо книг, наших «улюбленців», не так вже й просто знайти в просторах інтернету. Інколи, ми витрачаємо цілі дні на пошуки книги та не знаходимо шуканого.

Мета завдання полягає у створення веб-сайту для накопичення та поширення україномовних аудіо книг. Веб-сайт дозволить виконати наступне:

- Переглянути та прослухати опубліковані аудіо книги;
- Створити попит на озвучення книги;
- Долучитись до озвучення книги;
- Контролювати процес озвучення книги;
- Контролювати процес публікації аудіо книги;
- Зберігати аудіо книги з інших веб-ресурсів;
- Якісне авто озвучення книги системою.

Веб-портал реалізований за допомогою:

ASP.NET Core 2.2 Web API – вільна та відкрита система для розробки серверного програмного забезпечення. Мова програмування *C#*.

EF Core – технологія доступу до даних

MS SQL – система керування базами даних

SendGrid – сервіс, email as a service, для надсилання повідомлень на поштові скриньки користувачів.

Azure – це хмарна платформа та інфраструктура, призначена для розробників застосунків хмарних обчислень і покликана спростити процес створення онлайнових додатків.

Azure AD – сервіс, authorization as a service, для авторизації користувачів у систему

Azure DevOps – продукт, який є комплексним рішенням, що об'єднує в собі систему керування версіями, збір даних, побудову звітів, відстеження статусів та змін по проекту, тестування та призначений для спільної роботи над проектами з розробки програмного забезпечення.

Angular 7 – front-end фреймворк написаний на мові програмування TypeScript.

Angular material – бібліотека, яка реалізовує принципи дизайну сайтів, програмного забезпечення і застосунків, а також правила дизайну інтерфейсів для операційної системи Android від компанії Google.

Література:

1. https://material.angular.io/
2. https://css-tricks.com/snippets/css/a-guide-to-flexbox/
3. https://aclottan.wordpress.com/2016/12/30/load-configuration-from-external-file/
4. https://medium.com/@sambowenhughes/configuring-your-angular-6-application-to-use-microsoft-b2c-authentication-99a9ff1403b3
5. https://spikesapps.wordpress.com/2017/07/27/securing-an-angular-application-with-azure-ad/
6. https://en.wikipedia.org/wiki/Onion_model
7. https://martsound.com.ua/uk/recording-audio-books/
8. https://www.udemy.com/the-complete-guide-to-angular-2
9. Jeffrey Richter – CLR via C# (4th edition)
10. Adam Freeman – Pro ASP.NET Core MVC 2

РОЗРОБКА ІГРОВОГО МОБІЛЬНОГО ДОДАТКУ ДЛЯ ПЛАТФОРМИ IOS З МЕТОЮ ВИВЧЕННЯ АНГЛІЙСЬКОЇ МОВИ

Звізло Ю.З., Клакович Л.М.
Львівський національний університет імені Івана Франка, м. Львів

Ключові слова: ігровий мобільний додаток, шаблони проектування, збереження прогресу користувача, машинне навчання, розпізнавання мови, підготовка до складання іспиту, платформа iOS, середовище Xcode, мова Swift.

Keywords: gaming mobile application, design patterns, progress saving, machine learning, speech recognition, exam preparation, iOS, Xcode, Swift.

У нашому глобальному суспільстві багато хто потребує вивчення нової мови (для міжнародних подорожей, ділових відносин тощо). Мовні додатки є достатньо великими та громіздкими. Один із найпопулярніших на сьогодні, Duolingo, був нагороджений Apple App в 2013 році і Google Play в 2014 році.

Мовні класи історично мали високий рівень «виснаження», і не дивно, що курси, засновані на програмному забезпеченні, зазнають тієї самої долі. У 2008 році Джефф Маккуйлан використав метод «зносу», щоб визначити, як далеко люди просунулися через книжки з вивчення мови, запозичені в публічних бібліотеках. Він виявив, що середній читач читає менше 20% кожної книги. Дослідження іспанського курсу додатку Duolingo показало, що більшість студентів вибули після менш ніж 2 годин навчання.

Незважаючи на те, що кількість людей, які вивчають мову на рівні освіти, знизилася, все ще існує потреба в досконалому володінні мовою. Дослідження показують, що початківці, які вивчають іспанську мову, візьмуть у середньому від 26 до 49 годин навчання з Duolingo, щоб покрити матеріал для першого семестру іспанського коледжу.

Вивчення нової мови завжди залишатиметься актуальним заняттям для багатьох людей (незважаючи на вік), а англійська мова перебуває в числі найпопулярніших.

Мета роботи полягає в тому, щоб створити мобільний додаток-гру для вивчення англійської мови, який не лише дозволяє користувачу швидко опанувати граматичний матеріал та збагатити власний словниковий запас, а також підготуватися до складання іспиту для подальшого проходження сертифікації.

Особливості програми:

1) розподілення кожного уроку на тематичні частини:
   - складання слів;
   - вивчення граматики;

- складання речень;
- урок читання;
- урок аудіювання;
- урок говоріння.

2) збереження прогресу користувача;
3) необмежений час на проходження уроку;
4) повернення до питання, на яке користувач відповів неправильно;
5) перевірка після кожної відповіді;
6) підказки у вигляді аудіозаписів;
7) можливість багаторазового проходження уроку;
8) розпізнавання мови користувача під час проходження уроку говоріння;
9) підготовка до складання іспиту з англійської.

Шаблони проектування – це напрацьовані ефективні підходи, техніки та правила вирішення задач при створенні програмного забезпечення. Вони не прив'язуються до конкретної мови програмування. Для написання мобільного додатку я використала такі шаблони: MVVM, стратегія. MVVM (Model-View-ViewModel) полегшує відокремлення розробки графічного інтерфейсу від розробки бізнес логіки (бек-енд логіки), відомої як модель (можна також сказати, що це відокремлення представлення від моделі). Шаблон стратегія (Strategy) дає змогу змінювати вибраний алгоритм незалежно від об'єктів-клієнтів, які його використовують. В моїй програмі цей шаблон використовуватиметься при виборі відповідного матеріалу (на основі попередньої успішності) та побудові наступних уроків для проходження користувачу.

SFSpeechRecognizer - об'єкт, який використовується, щоб перевірити наявність служби розпізнавання мовлення та ініціювати процес розпізнавання мовлення. Двигун є доволі швидкий, точний і сьогодні може інтерпретувати понад 50 мов та діалектів. Він навіть адаптує результати для користувача, використовуючи інформацію про свої контакти, встановлені додатки, медіа та різні інші дані. Звук, що подається на розпізнавальник, записується в реальному часі, а результати надаються поступово Це дозволяє реагувати на голосовий ввід дуже швидко, незалежно від контексту.

iOS — це власницька мобільна операційна система від Apple. iOS є похідною від OS X, отже, є за своєю природою Unix-подібною операційною системою.

Swift — багатопарадигмова компільована мова програмування, розроблена компанією Apple. Swift успадковує найкращі елементи мов C і Objective-C. Swift щільно інтегровано до власницького середовища розробки Xcode.

Xcode — інтегроване середовище розробки (IDE) виробництва Apple. На сьогодні є єдиним засобом написання «універсальних»

прикладних програм для Mac OS X. Xcode включає в себе більшу частину документації розробника від Apple та Interface Builder — застосунок, який використовується для створення графічних інтерфейсів.

Література:

1. Mastering Swift 5: Deep dive into the latest edition of the Swift programming language, 5th Edition / Jon Hoffman.
2. Advanced iOS App Architecture / Rene Cacheaux, Josh Berlin.
3. https://medium.com/ios-os-x-development/ios-architecture-patterns-ecba4c38de52
4. https://slack-files.com/T051G5Y6D-F0HABHKDK-8e9141e191
5. https://github.com/github/swift-style-guide

УДК 339.944:004

ОСОБЛИВОСТІ ДИНАМІКИ РОЗВИТКУ СФЕРИ ІТ В УКРАЇНІ

Івановський М.Б., Бурак Н.Є.
Львівський державний університет безпеки життєдіяльності, Львів

У роботі здійснено огляд сучасного стану розвитку ІТ сфери в Україні. Проведено аналіз динаміки росту ІТ компаній та її вплив на розвиток держави.
Ключові слова: інформаційні технології, динаміка розвитку, спеціалісти, менеджмент, інформаційний продукт.

The paper reviews the current state of IT development in Ukraine. The dynamics of the growth of IT companies and its impact on the development of the country are analyzed.
Keywords: information technologies, dynamics of development, specialists, management, information product.

В умовах сьогодення суспільство перебуває в активній фазі розвитку та поширення «інформаційної революції», основним рушієм якої є засоби обчислювальної техніки, які стрімко інтегруються у повсякденні життя. Результатами перших етапів цих поді є появи новітніх технологій, основними вхідними та вихідними ресурсами, а також продуктом яких є інформація.

Сьогодні сфера інформаційних технологій (далі – ІТ сфера) є одна з найбільш стрімко зростаючих в Україні. За досить незначний час, у порівняні з іншими «гігантами» ІТ, наша держава вийшла на світовий ринок інформаційних продуктів і має високий показник конкурентоспроможності, що забезпечує значний інтерес світової ІТ спільноти до наших спеціалістів і їхніх розробок. Позитивом є також прогнози експертів даної галузі

щодо подальшого росту попиту на український продукт. Загалом передбачається до завершення 2019 року зростання ринку IT послуг на 30 %, що є великим досягненням у такий складний економічний та політичний час.

IT сфера – це бізнес, який оперує інформаційними ресурсами та надає послуги з їх реалізації. Як Загалом, можна виділити три основні фактори, які сприяють динаміці розвитку інформаційного бізнесу країни, а саме:

- висококваліфіковані спеціалісти;
- сприятливе зовнішнє та внутрішнє середовище реалізації;
- правильний та ефективний менеджмент діяльності та використання ресурсів при виконанні проектів.

На початок 2019 року в Україні налічувалось більше 12 тисяч офіційно зареєстрованих IT компаній (див. Рис. 1). Однак у даний список юридичних осіб потрапляють і ті, які перебувають на стадії ліквідації, тому показники реально діючих можуть відрізнятись.

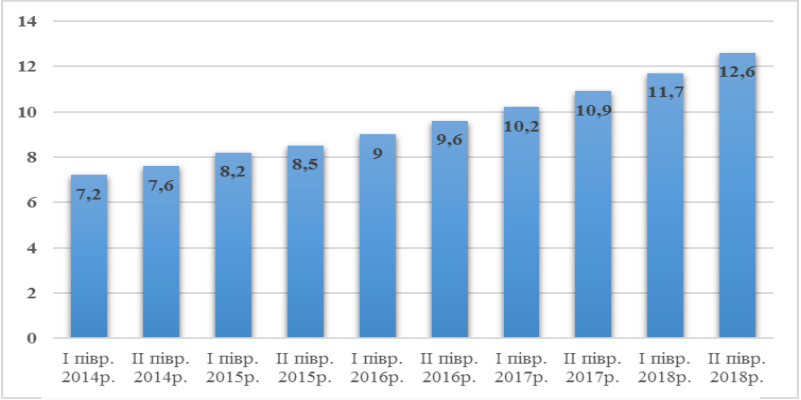


Рис. 1. Кількість юридичних осіб в період з 2014 по 2019 роки.

Важливим фактором є і те, що більшість компанії можуть мати дві і більше юридичних осіб, що також впливає на загальний показник. Не менш важливим фактором є фізичні особи підприємців, більшість яких є працівниками тих же ж компаній, однак можуть вести «фрі-лансерну» діяльність на ринку – таких фахівців є надзвичайно велика кількість, що також здійснює вплив на загальну статистику.

У наш час, IT сфера України налічує більше 58 тисяч працівників. Серед компаній, можна виділити 5 лідерів, зокрема EPAM, SoftServe, Luxoft, GlobalLogic та Ciklum, станом на початок року загальна кількість фахівців яких складає 23 865 спеціалістів (див. Рис. 2), що відповідає 41% від загальної кількості усіх спеціалістів нашої держави, задіяних в IT. В середньому, персонал даних компаній зріс на 15 % за 2018 рік.

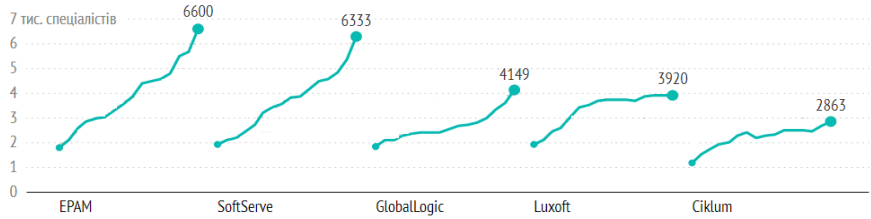


Рис. 2. Динаміка росту кількості працівників EPAM, SoftServe, Luxoft, GlobalLogic та Ciklum впродовж 2011 – 2019 років

Разом тим, у згаданих компаніях, є значна кількість вільних вакансій, що передбачає їх подальше збільшення та зміну розподілу на ринку (Рис. 3).

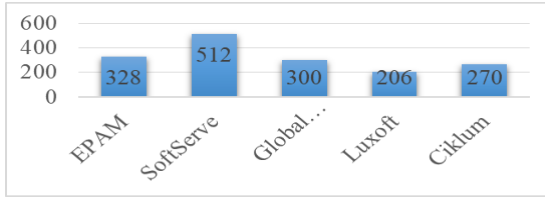


Рис. 3. Доступна кількість вакансій в EPAM, SoftServe, Luxoft, GlobalLogic та Ciklum на початок 2019 року

Таким чином, можна зробити висновок, що сьогодні в Україні створені сприятливі умови для розвитку ІТ сфери. Динаміка росту зайнятості у цій діяльності з кожним роком збільшується і згідно прогнозів експертів до кінця 2020 року кількість працівників (зокрема технічних) досягне позначки у 80 тисяч, що є хорошим показником та дає підгрунтя посідати високе місце в світових рейтингах.

Література:

1. Топ-50 ІТ-компаній України, січень 2019: зростання на 18% за рік і подолання відмітки «6 000 спеціалістів». [Електронний ресурс]. – Режим доступу: https://dou.ua/lenta/articles/top-50-jan-2019/.

2. Розвиток української ІТ-індустрії. Аналітичний звіт. [Електронний ресурс]. – Режим доступу: https://ko.com.ua/files/u125/Ukrainian_IT_Industry_Report_UKR.pdf

3. Software development in Ukraine: 2019-2020 IT market report. [Електронний ресурс]. – Режим доступу: https://www.n-ix.com/software-development-in-ukraine-2019-2020-market-report/

4. Бурак Н.Є. Проектно-орієнтований підхід до інтеграції ринку інформаційних послуг в освітню сферу / Н. Є. Бурак // Збірник тез доповідей ІІІ Міжнар. конф. «Інформаційні технології та взаємодії (IT&I – 2016)» . – К: Вид-во КНУБА, 2016. – С. 84–85.

ПРОВЕДЕННЯ ВНУТРІШНЬОГО АУДИТУ ТЕХНІЧНОЇ СКЛАДОВОЇ САЙТУ НАВЧАЛЬНОГО ЗАКЛАДУ

Райта Д., Головатий Р.
Львівський державний університет безпеки життєдіяльності

Аналіз існуючих алгоритмів оцінки сайтів показує, що всі вони мають загальний недолік – розглядається лише невелика частина інструментів інтернет-маркетингу, що не дозволяє адекватно оцінити сайт, як бізнес-інструмент.
Ключові слова: page rank. оцінка сайту.

An analysis of existing site evaluation algorithms shows that they all have a common drawback – only a small portion of internet marketing tools are considered, which does not adequately evaluate a site as a business tool.
Keywords: page rank. site evaluation.

На сьогоднішній день існує безліч інструментів залучення відвідувача (потенційного студента) на сайт закладу вищої освіти. Розглянемо найбільш значущі інструменти аудиту технічної складової.

Анонсування в пошукових системах та пошукова оптимізація.

Одним з найбільш дієвих способів по залученню трафіку на сайт університету є анонсування (видимість) в пошукових системах (зокрема Google Search). В основному, відвідувач, шукає інформації конкретного закладу вищої освіти, проте є загальні пошукові запити, які при правильній обробці, залучать користувача на ваш сайт (наприклад: «комп'ютерні науки бакалаврат Львів»). Як правило, в пошуковій видачі, необхідно приділяти увагу пошуковій оптимізації. Проаналізуємо параметри пошукової оптимізації. Можна виділити наступні аспекти:

I. Google Page Rank

Google Page Rank (PR) – індекс цитування сторінки сайту за версією пошукової системи Google. Варіює від 0 до 10. Чим вище PR, тим вища «важливість» сайту. Тому в якості критерію оцінки, цілком очевидно, логічно вибрати величину даного параметра з високим ранжуванням сайтів вузів по ній (нижчий рейтинг 1 виставляться найнижчому значенню параметра PR). Відповідно, чим вище рейтинг сайту вищого навчального закладу, тим вище значення цього параметра і тим краще заклад вищої освіти використовує даний інструмент інтернет-маркетингу.

II. Відвідуваність та статистика сайту

Для ефективного управління сайтом необхідно збирати інформацію про вхідний трафік (загальна кількість відвідувачів, кількість відвідувачів в певний період, їхній соціальний тощо). Ці дані можна отримати при наявності такого інструмента, як лічильник збору статистики (для прикладу Google Analytics).

III. Метаінформація (HTML-код)

Внутрішній фактор ранжування в пошукових системах. Теги розмітки, котрі маркують сторінку сайту, щоб пошукова система могла легко ідентифікувати її об'єкти (різноманітні заголовки, назви сторінок, підписи

до картинок тощо). І оскільки теги використовуються в пошукових системах в ранжування лінків в пошуковій видачі, при оцінці сайту необхідно брати до уваги метаінформації.

IV. Реєстрація на порталах і наявність на порталах

На регіональних порталах розміщуються великі об'єми оперативно-оновлювальної інформації, і як наслідок, вони можуть бути генератором трафіку для багатьох регіональних сайтів. На відмінну від регіональних порталів, аудиторія яких різноманітна, тематичні портали мають строго визначених користувачів (для прикладу, osvita.ua). Крім того, часто в пошуковій видачі по запитам, котрі нас цікавлять тематичні і регіональні (наприклад: "Заклад вищої освіти Львів") портали займають перші позиції, відповідно, наявність інформації на них має велику цінність.

V. Банерна реклама

Розміщуючи банери на різноманітних сайтах, котрі відвідують потенційні відвідувачі, можна очікувати їх переходу на сайт навчального закладу.

VI. Обмін лінками.

Принцип обміну лінками простий: на одному сайті розміщується лінк на сайт-партнер (як правило, суміжний по тематиці). Текстовий лінк з позитивною анотацією часто працює набагато ефективніше, чим банер. Оскільки до банеру багато хто відноситься як до реклами, тоді як текстовий лінк означає, що даний ресурс дійсно заслуговує уваги свої відвідувачів (наприклад, якісна вища освіта. Крім того цей спосіб дозволяє підвищити індекс цитування в пошукових системах і привернути цільову аудиторію.

Література:

1. Haveliwala, Taher H. "Topic-sensitive pagerank." Proceedings of the 11th international conference on World Wide Web. ACM, 2002.

2. Зачко О. Б. Імітаційне моделювання потоку відвідувачів торговорозважального центру / О. Б. Зачко, Р. Р. Головатий // Управління проектами: стан та перспективи: матер. XII міжнар. наук.-прак. конф. – Миколаїв: МНУК, 2016 - С. 96 – 98.

3. Coskun, Mustafa. "Graph Convolutional Networks Meet with High Dimensionality Reduction." arXiv preprint arXiv:1911.02928 (2019).

4. Зачко О. Б. Управління безпекою на стадії планування проектів з масовим перебуванням людей з врахуванням категорії складності / О. Б. Зачко, Д. С. Кобилкін, Р. Р. Головатий // Вісник НТУ «ХПІ». Серія: Стратегічне управління, управління портфелями, програмами та проектами. – Х. : НТУ «ХПІ», 2018. – № 2 (1278). – С. 53–58. – Бібліогр.: 17 назв. – ISSN 2311–4738.

5. Купчак М. І., Смотр О. О., Купчак М. Я. Тенденції та проблеми впровадження інформаційних технологій в управління підрозділами університету. Вісник Львівського державного університету безпеки життєдіяльності. 2013. № 7. С. 28–32.

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ УДОСКОНАЛЕННЯ ПРОЕКТУВАННЯ БАГАТОКОЛОНКОВИХ ВИДАНЬ

Сельменська З.М., Комар С.М., Цебрик А.Б.
Українська академія друкарства, м. Львів

Розглянуто основні принципи впорядкування багатоелементної композиції сторінки видання. Вказано методи удосконалення процесу композиційно-модульного проектування. Зазначені сильні сторони використання модульного проектування. Здійснено удосконалення технології проектування друкованих багатоколонкових видань.

Ключові слова: архітектоніка, проектування, багатоколонкове видання.

The basic principles of streamlining the multielement composition of the edition page are considered. Methods improvement of composite-modular design process are indicated. These strengths are the use of modular design. The design technology of printed multi-column publications was carried out.

Ключові слова: architectonics, design, multi-column publication.

На сьогодні інформаційні технології займають все більше простору в сучасних видавничих процесах. Без них не обходяться жодні технологічні процеси у видавництві та поліграфії. У практиці оформлення видавництва прагнуть до розкриття художнього образу видання і його архітектоніки (побудови), забезпечення зручності читання тексту, користування виданням, доцільності вибору матеріалів, проектуванні технологічних процесів. Не варто забувати важливий принцип - економічність видання, що забезпечується правильним вибором шрифтів, розмірних характеристик, правильною композицією, а також дотримання технічних та технологічних умов проектування видань.

Впорядкування багатоелементної композиції сторінки можливе після структурно-змістовного аналізу, що визначає призначення, кількість компонентів, архітектонічні, змістовні та функціональні зв'язки. Удосконалити процес композиційно-модульного проектування можна як технологічними так і програмними засобами. А створення гнучкої моделі дозволяє автоматизувати та оптимізувати процес проектування, надає максимальної свободи для макетування, водночас забезпечує однотипність та єдність оформлення.

Спосіб модульного проектування є одним з найефективніших для надання чіткої візуальної структури виданню, для створення якісного, гармонійного і функціонального макету з чітко визначеними зв'язками між елементами композиції, та є оптимальним методом проектування друкованих видань.

В процесі досліджень використано методи емпіричного, теоретичного аналізу та методи класифікації для вивчення модульного та композиційно-графічного проектування, принципів створення композиційно-графічної моделі. Розроблено рекомендації ієрархічно правильного їх застосовування виключно для багатоколонкових проектування.

З метою удосконалення технології проектування друкованих багатоколонкових видань досліджено теоретичні та практичні аспекти процесу проектування друкованих багатоколонкових видань; встановлено архітектонічних зв'язки між елементами видання та визначено множини факторів, які впливають на технологічний процес проектування друкованого видання; визначено ієрархічні структури пріоритетності факторів та критеріїв впливу на процеси проектування та композиційно-графічного моделювання полоси, роз-вороту та видання в цілому, розроблено на цій основі математичну модель та алгоритм для оптимізації технології проектування багатоколонкових видань.

Проведений аналіз засобів побудови композиції та її законів дозволив згрупувати і об'єднати фактори впливу на остаточний продукт, виокремити узагальнені критерії, що впливають на процес проектування журнальних видань. Встановлено зв'язки між критеріями композиційного оформлення багатоколонкового видання та ієрархію залежностей між ними.

В результаті розв'язано загальну задачу лінійного програмування оптимізації проектування, що дає змогу отримати оптимальні значення параметрів, виходячи з точки зору зниження собівартості підготовки видання.

РОЗРОБКА ІГРОВОЇ ПРОГРАМИ З ВИВЧЕННЯ ТРАЄКТОРІЇ РУХУ ОБ'ЄКТІВ ПРИ ЇХ ВЗАЄМОДІЇ В СЕРЕДОВИЩІ РОЗРОБКИ UNITY МОВОЮ C#

Слободянюк Н.А., Клакович Л.М.
Львівський Національний Університет імені Івана Франка

Ключові слова: ігрова програма; матеріальна точка; траєкторія; шлях; середовище розробки Unity Personal; модуль UnityEngine.PhysicsModule; середовище розробки Microsoft Visual Studio Community; мова C#.

Keywords: game application; point particle; trajectory; path; Unity Personal; UnityEngine.PhysicsModule; Microsoft Visual Studio Community; C#.

Сучасна психологія визнає, що гра охоплює всі періоди життя людини. Це важлива форма її життєдіяльності, а не вікова ознака. З грою людина не розлучається усе життя, змінюються лише її мотиви, форми проведення, ступінь вияву почуттів та емоцій [1].

Здавна людство зрозуміло, що найкращим способом навчання є гра. Ще в Давній Греції [2] в навчальних закладах проводились спортивні та музичні змагання, дебати. Так, в процесі суперництва і змагань, учні краще відточували свої навички і засвоювали нові.

Гра допомагає вивчити нове, засвоїти науки та запам'ятати складні поняття. Із сторони психології, це працює дуже просто: в ігровому навчанні людина концентрується не на самому процесі засвоєння інформації і навичок, а на грі. В таких ситуаціях мозок сприймає процес, пов'язані з

навчанням, як розвагу: легше запам'ятовує інформацію, концентрує увагу та будує нові логічні зв'язки.

Учасники максимально зосереджені на грі в емоційному та розумовому плані. Тобто вони сконцентровані не на навчальному, а на ігровому процесі. Гравці не підозрюють, що, вирішуючи ігрові завдання, вони вивчають щось нове.

В грі легко пояснити складні незрозумілі моменти, навчити чомусь новому, і, водночас, розважити її учасників. Також гра мотивує проявляти ініціативу, наполегливість та цілеспрямованість.

Найважливішим є те, що людина стає учасником гри добровільно, тому зникає психологічний захист. Саме він заважає приймати, розуміти і засвоювати нові знання та навички. Грі, на противагу навчальному процесу, не властива жорстка дисципліна та примусовість уваги. Тут гравці мають свободу дій і захоплюються процесом [2].

Вивчати фізику, а саме такі її поняття, як фізичне тіло, траєкторія руху, шлях, залежність шляху та траєкторії руху від фізичних властивостей тіла [4], на нашу думку, за підручником є досить складно. Наочність не завадила б. Так виникла ідея перевести процес навчання в гру.

Матеріальна точка – це фізична модель, що застосовується для спрощення опису руху тіла й відповідає тілу, розмірами якого в умовах даної задачі можна знехтувати.

Траєкторія – уявна лінія, в кожній точці якої послідовно перебувала матеріальна точка під час руху в просторі.

Шлях – це фізична величина, що дорівнює довжині ділянки траєкторії, яка пройдена тілом за даний проміжок часу.

Зараз існує велика кількість жанрів комп'ютерних ігор: екшн, стратегія, симулятор, пригоди, головоломки. Останні вимагають від гравця вирішення логічних завдань, передбачення можливих ситуацій [3]. На цей жанр і пав наш вибір.

Unity Personal – безкоштовна версія міжплатформного середовища розробки комп'ютерних ігор, дозволяє створювати додатки, що працюють під багатьма операційними системами, включаючи персональні комп'ютери, ігрові консолі, мобільні пристрої та інтернет-додатки.

UnityEngine.PhysicsModule [11] – модуль фізики, що реалізує тривимірну фізику в середовищі розробки Unity.

В програмі ми визначаємо різні фізичні матеріали для різних ігрових об'єктів за допомогою PhysicMaterial [11], щоб змінити спосіб їх взаємодії між собою та навколишнім середовищем.

Додавання компонента Rigidbody [11] до об'єкта приводить його рух під контроль фізичного двигуна Unity. Навіть без додавання будь-якого коду, Rigidbody об'єкт тягне вниз по гравітації, і він реагує на зіткнення з вхідними об'єктами, якщо, право, компонент Collider [11] також є присутній.

Rigidbody також має набір функцій, виклик яких з коду дозволяє нам застосовувати сили до об'єкта і керувати ним фізично реалістичним способом.

В цій програмі ми застосовуємо Rigidbody.AddForce. Він дозволяє надати силу об'єкту безперервно вздовж напрямку вектора сили. Визначення режиму ForceMode дозволяє нам змінити тип сили на зміну прискорення, імпульсу або швидкості.

SphereCollider [11] – це примітивний компонент Collider сферичного типу, що ми використовуємо для ігрових об'єктів.

Microsoft Visual Studio 2017 Community – безкоштовна версія інтегрованого середовища розробки програмного забезпечення, що дозволяє розробляти як консольні програми, так і програми з графічним інтерфейсом, а також веб-сайти, веб-застосунки, веб-служби як в рідному, так і в керованому кодах для всіх платформ, що підтримуються Microsoft Windows, Windows Mobile, Windows Phone, Windows CE, .NET Framework, .NET Compact Framework та Microsoft Silverlight.

Таким чином ми розробили ігрову програму з елементами вивчення таких фізичних понять, як фізичне тіло, траєкторія руху, шлях, залежність шляху та траєкторії руху від фізичних властивостей тіла. Програма написана на сучасних технологіях і її архітектура спроектована з врахуванням сучасних патернів програмування [8, 9, 10] та підходів для проектування комп'ютерних ігор [5, 6, 7] жанру головоломка. Розробку рекомендуємо використовувати в освітніх цілях.

Література:

1. http://samborska.at.ua/metod_tabir/igrovi_programi.pdf
2. http://gameblog.woc.org.ua/
3. https://uk.wikipedia.org/
4. http://edufuture.biz/
5. Е. Роллінгз, Д. Морріс. Проектування й архітектура ігор / 2ге видання – 2006р.
6. Design Patterns: Elements of Reusable Object-Oriented Software (Addison-Wesley Professional Computing Series) / Erich Gamma, Richard Helm, Ralph Johnson, John Vlissides; Addison-Wesley Professional, 1994. - 416p.
7. http://it-ua.info/news/2015/04/13/priyomi-pri-proektuvann-arhtekturi-gor.html
8. http://www.vitaliypodoba.com/2014/06/programming-patterns-intro/
9. Heer, J.; Agrawala, M. (2006). "Software Design Patterns for Information Visualization". IEEE Transactions on Visualization and Computer Graphics. 12 (5): 853-60.
10. "Introduction to Software Engineering/Architecture/Design Patterns - Wikibooks, open books for an open world". Retrieved 2015-12-26.
11. https://docs.unity3d.com/Manual/index.html

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОСВІТНЬОМУ ПРОЦЕСІ

Тютченко С. М.
Дніпропетровського державного університету внутрішніх справ

Анотація: сучасні інтернет-технології підвищують якість та рівень освіти, дають змогу здобувачу вищої освіти успішніше й швидше адаптуватися до навколишнього середовища та соціальних змін, в майбутньому бути конкурентноздатним на ринку праці. Активне та ефективне впровадження технологій в освіту є важливим чинником створення нової системи освіти, що відповідає вимогам інформаційного світового суспільства і процесу модернізації традиційної системи освіти.

Ключові слова: Інформатизація, інтернет-технології, освіта, Інтернет, ресурс.

Abstract: Modern Internet technologies increase the quality and level of education, enable higher education graduates to adapt to the environment and social change more successfully and faster, and be competitive in the labor market in the future. Active and efficient implementation of technology in education is an important factor in creating a new education system that meets the requirements of the information world society and the process of modernization of the traditional education system.

Keywords: Informatization, Internet technologies, education, Internet, resource.

Інформатизація суспільства – це перспективний шлях до економічного, соціального та освітнього розвитку. Інформатизація освіти спрямовується на формування та розвиток інтелектуального потенціалу громадян, удосконалення форм і змісту освітнього процесу. Це надає можливості вирішувати проблеми освіти на більш високому рівні з урахуванням світових вимог.

Становлення та розвиток інформаційного суспільства передбачає широке застосування інтернет-технологій в освіті, що визначається багатьма чинниками. Сучасні інтернет-технології підвищують якість та рівень освіти, дають змогу здобувачу вищої освіти успішніше й швидше адаптуватися до навколишнього середовища та соціальних змін, в майбутньому бути конкурентноздатним на ринку праці. Активне та ефективне впровадження технологій в освіту є важливим чинником створення нової системи освіти, що відповідає вимогам інформаційного світового суспільства і процесу модернізації традиційної системи освіти.

Інтернет-технології активно впливають на процес навчання і виховання студентів, оскільки змінюють схему передавання знань і методи навчання. Впровадження інтернет-технологій у систему освіти якісно впливають на всі етапи та напрямки освітнього процесу та надають їм рис сучасності та конкурентноздатності

Інформатизація освітнього процесу – це перспективний шлях до економічного, соціального та освітнього розвитку. Інформатизація освіти спрямовується на формування та розвиток інтелектуального потенціалу нації, удосконалення форм і змісту навчального процесу, упровадження комп'ютерних методів навчання та тестування, що дає можливість вирішувати проблеми освіти на вищому рівні з урахуванням світових вимог [3].

На сучасному етапі в усіх галузях людської діяльності, в тому числі і освітній, постійне використання новітніх технологій стало нормою. Інтернет та електронні ресурси вважаються найпотужнішими засобами розвитку інтелектуального потенціалу майбутніх спеціалістів, важливим джерелом нової та важливої навчальної інформації. З кожним днем все більше і більше вищих навчальних закладів підключається до всесвітньої мережі з метою не лише залучення до відкритого інформаційного простору, а й для пошуку нових можливостей щодо реалізації освітніх цілей і завдань [2].

До основних освітніх форм організації навчального процесу відносять лекції, семінарські, практичні та індивідуальні заняття, самостійну роботу. При підготовці до семінарських занять та під час самостійної роботи студенти можуть працювати з електронними підручниками та посібниками, спілкуватися в системі on-line через електронну пошту, використовувати тестові програми з метою удосконалення знань, здобуття нової інформації та для перевірки засвоєння вивченого матеріалу [1, с. 15].

Щоб встигати за розвитком сучасного мінливого світу, студенти мають мати високий рівень освіти, а без впровадження сучасних інтернет-технологій це не можливо. Враховуючи те, що існує безпосередній зв'язок між рівнем освіти людини і її професійним та економічним добробутом, впровадження інноваційних технологій в навчальний процес вищого навчального закладу є актуальним питанням. Вирішення цього питання потребує консолідації свідомості, спільних зусиль, мобільності навколо ідеї побудови інформаційного, гуманістичного, демократично орієнтованого освітнього простору, який забезпечить умови для всебічного, гармонійного розвитку особистості та конкурентоспроможності майбутнього фахівця.

Отже, застосування комп'ютерів у освіті зумовило появу нового покоління інформаційних освітніх технологій, що дали змогу підвищити якість навчання, створити нові засоби впливу, ефективніше взаємодіяти педагогам зі студентами. На думку багатьох фахівців, нові інформаційні освітні технології на основі комп'ютерних засобів дають можливість значно підвищити ефективність навчання.

Література:

1. Бріскін Ю.А. Галузеві особливості Internet-освіти / Ю.А. Бріскін // Комп'ютер у школі та сім'ї. – 2004. – № 1. – С. 15–17.

2. Шаповалова Н.О. Використання комп'ютерних мереж у навчальному процесі [Електронний ресурс] / Н.О. Шаповалова. – Режим доступу: http://schoolcollection. edu.ru/about/ filling/textbook/

3. http://www.youtube.com/watch?v=LtmdiPUGGe8)

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ОПТИМІЗАЦІЇ СЦЕНАРІЮ НАВЧАЛЬНОЇ НАСТІЛЬНОЇ ГРИ

Хлевной О.В., Жезло Н.В.
Львівський державний університет безпеки життєдіяльності

Одним з ефективних засобів навчання дітей молодшого шкільного віку є настільні ігри. Доведено, що їх застосування в початкових класах позитивно впливає на розвиток особистісних якостей і ініціативності, привчає до усвідомленого підпорядкування правилам (що, в свою чергу, сприяє корекції імпульсивної поведінки), а також формує навички взаємодії з іншими дітьми і дорослими, розвиває терпіння і емпатію.

Виходячи з вищезазначеного, проведемо аналіз і обгрунтуємо вихідні дані (тип, сеттинг, інформаційне наповнення та статистичні параметри) для створення і впровадження в навчальний процес настільної гри, яка б сприяла вивченню ключових правил пожежної безпеки в початковій школі.

Перш за все, необхідно обрати тип гри. Потрібно враховувати, що при роботі з дітьми молодшого шкільного віку дуже важливо, аби настільні ігри були максимально простими і практично не залежали від умінь гравців (надавали рівні шанси на перемогу). Такі умови можуть забезпечити гри з механікою на гральному кубику. Найвідомішим представником цього типу ігор є «Snakes and Ladders», оригінальна версія якої була створена Мілтоном Бредлі в 1943 році (автор взяв за основу староіндійську гру «Ліла») [3]. Суть гри зводиться до переміщення ігрової фігури на кількість позицій, визначену шляхом кидання грального кубика. При потраплянні на поля, з яких починаються «сходи» або «змії», фігуру слід перемістити вперед або назад на поля, які є кінцями «сходів» або «змій» відповідно. Переможцем стає гравець, що першим дістався позначки «Фініш». На сьогодні подібні ігри широко використовуються при вивченні різних дисциплін (від іноземних мов до математики).

З метою формування повноцінного уявлення про небезпечні фактори пожежі та засвоєння основних правил безпечної поведінки доцільно використовувати реалістичний сеттинг (сюжетна мета гри – вибратися з будівлі, охопленої пожежею). Це дасть можливість учасникам «приміряти на себе» змодельовані в грі ситуації.

В якості інформаційного наповнення оптимальним варіантом є формування картотеки типових ситуацій, з якими може зіткнутися дитина на різних етапах розвитку пожежі. Кожна така ситуація повинна бути проілюстрована графічно на окремій ігровій карті. При цьому картки доцільно розділити на 2 групи. Перша група (так звані «зелені» картки - будуть виконувати функцію «сходів») - ілюстрації з прикладами правильних варіантів дій в різних ситуаціях. Друга («червоні» картки, які будуть виконувати функцію «змій») - зображення ключових помилок, які найчастіше призводять до негативних наслідків. На кожній з карт, поряд з графічним матеріалом, необхідно описати в зрозумілій для дитини формі суть зображеного і вказати на скільки позицій

вперед або назад потрібно перемістити фігуру. Практична реалізація буде виглядати наступним чином: на ігровій дошці окремі поля слід обо-значити зеленим і червоним кольором. При потраплянні фігури на зелене або червоне поле, гравець навмання бере одну з «зелених» або «червоних» карток відповідно і здійснює вказану на ній кількість ходів вперед або назад. Таким чином, крім візуального і аудиального сприйняття правил, у дитини підсвідомо буде формуватися позитивне ставлення до правильних і негативне - до помилкових дій під час пожежі. Варто зазначити, що кількість «червоних» карток буде більшою, ніж «зелених». Цей факт необхідно врахувати при розміщенні червоних і зелених полів на ігровій дошці.

Основними статистичними параметрами гри є: загальна кількість ігрових полів на дошці (N), загальні кількості зелених (G) і червоних (R) полів, середнє значення кількості ходів, необхідних для досягнення поля «Фініш» (n), частота влучень на зелені (g) і червоні (r) поля в середньому за гру.

Значення n дає можливість оцінити приблизну тривалість гри (в хвилинах). Відомо, що дітям молодшого шкільного віку досить важко концентрувати увагу на певному виді діяльності протягом тривалого часу, тому важливо, щоб середня тривалість однієї гри не перевищувала 20 хвилин.

Нами було проведено експериментальне дослідження залежності тривалості гри в типовий варіант «Snakes and Ladders» (1943) від кількості ходів і числа учасників. Встановлено, що найкращого ефекту можна досягти при n = 20 ... 40 і при кількості гравців не більше 5.

Для достовірної оцінки величини параметра n і розробки пропозицій щодо кількості і розміщення червоних і зелених полів на ігровій дошці в середовищі програмування Java була створена програма, що моделює можливі варіанти проходження гри в залежності від таких параметрів як N, G і R. Для розрахунку значень n, g і r на кожній з проаналізованих конфігурацій ігрової дошки було відіграно по 1000 ігор. Застосування програми дозволило сформулювати наступні положення:

1. Якщо $N = 100$, $G = R = 0 \rightarrow n = 29{,}1$; тобто при наявності на дошці 100 ігрових полів і при відсутності зелених і червоних полів для досягнення позиції «Фініш» необхідно провести в середньому 29 кидків кубика;

2. Якщо $N = 100$, $G \leq 8$, $R \leq 8 \rightarrow g \leq 2{,}4$, $r \leq 2{,}7$; тобто при розміщенні на ігровій дошці не більше 8 зелених і червоних полів, середня кількість попадань на ці поля за одну гру буде занадто малим (відповідно, дитина зможе засвоїти меншу кількість інформації);

3. При $G>R$, $g> r$, а при $G <R$, $g <r$, відтак, з огляду на той факт, що кількість «червоних» карток в картотеці типових ситуацій апріорі більша кількості «зелених», оптимальним є варіант гри, при якому $G <R$.

4. Якщо $N = 100$, $R> G + 1 \rightarrow n> 40$. Це означає, що якщо кількість червоних полів на ігровій дошці буде перевищувати кількість зелених полів більш ніж на 1, середнє значення кількості ходів, необхідних для досягнення позиції «Фініш» буде становити більше 40, що вкрай небажано.

5. Оскільки кількість карток типових ситуацій є обмеженою (від 15 до 25 «червоних» і від 10 до 17 «зелених»), а максимальна рекомендована кількість гравців дорівнює 5, на ігровій дошці не повинно бути більше 11 червоних або зелених полів. При цьому оптимальна кількість полів, на які слід переміщати фігуру при попаданні на червоне або зелене поле повинно коливатися в інтервалі 8 ... 15.

Керуючись наведеними вище рекомендаціями, наведемо найбільш вдалі, на нашу думку, конфігурації ігрових полів і розрахуємо статистичні параметри запропонованих варіантів ігор (таблиця 1).

Таблиця 1 – Статистичні характеристики запропонованих варіантів ігор

Характеристика	*Snakes and ladders (1943)*	I	II	III
N	100	100	100	100
G	9	10	10	11
R	10	10	11	11
n	39,2	33,8	28,6	30.8
g	3,3	2,8	3,6	3.1
r	4,1	4,3	4,6	3.6
Зелені поля	(1,38), (4,14), (9,31), (21,42), (28,84), (36,44), (51,67), (71,91), (80,100)	1, 5, 9, 17, 28, 36, 49, 58, 76, 83	1, 5, 9, 17, 28, 36, 49, 58, 76, 83	1, 5, 8, 15, 24, 33, 43, 52, 64, 76, 83
Червоні поля	(16,6), (47,26), (49,11), (56, 53), (62,19), (64,60), (87,24), (93,73), (95,75), (98,78)	16, 31, 44, 54, 65, 73, 85, 93, 95, 99	16, 31, 44, 51, 61, 69, 77, 85, 93, 95, 99	16, 31, 44, 51, 61, 69, 77, 85, 93, 95, 99

Таким чином, ми прийшли до висновку, що, для поліпшення процесу навчання правилам пожежної безпеки в початковій школі, необхідно впровадити в навчальний процес настільну карткову гру типу «Snakes and Ladders» з механікою на гральному кубику і реалістичним сеттингом. Інструментарій гри повинен включати набір карток з якісними зображеннями типових ситуацій, в яких можуть виявитися діти під час пожежі. Оптимальна кількість зелених і червоних полів на ігровій дошці має становити 10 і 11 відповідно (при загальній кількості полів N = 100).

Література:

1. Горбань В.Б. Діагностика рівня знань правил пожежної безпеки серед дітей молодшого шкільного віку / В. Б. Горбань, Н .В. Жезло, О.В. Хлевной // Вісник ЛДУ БЖД. – 2015. – №11. С. 144-151.

2. Understanding the Impact of Fire and Life Safety Messages on Children. A project for the National Fire Protection Association conducted with funding from the U.S. Department of Homeland Security Federal Emergency Management Agency Fire Prevention and Safety Grant Program. Final Report. November 30 2010

3. Класифікація настільних ігор. – Режим доступу: http://hobbygames.ru/klassifikacija-nastolnih-igr

АКТУАЛЬНІСТЬ ЗАСТОСУВАННЯ СИСТЕМ АВТОМАТИЧНОГО КЕРУВАННЯ АВТОМОБІЛЯМИ

Чорний А., Муха С.-А., Руденко Д.
Львівський державний університет безпеки життєдіяльності, Львів

У сучасному темпі життя в період застосування передових технологій в автомобілебудуванні чи не найважливішою складовою успіху є мобільність та незалежність, швидкість пересування. Саме тому, сучасний автомобіль, комфортабельний та укомплектований найновішими досягненнями електроніки з застосуванням технологій з інтелектуальною електронікою, яка забезпечує відповідний рівень активної безпеки автомобіля під час його експлуатації, не є вже розкішшю, а дійсно є засобом для безпечного та надійного способу пересування.

Ключові слова: безпілотне керування автомобілем, автоматичні системи паркування, інтелектуальні системи.

At the present pace of life, in the period of application of advanced technologies in the automotive industry, perhaps the most important component of success is mobility and independence, speed of movement. That is why a modern car that is comfortable and equipped with the latest electronics technology with the use of intelligent electronics technology, which ensures an adequate level of active safety of the car during its operation, is no longer a luxury, but indeed a means of safe and secure travel.

Keywords: unmanned vehicle control, automatic parking systems, intelligent systems.

Безпілотний автомобіль – транспортний засіб, який обладнаний системою автоматичного управління і може пересуватися без участі людини. До таких розробок можна віднести автономні автомобілі Google, автомобілі-роботи MIG (Made in Germany), AKTIV (Adaptive und Kooperative Technologien fur den Intelligenten Verkehr – консорціум компаній (всього 28, у тому числі AUDI, BMW, Daimler, Siemens, Volkswagen), спільних розробників техніки для автотранспорту). Деякі автомобілі використовують інфраструктурні системи (які, наприклад, можуть бути вбудовані в дорогу чи біля неї), однак більш новітні технології дозволяють симулювати присутність людини на рівні прийняття рішень про керування і швидкість автомобіля завдяки набору камер, сенсорів, радарів і систем супутникової навігації.

Як відомо, перші спроби по створенню безпілотних автомобілів датуються 20-ми роками минулого століття, а обіцянки ще з 50-х. У 1984 році проект Navlab и ALM показав нам перший безпілотний автомобіль, а трьома роками пізніше і Мерседес-Бенц та Eureka Prometheus Project [1].

У наш час розвиток безпілотного автотранспорту розподілився на 3 основні напрямки:

– споживчий (приватне авто, таксі, міська автотранспортна мережа)

- промисловий (спеціалізована техніка)
- військовий (бойові машини різного спектру завдань)

На даний момент розвиток безпілотного транспорту йде по всіх перерахованих напрямках. Однак саме розвиток споживчого безпілотного автотранспорту є основним завданням для суспільства.

Переваги безпілотного автомобіля:

- перевезення вантажів у небезпечних зонах, під час природних та техногенних катастроф або військових дій
- зниження вартості транспортування вантажів і людей за рахунок економії на заробітній платі водіїв
- більш економічне споживання палива і використання доріг за рахунок централізованого управління транспортним потоком
- мінімізація ДТП, людських жертв
- виключення зловживання високою швидкістю
- виключення водіння в нетверезому стані

Неабиякого успіху у розробці автопілоту досягли такі компанії як [2]:

- General Motors. Компанія інвестувала 500 мільйонів доларів у Lyft та анонсувала, що впродовж року тестуватиме самокеровані електротаксі на дорогах загального використання. Також компанія придбала систему автоматизації круїз-контролю за мільярд доларів та планує побудувати центр розробки у Сан-Франциско.
- Ford. Компанія анонсувала мільярд доларів інвестицій в Argo AI, штучний інтелект, заснований колишніми працівниками Google та Uber. Ford планує до 2021 року мати повністю автономні машини для комерційного використання каршерінговими компаніями.
- Tesla. Компанія з кремнієвої долини заявила, що її машини незабаром постачатимуться повністю автономними. Вона також продовжує оновлювати суперечливе програмне забезпечення Autopilot (яке використовувалося під час першої летальної ДТП за участі самокерованого авто).
- Fiat Chrysler. Автовиробник досяг згоди з компанією Alphabet про встановлення її програмного забезпечення для самокерованих авто у мікроавтобуси Chrysler (після того, як спробував звернутися з цією ж ідеєю до Apple).
- Honda. Працюючи над прототипами автомобілю, японська компанія розробила так званий "емоційний двигун", який вивчає судження водія і застосовує їх для прийняття подальших рішень та рекомендацій.
- Volvo. Компанія почала пілотний проект, в межах якого надаватиме безпілотні автомобілі жителям шведського міста Гетеборг. Цей експеримент має всі шанси перекочувати до Лондона чи Китаю. Volvo також співпрацює з компанією Uber над пілотним проектом у Пітсбурзі.

- BMW Group та Daimler AG почали співпрацювати над розробкою автоматичного управління автомобілем. Представники компаній сьогодні підписали договір про довготривалу стратегічну співпрацю

Система автоматичного паркування (інша назва - інтелектуальна система допомоги при паркуванні, паркувальний автопілот) відноситься до активних паркувальних систем, тому що забезпечує паркування автомобіля в автоматичному або автоматизованому режимі. Різні системи автоматичного паркування допомагають при виконанні паралельної або перпендикулярного паркування. Більше поширені системи з паралельним паркуванням. Автоматичне паркування здійснюється за рахунок узгодженого управління кутом повороту рульового колеса і швидкості руху автомобіля.

Відомими інтелектуальними системами допомоги при паркуванні є:

- Park Assist на автомобілях Volkswagen;
- Park Assist Vision на автомобілях Volkswagen;
- Intelligent Parking Assist System на автомобілях Toyota, Lexus;
- Remote Park Assist System на автомобілях BMW;
- Active Park Assist на автомобілях Mercedes -Benz, Ford;
- Advanced Park Assist на автомобілях Opel.

Конструкція системи автоматичного паркування включає ультразвукові датчики, вимикач, електронний блок управління, а також виконавчі пристрої систем автомобіля. В інтелектуальній системі допомоги при паркуванні використовуються ультразвукові датчики, аналогічні пасивній паркувальній системі, але вони мають більшу дальність дії (до 4,5 м). Кількість датчиків залежно від різновиду системи розрізняється. Наприклад в системі Park Assist останнього покоління встановлюється 12 ультразвукових давачів: 4 попереду, 4 ззаду і 4 з боків автомобіля. Електронний блок управління приймає сигнали від ультразвукових датчиків і перетворює їх в управляючі сигнали на виконавчі пристрої, в якості яких виступають інші системи автомобіля: курсової стійкості, управління двигуном, електропідсилювач рульового управління, автоматична коробка передач. Взаємодія з зазначеними системами здійснюється через відповідні електронні блоки управління.

Література:

1. Інтернет ресурс за адресою: https://uk.wikipedia.org/wiki/%D0%91%D0%B5%D0%B7%D0%BF%
2. Інтернет ресурс за адресою: http://thefuture.news/selfdrivingcar

Напрям 9

Прикладне та системне програмування

ІНФОРМАЦІЙНА ПІДТРИМКА ЛЮДЕЙ З ПРОБЛЕМАМИ ЗОРУ НА ОСНОВІ МІКРОХВИЛЬОВОГО РАДАРУ AWR 1843

Антощук С.Г., Горбатенко А.А.
Одеський національний політехнічний університет, Одеса

Розроблено метод детектування обраних видів перешкод для інформаційної підтримки людей з проблемами зору на основі мікрохвильового радару AWR 1843. Дана розробка має мету допомогти людям з проблемами зору пересуватися в просторі. У розробці використовується новітній мікрохвильовий радар AWR 1843, який має переваги в порівнянні з іншими існуючими методами детектування перешкод, що було доведено експериментально у роботі.

Ключові слова: проблеми зору, мікрохвильовий радар, AWR 1843, детектування перешкод.

A method for detecting some types of obstacles has been developed to informational support for people with visual impairement based on mmWave radar AWR 1843. The development uses the latest AWR 1843 microwave radar, which has advantages over other existing obstacle detection methods, that has been proven experimentally.

Keywords: visual impairement, microwave radar, AWR 1843, obstacle detection.

За допомогою зору людина отримує 80-90% інформації про навколишній світ. За даними Всесвітньої організації охорони здоров'я, в усьому світі налічується близько 39 мільйонів сліпих людей і 246 мільйонів з поганим зором. 22% становить молодь працездатного віку, тобто практично кожен п'ятий з усіх сліпих і слабозорих. У процентному співвідношенні, кількість інвалідів по зору по відношенню до населення Землі (за даними ООН) становить:

39000000 ÷ 7021836029 = 0,0055 повністю сліпі (або 0.55% населення)
246000000 ÷ 7021836029 = 0,035 інваліди по зору (або 3.5% населення)

Людей, які позбавлені можливості бачити від народження або через хворобу, в даний час в Україні налічується 300 тисяч. Актуальною задачею є інформаційна підтримка людей з проблемами зору. Для вирішення цього завдання було обрано використовувати мікрохвильовий радар AWR1843. Обрання мікрохвильовий радар AWR1843 обумовлено рядом факторів [1]. Це інноваційний пристрій, який існує на закордонному ринку близько 1,5 роки та для використання у нашому проекті довелось чекати доставку близько 2 місяців, так як на українському ринку він на дану мить не представлений. Існує безліч найрізноманітніших додатків, в яких доводиться вирішувати завдання виявлення об'єктів і перешкод [2]. Як приклади можна привести автомобільні системи автоматичного паркування, системи захисту від зіткнення з пішохо-

дами та комплекси управління дорожнім рухом на перехрестях. У промисловості схожі завдання виникають при створенні систем контролю присутності і комплексів радіолокації для роботів і дронів. Однак ми пропонуємо вирішити соціально-значущу проблему підтримки людей з проблемами зору за допомогою сенсорів mmWawe від компанії Texas, які об'єднують в одному корпусі датчики наближення і потужне процесорний ядро ARM Cortex R4F з робочою частотою до 200 МГц. Даний радар має ряд переваг в порівнянні з іншими методами технічного зору:

- може вимірювати перешкоди на близькій відстані;
- може помічати перешкоди на максимальній відстані до 150 метрів;
- бачить в умовах поганих погодних умов (бруд, сніг, дощ, яскраве світло) і т.д.

Усі переваги мікрохвильового радару AWR1843 були підтверджені експериментами та закладені в основу методики детектування перешкод на основі даного радару. Огляд існуючих рішень дозволив зрозуміти, що робляться вони без структурного підходу, дозволяючи лише частково вирішити поставлене завдання технічного зору для сліпих та не можуть задовільнити усі потреби людей з проблемами зору. Тому в даній роботі розроблено метод детектування перешкод, з розумінням можливостей і обмежень сліпої людини на рівні органів почуттів. Принцип роботи радіолокатора має на увазі наявність двох основних компонентів: приймача і передавача. Передавач формує високочастотний сигнал, який, відбиваючись від перешкод, фіксується приймачем. За величиною затримки між переданим і прийнятим сигналом можна розрахувати відстань до об'єкта [3]. Компанія TI для вирішення завдання виявлення об'єктів пропонує використовувати технологію mmWave (Millimeter wave) з міліметровим діапазоном довжин хвиль. Розглянемо деякі особливості її фізичної реалізації. На відміну від традиційних радарних систем, в яких використовують імпульсну передачу сигналу, в mmWave застосовується частотно-модульований безперервний сигнал (frequency modulated continuous wave, FMCW) (рис. 1). Частота сигналу лінійно змінюється в часі від 77 ГГц до 81 ГГц.

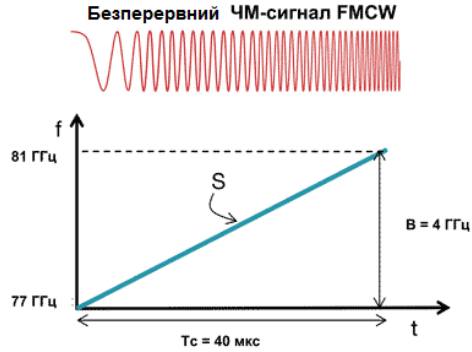


Рис. 1. Початковий сигнал в датчиках mmWave від Texas Instruments

Як і в звичайному радіолокаторі, в mmWave пряма радіохвиля досягає об'єкта, відбивається і повертається назад до датчика, де фіксується приймачем. Після цього вихідна і відбита хвилі микшируются в перетворювачі частоти. Результуючий вихідний сигнал IF (intermediate frequency) цікавий тільки в момент перекриття вихідних сигналів. При цьому він має постійну частоту і фазу, рівну різниці фаз вихідних сигналів. Використовуючи нескладні перетворення, за отриманими даними можна визначити відстань до об'єкта. Наша система на верхньому рівні абстракції має два основні компоненти – це апаратна частина та клієнтська частина. На апаратній частині ми маємо прошивку (яка також може виконувати попередню обробку даних), яку ми завантажуємо безпосередньо на AWR1843 та друга частина, яка уявляє собою клієнтську частину це програмна взаємодія та обробка отриманих даних. Ми створюємо конфігураційний файл з параметрами та відправляємо з клієнтської частини на AWR1843, в результаті чого ми задаємо дані, які нам необхідно отримати та в якому вигляді. Використовується схема кодування TLV (Type-length-value) для обміну даними між AWR1843 та програмою на комп`ютері (рис. 2). Для кожного кадру надсилається пакет, що складається з фіксованого розміру заголовка кадру, а потім змінної кількості TLV.

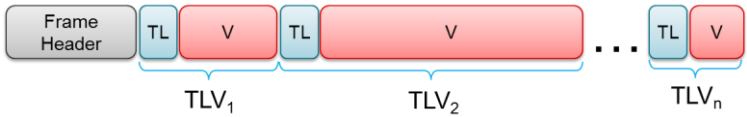


Рис. 2. Формат даних

Висновки. Розроблена методика інформаційної підтримки людей з проблемами зору на основі AWR1843, експериментально підтверджено релевантність використання даного мікрохвильового радару у порівняні з іншими найполулярнішими методами технічного зору, розроблено метод детектування деяких характерних перешкод.

Література:

1. E. R. Davies (2004). Machine Vision : Theory, Algorithms, Practicalities. Morgan.

2. Batchelor B.G. and Whelan P.F. (1997). Intelligent Vision Systems for Industry. Springer-Verlag. ISBN 3-540-19969-1

3. Demant C., Streicher-Abel B. and Waszkewitz P. (1999). Industrial Image Processing: Visual Quality Control in Manufacturing. Springer-Verlag. ISBN 3-540-66410-6

УДК 681.787

РОЗПІЗНАВАННЯ ДЕФЕКТІВ ТЕХНІЧНОЇ КЕРАМІКИ З ВИКОРИСТАННЯМ АЛГОРИТМІВ ЦИФРОВОЇ ФІЛЬТРАЦІЇ ТА АЛГОРИТМІВ ГЛИБИННОГО НАВЧАННЯ

Гаврилів Д., Семенченко М.
Національний університет «Львівська політехніка», Львів, Україна

Ключові слова: цифровий мікроскоп, фільтрація, глибинне навчання, цифрова фільтрації, сканування, виявлення дефектів.

Анотація: Використання цифрового мікроскопа, як засобу автоматизації процесу оцінки керамічних дисків, уможливлює наочне виявлення дефектів розміром порядку 50-500 мкм., отримати зображення яке з наступним застосуванням цифрової фільтрації шумів, підвищення контрасту, застосування функції порогового значення, та методу машинного розпізнавання дає змогу мікропроцесору прийняти рішення про відбракування деталі (допуск деталі до наступних стадій виробництва).

Abstract: A digital microscope is considered as an instrument for automatisation of the evaluation process of the ceramic disks for the textile industry. Furthermore, It provides an opportunity for visual defect detection in range 50 to 500 μm. Finally, after the use of digital filtration, contrast increase, threshold function, the defect detection software decides to reject the part(or allow the workpiece to the next stages of production)

Перевірка якості виготовлення виробів і обробки поверхонь є важливим кроком для дотримання технології на виробництві. Застосування оптичних засобів вимірювальної техніки та цифрових методів розпізнавання зображення дає змогу автоматизувати, прискорити, та здешевити відбракування дефектних деталей. До переваг застосування цифрового мікроскопа, як оптичного метода, можемо віднести наочне виявлення дефектів розміром порядку декількох десятків мікрометрів, отримане цифрове зображення яке з використанням операцій фільтрації, підвищення контрасту, застосування функції порогового значення, та методів машинного розпізнавання дає змогу мікропроцесору прийняти рішення про відбракування деталі[3] (допуск деталі до наступних стадій виробництва). Встановлено сильну залежність якості, а саме для алгоритмів машинного розпізнавання, отриманих зображень від освітлення. Використання декількох, умовно точкових джерел освітлення, під ковзким кутом до поверхні, в межах 5-10° дає змогу отримати морфологічно контрастне зображення. Тонке налаштування параметрів фільтрації, контрасту, параметрів функцій оцінки дефекту сьогодні потребує спеціаліста з цифрового опрацювання зображень для отримання достовірної інформації з зображення (рис. 1).

а) б) в)

Рис 1. Зображення краю керамічного диску отримані за допомогою цифрового мікроскопа та функції з бібліотеки OpenCV-Python: а) – зображення отримане з мікроскопа; б) – після підвищення контрасту; в) – після використання порогової функції

Аналіз отриманих зображень дефектів показав складність розробки алгоритму з використанням класичного підходу. Зміни в технічних характеристиках дисків, викликані залежністю цих характеристик від сировини, процесу виготовлення та спікання, мають великий вплив на методи класичного підходу. Використання машинного навчання для автоматизованого визначення дефектних деталей довело свою ефективність у проведених експериментах. Для ефективної роботи необхідна велика кількість тестових зразків та їх точна подальша обробка. У своїй роботі ми використали бібліотеки TensorFlow та Keras, для тренування спеціалізованого детектора об'єктів [1]. Використано алгоритм Inception Single Shot MultiBox Detector [2] для отримання ймовірності та координат дефектної області. Труднощі з якими ми зіткнулися це в першу чергу нестача потрібних для тренування даних. Для навчання точних детекторів необхідно близько 5000 зображень різних дефектів на один клас. Для вирішення цього завдання було застосовано синтетичне створення зображень. Наступним завданням є тренування моделі. Для тренування вибраної нами моделі у випадку достатньої кількості зображень необхідно, згідно з розробниками, 200 тисяч операцій, що у нашому випадку було неможливо адже на доступному нам обладнанні це зайняло б 28 днів безперервної роботи. Було проведено 5 тисяч навчань у результаті яких отримано результати для одного типу дефектів (при 1200 синтетичних зразках) (рис. 2). Отриманий результат - розпізнавання дефекта з 96% ймовірністю є важливим для ілюстрації можливостей машинного навчання. Для отримання якісних результатів для дефектів різної форми та розмірів та встановлення особливих рис дефектів необхідно збільшити кількість зразків для навчання та кількість тренувань. Оцінка швидкості тренування, середньої точності, та здатності до узагальнення отриманої моделі від попередньої обробки зображень є важливим завданням для майбутніх досліджень.

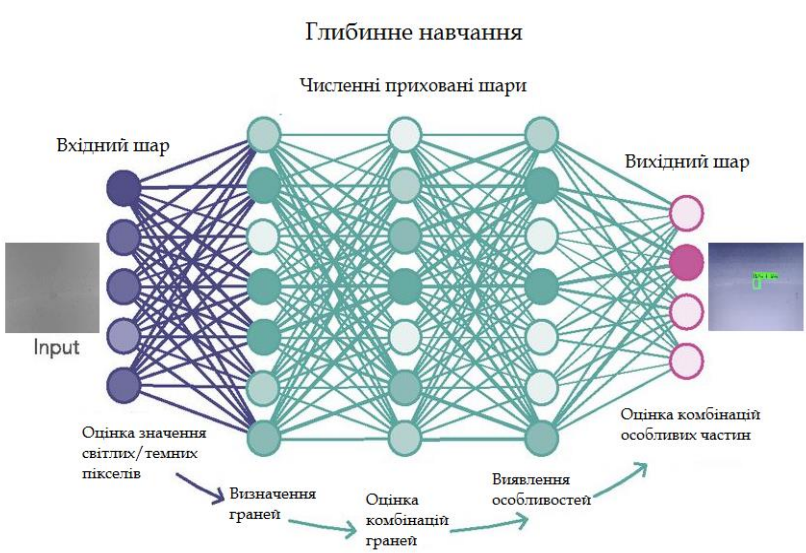


Рис. 2. Ілюстрація роботи алгоритму глибинного навчання.

Література:

1. Vladimirov L. Training Custom Object Detector / Lyudmil Vladimirov // TensorFlow API. – 2019. URL: https://tensorflow-object-detection-api-tutorial.readthedocs.io /en/latest/training.html (access date: 01.06.2019).

2. Inception Single Shot MultiBox Detector for object detection / N.Chengcheng, Z. Huajun, S. Yan, T. Jinhui. // 2017 IEEE International Conference on Multimedia Expo Workshops (ICMEW) (Hong Kong, 10-14 July 2017). Hong Kong, 2017. p. 549–554. URL: https://ieeexplore.ieee.org/document/8026312 (access date: 01.06.2019).

3. Rauschert. Ceramic Friction and Guide Discs [Електронний ресурс] // RAUSCHERT GmbH. – 2013. – Режим доступу до ресурсу: http://www.leclairmeert.be/files/6714/5769/8812/PB_Ceramic_Discs_GB.pdf.

РОЗРОБКА ІНТЕРАКТИВНОЇ СИСТЕМИ ОБРОБКИ ЗАВДАНЬ МАШИННОГО НАВЧАННЯ

Гейван М. О, Шибаєв Д.С
Міжрегіональна академія управління персоналом

Розроблена інтерактивна система дає можливість будувати, аналізувати, зберігати та застосовувати моделі машинного навчання та використовувати отримані результати в різних науково-практичних задачах.
Машинне навчання, інтерактивні системи, обробка даних.

The developed interactive system makes it possible to build, analyze, store and apply models of machine learning and use the results obtained in various scientific and practical tasks.
Machine learning, interactive systems, data processing.

Вступ. Процес розробки моделей машинного навчання завжди складається з великої кількості експериментів, перевірки результатів, підбору оптимальних ознак. Ці результати необхідно запам'ятовувати і мати можливість відтворювати. Однак більшість сучасних програмних засобів для взаємодії з моделями машинного навчання є досить складними, та потребують використання додаткової інформації щодо їх функціонування. Розробка сучасного програмного засобу, який поєднує інтерактивні особистості взаємодії з задачами машинного навчання та має спрощений та доступний інтерфейс – є сучасною науково-практичною задачею.

Мета роботи. В роботі виконано описан одного з варіантів організації інтерактивного оточення, для стандартних етапів машинного навчання. Система орієнтована на взаємодію з історично-впорядкованими даними, але може бути адаптована для роботи з даними інших типів.

Основна частина. Для організації роботи з вхідними даними створено сховище, яке у вигляді файлів зберігає інформацію по кожному об'єкту вхідного набіру даних (датасету). Датасетів може бути декілька, та з кожним з них можливо взаємодіяти окремо та незалежно від інших. Додавання нових об'єктів в файли відбувається поелементно [1]. Це уповільнює первісну обробку даних, але в робочих умовах дозволить обробляти їх в режимі реального часу (у міру надходження нових елементів) та дозволить виконувати наступні дії:

- отримання / генерація вхідних даних для побудови моделі;
- побудова і збереження моделі;
- застосування моделі в реальних умовах;

Перед етапом побудови моделі, необхідно згенерувати/розрахувати цільову змінну. Це може бути виконано як на етапі отримання даних, так і під час розрахування інших ознак об'єктів [2].

Однією зі складових можливостей побудови моделі є первісна обробка та аналіз вхідних даних, перед етапом тренування моделі. Як правило необроблених вхідних даних для роботи моделей недостатньо. По-перше, через особливості роботи тієї чи іншої моделі. Наприклад, лінійні моделі дуже чутливі до розподілів ознак даних. По-друге, початкових даних (кількість ознак для кожного об'єкта) може бути недостатньо, що не дозволить тренувати модель згідно початкових умов [3].

Генерація і розрахунок всіх додаткових ознак відбувається на етапі додавання елемента в сховище, що зменшує кількість розрахунків, так як багато ознак формується на основі тієї ж ознаки але на множині попередніх елементів. Також для обчислення деяких ознак може знадобитися вся історія виконаних операцій та подій.

Після генерації тих чи інших ознак потрібно перевірити, чи допоможуть вони краще прогнозувати цільову змінну. Тобто, потрібно оцінити залежність цільової змінної від спостережуваних ознак. На цьому ж етапі відбувається відбір найкращих ознак, що дозволить зменшити час тренування моделі, а також в деяких випадках підвищити якість класифікації [4].

Висновки. Для можливостей порівняння підсумкових результатів по декількох моделях і для використання різних моделей під кожен датасет, реалізован механізм збереження моделей. Його завданням є збереження серіалізованих об'єктів, які в свою чергу містять вже натреновані моделі, ознаки які були використані для тренування моделі, а також методи і настройки для нормалізації даних.

Для застосування тієї чи іншої моделі, требо викликати Python скрипт по мірі того як надходять нові історичні дані. Передавати йому необхідно: останній єлемент у ряді історичних даних, номер сховища даних (спочатку буде створено нове) та номер моделі яку потрібно застосувати. Як результат, скрипт запише нові дані у сховище та поверне прогноз вибраної моделі для переданного єлементу.

Література:

1. Coelho L., Richard W. Построение систем машинного обучения на языке Python. ДРК Пресс, 2016. 302 с.
2. Bishop M. C. Pattern Recognition and Machine Learning. New York : Springer-Verlag, 2006. 738 с.
3. Вьюгин В. В. Математические основы машинного обучения и прогнозирования МЦНМ, 2016. 384 с.
4. Raschka S. Python Machine Learning. Packt Publishing, 2015. 456 с.

ПРИМЕНЕНИЕ АЛГОРИТМОВ ТЕКСТОВОГО АНАЛИЗА В ЛИЗИНГОВЫХ СИСТЕМАХ

Діденко В.О., Годовіченко М.А.
Одесский национальный политехнический университет

Анотація. Розробка сучасних систем аналізу великих масивів текстової інформації є актуальною задачею, придатною для різних областей сучасної діяльності. Одним з таких напрямків є сучасні лізингові системи, що використовують великі обсяги документації. В роботі розглядається актуальність розробки сучасного програмного засобу орієнтованого на аналіз великих обсягів текстової інформації для підвищення ефективності електронного документообігу.
Ключове слово. Text Mining, семантичний аналіз тексту, Data Mining.

Annotation. The development of modern systems for analyzing large amounts of textual information is an urgent task applicable to different areas of modern activity. One of these areas are modern leasing systems that use large amounts of documentation. The paper discusses the relevance of the development of modern software tools focused on the analysis of large volumes of text information to improve the efficiency of electronic document management.
Keyword. Text Mining, семантический анализ текста, Data Mining.

Современные лизинговые системы стремительно развиваются за счет роста и популяризации такого рода услуг. Одним из факторов, влияющих на прогресс развития лизинговых систем, являются компьютерно-информационные технологии социализация которых имеет высокую динамику. Проведение сделок, заключение договоров, работа с документацией все больше переноситься в электронное пространство, а значит и системы верификации таких документов должны развиваться и использоваться на постоянной основе. К методам верификации цифровой документации относятся: проверка стилистики текстовой информации, ее достоверность, оригинальность и соответствие предметной области. Все эти факторы прямо или косвенно способствуют ее восприятию, а также могут влиять на итог сделки или успешности контракта.

Однако, объемы текстовой информации стремительно увеличиваются и проанализировать цифровой документ становиться сложнее, требуется больше времени на обработку данных, которого на бизнес встрече может и не быть. Возможным решением является разработка современной программной системы способной анализировать текстовую информацию и применяя соответственные алгоритмы (морфологического, семантического, синтаксического, лингвистического анализа) получать результирующую статистику по каждому виду анализа [1].

Особенности разработки систем распознавания текстов выделяют несколько типов структур, каждая из которых отражает анализ текстов на некотором уровне:

- Лингвистические структуры предложений. Структуры такого типа фиксируют результат локального (в пределах одного предложения) анализа текста и представления смысла.
- Семантическая сеть целого текста. Эти структуры включают глубинно-семантический компонент и отражают смысловое содержание целого текста как единой системы.
- Информационные структуры целого текста (потоков текстов). Эти структуры отражают результат обработки коллекции текстов в терминах некоторого тезауруса, что описывает предметную область рассмотренных текстов.
- Структуры баз данных и знаний. Структуры такого типа фиксируют выборочное специальное «понимание», в максимальной степени учитывает лингвистическое представление, отражение действительности.

В рамках систем распознания текстов необходимо использовать процедуры концептуального анализа текстов, то есть выявление понятийного состава. В первую очередь процедура концептуального анализа текстов рассматривается при создании систем машинного перевода, концептуальный анализ позволяет выбирать переводные эквиваленты для слов с учетом окружающего их контекста. Однако процедуру концептуального анализа необходимо осуществлять при решении многих других задач обработки текстов (кластеризации, классификации, реферирования, поиска и т. д.) [2]. Реализация работы таких алгоритмов касательно больших объемов текстовой информации становиться возможно за счет использования систем углубленного анализа с последующей классификацией текстовой информации. Для этих целей актуально применить концепцию Data Mining ориентированную на взаимодействие с текстовыми данными. Методы Text Mining, предназначенные для проведения смыслового анализа текстов, тесным образом связаны со статистическим и лингвистическим анализом, а также методами, которые разрабатываются в рамках области искусственного интеллекта. Задача Text Mining - выбирать из текстов наиболее важную и значимую информацию для пользователей. К основным элементам Text Mining относятся:

- классификация (classification, categorization);
- кластеризация (clustering);
- выписка фактов, понятий (feature extraction);
- реферирования (summarization);
- ответ на запросы (question answering);
- тематическое индексирование (thematic indexing);
- поиск по ключевым словам (keyword searching).

При классификации текстов используются статистические корреляции для отнесения документов к определенным категориям. Задача классификации — это классическая задача распознавания, где по некоторой контрольной выборке система определяет категорию нового объекта [3].

Разработка информационной системы, ориентированной на обработку больших массивов текстовой информации, поможет существенным образом увеличить эффективность работы лизингового направления, улучшить качество составляемой документации, а также упросить пользовательскую обработку деловой документации. В качестве средств разработки следует использовать многофункциональный язык программирования C/C++, а также Java Script для разработки адаптивного пользовательского интерфейса. Разрабатываемая система может являться самостоятельным программным продуктом либо дополнительным функциональным модулем, который может быть интегрирован в рабочее окружение готовых лизинговых продуктов.

Литература:

1. Lyashevskaya O. N. Evaluation of frame-semantic role labeling in a case-marking language / O. N. Lyashevskaya, E. V. Kashkin // Papers from the Annual International Conference "Dialogue" (2014). — 2014. — P. 350–365.

2. Ермаков А. Е. Семантическая интерпретация в системах компьютерного анализа текста / А.Е. Ермаков, В.В. Плешко // Информационные технологии. — 2009. — Т. 6. — С. 2–7.

3. Pady S., Cross-lingual annotation projection for semantic roles / S. Pady, M. Lapata // Journal of Artificial Intelligence Research. — 2009. — Vol. 36. — P. 307–340.

АНАЛІЗ ТОНАЛЬНОСТІ ТЕКСТУ З ВИКОРИСТАННЯМ НАЇВНОГО КЛАСИФІКАТОРА БАЙЄСА

Каськун М.Д., Посівнич Ю.М., Гошко Б.М.
Львівський національний університет імені Івана Франка, м.Львів

Ключові слова: аналіз тональності; класифікатор; наївний класифікатор Байєса; N-грами; стоп-слова; стемінг; лематизація; середовище Google Colab; Jupyter Notebook; мова Python.

Keywords: sentiment analysis; classifier; naive Bayes classifier; N-grams; stop-words; stemming; lemmatization; Google Colab; Jupyter Notebook; Python.

Актуальність теми. Стрімкий розвиток інформаційних технологій та їх використання ледь не у всіх сферах нашого життя дозволяє говорити про те, що людство невпинно працює аби зробити своє існування кращим. Від досягнень у сферах інформатизації значною мірою залежать стандарти життя суспільства, форми праці, системи освіти та охорони здоров'я. Пошукові системи, діагностика захворювань, сканери баркодів у супермаркетах, системи розпізнавання голосу – це все стало можливим завдяки розвитку таких напрямків в комп'ютерній науці як *класифікація образів (pattern classification*), *машинне навчання (machine learning)* та *штучний інтелект (artificial intelligence)* [2].

Наївний класифікатор Байєса [1,2,3] вважається одним із найпопулярніших алгоритмів машинного навчання в сфері класифікації. Попри свою назву, результати його роботи аж ніяк не «наївні». Класифікатор Байєса є стійким до несуттєвих ознак, швидко вчиться і робить доволі точний прогноз. До того ж не вимагає багато місця для зберігання у пам'яті комп'ютера. Слово «наївний» описує припущення, що поява та особливості одних об'єктів не впливають на інші об'єкти. Таке рідко коли трапляється в реальних умовах, тим не менш точність алгоритму залишається на високому рівні.

Одним з найпоширеніших прикладів застосувань класифікатора Байєса є класифікація спаму. В такому випадку навіть якщо точність класифікації не буде максимальною (наприклад 85%), цього може бути достатньо для виконання поставленого завдання. Але якщо класифікатор застосовувати для діагностування хвороб за певними симптомами, то кожен відсоток є важливим. Тому доцільно використовувати методи покращення роботи класифікатора. В цьому й полягає актуальність теми.

Метою роботи є дослідження впливу методів покращення наївного класифікатора Байєса при визначенні тональності тексту, а також порівняння результатів класифікації між собою.

Для досягнення цієї мети в роботі поставлено такі **завдання**:

– Нагадати основи роботи класифікатора, його особливості, моделі.
– Розглянути способи покращення точності алгоритму.
– Виконати техніки лематизації, видалення стоп-слів та стемінгу.
– Перевірити вплив параметра згладжування
– Провести аналіз тональності тексту.
– Зробити детальний аналіз результатів роботи та порівняти їх між собою.

Об'єктом дослідження є наївний класифікатор Байєса.

Предметом дослідження є способи та методи покращення роботи класифікатора.

Наукова новизна. Основний науковий результат роботи полягає у застосуванні технік покращення класифікації на базі наївного класифікатора Байєса з використанням набору відгуків Amazon Reviews for Sentiment Analysis.

Практичне значення одержаних результатів дослідження полягає у використанні мови Python та платформи *Jupyter Notebooks*[4], зокрема *Google Colab*[5] для реалізації як самого класифікатора так і технік покращення його роботи з використанням бібліотек scikit-learn та nltk. Також наведена детальна статистика використання наївного класифікатора Байєса та впливу різних технік покращення на точність алгоритму. Ця статистика може бути предметом подальших досліджень і допомогти іншим у використанні наївного класифікатора Байєса та способів збільшення точності класифікації.

На рис. 1 наведено деякі результати досліджень.

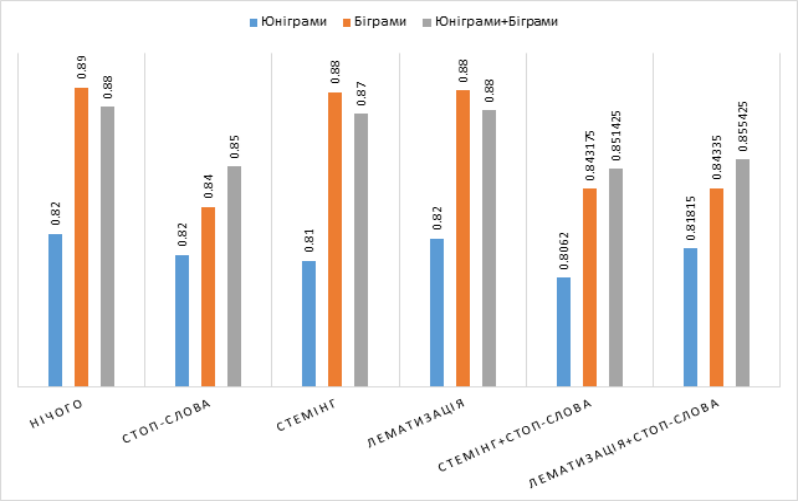


Рисунок 1

Тут зображено точність класифікатора з використанням tf-idf векторизатора для побудови словника. Як вхідні дані було використано набір із 400,000 відгуків з розподілом 90/10 на тренування та перевірку. Серед методів покращення присутні наступні: *стоп-слова*, *стемінг*, *лематизація*, *N-грами*[2, 6, 7]. З цього графіку видно, що такі методи покращення, як стоп-слова, стемінг та лематизація, виявилися методами погіршення для нашої вибірки відгуків. Проте використання N-грам, зокрема біграм, показує значне покращення точності класифікації, а саме на 7% у порівнянні з юніграмами.

Література

1. Онищук Р.М. Опис алгоритму для побудови наївного байєсовського класифікатора / Р.М. Онищук, І.М. Терещенко. - НТУУ КПІ.
2. Sebastian Raschka. Naive Bayes and Text Classification I - Introduction and Theory. – 2015.
3. Shimodaira Hiroshi. Text Classification using Naive Bayes. – 2015.
4. Jupyter Documentation. URL: https://jupyter.org/documentation
5. Google Colaboratory. URL: https://colab.research.google.com
6. Kavita Ganesan. What are stop words? URL: http://kavita-ganesan.com/what-are-stop-words
7. Tita Risueño. What is the difference between stemming and lemmatization? URL: https://blog.bitext.com/what-is-the-difference-between-stemming-and-lemmatization/

РОЗРОБКА ПРОЕКТУ МОБІЛЬНОГО ЗАСТОСУВАННЯ ОБЛІКУ ФІТНЕС ДІЯЛЬНОСТІ КОРИСТУВАЧА

Міропольцев В.В., Гунченко Ю.О.
Одеський національний морський університет, Одеса

Анотація. В роботі обґрунтовано актуальність розробки мобільного застосування обліку фітнес діяльності користувача, наведено опис основних компонентів та основних варіантів його використання.
Ключові слова: мобільні застосування, Android, рекомендаційні системи, електронний фітнес-помічник

Abstract. The relevance of the development of mobile application of accounting of fitness activity of the user is substantiated in the work, the description of the main components and the basic variants of its use is given.
Keywords: mobile applications, android, recommendation systems, electronic fitness assistant

На сучасному ринку програмних додатків в області підтримки процесів прийняття рішень з підтримки користувачів в необхідній фізичній формі спостерігається активне зростання пропозицій різної тематичної спрямованості [1]. Зокрема, активно розвивається напрямок раціонального управління

живленням для нарощування м'язової маси, яка ґрунтується на роздільної моделі вживання продуктів, що містять білки, жири і вуглеводи [2]. Однак, існуючі програмні рішення для операційної системи Android не позбавлені ряду істотних недоліків, зокрема, вони не завжди мають достатньо гнучкий і адаптивний інтерфейс користувача, складні в експлуатації і є вимогливими до обчислювальних ресурсів мобільного пристрою, а також у багатьох з представлених в Play Market додатків відсутні можливості персоналізованого підбору стратегій харчування з урахуванням фізичних навантажень [3]. У зв'язку з цим актуальним завданням є розробка прикладного мобільного додатка, здатного здійснювати комплексне управління і персоналізований контроль виконання завдань користувачем в тематиці фітнесу.

Ключовими функціями у користувача мобільного застосування є: авторизація, реєстрація, управління раціоном харчування, управління фізичною активністю, створення індивідуальної мети. Вхідними потоками застосування є: облікові дані користувача; особисті параметри користувача; дані про продукти, цілі та фізичні активності. До вихідних потоків належать: дані про зареєстрованих користувачів, розраховані значення харчової цінності продуктів, сформований раціон харчування, перелік фізичних активностей.

Основними функціональними компонентами програми є: RegActivity – реалізує управління процесом обробки реєстрації та авторизації в додатку; MainActivity – забезпечує процес взаємодії з головною формою додатка; PersonInfo – реалізує можливості управління персональними даними за параметрами користувачів; DietManager – виконує процеси організації раціону харчування користувача; ActivityManager – реалізує можливості по управлінню фізичними активностями користувача; GoalsManager – забезпечує вибір і формування цілей користувачем; RecomendationManager – відповідає за видачу рекомендацій по харчуванню; ProductsManager – організовує процес управління та обробки даних по продуктах харчування.

Висновки. Розроблений проект мобільного додатка успішно програмно реалізовано, він дозволяє автоматизувати і спростити виконання ряду рутинних операцій з обліку споживаних продуктів, а також забезпечити персоніфікований підбір фітнес-цілей для користувача з урахуванням його харчування.

Література

1. Аксенов К. В. Огляд сучасних засобів для розробки мобільних додатків // Нові інформаційні технології в автоматизованих системах. – № 17. – 2014. – С. 508-513

2. 13 додатків для схуднення [Електронний ресурс]. – Режим доступу: https://lifehacker.ru/13-prilozhenij-dlya-poxudeniya/. – Дата доступу: 23. 09.2019.

3. 9 додатків для здорового способу життя [Електронний ресурс]. – Режим доступу: https://www.gazeta.ru/tech/2015/04/06/6627665/9_fitness_prilozheniy.shtml. – Дата доступу: 25. 09.2019.

РОЗРОБЛЕННЯ ПРОЕКТУ ВЕБ-СИСТЕМИ ПІДТРИМКИ КЕШБЕК СЕРВІСУ

Рудніченко М.Д., Голопотилюк Є. А., Гавриленко Є. Б.
Одеський національний політехнічний університет, Одеса

Анотація. В роботі наведено опис концепції проекту веб-системи підтримки функціонування кеш-бек сервісу на базі використання мікросервісної архітектури, розглянуто три ключових функціональних компоненти її структури.
Ключові слова: кеш-бек**,** веб-система, управління транзакціями, білінгові системи

Abstract. The paper describes the concept of the project of a web-based system to support the operation of the cashback service based on the use of microservice architecture, considers three key functional components of its structure
Keywords: cashback, web system, transaction management, billing systems

В даний час в умовах розвитку сучасного інформаційного бізнесу, постійного впровадження білінгових систем і електронних платежів актуальними завданнями є програмно-технічна підтримка процесів захищеної обробки і відправки різних фінансових даних, а також пошук шляхів підвищення конкурентоспроможності пропонованих послуг [1,2]. Зокрема, ряд віддалених від центральних регіонів населених пунктів зазнає труднощів із забезпеченням можливостей оплати клієнтами і споживачами послуг за допомогою електронних платежів банківськими картами через відсутність відповідних термінальних станцій.

Організації, що надають подібні послуги не завжди забезпечують гнучкі та вигідні умови співпраці і не здатні здійснювати відповідний контроль транзакцій з підтримкою шифрування даних, тому що доступних і функціональних програмних засобів підтримки цих процесів на ринку практично немає [3].

У зв'язку з цим виникає необхідність розробки зручного кроссплатформенного програмного застосування, яке може бути розгорнуто як в рамках браузера, так і на існуючих мобільних платформах, здатного інтегрувати в своєму складі 3 ключові компоненти імплементації бізнес-логіки системи: модуля реалізації кеш-бека для повернення коштів користувачам після здійснення фінансових транзакцій; модуля інтеграції з існуючими партнерськими рекламними сервісами для розширення цільової ніші; модуля відстеження та обліку статистичних даних по виконаним транзакціями в захищеному режимі.

Пропонований проект реалізації веб-системи підтримки кеш-бек сервісу ґрунтується на використанні мов програмування Java і JavaScript,

не реляційної системи управління базами даних MongoDB і мікросервісної архітектури Restfull API. Основними сервісами системи є: створення облікового запису в кеш-бек сервісі, прив'язка номера карти до діючого аккаунту, облік виконаних фінансових операцій, збір і зберігання даних про транзакції з підтримкою їх захисту на базі криптоалгоритма DFC, рекомендаційний блок з наданням переліку найбільш вигідних пропозицій від існуючих партнерів, формування зведеного звіту.

Висновки. Розроблений проект кроссплатформеної веб-системи підтримки кеш-бек сервісу є основою для подальшої програмної реалізації і може бути використаний фізичними та юридичними особами для контролю і управління виконаних фінансових операцій, а також для підвищення ефективності проведення рекламних компаній з метою розширення цільової аудиторії.

Література:

1. Габдрашітов А. М. Cashback реальний і віртуальний / А. М. Габдрашітов // Питання науки і освіти. – №.11(12). – 2017. – С. 125-127.

2. Строїтєлєва Є.В. Електронні гроші: види, сутність і перспективи розвитку / Є.В. Строїтєлєва, І.Б. Мигачев // Дискусія. – №. 6 (47). – 2014. – С. 54-60.

3. Соколов Б.І. Роль платіжних систем в забезпеченні стійкого розвитку національної економіки / Б.І. Соколов С.В. Міщенко // Проблеми сучасної економіки. – № 2 (54). – 2015. – С. 163-167.

РАЗРАБОТКА МЕТОДОВ ОПТИМИЗАЦИИ ХРАНЕНИЯ ТОВАРОВ В СКЛАДСКИХ ПРОГРАММНЫХ СИСТЕМАХ

Самара І.О., Гунченко Ю.О.
Одеський національний морський університет, м. Одеса

Анотація. У роботі розглянута проблема складського обліку розміщення товарів. У роботі запропонована до розробка інформаційна система, що дозволяє контролювати розміщення складської мережі, регулювати складування і підготовку вантажу до поставок, управляти товарними запасами і організовувати складські поставки.

Ключові слова: логістика, оптимізація складу.

Annotation. The paper deals with the problem of warehouse accounting and placement of goods. The paper proposes the development of an information system that allows you to control the placement of the warehouse network, regulate warehousing and preparation of cargo for delivery, manage inventory and organize warehouse deliveries.

Keywords: logistics, warehouse optimization.

Разработка современных информационных систем является неотъемлемой частью по автоматизации различных отраслей и направлений современного бизнеса. Это связано с применением компьютерной техники в большинстве областей жизнедеятельности человека. Однако, обновление и модернизация уже разработанных программных продуктов выполняется медленно и требует существенного инвестирования финансовых средств. В связи с этим рациональным является разработка обновленных программных систем с применением различных оптимизационных алгоритмов и решений, направленных на повышение общей эффективности работы предприятий или направлений для которых применяются программные системы [1].

Одним из таких направлений, является система складского учета и размещения товаров. Это очень масштабное направление, которое требует внедрения современных оптимизационных и математических алгоритмов, способных улучшить работу и обеспечить возможность масштабировать задачи, выполняемые в рабочих процессах.

При разработке программной системы по оптимизации хранения товаров решаются такие задачи:

- размещение складской сети;
- складирование и подготовка груза к поставкам (производственные и другие услуги);
- управление товарными запасами;
- организация складских поставок.

Выводы.

Решение этих задач позволяет разработать систему прогнозирования наполненности склада, построить электронную очередь для выполнения погрузочных операций и рассчитать количество необходимой техники и ресурсов, для осуществления таких операций [2]. В качестве языка разработки оптимально использовать функциональный язык Python и фреймворк Django которые обеспечат качественную разработку программной системы и возможность расширять функциональные возможности системы при добавлении нового функционала. В качестве системы хранения данных, оптимально использовать крупные SQL системы, которые позволят хранить большие объемы данных и использовать их в разных сценариях. К таким системам относится PostgreSQL, а взаимодействие с Python позволяет добиться хорошего быстродействия.

Литература:

1. Дыбская В.В. Логистика складирования для практиков / В.В. Дыбская. – М.: Альфа-Пресс, 2010. – 208 с.

2. Гревцова Т.В. Основные направления оптимизации склада на предприятиях оптовой торговли / Т.В. Гревцова // Риск: Ресурсы, Информация, Снабжение, Конкуренция. – 2015. – No2. – С.39-42.

Напрям 10

Мережні інформаційні технології

УДК 004.738

АНАЛІЗ МЕТОДІВ ПІДВИЩЕННЯ ПРОДУКТИВНОСТІ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Киричик Б.М., Бурак Н.Є.
Львівський державний університет безпеки життєдіяльності

У роботі здійснено аналіз основних проблем забезпечення продуктивності комп'ютерної мережі та наведено рекомендації шляхів їх вирішення. Описано елементи, які впливають на рівень продуктивності роботи мережі.

Ключові слова: комп'ютерна мережа, маршрутизації, інформаційні технології, протокол, продуктивність.

In this paper we analyzed of the main problems in network throughput providing and gave recommendations for solving them. Also were described the elements that affects to level of network throughput.

Keywords: computer network, routing, information technologies, protocols, throughput

У сучасному суспільстві засоби комп'ютерної техніки відіграють важливе місце. Обмін даними, автоматизація процесів виробництва та життєдіяльності, зв'язок тощо – дані та їх потік постійно циркулюють навкруги. Сьогодні важко уявити життя без смартфонів, Інтернету, лептопів, планшетів чи настільних персональних комп'ютерів. Усі ці пристрої увійшли у наше повсякденне життя і стали його частиною.

Поява комп'ютерів та їх поширення зумовило появу комп'ютерних мереж – система зв'язку з допомогою кабельного чи бездротового середовище, самі комп'ютери різного функціонального призначення, а також мережеве обладнання. Такі системи поєднують велику кількість комп'ютерів та іншої техніки з метою ефективного використання їх ресурсів.

За сучасних умов інформатизації суспільства, процес забезпечення якісного та швидкого обміну даними є необхідною умовою функціонування засобів телекомунікацій. При побудові мережі, а також при її масштабуванні, перед адміністраторами постає проблема зниження швидкодії та пропускної здатності мережевих пристрої і, як результат, загальна продуктивність роботи мережевих комунікацій істотно зменшується. Причинами таких ситуації можуть бути апаратне, програмне або комунікаційне обладнання. Загалом, можна виділити декілька категорій елементів комп'ютерної мережі, які впливають на її продуктивність (Рис. 1).

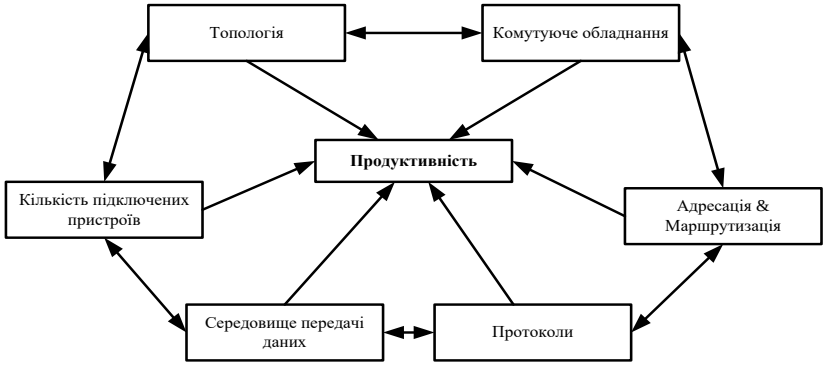


Рисунок 1 – Елементи впливу на продуктивність комп'ютерної мережі

Розглянемо кожен елемент впливу (див. Рис. 1) окремо.

Топологія – схема організації підключення пристроїв до мережі. Вибір оптимальної топології забезпечить легкість масштабованості мережі та забезпечить стабільність її роботи. Найпопулярніший сьогодні тип – зірка – використовується у більшості мережах.

Середовище передачі даних – метод передачі даних між пристроями. В залежності від умов майбутнього розгортання мережі обирається тип середовища – дротове, бездротове або оптоволоконне. Сьогодні найшвидшим є останній тип, який використовується для прокладання магістральних ліній зв'язку. Оптоволоконні мережі мають високу швидкодію, пропускну здатність, а від так і – продуктивність.

Кількість підключених пристроїв – кількість хостів залежить від топології мережі та можливостей комутуючого обладнання. У разі збільшення пристроїв, необхідно забезпечити вибір правильної топології, середовища та обладнання, яке максимально ефективно використовуватиме пропускну здатність мережі.

Комутуюче обладнання – правильно підібраний та налаштований пристрій комутації дозволить побудувати оптимальну топологію, забезпечити під'єднання необхідної кількості хостів, управляти усім трафіком в мережі та підтримувати її продуктивність. У більшості випадків з метою економії коштів, організації встановлюють недорогі концентратори, які через особливості розподілу трафіку мають пропускну здатність набагато нижче, ніж комутатори. Тому першим кроком у підвищенні продуктивності є заміна концентраторів на комутатори.

Адресація та Маршрутизація – дані дві процедури відповідають за ідентифікацію комп'ютерів кінцевих користувачів та правильний обмін даним в середині мережі. Функцію адресації може виконувати спеціально виділений апаратно чи програмно DHCP сервер або у ручному режимі ад-

міністратор. Маршрутизація здійснюється окремим сервісом на пристрої, завдання якого здійснити вибір найбільш раціонального маршруту з декількох можливих та надіслати ним пакет даних адресату.

У разі використання односегментної мережі функції маршрутизації здійснює комутатор, оскільки трафік не виходить за межі сегменту. Коли ж використовується сегментована мережа – застосовуються маршрутизатори – комунікаційний пристрій, що утворює логічні сегменти за допомогою явної адресації [3]. Також однією із функцій маршрутизаторів є можливість об'єднувати в єдину мережу кілька підмереж, побудованих на основі різних мережних технологій. Дані пристрої ізолюють трафік кожної з під'єднаних мереж, тим самим, підвищують пропускну здатність. Однак, продуктивність маршрутизатора значно менша продуктивності комутатора. Це пояснюється тим, що перший працює з різними мережами та різною адресацією, тому він витрачає на обробку одного пакету в 5-10 разів більше часу, ніж комутатор. У зв'язку з цим, їх доцільно застосовувати для з'єднання сегментів мереж з не дуже інтенсивний міжмережним трафіком.

Протоколи – набір правил обміну даними, які забезпечують інкапсуляцію та доставку інформації адресату. Вибір правильного протоколу дасть змогу зменшити надлишковість трафіку та підвищити швидкодію мережі.

Таким чином, можна зробити висновок, що зазначені елементи є взаємопов'язаними чинниками, які впливають на роботу мережі загалом, і підвищення продуктивності якої можливе за умови вжиття комплексних заходів.

Література:

1. Чмир П.О. Оптимізації ресурсів комп'ютерних лабораторій навчальних закладів шляхом використання термінального сервера / П.О. Чмир, Н.Є. Бурак // Проблеми та перспективи розвитку системи безпеки життєдіяльності: Зб. наук. праць XIV Міжнар. наук.-практ. конф. молодих вчених, курсантів та студентів. – Львів: ЛДУ БЖД, 2019. – С. 240-241.

2. Жовтянський М. С. Моделювання проектного середовища впровадження «хмарних сервісів» у вищі навчальні заклади системи цивільного захисту / М. С. Жовтянський, Н. Є. Бурак // Управління проектами, програмами, портфелями : Тези доповідей І Міжнар. наук.-практ. конф.: [у 2т.]. – Одеса, 2016. – Том 1. – С. 54–56.

3. Олифер Н.А. Компьютерные сети: принципы, технологии, протоколы [Текст] / Н.А. Олифер, В.Г. Олифер. – СПб.: Питер, 2012. – 944 с.

4. Пахомова В. М. Можливості модернізації комп'ютерної мережі інформаційно-телекомунікаційної системи Придніпровської залізниці / В. М. Пахомова // Інформаційно-керуючі системи на залізничному транспорті. – 2015. – № 5. – С. 32-38. – Режим доступу: http://nbuv.gov.ua/UJRN/Ikszt_2015_5_7.

5. Рак Ю.П. Формування проектів методом візуалізації інформації для підвищення стану безпеки торгово-розважальних центрів / Ю.П. Рак, Р.Р. Головатий // Управління проектами у розвитку суспільства: зб. тез доповідей XII Міжнар. конф. – Київ: КНУБА, 2015. – С. 226 – 228.

ПРОЕКТ «КОРПОРАТИВНИЙ ЧАТ» ДЛЯ ШВИДКОГО ОБМІНУ ТЕКСТОВИМИ ПОВІДОМЛЕННЯМИ МІЖ КОРИСТУВАЧАМИ МЕРЕЖІ INTERNET

Пенхерський М., Тригуба А.
Львівський національний аграрний університет, м. Дубляни

Виконано аналіз існуючих чатів, форумів та сайтів для швидкої обміну інформацією. Обґрунтовано доцільність розроблення проекту «Корпоративний чат» для швидкого обміну текстовими повідомленнями між користувачами інтернету. Запропонований проект спрощений аналог web версії одного із існуючих мессенджерів. Він забезпечує реєстрацію, авторизацію (з захищеним зберіганням даних користувача), створення діалогів між користувачами, а також надсилання текстових повідомлень в реальному часі.

Ключові слова: проект, повідомлення, корпоративна мережа, користувачі, мережа Internet.

An analysis of existing chats, forums and sites for quick information sharing. The expediency of developing the Chat project for the rapid exchange of text messages between Internet users is substantiated. The proposed project is a simplified analogue of the web version of one of the existing messengers. It provides logging, authorization (secure storage of user data), creating dialogs between users, and sending real-time text messages.

Key words: project, messaging, corporate network, users, Internet.

На даний момент існує багато досить популярних чатів, форумів та сайтів для швидкої обміну інформацією та спілкування між користувачами [1-4]. Саме ці засоби забезпечують миттєвий обмін повідомленнями між користувачами. З-поміж них заслуговує на увагу Messenger. Він являє собою програмний засіб та протокол передачі даних, що дозволяють інтернет-користувачам спілкуватися в реальному часі. При цьому Messenger включають в себе програми-клієнти, що встановлюються на локальних комп'ютерах. Передача даних, як правило, здійснюється через сервер служби зі спеціального протоколу. Недосвідчені користувачі часто плутають назву протоколу і назву програми-клієнта. Це призводить до того, що часто необґрунтовано роблять різницю між «спілкуванням по Асьці» і «спілкуванням по Квіп», хоча QIP також використовує протокол ICQ.

Досить популярними мессенджерами на даний час є ICQ, що працює по протоколу OSCAR, QIP Infium, що підтримує декілька протоколів, Skype, який має власний закритий пропрієтарний протокол), а також Telegram, який заснований на відкритому програмному забезпеченні.

У корпоративних мережах ІМ часто забороняються, з тією метою, щоб працівники не витрачали час на спілкування в Інтернеті замість виконання роботи. Часто залишається відкритим тільки 80-й порт. Обійти бло-

кування месенджерів можна використанням проксі-серверів. Нами пропонується проект «Корпоративний чат» для швидкого обміну текстовими повідомленнями між користувачами мережі Internet (рис. 1).

Запропонований «Корпоративний чат» являє собою мережевий засіб для швидкого обміну текстовими повідомленнями між користувачами Internet в системі реального часу. Зазвичай, під словом «Чат» мається на увазі Internet-ресурс з можливостями чату, чат-програма, рідше — сам процес обміну текстовими повідомленнями.

Запропонований нами проект «Корпоративний чат» передбачає створення спрощеного аналогу Web версії одного з вище наведених мессенджерів. В мінімальному працездатному вигляді даний Web додаток передбачає наступні функціональні можливості – реєстрація, авторизація (з захищеним зберіганням даних користувача), створення діалогів між користувачами і надсилання текстових повідомлень в реальному часі. На даний момент проект «Корпоративний чат» знаходиться в стадії розробки і покращується з кожним днем (в майбутньому можливе розширення можливостей до надсилання бінарних файлів і створення розмов між кількома людьми).

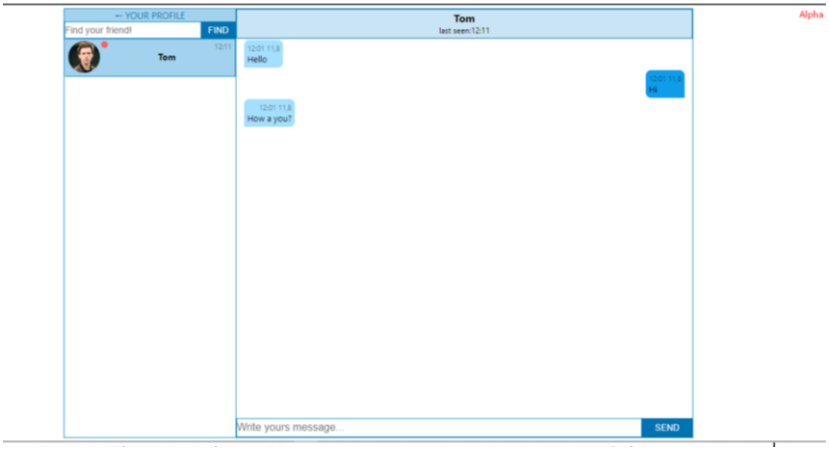


Рис. 1. Діалогове вікно «Корпоративний чат» для швидкого обміну текстовими повідомленнями між користувачами мережі Internet

В нашому проекті «Корпоративний чат» використано множину технологій. Зокрема, у Beck-end використано JavaScript, Node.js, Express, REST, Socket.io. Окрім того, у Front-end використано JavaScript, React, Redux, Socket.io [5-9].

Із вікна користувацького інтерфейсу «Корпоративний чат» можна налаштовувати порти, керувати каналами. За потреби можна користуватися користувачами та включити ведений логотип.

Література:

1. Хавкіна Л. М. Феномен корпоративних медіа в сучасному медіапросторі. Рецензія на видання: Олтаржевський Д. О. Основи та методи діяльності сучасних корпоративних медіа / Л. М. Хавкіна // Вісник Харківського національного університету імені В. Н. Каразіна. Серія : Соціальні комунікації. 2015. Вип. 7-8. С. 96-99. Режим доступу: http://nbuv.gov.ua/UJRN/VKhISK_2015_7-8_21

2. Ryabyy M., Hatyan O., Bagatskyy S. The model of PR-impact detection by means of Internet mass-media». Ukrainian Scientific Journal of Information Security. Vol. 21. Issue 2. 2015. P. 131-139.

3. Polishchuk Yu., Gnatyuk S., Seilova N. Mass media as a channel of manipulative influence on society. Ukrainian Scientific Journal of Information Security. Vol. 21. Issue 3. 2015. P. 301-308.

4. Олтаржевський Д. Основи та методи діяльності сучасних корпоративних медіа. – К.: Центр вільної преси, 2013. 312 с.

5. Java Script [Електронний ресурс]. Режим доступу: https://uk.wikipedia.org/wiki/JavaScript

6. Документація NodeJS. – Електрон. дані (1 файл). – 2017-2019. – Режим доступу: https://nodejs.org/docs/latest-v9.x/api/.

7. Ітан Браун. Веб-розробка із застосуванням Node і Express. Повноцінне використання стека JavaScript = Web Development with Node and Express / Ітан Браун. - Санкт-Петербург: Пітер, 2017. - 336 с

8. React documentation. – Електрон. дані (1 файл). – 2015-2016. – Режим доступу:https://reactjs.org/docs/getting-started.html.

9. Introduction to MobX. – Електрон. дані (1 файл). – 2012. – Режим доступу: https://mobx.js.org/.

ПЕРСПЕКТИВНІ СФЕРИ ДІЯЛЬНОСТІ: «Smart Cities» та «Smart Homes»

Чорнобай А.А., Смотр О.О.
Львівський державний університет безпеки життєдіяльності, м. Львів

Роботу присвячено розгляду сучасних технологій «smart cities» та «smart homes» та аналізу перспективних сфер діяльності для фахівців ІТ спеціальностей.
Ключові слова: "smart home" ("розумний" будинок), "smart city" ("розумне" місто).

The work is devoted to the review of modern technologies of "smart cities" and "smart homes" and prospective areas of activity for employees of IT-services.
Key words: "smart home", "smart city", IT- specialist.

Smart City («розумне» місто) – це узгоджена система технологій та інновацій, які використовуються для взаємодії з державними органами та отримання адміністративних послуг в транспортній мережі і дорожньому русі, енергетиці та водопостачанні, керуванні житлом, громадській безпеці та охороні здоров'я [1].

Мета будь-якого «розумного» міста - бути корисним для своїх жителів, забезпечувати економічність та енергоефективність, а також заощаджувати для суспільства один з найбільш цінних на сьогодні ресурсів – час. Згідно досліджень британської аналітичної компанії Juniper Research близько 70 годин, тобто майже три доби, людина щорічно втрачає при використанні транспорту [2]. Однак «розумна» система «smart city», яка включає в себе: мобільні додатки, систему паркування, відкриту базу даних про перевантаження трафіку на дорогах, можливість побудови оптимального маршруту з пункту А в пункт Б, з врахуванням відстані, трафіку на маршруті, якості дорожнього полотна та метео-умов, дозволяє зберегти 60 годин. Загалом, аналітики стверджують, що «розумне» місто має потенціал повернути кожній людині 125 годин щорічно [2,3].

Збереження вільного часу можна досягти шляхом впровадження технологій IoT (інтернету речей) в чотири ключових сфери: транспорт, охорона здоров'я, громадська безпека та отримання державних послуг. Це, усім нам добре відомі, зупинки, що містять табло з інформацією про прибуття транспорту і визначні пам'ятки; це міні-сенсори на парковках, які спрощують пошук вільного місця для паркування, це цифрові чіпи в сміттєвих баках, які повідомляють про їх наповненості; це ліхтарі, оснащені системами, які здатні вимірювати шум, трафік, забруднення, температуру, чисельність натовпу та навіть кількість селфі, які були залиті в мережу з цієї вулиці.

Очевидно, що в наше сьогодення, щодня все більше вплітаються технології «Smart Cities» та «Smart Homes». Зважаючи на їх популярність та ефективність можемо стверджувати, що зовсім скоро ми відчуємо недостачу спеціалістів, що зможуть взаємодіяти з «розумними» містами та забез-

печувати їх ефективне та стабільне функціонування. Тому пропонуємо звернути увагу на такі перспективні спеціальності, як:

- VR-дизайнери – спеціалісти з дизайну віртуальної реальності в сфері «розумних» міст, завданнями яких є створення і забезпечення функціонування точної копії міста, яка існує на екрані в онлайн-режимі. Адже завдяки віртуальному місту його мешканці можуть дізнаватися про рівень забруднення в тому чи іншому районі, завантаженість трафіку на дорогах та наявність вільного місця для паркування.
- Інженери з енергоефективності забезпечення стабільності енергоспоживання. Адже без ефективного управління споживанням енергії, діяльність «розумних» міст, що використовують мільйони кіловат електроенергії, буде під загрозою.
- Архітектори активних (енергонульових) будинків, завданням яких є не лише проектування "активних" будинків, але й проведення енерго-аудиту. Адже, "енергонульові" будинки це не просто енергоефективні будинки, це будинки, які здатні виробляти більше енергії, ніж споживати..
- Machine Learning – спеціалісти по машинному навчанню, завданням яких є: навчити комп'ютер вирішувати складні завдання, які важко вирішити алгоритмічно (розпізнавати людські обличчя або інші об'єкти, керувати автомобілем та «розумним» трафіком, діагностувати захворювання тощо).
- Cloud architect – архітектори хмарних систем, завданням яких є раціоналізація різноманітних застосунків і створення потенційно єдиної платформи для інтеграції міста з обраними застосунками (щодо паркування, освітлення, моніторингу датчиків, управління водою тощо).

З огляду на наведені вище факти та зважаючи на те що, до 2050 року понад 60% населення планети буде проживати в містах [2], ми можемо стверджувати, що зовсім скоро знадобиться велика кількість фахівців, які будуть забезпечувати функціонування «розумних» міст і будинків. Поруч з IT-фахівцями, розробниками мобільних додатків і класичними знавцями конкретних сфер, з'являться будівельники «розумних» доріг, VR-дизайнери, IT-медики, інформаційні стилісти або проектувальники роботів. Це будуть одні з найперспективніших професій майбутнього.

Література

1. Carol L. Stimmel. Building Smart Cities, Analytics, ICT, and Design Thinking. – CRC Press, 2015. – 290c.

2. Офіційний сайт аналітичної компанії "Juniper Research" [Електронний ресурс] – Режим доступу до ресурсу: https://www.juniperresearch.com/researchstore/innovation-disruption/top-10-disruptive-technologies/top-10-disruptive-technologies-in-fintech.

3. Golovatyi R. R. Safety management in project of creation the shopping malls. News of Science and Education: Sheffield. 2016, no. 20 (44), pp. 75–79.

Напрям 11

3D моделювання та 3D друк

УДК 004.94

ІНТЕГРАЦІЇ ТЕХНОЛОГІЇ 3D-ДРУКУ В МЕДИЦИНУ

Богданов О.С. Борзов Ю.О.
Львівський державний університет безпеки життєдіяльності, Львів

Роботу присвячено актуальному розвитку 3D-друку – широким можливостям застосування в медицині.

На даний час можливості 3D-друку активно використовуються в медицині. За останні кілька років, технологія перекочувала з області наукової фантастики, в окрему галузь, яка розвивається стрімкими темпами. Технології 3D-друку і сканування активно використовуються в процесі створення імплантатів і протезів, здатних замінити кісткову тканину. Компанія Oxford Performance Materials в США успішно провела операцію з відновлення шматка черепа пацієнта, роздрукувавши точну модель відсутнього фрагмента на 3D-принтері.

Ще більших успіхів досягли фахівці з компанії LayerWise, що зуміли відновити пацієнтові нижню щелепу, роздрукувавши її титанову копію на 3D-принтері. У свою чергу китайські хірурги, зуміли врятувати пацієнтці руку після того, як відсталий рак знищив практично всю лопатку дівчини. Для цього вчені замінили уражену кісткову тканину штучним титановим протезом, який змоделювали за допомогою 3D-сканування.

Таке стрімке поширення 3D-друку в протезуванні пояснюється можливістю «підігнати» імплантат під індивідуальні потреби пацієнта. До речі, це одна з найбільш обговорюваних тем останніх конференцій 3D Print Conference в Києві, особливо зараз, коли необхідність в подібних операціях відчувається особливо гостро в країні.

Крім того, ще однією перевагою технології є висока швидкість створення нових тканин. Наприклад, за допомогою 3D-друку стало можливим оперування розщеплення хребта у дітей. Захворювання проявляється на останніх місяцях вагітності і, не дивлячись на малу відомість, зустрічається набагато частіше ніж можна собі уявити: приблизно в 0,7 випадках на кожну 1000 новонароджених.

Розщеплення хребта або неповне закриття нервової трубки призводить до дефектів спинного мозку, що позначається на майбутній здібності дитини ходити і утрудняє відтік церебральної рідини з мозку. Так як лікування вже після народження дитини особливо небезпечно і скорочує три-

валість життя внаслідок частих ускладнень – операцію потрібно проводити безпосередньо під час розвитку плоду.

Головним ускладненням в такої операції є індивідуальність дефекту у кожної дитини, що збільшує час проведення операції, а адже зволікання з кожною секундою збільшує ризик летального результату.

Тому недавно, в ході операції, щоб швидко і з максимальною точністю змоделювати необхідну «латочку» для спини немовляти, хірурги з Центру спостереження вагітності в Колорадо використовували 3D-сканер і принтер, щоб попередньо виготовити необхідну тканину.

Адже крім друку штучних імплантатів, медики постійно оновлюють список «живих» матеріалів, які можна використовувати під час 3D-друку. Вчені вже успішно роздрукували органели серця і тканини печінки. Єдина проблема на даному етапі є питання кровопостачання штучного органу, адже кожна клітина вимагає доступу до капілярів для очищення крові. Тому поки що ці тканини планують використовувати для тестування препаратів і хімічних сполук у фармакології.

З іншого боку,швидкими темпами йде налагодження технології 3D-друку міжхребцевих дисків. Команда фахівців з Корнельського університету в США успішно завершила серію тестів з пересадки штучних дисків піддослідним щурам і вже приступила до операцій на людях. За розрахунками фахівців час відновлення після такої операції буде займати не більше 2 тижнів, що в рази скорочує звичну зараз терапію, яка може розтягнутися на кілька місяців і навіть років.

Разом з тим, можливості застосування 3D-друку в медицині активно обговорюється і у вітчизняній охороні здоров'я. Більш того, у світлі останніх досягнень, на щорічній конференції 3D Print Conference Kiev, цю тему виділили в окрему секцію, під час якої будуть представлені розгорнуті звіти фахівців за можливостями інтеграції технології 3D-друку в медицину.

Все більше компаній виходять на Український ринок 3D-друк: адже впровадження технологій не вимагає значимих витрат на обладнання та підготовку кадрів .

На основі описаного вище можемо з впевненістю стверджувати що в найближчій час 3D-друк набуде максимального застосування в медецині та протезуванні! Завдяки цьому паціентам не потрібно витрачати місяці та роки на відновлення після операцій вони зможуть в періоді декількох місяців повноцінно повернутись до колишнього життя без жодних причин хвилюватись про якість імпланту або нового органу .

Література:

1. 3D-біодрук: медицина майбутнього https://community.com.ua/ru/statti/3d-biodruk-meditsina-maybutnogo/
2. Приклади використання 3D-друку в медицині https://3dprinter.ua/prikladi-vikoristannya-3d-druku-v-meditsini/

УДК 004.94

3D ДРУК. РОЗВИТОК ТА ЗАСТОСУВАННЯ

Гулковський М.М., Борзов Ю.О.
Львівський державний університет безпеки життєдіяльності, Львів

Роботу присвячено процесу розвитку 3D друку – залучення його до найрізноманітніших сфер людського життя.

Якщо ви вважаєте, що 3D-друк це новітня технологія, то ваше твердження помилкове. Насправді їй вже понад 30 років. Все почалося в 1981 році, коли доктор Хідео Кодама з Нагойського інституту, що в Японії, продемонстрував систему швидкого прототипування з використанням фотополімерів. Модель створювалась накладання шарів один за одним.

А вже у 1984, відбувся справжній прорив в цій галузі. Чарльз Халл показав світу стереолітографічний апарат, завдяки якому можна було друкувати 3D-об'єкти, моделювання яких виконувалось на комп'ютері. В якості матеріалу для друку використовувався рідкий полімер на основі акрилу, який під дією ультрафіолету моментально застигав в необхідній формі.

Незабаром, компанія Stratasys, вигадала кращу технологію – моделювання методом наплавлення . Одним словом це метод накладання шарів, які повторюють контури цифрової моделі. Як матеріал найчастіше вибирають термопластики, які подаються в принтер у вигляді спеціальних котушок ниток.

Цей метод 3D друку і використовується на даному етапі

Сам термін "3D-друк" вигадали не так давно - у 1995 році. І з того часу всі машини, що надають нам 3D-друк, прийнято називати 3D-принтерами.

А де ж саме застосовують це 3D-друк? Якщо коротко то – всюди, проте найцікавіші та найбільш перспективні сфери:

Модна індустрія

Дизайн, мистецтво та архітектура

Будівництво

Медицина

Авіабудування

Ракетобудування

Автомобілебудування: В той час як великі автомобільні гіганти видруковують тільки деякі частинки для своїх авто, хтось намагається друкувати автомобілі вцілому. Осінню 2014 року світ побачив перший електрокар «Strati». Він не схожий на звичайні авто та має скромні характеристики, проте це тільки перша спроба. Якщо згадати перше авто Tesla і порівняти його із ModelS в них також велика відмінність,але це ж тільки поча-

ток. Тому в майбутньому Strati може змінити індустрію автомобілебудування, адже на виготовлення одного авто вистачає 44 години.

Якщо ви маєте 3D-принтер , можете надрукувати майже будь-яку дрібницю з пластику. Наприклад, частинки зламаних деталей до побутової техніки, меблів або ж господарських речей. Невелику іграшку, елемент декору з простим дизайном, чи з супер складним та багатьма рухомими елементами і в декількох кольорах.

Проте 3D-друк зараз ще як і всі винаходи не досконалий. Наприклад: не можуть друкувати гнучкі матеріали, не можуть моделюватись якісь міцні деталі . Але це все дрібниці порівняно із його можливостями.

Отже враховуючи той факт що в 3D моделюванні завжди ведуться пошуки дешевших і кращих матеріалів, а сам друк стає набагато кращим і швидшим, його вже розпочали використовувати в багатьох сферах життя. Тому майбутньому нас чекає суттєве змінення багатьох процесів виробництва. Речі стануть більш доступнішими та якіснішими. І це може повністю змінити наше життя.

Література:

1. http://thefuture.news/3d-printing
2. https://3d4u.com.ua/uk/blog/post/64-kak-3d-printery-ispolzuyutsya-v-avtomobilestroenii

АНАЛІЗ ВИКОРИСТАННЯ SKETCH UP, ЯК 3D ТЕХНОЛОГІЇ ІНТЕРАКТИВНОГО НАВЧАННЯ

Лемішко М., Гаврилюк А.
Львівський державний університет безпеки життєдіяльності, Львів

Наведено актуальність використання 3D технологій у освітньому процесі. Проаналізовано доступні та безкоштовні програмні ресурси для створення 3D моделей. Встановлено, що зручним для використання в освітньому середовищі є Sketch Up. З використанням даного програмного забезпечення створенні 3D моделі, які можуть бути використанні в навчальному процесі та значно покращити його якість.

Ключові слова: 3D-модель, Sketch Up, інформаційні технології.

The urgency of using 3D technologies in the educational process is given. Available and free software resources for creating 3D models are analyzed. Sketch Up has been found to be easy to use in an educational environment. Using this software, create 3D models that can be used in the learning process and greatly improve its quality.

Keywords: 3D model, Sketch Up, information technology.

Сучасний розвиток передових інформаційних технологій надає можливість викладачеві та, головне, студентові значно активізувати свою діяльність під час навчання. Всебічне залучення методів інтерактивності, комп'ютерного моделювання та 3D друку, різноманітних процесів, вирішення завдань в режимі реального часу з допомогою інформаційних технологій дозволяє активно та цікаво навчатись як за груповою моделлю так індивідуально [1,2]. Подекуди використання інформаційних технологій дозволяє досягти високої якості підготовки із значною економією ресурсів [3].

Запровадження 3D-інтерактивних технологій в освітнє середовище закладів вищої освіти спонукає до покращення рівня здобуття знань безліч спеціальностей. Адже хаотичне нагромадження сучасних технологій навчання в процес підготовки фахівців різних професій, де найважливішу роль відіграє практична складова, може призвести до погіршення становища.

Наглядно продемонструвати об'єкт дослідження, а також описати порядок роботи з ним завжди складало труднощі. 3D моделювання ефективно вирішує цю задачу. Ефективне використання 3D моделювання можливе за умови грунтовних знань фізичних явищ та законів, математичного апарату та інформаційних технологій. З іншого боку - чинників людського сприйняття мультимедійних сигналів. Дані технології забезпечують високу деталізацію фізичних об'єктів, що збільшує наочність що представляються, та дає близько 20 % запам'ятовування інформації, що представлена, наявність відео – 30%, а з використанням 3D моделей та інтерактивних зображень сягає близько 60 %.

Сьогодні існує ряд програмного середовища, що дає можливість створити 3D графіку та 3D анімацію, серед яких 3D Editor, K – 3D, Cinema – 4D, Now – 3D, 3D Studio Max, Maya, а також безкоштовний програмний продукт Sketch Up. Саме дозволяє з легкістю, простотою та зручністю здійснювати перші 3D моделі.

Sketch Up — програма для моделювання відносно простих тривимірних об'єктів — будівель, меблів, інтер'єру. У порівнянні з багатьма іншими популярними пакетами, цей володіє рядом особливостей, що позиціонуються її авторами як переваги. Основна особливість — майже повна відсутність вікон попередніх налаштувань. Всі геометричні характеристики під час або зразу після закінчення дії інструменту задаються з клавіатури в поле Value Control Box (поле контролю параметрів), яке знаходиться в правому нижньому кутку робочої області, справа від напису Measurements (панель вимірів). Ще одна ключова особливість — це інструмент Push/Pull («Тягни/Штовхай»), завдяки якому будь-яку площину можна «витягнути» в сторону, створивши по мірі її руху нові бокові стінки. Стверджується, що інструмент запатентований. Рухати площину можна в притик до наперед заданої кривої, для цього служить спеціальний інструмент Follow Me («Ведення»). Відсутність підтримки карт зміщення пояснюється націленістю продукту на непрофесійну цільову аудиторію.

Sketch Up дозволяє з легкістю створювати 3D модель будівель шляхи евакуації наявність первинних засобів пожежогасіння, а також автоматичні протипожежні системи. Разом з тим за допомогою даного продукту можна створювати 3D моделі конструктивних елементів автомобілів пожежної техніки та обладнання , їх складових частин, що дасть змогу всебічно та ефективно засвоювати матеріал, який викладається. Крім того, дане середовище можна використовувати для проектування нових чи удосконалення старих підходів у протипожежній техніці.

На рисунку 1 Представленні 3D моделі які змодельовані у програмному середовищі Sketch Up.

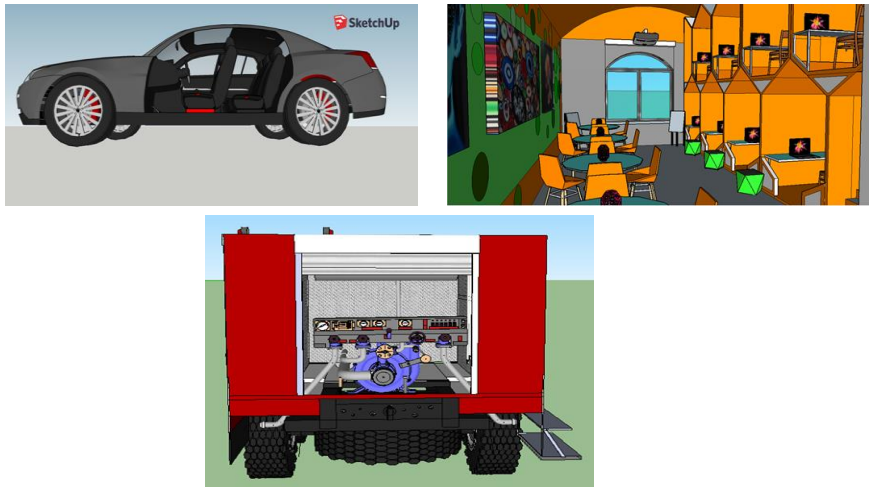


Рисунок 1 – 3D-моделі пожежної техніки, автомобіля та приміщення з використання Sketch Up

Висновки**.** Використання 3D технологій в освітньому середовищі в умовах сьогодення значно покращує якість підготовки мінімізуючи витрати і зусилля, а також активізує навички для розвитку інших професійних компетентностей.

Література

1. Гуревич Р. С. Інформаційно-комунікаційні технології в професійній освіті майбутніх фахівців : монографія / Р. С. Гуревич, М. Ю. Кадемія, М. М. Козяр. – Львів : ЛДУБЖД, 2012. – 380 с.

2. Козяр М. М. Інтерактивні методики навчання у ВНЗ / М. М. Козяр // Проблеми та перспективи формування національної гуманітарно-технічної еліти : зб. наук. праць. – Харків : НТУ «ХПІ», 2015. - №42(46). – С. 285-292.

3. Prydatko O. V. Investigation of the processes of the information technologies integration into the training of specialists at mine rescue departments // O. V. Prydatko, I. V. Pasnak // Scientific Bulletin of National mining university: Scientific works. Dnipro : National Mining University, 2017. – №1 (157) – p. 108-113.

ТЕНДЕНЦІЇ ВИКОРИСТАННЯ 3D МОДЕЛЕЙ ДЛЯ ДОСЛІДЖЕННЯ ПОЖЕЖ У ПРИРОДНИХ ЕКОСИСТЕМАХ

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

Проведено аналіз актуальних досліджень пожеж у природних екосистемах. Відзначено комп'ютерне моделювання як одних з напрямків дослідження лісових пожеж. Охарактеризовано програмне забезпечення WFDS, призначене для 3D моделювання пожеж у природних екосистемах. На прикладі експериментальних польових досліджень та моделювання пожежі молодих соснових насаджень в WFDS отримано результати, які підтверджують адекватність такої моделі та її придатність для застосування в системі забезпечення пожежної безпеки лісу. Ключові слова: програмне забезпечення, 3D моделювання, природні екосистеми.

The analysis of actual studies of fires in natural ecosystems is carried out. Computer modeling has been noted as one of the areas of forest fire research. WFDS software designed for 3D modeling of fires in natural ecosystems was noted. On the example of experimental field research and fire modeling of young pine plantations, WFDS obtained results confirming the adequacy of such a model and its suitability for use in the forest fire safety system. Keywords: software, 3D modeling, natural ecosystems.

Дослідження процесів виникнення та поширення пожеж у природних екосистемах є важливим завданням. Це пояснюється частотою щорічного виникнення зокрема лісових пожеж, які спричиняють значні матеріальні збитки. Експериментальні дослідження в цій галузі є ефективними, проте складними з огляду на організацію їх проведення. Але оцінити пожежну небезпеку необхідно до виникнення пожежі. Тому актуальним методом досліджень таких пожеж є комп'ютерне моделювання.

Поширення пожежі у лісі є складним для побудови моделі, оскільки на процеси горіння впливають багато чинників, які потрібно врахувати в параметрах моделі. Емпіричні моделі для створення потребують результатів реальних пожеж для кожного конкретного набору таких чинників. Тому для досліджень актуальним є використання моделей, в основу яких покладено рівняння математичної фізики процесів тепломасообміну в умовах пожежі. До таких моделей належить програмне забезпечення WFDS (Wildland Fire Dynamics Simulator) [1], яке застосовується для досліджень лісових пожеж.

Дане програмне забезпечення реалізує обчислювальну гідродинамічну модель (CFD) тепломасоперенесення при горінні. Базовим її продуктом є FDS (Fire Dynamics Simulator), який розроблено Національним інститутом стандартів і технологій США. У WFDS чисельно вирішуються рівняння Нав'є-Стокса для низькошвидкісних температурно-залежних потоків, розраховуються про-

цеси тепломасоперенесення, а також поширення диму при пожежі. Модель використовує диференціальні рівняння в похідних, що описують просторово-часовий розподіл температури і швидкостей газового середовища, концентрацій компонентів газового середовища (кисню, продуктів горіння і т.д.). Для реалізації моделі пожежі у WFDS окрім геометричних параметрів застосовують мікрокліматичні показники. Моделювання здійснюють на тривимірній сітці, попередньо зазначивши геометричні розміри обчислювального домену.

Важливою передумовою практичного застосування таких моделей є їх перевірка на адекватність порівнянням результатів з реальною пожежею. У разі позитивних результатів такої перевірки модель можна застосовувати для дослідження пожеж у екосистемах. Так, зокрема у [2] проведено моделювання пожежі молодих соснових насаджень віком до 10 років та встановлено, що розбіжності між експериментальними результатами та розрахунковими значеннями моделі практично відсутні і знаходяться в межах похибки обчислень. Це підтверджує адекватність такої моделі та її придатність для застосування в системі забезпечення, зокрема пожежної безпеки лісу.

Література

1. Mell W., McNamara D., Maranghides A., McDermott R., Forney G., Hoffman C, Ginder M. Computer modelling of wildland-urban interface fires. Fire & Materials. San Francisco, 2011. 12 Pp.

2. Товарянський В. І., Кузик А. Д. Дослідження пожежі молодих соснових насаджень. Пожежна безпека: Збірник наукових праць. ЛДУ БЖД. Львів, 2016. № 28. С. 113−120.

Напрям 12

Математичне та комп'ютерне моделювання складних систем

METHOD OF FIRE AREAS LOCALIZATION ON THE BASIS OF REMOTE SENSING DATA

Andrii Havrys, Roksolana Moreniuk
Lviv State University of Life Safety, Lviv

In the paper data of remote sensing of the Earth from the MODIS satellite was analyzed. The use of current method of fire areas localization together with historical data on fires of the selected region for the prediction and analysis the probability of fires occurrence in the individual investigated territories was proposed.

Keywords: computer simulation; fire; satellite data; wildfire; cluster analysis.

Today we can prevent fires with the help of modern technologies and exchange of international experience, gain new useful knowledge to prevent such disasters.

Every day we receive information from satellites for rapid remote monitoring of forest fires. Wildfire monitoring allows them to be eliminated in the early stages. Modern GIS technologies allow you to receive information from all over the globe and even from space. In order to reduce the occurrence of forest fires and timely monitoring of emergencies, it is advisable to use data obtained by remote sensing of the Earth.

The data we used is for wildfire in Australia in January 2013 obtained from the NASA Earth Observation System Data Information Service (EOSDIS). EOSDIS provides near real-time monitoring of global fires as well as an archive. We used various statistical approaches, to identified and tested patterns of clustering in the data.

The points are the centroids of remotely sensed image pixels with an approximate resolution of 1km² acquired during several satellite passes. Points have a 'brightness' sufficiently high to be considered a fire, and do not correspond to a known natural or anthropogenic source.

All points are interdependent. If we model 'individual fires' from the fire points, then our 'fire observations' are now independent of one another (one record for each fire) and free of within-fire variation.

One simple clustering approach is to measure the distance between all pairs of points, and then to cluster pairs of points that are within a threshold dis-

tance of one another. The points within each of cluster are all within one unit of at least one other point in the cluster, whereas the nearest points in different clusters are over two units apart. A clustering threshold of one would thus group the points into two sets in which all points within a set are within one unit of another point in the set.

The Density-based Clustering tool implements three algorithms that cluster features into groups based on the distance between features and/or their density in space. The defined distance method is the simplest and are going to use this approach here, however, instead of the using the Density-based Clustering tool we shall use the Aggregate Points(Cartography) tool that also generates polygons around each cluster.

We shall compare the different fire clusters to historical Google Earth imagery to see how well the clusters match visible fire scars.

The fire points are the centroids of roughly 1km² pixels and, thus, the threshold must be greater than 1km to cluster points captured at the same time. Bush fires can jump up to 20km, so this is the maximum realistic threshold. [1].

Clustering is weaker above a threshold distance of approximately 7km (from the graph).7km threshold has the best visual match with Google Imagery for the example Tasmanian fire and others.

The Bright_T31 field of the fire points stores surface temperature estimated from 'channel 31' but this information was lost the in the process of amalgamating fire points into polygon scars. The fire points within a scar are a sample of the temperature of the fire that created the scar. We can estimate a temperature of each fire scar by calculating the mean of the points making up each fire scar.

The aim of a hazard impact map is to show where the hazard occurred and to what degree. The point map gives us a crude overview of the spatial distribution of wildfires in January 2013, but points that are near one another occlude each other, obscuring pattern. We could use smaller dots, but the viewer would still need to visually search the map to identify regions a high fire density. As always different viewers would identify different regions.

The Hot spot analysis calculates the Getis-Ord Gi statistic, which tests whether a feature clusters in space with other features with similar high and low values than expected. where the expectation is that features, and their values are randomly distributed [2].

ArcGIS support two tools that undertake hot spot analysis, the Optimized Hot Spot Analysis tool that automatically optimizes the function parameters, in particular, the spatial relationship model as a distance band (sphere of influence) [3,4]. The Hot Spot Analysis tool that provides greater control over analysis parameters was created.

We used empirical data (observations) to model fire extent, nature (temperature) and impact for January 2013 Australian wildfire season. While analy-

sis like this are suitable for assessing event impact after it occurred it does not tell us how likely wildfire is at any place. To model overall risk requires the integration of information on spatial distribution of the necessary conditions for wildfire and sources of ignition.

References:

1. Volume 1: The Kilmore East Fire. 2009 Victorian Bushfires Royal Commission. Victorian Bushfires Royal Commission, Australia. July 2010.

2. Official website of the ArcGIS Pro. Retrieved from: http://pro.arcgis.com.

3. Starodub Y.P., Kuplovsky B.E., Shelyuh Y.E., Havrys A.P. (2013) Lokalizatsiia pozhezhonebezpechnykh dilianok z vykorystanniam suputnykovykh danykh dlia seismoaktyvnykh zon Ukrainy [Fire areas localization using satellite data for seismic zones of Ukraine] Fire Safety: Lviv: LSU LS, №23, 151-158 p. [In Ukrainian].

4. Starodub Y.P., Havrys A.P. (2015) Increasing areas security project for the risk flooding territories of Ukraine. Central European Journal for Science and Research Stredoevropsky Vestnik pro vedu a vyzkum", Praha, 42-46 p.

ЗАСТОСУВАННЯ НЕЙРОННИХ МЕРЕЖ В МЕТОДІ АНАЛІЗУ ІЄРАРХІЙ ДЛЯ ОЦІНКИ СТАНУ ОХОРОНИ ПРАЦІ

Андрусик М.Я., Ковтан Б.І., Фірман Т.В.
Львівський національний університет імені Івана Франка

За сучасних умов прийняття ефективних рішень оцінюючи стан охорони праці на базі тільки якісного аналізу, досвіду й інтуїції стає дедалі важчим. Центральне місце в процесіобробки інформації в різних ланках управління займає прогнозування можливих варіантів розвитку стану і на їх основі формування рішення на охорону праці. Саме прогнозування на сьогодні є відносно новим і мало вивченим процесом для штабів різних рівнів.

На сучасному етапі інформатизації управління відбувається інтеграція в єдиний комплекс математичних методів моделювання, теорій прогнозування і прийняття рішень, теорії управління і т. ін. Головними напрямками підвищення ефективності управління є розвиток методів одержання раціональних управлінських рішень для забезпечення ефективної охорони державного кордону.

Найбільш відповідає наведеним вимогам і дає кількісні оцінки можливих сценаріїв розвитку стану охорони праціметод аналізу ієрархій (МАІ). Метод аналізу ієрархій – це математична процедура для ієрархічного зображення елементів з метою визначення суті будь-якої проблеми.[3] Метод полягає в декомпозиції проблеми на простіші складові частини, а також в обробленні суджень особи чи осіб, котрі приймають рішення (ОПР) на підставі парних порівнянь пріоритетів (критеріїв) доцільності. Це дає змогу оцінити рівень взаємодії елементів ієрархії. МАІ охоплює однаково як фактори, за якими можливе проведення окремих вимірювань, так і невідчутні фактори, за якими потрібні судження експертів.

Ключовим моментом використання МАІ є уявлення стану, формування його сценаріїв у вигляді ієрархії.

– На найнижчому рівні ієрархії представлений основний зміст альтернативних варіантів сценаріїв.

– Після ієрархічного представлення проблеми розробки найімовірнішого сценарію розвитку обстановки на ділянці кордону складаються матриці для парних порівнянь важливості показників від нижнього до найвищого рівнів.

– Далі за процедурою методу аналізу ієрархій здійснюється оцінка і вибір найбільш можливого сценарію та визначається вплив (значення, місце) кожного елемента ієрархії на можливий сценарій, тобто на найвищий рівень.

Запропонований метод дослідження сценаріїв розвитку обстановки ґрунтується на об'єднанні переваг управління з використанням експертних методів і методів кількісного аналізу.[3] Метод дозволяє на основі поетапного системного аналізу прогнозувати сценарії розвитку станів та кількісно оцінити можливість їх здійснення. Метод також дозволяє упорядкувати процес обробки різної інформації, яка може бути використана не тільки для формування чи вибору сценаріїв розвитку станів, але й для виявлення тенденцій накопичення протиріч, розвитку й еволюції дестабілізуючих сил і їх впливу на процеси охорони праці.

Розглянуті процедури методу прогнозування обстановки в штабах дозволять визначити вплив загроз у різних сферах, спрогнозувати зародження, нагромадження і дестабілізуючих факторів, що закладається як вихідні дані для планування охорони праці чи корекції моделі її побудови.

Використання методу дає можливість при обробці інформації використовувати сучасні інформаційні технології, проводити кількісні оцінки й одночасно підвищувати оперативність, вірогідність та об'єктивність результатів прогнозування, що подаються для прийняття рішень. Нагромадження інформації стосовно стану охорони праці доцільно здійснювати щодо обраних сфер відносин на державному кордоні, а усередині кожної сфери сортування інформації - стосовно до обраних показників.

Для подальшого дослідження питань, що розглядалися, доцільно розробити програмне забезпечення для обробки інформації, зокрема за методом аналізу ієрархій, і методики здійснення постійного моніторингу та на його основі своєчасного прогнозу можливих сценаріїв розвитку стану для своєчасної розробки пропозицій щодо побудови чи перебудови методів охорони праці.

Саме для виконання вище сказаного і використовуватимуться нейронні мережі.

Нейронна мережа – це певна комплексна функція, яка має величезну кількість параметрів. Кожен із цих параметрів (т.зв. ваги) адаптується для того, щоб наблизити функцію до стану, як розподілені дані у тестувальній вибірці. Дуже часто кількість цих параметрів набагато більша, ніж необхідно опису тестових даних. [2]

Нейронні мережі займаються поетапним проектування вхідних векторів таким чином, щоб на виході отримати правильний вектор очікуваної розмірності. Якщо зрозуміти, як працюють між собою всього-на-всього два нейрони, можна зрозуміти, що відбувається в масштабі всієї нейронної мережі. Кожен нейрон має зв'язки зі своїми сусідами. У процесі навчання, сила цих зв'язків може корегуватися – посилюватися або послаблюватися. Якщо сила зв'язку велика, це означає, що стан сусіда сильно залежить від стану нейрона у попередньому шарі. Якщо сила зв'язку мала, це значить, що стан сусіда не сильно залежить від того, наскільки активований поточ-

ний нейрон. На початку тренування мережі, як правило, сили зв'язків між всіма нейронами обираються випадковими. В процесі тренування, кожного разу, коли ми проходимо і отримуємо новий і новий вектор, на виході ми отримуємо певну помилку, яку ми отримали внаслідок застосування функції втрат, наприклад, квадратичної помилки. Далі система проходиться в зворотному напрямку і корегує силу зв'язків між нейронами таким чином, щоб на наступній ітерації помилка була меншою. Якщо в нашій тренувальний вибірці різноманітність прикладів достатньо велика, то нейрони корегують між собою таким чином, щоб на виході ми могли отримати результати максимально наближені до очікуваних.

Таким чином маючи достатню кількість статистичних даних і критерії за якими вони оцінюватимуться, виникає питання як визначити вагові коефіцієнти для критеріїв МАІ. Зазвичай застосовують суб'єктивну думку експерта (ОПР) для визначення пріоритетів, проте зі збільшенням кількості критеріїв втрачається точність обрахунків.[3] Саме для цього і варто використати нейронній мережі. Їхня суть полягає в тому, щоб маючи тестові вибірки, яку створили на основі роботи кількох осіб, що приймають рішення, так щоб загалом були враховані усі можливі критерії, що застосовуються в МАІ, навчити нейронну мережу моделювати оцінку експерта (ОПР) для визначення критеріїв доцільності і, відповідно, для побудови матриць попарних порівнянь важливості показників. В результаті отримуємо ефективну оцінку стану охорони праці

Література:

1.Вступ | Тема 1. Що таке машинне навчання? | ML101 Зміст курсу |Prometheus[Електронний ресурс]. – Режим доступу: https://courses.prometheus.org.ua/assets/courseware/v1/cdf163c83c64f8357ddbcdac82f7d624/c4x/IRF/ML101/asset/Тиждень_1_конспект.pdf. – Назва з екрана.

2.Основи машинного навчання. | Travels&Code [Електронний ресурс]. – Режим доступу: https://travelscode.com/osnovi-mashinnogo-navchannya/ . – Назва з екрана.

3. Саати Т. Л. Принятиерешений при зависимостях и обратныхсвязях: Аналитические сети. — М.: Издательство ЛКИ, 2008. — 360 с

ЗАСТОСУВАННЯ ТЕОРІЇ ГРАФІВ ДЛЯ АНАЛІЗУ І ОЦІНКИ ЗБИТКІВ ЕЛЕМЕНТІВ ТЕХНІЧНИХ СИСТЕМ

Бубіс М.І.
Одеський національний морський університет, Одеса

Анотація. У роботі наведено результати дослідження можливостей застосування теорії графі для аналізу та оцінок збитків виходу з ладу елементів технічних систем з метою підвищення ефективності їх експлуатації.
Ключові слова: теорія графів, діагностика, технічні системи, аналіз збитків, оцінка ризиків.

Abstract. The paper presents the results of investigating the possibilities of applying graph theory for the analysis and estimation of failures of elements of technical systems in order to increase the efficiency of their operation.
Keywords: graph theory, diagnostics, technical systems, loss analysis, risk assessment.

Сучасна технічна система (ТС) це сукупність взаємопов'язаних і взаємозалежних структурних компонентів, схильних до змін технічного стану в різних умовах експлуатації. Вихід з ладу однієї або декількох елементів ТС призводить до зниження ефективності експлуатації всієї ТЗ, аварій, що супроводжується пошкодженням обладнання. Збиток від аварій в ТС може бути як прямим (вихід з ладу всієї системи), так і непрямим (вихід з ладу будь-якої підсистеми або вузла) [1]. Для відновлення необхідних режимів роботи функціонування елементів ТС необхідно чимало часу і істотні трудові витрати. Можливі аварійні наслідки від змін стану ТЗ в різних умовах експлуатації можуть бути запобігти діагностикою та прогнозуванням технічного стану при оцінці і управлінні ризиками ТС на базі застосування теорії графів, для уявлення системи у структурованому вигляді, де вершини графу системи відповідають елементам, а ребра – зв’язкам [2]. Таким чином, існує об'єктивна необхідність в дослідженні використання теорії графі для аналізу та оцінок збитків виходу з ладу елементів ТС з метою підвищення ефективності їх експлуатації. Розроблений підхід аналізу та оцінки структурного і функціонального збитків і ризиків елементів взаємопов'язаних і взаємозалежних ТС в різних умовах експлуатації спирається на реалізацію наступних етапів: виявлення взаємозв'язку і взаємозалежності елементів в ієрархії і топології ТС, побудова і дослідження моделі графу ТС, оцінки ймовірностей втрат працездатності елементів ТС, оцінки структурного і функціонального збитків ТЗ від уражених елементів та оцінки структурного і функціонального ризиків ТС. Для дослідження даного підходу розроблене програмне забезпечення на базі використання мови

програмування C# та середовища розробки Visual Studio 2017. Основними варіантами використання системи є: створення моделі необхідної системи у вигляді графа, з підтримкою функцій введення назви моделі, завдання короткого опису, створення нової вершини і її відтворення на панелі, створення зв'язку між вершинами (шляхом вибору вершини-джерела і вершини-приймача), вибору алгоритму розташування і відображення структури в графічному контейнері; перегляд назви і короткої структури раніше створеної моделі у вигляді графа з відображенням загального числа вершин і ребер, підтримуючи операцію її завантаження в робочий простір програми; проведення розрахунку значень ризиків і збитків елементів модельованої системи і відображення отриманих результатів у вигляді зведеної таблиці; побудова графіків візуалізації отриманих результатів в ранжируваному вигляді.

Висновки. Отримані результати проведеного дослідження використання теорії графі для аналізу та оцінок збитків виходу з ладу елементів технічних систем показали ефективність застосування даного підходу для оцінки технічного стану систем.

Література:

1. Панфилова Э.А. Понятие ущерба и риска: многообразие подходов и опреедлений / Э.А. Панфилова //Теория и практика общественного развития, 2010. – №4. – С. 30–34.

2. Райншке К. Оценка надежности систем с использованием графов / К. Райншке, И. А. Ушаков. – М.: Радио и связь, 1988. – 208 с.

ВИКОРИСТАННЯ АЛГОРИТМІВ БІНАРИЗАЦІЇ ДЛЯ ПРОЦЕСІВ РАСТЕРИЗАЦІЇ

Гавриш Б., Сельменська З., Комар С.
Українська академія друкарства, Львів

Анотація. Методи опрацювання цифрових зображень знайшли застосування для розв’язку великої кількості завдань з різних областей, до яких належить сучасна поліграфія. Для виведення на друк цифрове зображення перетворює Raster Image Processor (RIP), що представляє собою програмно-апаратний комплекс, який здійснює процедуру цифрової растеризації. Оскільки RIP розробляється для комерційних цілей і практично кожна цифрова друкарська машина або принтер має свій власний RIP, то використовувані алгоритми є вузькоспеціалізованими. Хоча нестачі в алгоритмах бінаризації немає, проте захищеність їх коду, не дозволяє простежити методи, покладені в їх основу і визначити їх можливості. У зв'язку з цим завдання розробки і дослідження нових алгоритмів бінаризації зберігає актуальність.

Ключові слова: бінаризація, растеризація, цифрове зображення, алгоритм

Annotation. Digital imaging techniques have been used to solve many of the challenges in the various fields of nowadays polygraphy. For printing, the digital image is converted by the Raster Image Processor (RIP), which is a hardware and software complex that performs the digital rasterization procedure. Since RIP is designed for commercial purposes and virtually every digital printing machine or printer has its own RIP, the algorithms used are highly specialized. Although there are no shortcomings in the binarization algorithms, the security of their code does not allow us to trace the methods underlying them and to determine their feasibility. In this regard, the task of developing and researching new binarization algorithms remains relevant.

In this regard, the task of developing and researching new binarization algorithms remains relevant.

Keywords: binarization, rasterization, digital image, algorithm

Бінаризація є важливим інструментом опрацювання зображень. Бінаризацію напівтонових зображень можна розглядати як процес квантування з двома рівнями, при якому виникають втрати інформації. Справа в тому, що у більшості випадків властивості об'єктів, які нас цікавлять, досліджуються за його зображенням, методи аналізу яких різноманітні. За допомогою бінаризації півтонове зображення (grayscale) перетворюється в двокольорове або бінарне. Таке перетворення переслідує різні цілі, наприклад:

1) виявлення особливостей об'єктів, які несуть потрібну інформацію;
2) компактний опис;
3) створення ілюзії великої кількості відтінків або кольору.

Бінаризація використовується в завданнях дослідження і діагностики складних технічних і біологічних систем, до яких належить розпізнавання образів, контроль і аналіз матеріалів, відеоспостереження, відеокодування тощо.

Бінаризація є основою Raster Image Processor (RIP), який здійснює процес растеризації.

Процес растеризації є складним. Алгоритми растеризації повинні враховувати особливості зорової системи людини, технологію друку, і бути простими з обчислювальної точки зору. Остання умова є важливою, оскільки цифрове зображення має великий обсяг і його опрацювання вимагає великих обчислювальних витрат. Бінаризація – перетворення напівтонового зображення, представленого в цифровому вигляді, в зображення, в якому піксель приймає два значення. Отримане зображення є бінарним. Значення, яке приймає піксель, назвемо яскравістю.

Процес бінаризації можна розглядати як перетворення яскравості, коли елемент $f(x,y)$, де $x=1,2,...,M$, $y=1,2,...,N$, $M\times N$ розмір зображення, матриці півтонового зображення, що приймає 2^k значень, де $k=1,2,...$, і в результаті перетвориться в матрицю R, що складається з нулів і одиниць

$$R = \{ g(x,y) : g(x,y) \in \{0,1\} \} \quad (1)$$

Кількість елементів $|R|$ матриці R визначає характер перетворення. Якщо $|R| \geq 2^k$, то перетворення відбуватиметься без втрати інформації, в цьому випадку інформація не зменшується, і саме перетворення може бути оберненим.

Однак при цьому збільшується розмір матриці бінарного зображення, яке буде містити в $|R|$ разів більше елементів, ніж вихідне півтонове зображення.

При $|R| = 2$

$$f(x,y) \to g(x,y) \in \{0,1\}. \quad (2)$$

Розмір зображення не змінюється, але це перетворення з втратами і, отже, не є оберненим. Якісна бінаризація цифрових зображень, створена у вигляді програмного комплексу, дозволить коригувати алгоритми растрових процесорів вивідних пристроїв, уникаючи при цьому виникнення побічних ефектів у вигляді втрати якості при друці, нечіткої передачі контурів, кольору, змазування контурів тощо.

Література

1. Прэтт У. Цифровая обработка изображений. В 2 т. М.: Мир, 1982.

2. H. Xie and X. Tong, "An inproved binary encoding algorithm for classification of hyperspectral images," 2012 4th Workshop on Hyperspectral Image and Signal Processing: Evolution in Remote Sensing (WHISPERS), Shanghai, 2012, pp. 1-4. doi: 10.1109/WHISPERS.2012.6874331.

3. A. Ertürk, M. K. Güllü, D. Çeşmeci, D. Gerçek and S. Ertürk, "Spatial Resolution Enhancement of Hyperspectral Images Using Unmixing and Binary Particle Swarm Optimization," in IEEE Geoscience and Remote Sensing Letters, vol. 11, no. 12, pp. 2100-2104, Dec. 2014. doi: 10.1109/LGRS.2014.2320135.

4. Otsu N. A threshold selection method from gray-level histograms / N. Otsu // IEEE Trans. Syst., Man. and Cybern. – v. SMC. - υ9. – 62-66.

5. W. Zhao, R. Chellappa, P.J. Phillips and A. Rosenfeld. Face recognition: A literature survey. ACM Computing Surveys, 35(4): 399 – 458, 2003.

6. Zhang, G., Huang, X., Li, S.Z., Wang, Y., Wu, X.: Boosting local binary pattern (LBP)-based face recognition. In: Li, S.Z., Lai, J.-H., Tan, T., Feng, G.-C., Wang, Y. (eds.) SINOBIOMETRICS 2004. LNCS, vol. 3338, pp. 180– 187. Springer, Heidelberg (2004).

ПРОГРАМНІ ТА АПАРАТНІ ЗАСОБИ ІДЕНТИФІКАЦІЇ СПОЖИВАЧІВ ЕЛЕКТРОЕНЕРГІЇ ДЛЯ СИСТЕМ РЕЗЕРВНОГО ЖИВЛЕННЯ «РОЗУМНИХ СПОРУД»

Димид Р., Гороховський В., Пташник В.
Львівський національний аграрний університет, Львів

Анотація. У роботі проаналізовано сучасні підходи до забезпечення резервного живлення «розумних споруд». Запропоновано низку програмних та апаратних засобів ідентифікації підключених споживачів електроенергії. Розроблено алгоритм аварійного відключення окремих споживачів з метою ефективного використання резервних ресурсів та продовження терміну використання пріоритетних функцій «розумних споруд».
Ключові слова: «розумний будинок», алгоритм оцінювання, резервне живлення.

Summary. Modern approaches to providing backup power of "smart houses" were analyzed. A number of software and hardware identifiers for connected electricity consumers were proposed. An algorithm for emergency shutdown of individual consumers was developed with the purpose of efficient use of reserve resources and extension of the term of use of priority functions of "smart houses".
Key words: "smart houses", evaluation algorithm, backup power.

Забезпечення резервного живлення функціональних систем «розумних споруд» та користувацького обладнання є важливою прикладною задачею. Її вирішення сприяє значному підвищенню рівня безпеки та комфорту мешканців, а також дозволяє скоротити вартість електроенергетичного обладнання. Використання інформаційних технологій для інтелектуального управління процесом енергоспоживання дозволить істотно вдосконалити наявні методи резервного електропостачання «розумних споруд».

У більшості випадків «розумний будинок» обладнують системою резервного живлення призначеною, у першу чергу, для підтримання функціонування пріоритетних систем: центрального та периферійних контролерів, охоронної сигналізації, пожежної сигналізації, системи контролю витоків води та газу тощо. Тому у разі позапланового відключення електропостачання «розумного будинку» відбувається миттєве знеструмлення усіх інших споживачів. Якщо ж «розумну споруду» обладнано власною системою генерації електроенергії, або високоємнісними акумуляторними батареями то вони забезпечують одночасне живлення функціональних систем будинку та інших споживачів. Такий метод не забезпечує необхідного рівня селективності і є виправданим лише при короткотривалих відключеннях. Селективна ідентифікація кінцевих споживачів дозволить визначати рівень їх вагомості і здійснювати їх поступове відключення від енергоспоживання Це забезпечить максимальний рівень комфорту користувача та

продовжить термін автономного функціонування пріоритетних систем «розумного будинку».

Для ідентифікації підключених споживачів запропоновано використати датчик миттєвої споживаної потужності розміщений на вводі електроенергії у будинок. Такий датчик забезпечує збір інформації про напругу та силу струму у ввідному контурі. Аналогічно збір інформації можна реалізувати за допомогою лічильників електроенергії з імпульсним виходом.

Ідентифікація споживачів може відбуватись за зміною кривої споживаної потужності. Такий метод дозволяє розділити споживачів електроенергії на три групи: обладнання з імпульсним блоком живлення (комп'ютерна техніка, телевізори тощо), споживачі з електродвигуном (пральна машина, болгарка) та електронагрівальні прилади (електричний чайник, духовка, калорифер тощо). Для досягнення кінцевої мети необхідно провести розділення графіку сумарного навантаження на окремі компоненти. Ця задача вирішується шляхом «навчання» системи – запису кривих електроспоживання окремих споживачів.

Таким чином використання інформаційних технологій дозволяє «розумному будинку» розпізнати споживача електроенергії та оперативно прийняти рішення про відключення з залученням елементів не чіткої логіки. Водночас наявність бази даних наявних споживачів істотно підвищує ефективність роботи запропонованої системи.

ВИКОРИСТАННЯ MACHINE LEARNING У ШАХАХ

Краковський В.
Одеський національний політехнічний університет

Для створення штучного інтелекту, навчання штучного інтелекту грі в шахи. Machine Learning. Artificial intelligence. AlphaZero. Monte Carlo Tree Search.

На сьогоднішній день всю теорію гри у шахи можна об'єднати в єдину базу даних або бібліотеку, прикладом цього є відома програма Stockfish. За допомогою методів Machine Learning, можна написати програму, яка буде самовдосконалюватися завдяки власному досвіду, який вона отримує унаслідок гри з собою. Такою є програма з назвою AlphaZero, яка була розроблена компанією Google та має відкритий код для всіх охочих ознайомитися з нею.

На початку процесу навчання AlphaZero робила випадкові ходи і знала тільки те, що мета партії — поставити мат. Її успіхи оцінювалися за допомогою турнірів по одній секунді на хід проти власних більш ранніх версій і програми Stockfish. Після чотирьох годин гри з собою AlphaZero дізналася про шахи досить, щоб перевершити Stockfish.

AlphaZero навчається за допомогою нейронної мережі, яку можна зобразити так:

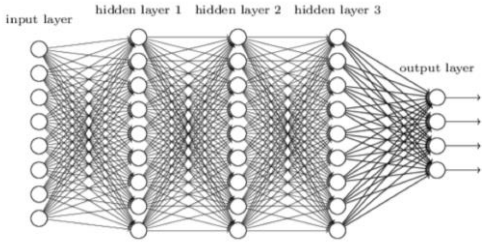


Рисунок 2 – Зображення нейронної мережі

Нейронна мережа — це спроба зробити комп'ютерну систему більш схожою на людський мозок. Дані на вході, тобто, позиція на дошці, приходять зліва. Їх обробляє перший шар нейронів, кожен з яких передає дані на виході нейронам наступного шару, і так далі, поки ми не отримаємо кінцеві дані від самого правого шару нейронів. У AlphaZero кінцеві дані складаються з двох частин:

1. Оцінка даної шахової позиції
2. Оцінка кожного можливого ходу в цій позиції

Перший крок, який необхідно зробити — навчити AlphaZero правилам шахів, щоб вона могла робити допустимі ходи, хоч і випадкові. На наступному етапі розробники використовували підхід, званий "навчання з підкріпленням". Це означає, що програма стала грати мільйони партій сама з собою. Після кожної партії вона змінювала вагові критерії, намагаючись запам'ятати, що принесло користь, а що — ні.

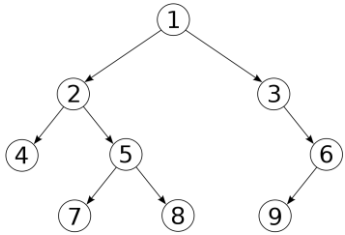


Рисунок 3 – Дерево варіантів

Основною проблемою шахів є вибухове розгалуження варіантів. Розрахунок на два ходи вперед з дебютної позиції для звичайних шахових аналітичних програм вимагає оцінки близько 150000 позицій і з збільшенням глибини ця кількість зростає експоненціально.

AlphaZero скорочує кількість варіантів, розглядаючи тільки ходи, рекомендовані її стратегічною мережею та використовує оціночну мережу, щоб припинити вивчення варіантів з ясною оцінкою (перемога/поразка).

AlphaZero для пошуку в дереві ходів використовує метод Монте-Карло (Monte Carlo Tree Search або MCTS). Чистий метод Монте-Карло оцінює позицію, випадковим чином створюючи кілька послідовностей ходів (званих “розіграші”) і отримуючи середній підсумковий результат (перемога / нічия / поразка), до якого вони ведуть. AlphaZero проводить 800 розіграшів для кожного ходу. Крім того, чистий метод Монте-Карло вдосконалений тим, що віддають перевагу раніше ні (занадто часто) застосовані ходи; ходи, що здаються можливими, і ходи, які, мабуть, ведуть до "гарних” позицій. "Гарні" - ті, для яких оціночна функція показує великі значення. Тобто, розіграші вибираються не випадково, а відповідно оціночної функції, що безперервно вдосконалюється. Таким чином програма розглядає можливі рішення й обирає одне, яке вважає найбільш ефективним.

Нейронна мережа AlphaZero працює на спеціальному обладнанні, тензорних процесорах Google (TPU). Для того, щоб грати з собою тренувальні партії AlphaZero використовувала 5,000 TPU першого покоління і 64 TPU другого покоління для навчання. Під час гри проти Stockfich використовувалися лише чотири тензорних процесора, щоб показати, що для ефективної роботи AlphaZero не потрібно великих обчислювальних потужностей.

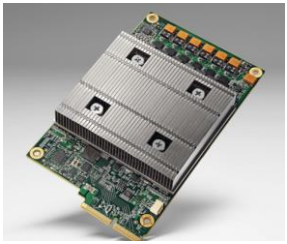


Рисунок 4 – Тензорні процесори Google (TPU)

Тензорний процесор був розроблений Google саме для навчання нейронних мереж, тому він спеціалізується на матричному множенні, яке вимагало б від звичайного процесора в комп'ютері довгої серії обчислень. Тензорний процесор виконує матричне множення за один тактовий цикл (а TPU першого покоління працює зі швидкістю 700 мільйонів циклів в секунду).

Отже, шахи є однією з найбільш широко розвинених областей, в яких успішно застосовується штучний інтелект з нейронними мережами для вирішення проблем, що раніше вважалися занадто складними для комп'ютеризації. На мою думку, у майбутньому разом з удосконаленням методів навчання штучного інтелекту будуть створені програми, кращі за AlphaZero у багатьох аспектах. А поки цей час не настав, можна спробувати розширити межі використання подібної технології в інших іграх, що є відмінною темою для подальших досліджень.

Література:

1. Silver, David & et al.. “Mastering Chess and Shogi by Self-Play with a General Reinforcement Learning Algorithm” (5 December 2017) – URL: https://arxiv.org/pdf/1712.01815.pdf

2. MikeKlein. Google’s AlphaZero Destroys Stockfish in 100-Game Match, Chess.com (7 December 2017) – URL: https://www.chess.com/news/view/google-s-alphazero-destroys-stockfish-in-100-game-match

3. Gibbs, Samuel. AlphaZero AI beats champion chess program after teaching itself in four hours, The Guardian (8 December 2017) – URL: https://www.theguardian.com/technology/2017/dec/07/alphazero-google-deepmind-ai-beats-champion-program-teaching-itself-to-play-four-hours

4. Mel_OCinneide. How Does AlphaZero Play Chess?, Chess.com (21 December 2017) – URL: https://www.chess.com/article/view/how-does-alphazero-play-chess

5. Mel_OCinneide. What’s Inside AlphaZero’s Chess Brain?, Chess.com (18 January 2018) – URL: https://www.chess.com/article/view/whats-inside-alphazeros-brain

ОСОБЛИВОСТІ ПОБУДОВИ МІКРОКОНТРОЛЕРНИХ СИСТЕМ ЦИФРОВОЇ ОБРОБКИ СИГНАЛІВ

Лагун Я., Вітер О.
Національний університет «Львівська політехніка», м. Львів

Створення недорогих та широкодоступних пристроїв для опрацювання сигналів в режимі реального часу для вирішення наукових та технічних завдань на основі мікроконтролера є альтернативою використання спеціалізованих цифрових сигнальних процесорів. Визначено розрядність, тактову частоту, швидкість виконання інструкцій як основні властивості для реалізації алгоритмів цифрової обробки сигналів на основі мікроконтролера.
Ключові слова: обробка сигналів, мікроконтролер.

Creating inexpensive and widely available devices of DSP in real-time on the microcontroller to reduce scientific and technical tasks is an alternative to specialized digital signals processor. The number of digits, clock speed, the number of clock cycles required to execute instructions, is determined as the primary properties of a microcontroller for the implementation of algorithms of digital signal processing.
Keywords: signal processing, microcontroller.

Цифрова обробка сигналів (ЦОС) – область науки та техніки, яка стрімко розвивалася останні півстоліття. Цей швидкий розвиток є результатом значного прогресу в цифровій комп'ютерній техніці та виробництві інтегральних мікросхем. Протягом останнього десятиліття з'явилися нові області застосування технологій ЦОС такі, як комп’ютерний зір, приладобудування та управління, стиснення даних, розпізнавання та синтез мовлення [1]. Паралельно із зростанням областей застосування методів ЦОС відбувалося зростання сировинної обчислювальної потужності, доступної для впровадження алгоритмів ЦОС та доступ до великої кількості прикладних проектів та високопродуктивних процесорів.

Алгоритми ЦОС традиційно реалізовуються за допомогою спеціальних мікросхем обробки цифрових сигналів - процесорів DSP, програмованих логічних схем FPGA або процесорів RISC [2]. Якщо для складних обчислювальних завдань ЦОС потрібен цифровий сигнальний процесор або FPGA [4], то для численних простих програм доцільним буде використання мікроконтролера.

Мікроконтролери (MCU) – це пристрої загального призначення для управління, моніторингу та зв’язку з зовнішніми пристроями, які можуть бути адаптовані до завдань ЦОС за допомогою відповідного програмного забезпечення. Вони використовують 4, 8 або 16-бітні дані, пам'ять програм та даних, а також пристрої вводу/виводу, таймери, набір інструкцій. Також мають у своєму складі деякі додаткові програмовані периферійні пристрої, недоступні на процесорах DSP (наприклад АЦП та ЦАП) [3]. Мікроконтролери є менш продуктивними ніж DSP-процесори. Це пов’язано з їх невеликою швидкістю обробки та обмеженням пам’яті.

Використання мікроконтролерів загального призначення для обробки цифрових сигналів стало актуальним із появою процесорів з високою швидкістю. Оскільки більшість систем обробки сигналів складаються з хост-процесора та спеціалізованої мікросхеми DSP, використання одного мікроконтролера для виконання обох цих функцій забезпечує більш просте і дешевше рішення. Крім того, однокристальна конструкція буде споживати менше енергії, що дозволяє створювати системи з акумуляторним живленням.

Загалом типова система обробки сигналів включає АЦП, ЦАП та процесор, який виконує алгоритм обробки сигналу, як показано на рис. 1.

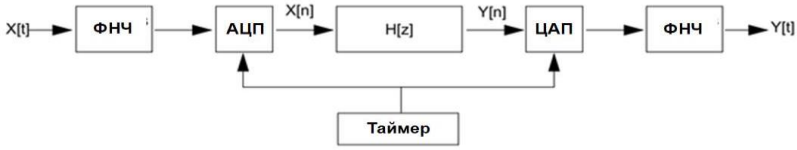


Рис. 1. Типова система обробки сигналів

Вхідний сигнал x(t), спочатку подається на вхідний фільтр, функцією якого є обмеження сигналу частотою Найквіста (половина частоти дискретизації) для запобігання спотворень. Потім сигнал дискретизується АЦП зі швидкістю, визначеною тактовою частотою вибірки, для отримання вхідної дискретної послідовності x(n). Передавальна функція системи H(z), реалізує алгоритм ЦОС, тобто ставить у відповідність кожному значенню x(n) значення y(n). Вихідна дискретна вибірка y(n), перетворюється в сигнал безперервного часу y(t) за допомогою ЦАП і вихідного фільтру низьких частот [5].

Дискретизація сигналу, обчислення вихідної послідовності та вихідного аналогового сигналу повинно бути завершене протягом періоду дискретизації. Швидкість, з якою це можна зробити, визначає максимальну пропускну здатність, яку можна досягти в системі. Відносно низька швидкість більшості мікроконтролерів є головним обмеженням для використання їх в системах ЦОС, але висока швидкість виконання інструкцій мікроконтролером може забезпечити продуктивність, необхідну для реалізації систем з низькою пропускною здатністю. Крім того, вбудовані модулі АЦП та ЦАП забезпечують усі функції, необхідні для реалізації системи ЦОС на мікроконтролері.

Необхідно відзначити, що для усіх основних операцій ЦОС необхідним є виконання тільки базових арифметичних дій, а саме множення, ділення, додавання, віднімання та операції зсуву. Розрахунок вихідної вибірки y(n) згідно алгоритму ЦОС вимагає операції множення з накопиченням (MAC). Це, як правило, одноциклова інструкція для процесорів DSP, але для виконання стандартним мікроконтролером може знадобитися більше циклів, оскільки вона повинна бути реалізована в програмному коді [6]. Це суттєво обмежує сферу

використання мікроконтролерів додатками, що потребують меншої потужності обробки (з точки зору кількості операцій множення з накопиченням).

Вбудований в мікроконтролер АЦП у більшості випадків використовує схему вибірки і зберігання, яка утримує вхідну напругу на постійному рівні до закінчення процесу перетворення сигналу в цифрову форму. АЦП працює за принципом послідовного наближення, порівнюючи опорні рівні напруги з вхідним сигналом для отримання дискретної послідовності. Якщо потрібна підвищена швидкість перетворення, то можна знехтувати точністю, зчитуючи тільки старші біти дискретної послідовності з відкиданням молодших біт перетворення. Перетворення опрацьованої дискретної послідовності вхідного сигналу в аналогову форму відбувається шляхом використання вбудованого в мікроконтролер блоку формування широтно-імпульсної модуляції (ШІМ). Вихід ШІМ разом із зовнішнім згладжувальним фільтром забезпечує вихід ЦАП для системи. Форма ШІМ кодує потрібну амплітуду сигналу за допомогою співвідношення тривалостей імпульсів логічного «0» і логічної «1» свого виходу.

Отже, мікроконтролери можуть забезпечувати необхідну продуктивність для реалізації операцій ЦОС з низькою пропускною здатністю. Це означає, що використання таких пристроїв в системах ЦОС може мати перевагу за рахунок економії витрат та енергії, замінивши спеціалізовані компоненти, які зазвичай виконують такі завдання.

Література:

1. Айфичер Э. Цифровая обработка сигналов: практический подход / Э. Айфичер, Б. Джервис. – М. : Вильямс, 2004. – 992 с.

2. Солонина А. И. Основы цифровой обработки сигналов. Курс лекций: Учебное пособие / А. И. Солонина, Д. А. Улахович, С. М. Арбузов, Е. Б. Соловьева. – СПб. : БХВПетербург, 2005. – 768 с.

3. Лэй Э. Цифровая обработка сигналов для инженеров и технических специалистов / Э. Лэй. – М. : Группа ИДТ, 2007. – 336 с.

4. Pinto S.E. Compressive sensing in FPGA and microcontroller / S. Pinto, L. Mendoza, F. Elkin // International Journal of Engineering and Technology. – 2016. – 7(6). – Pp. 2202-2206.

5. AN219: Digital Signal Processing with the PIC16C74. Silicon Labs. [Електронний ресурс]. – Режим доступу до ресурсу: https://www.silabs.com/documents/public/application-notes/an219.pdf

6. AN4841: Digital signal processing for STM32 microcontrollers using CMSIS. STMicroelectronics. [Електронний ресурс]. – Режим доступу до ресурсу: https://www.st.com/resource/en/application_note/dm00273990.pdf

ВИКОРИСТАННЯ MACHINE LEARNING І AI У МУЗИЦІ

Рокитенко В.
Одеський національний політехнічний університет

Для створення штучного інтелекту, навчання штучного інтелекту для створення музики. Machine Learning. Artificial intelligence. Music. Magenta. Google. Sony.

Музичне мистецтво розвивалося протягом усієї історії людства. Роль музики в житті людей досить велика, вона здатна впливати на настрій. Також музика має величезний вплив на інтелектуальні здібності та можливості людини, адже мелодія музики сприяє збільшенню емоційної людської активності.

Для створення музичного штучного інтелекту потрібна програма, алгоритм якої буде використовувати базу знань музики та набір композицій, наприклад у формі бази даних або бібліотеки. Невід'ємною частиною цього стане сольфеджіо - дисципліна, що розвиває уміння слухати музику, також інтонаційно та ритмічно точно, виразно і свідомо створювати музичний текст. Важливим частиною бази знань є приклади композицій різних жанрів, але насамперед «класики».

Музичний штучний інтелект може мати 2 основні мети та функції, а саме створення нових звуків та створення нових композицій.

Перша функція – створення нових звуків.

Будь-які звуки – це механічні коливання з різною частотою та амплітудою. Кожна нота має свою фіксовану частоту та саме це визначає її звучання. Наприклад нота «Ля» має частоту в 440 Герц та є камертоном. Якщо змінювати частоту та поєднувати різні ноти, тобто комбінувати їх, ми зможемо отримати різні звуки, але не тільки відносно регістру, але й відносно звучання.

Друга функція – створення композицій.

Існує безліч музичних інструментів з різним способом створення звуку, а саме клавішні, струнні, духові, ударні та багато інших. Найкрасивішим вважається поєднання інструментів кожного виду в один єдиний симфонічний оркестр. У наш час, коли електронна музика набуває все більшої популярності є альтернатива класичному використанню музичних інструментів, а саме використання overdrive або перевантаження. Отож можна створити навіть новий жанр музики за допомогою штучного інтелекту.

Схожу технологію розробляли компанії Sony та Google.

Компанія Google запустила інструмент Magenta на основі технології машинного навчання. Сервіс можуть використовувати не тільки музиканти і художники, але також всі бажаючі поекспериментувати з цифровими технологіями. Родзинка проекту — поступове навчання штучного інтелекту творчості. Головна мета Magenta – просування можливостей штучного інтелекту для створення музики та образотворчого мистецтва. Друга, не менш важлива мета проекту — дати всім бажаючим новий інструмент, який вони зможуть використовувати на свій розсуд.

Компанія Sony почала займатися музикою, створеної за допомогою штучного інтелекту — йдеться про систему, що спроможна творити “музично гармонійну” партію ударних на основі інших інструментів в композиції. Для навчання системи штучного інтелекту в Sony зібрали дані 665 пісень різних жанрів, включаючи поп, рок та електронну музику. Алгоритми штучного інтелекту здатні генерувати звуки ударних на основі іншого музичного матеріалу, незалежно від темпу, ритму і тривалості композиції.

Література

1. 2019/03/27; «Искусственный интеллект и создание музыки»; URL : http://www.tadviser.ru/index.php
2. Алексей Бондаренко; 24.10.18; «Искусственный интеллект и музыка. Отберет ли компьютер работу у композиторов?»; URL : https://karabas.live/ai_music/
3. Офіційний сайт сервісу AIV A : URL : https://www.aiva.ai/
4. Офіційний сайт сервісу Magenta : URL : https://magenta.tensorflow.org/

АНАЛІЗ ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ АНСАМБЛІВ МОДЕЛЕЙ МАШИННОГО НАВЧАННЯ

Рудніченко М.Д., Гежа Н.І., Бєляєв К.О., Кузьмін А.Д.
Одеський національний політехнічний університет, Одеса

Анотація. У роботі наведено аналіз специфіки машинного навчання, для підвищення якості моделей. Запропоновано підхід, що базується на використанні моделей-ансамблів, складених з окремих моделей. У роботі наведені результати експериментального порівняння моделей-ансамблів зі звичайними моделями.
Ключові слова: штучний інтелект, машинне навчання, ансамблі моделей

Abstract. This paper describes a machine learning method for improving the model quality, which is based on separate models working in an ensemble. The relevance, working principle, and results of an experimental comparison between ensemble and other models conducted by authors was provided.
Keywords: artificial intelligence, machine learning, ensemble models

В даний час у сфері інформаційних технологій триває стрімкий розвиток машинного навчання, побудовані за даним напрямком математичні та комп'ютерні моделі запроваджуються у різноманітні сфери діяльності, такі як бізнес, фінанси, медицина, наука. Опираючись на вихідні дані моделей, вирішуються такі питання як: вибір бізнес-стратегії, передбачення фінансової кризи, постановка діагнозу пацієнту, класифікація шахрайських транзакцій. Через це, критично важливим є вибір, налаштування та використ-

тання алгоритмів, які найбільш якісно моделюють залежності між даними [1]. На практиці з множини моделей обирають саме ту, яка після тренування має найкращий результат за обраною метрикою. Цей метод дозволяє забезпечити вибір моделі, яка більше за інших підходить до виконання певної задачі. Але недоліками цього методу є той факт, що обрана модель може бути схильною до певного результату, або не добре узагальнювати свій досвід [2]. Задля вирішення цієї проблеми пропонується використовувати на практиці ансамблі, складені з декількох найкращих моделей. Результат на виході з ансамблю є зваженою сумою значень з виходів його складових, що є ефективними при застосуванні у задачах класифікації та регресії. За умови того, що складові алгоритми мають похибки на різних даних, цей метод знижає схильність моделі, дозволяючи досягти кращих результатів на малих наборах даних та потребує менше обчислювальних ресурсів для досягнення подібного результату на великих об'ємах даних [3]. На відміну від таких алгоритмів як AdaBoost, запропонований метод використовує ансамблі з декількох "сильних учнів", а не з багатьох "слабких учнів" [4]. Також, у запропонованому методі коефіцієнти при обчисленні результату залежать від якості кожної моделі. Авторами работи було проведено експериментальне порівняння ансамблів з іншими моделями за метрикою AUC ().

Табл. 1: Порівняння ансамблів та інших моделей

Модель	RF + XGB + SVM	XGB + SVM	RF	XGB	SVM	AdaBoost
AUC	0,953	0,950	0,945	0,937	0,924	0,915

Висновки. Запропонований метод машинного навчання дозволяє досягти більшої якості моделі, що підтверджується результатами проведених експериментів. Даний метод може бути практично використаний для покращення точності вирішення завдань класифікації та регресії.

Література:

1. Machine learning: the power and promise of computers that learn by example – London: The Royal Society, 2017. – 125 p.

2. Rashka S. Model Evaluation, Model Selection, and Algorithm Selection in Machine Learning / Sebastian Rashka. – Wisconsin: University of Wisconsin–Madison, 2018. – 49 p.

3. Dietterich T. Ensemble Methods in Machine Learning / T. Dietterich– Corvallis, 2000. – 15 p.

4. Schapire R. A Short Introduction to Boosting / Schapire E. Robert, Freund Yoav 1999. – 14 p.

АНАЛІТИЧНО-МАТЕМАТИЧНІ МОДЕЛІ ДЛЯ ДОСЛІДЖЕННЯ ПОЖЕЖНИХ РИЗИКІВ

Семенов С., Ємельяненко С., Штойко Б.
Львівський державний університет безпеки життєдіяльності

В роботі розкрито поняття ризику, проаналізовано основні методи та методики оцінювання ризиків для будівель і споруд громадського призначення. Пожежні ризики характеризують можливість реалізації пожежної небезпеки у вигляді пожежі та оцінюють її можливі наслідки. Для оцінювання ризиків необхідно знати прогнозовані значення небезпечних факторів пожеж (НФП), для цього потрібно використовувати методи та методики моделювання.

Ключові слова: пожежний ризик, методи, програми, оцінювання ризиків, небезпечні фактори

The paper describes the concept of risk, analyzes the basic methods and techniques of risk assessment for public buildings. Fire risks characterize the possibility of realization of a fire hazard in the form of a fire and evaluate its possible consequences. To estimate the risks, it is necessary to know the predicted values of hazardous fire factors, and to do this, use modeling techniques and techniques.

Keywords: fire risk, methods, programs, risk assessment, hazardous factors

В країнах Євросоюзу та інших передових країнах світу вже багато років поспіль зосереджують увагу на питаннях ризиків, адже у процесі будь-якої діяльності людини завжди наявний ризик.

Ризик – це імовірнісна величина, яка дозволяє оцінити та усвідомити небажані події, що можуть виникнути. Імовірність в математиці це кількісна величина, і застосування цього терміну пояснює кількісне визначення, яке суперечить уявленням, що склалися в науці і на практиці, як добуток імовірності небажаної події на її наслідки (збиток, шкода).

Ризик – це кількісна характеристика можливості реалізації конкретної небезпеки чи її наслідків, яка вимірюється у відповідних величинах [1]. Відзначимо, що кожну небезпеку може характеризувати багато різних ризиків, які оцінюють різні сторони та параметри цієї небезпеки. Наприклад, з однієї сторони, – частоту її реалізації, з іншої – характер і розміри наслідків реалізації небезпеки.

Стосовно пожежного ризику то його оцінювання полягає в розрахунку індивідуального пожежного ризику для мешканців, персоналу і відвідувачів у будівлі чи споруді громадського призначення. Числовим вираженням індивідуального пожежного ризику є частота впливу НФП на людину, що перебуває в будівлі чи споруді. Частоту впливу НФП визначають для пожежонебезпечних ситуацій, які характеризуються найбільшою небезпекою для життя та здоров'я людей у будівлі.

Дослідженням пожежних ризиків присвячені праці багатьох науковців, серед яких Н. Н. Брушлінський, В. В. Холщєвніков, С. В. Пузач, Ю. А. Кошмаров, В. Бєгун, І. К. Бакиров, Є. М. Гуліда, Д. А. Самошин, О. Я. Корольченко, З. М. Яремко, В. М. Ярошевська, Ю. Н. Шебеко, Ф. Ш. Хафізов, Д. В. Сєдов, D. Yung, T. Aven, T. Barry, S. Jonkman, I. Miller, P. Janik та ін. Але більшість їх наукових праць не стосувалися громадських будівель.

Для оцінювання ризиків можна використовувати наступні програми, а саме: «СИТИС [2]: Флоутек ВД», «СИТИС: Блок», «СИТИС: ВИМ» і «СИТИС: Спринт», «ЭПОС: Индилайн 1.01». Вони дозволяють визначити пожежні ризики в будівлях і спорудах різних класів функціональної пожежної небезпеки.

«СИТИС: Флоутек ВД» – програма для моделювання процесу евакуації, яка базується на основі аналітично-математичної моделі руху людського потоку або імітаційно-стохастичній моделі.

«СИТИС: Блок» – програма для визначення критичного часу пожежі, часу блокування евакуаційних виходів, яка розраховує динаміку розвитку небезпечних фокторів пожежі за двох-зонною моделлю CFAST.

«СИТИС: ВИМ» – програма для визначення критичного часу пожежі, часу блокування евакуаційних виходів з врахуванням систем димовидалення та підпору повітря, яка базується на розрахунку динаміки розвитку небезпечних факторів пожежі за інтегральною моделлю розвитку пожежі в будівлі і ймовірнісною моделлю розповсюдження пожежі за площею.

«СИТИС: Спринт» – програма призначена для розрахунку індивідуального пожежного ризику, аналізу результату евакуації людей із будівель і часу блокування шляхів евакуації небезпечними факторами пожежі.

Для розрахунку евакуації також використовують програмне забезпечення «ЭПОС: Индилайн 1.01», яке використовує розрахунковий модуль FDS5-evac «Імітаційно-стохастична модель руху людських потоків», часу блокування шляхів евакуації небезпечними факторами пожежі «Польовий метод моделювання пожежі в будівлі», величину пожежного ризику в будівлі. Графічна оболонка «ЭПОС: Индилайн 1.01» дозволяє будувати гідродинамічну модель з розрахунком тепломасопереносу при горінні розрахунковим модулем FDS5. На гідродинамічну модель накладаються моделі евакуаційних процесів. Будується система евакуації, яка визначається в поєднанні з розрахунком тепломасопереносу під час горіння, з допомогою інтегрованого модуля FDS5+evac, що дозволяє оцінити різноманітні сценарії евакуаційних процесів різних масштабів числом, графічно і наочно. «ЭПОС: Индилайн 1.01» вираховує молекулярну частку одного чи декількох компонентів газу в даній точці потоку.

PyroSim – це програма, яка містить користувацький графічний інтерфейс для моделювання динаміки развитку небезпечних факторів пожежі польовим методом на основі Fire Dynamics Simulator (FDS).

Програма FDS (Fire Dynamics Simulator) реалізує розрахункову гідродинамічну модель тепломасопереносу при горінні [3]. FDS розв'язує рівняння Нав'є-Стокса для низькошвидкісних температурно-залежних потоків. Особливу увагу програма приділяє розповсюдженню диму і теплопередачі під час пожежі.

Smokeview – це програма, яка слугує для відтворення результатів FDS у вигляді анімаційних зображеннь. Програма має здатність візуально моделювати вогонь і дим. Трьохвимірне зображення фізичної моделі дає можливість оцінити видимість у межах зображуваних приміщень.

Модель CFAST призначена для оцінки динаміки небезпечних факторів пожеж в житлових, громадських і промислових будівлях та спорудах. Також модель може використовуватись для визначення розрахункових параметрів протипожежних систем – протидимної природньої чи штучної вентиляції, пожежної сигналізації. CFAST для розрахунку використовує двохзонну модель, яка ефективніше, ніж інтегральна, моделює пожежі у будівлях і визначає граничний час настання її небезпечних факторів, що дозволяє встановити необхідний час слідування пожежно-рятувальних підрозділів до місця виклику і необхідний час евакуації, який забезпечить безпеку для людей.

Отже, ризик-орієнтовні підходи дозволяють визначати значення пожежних ризиків і оцінювати їх рівень. Відомі моделі та програми для обчислень значень пожежних ризиків за відповідної адаптації можуть використовуватися для оцінювання ризиків в громадських будівлях.

Література:

1. 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.

2. Sitis Руководство пользователя [Електронний ресурс]. – Режим доступу : http://sitis.ru/media/documentation/PRS-RP-2012-1.pdf

3. Програма FDS (Fire Dynamics Simulator) [Електронний ресурс]. – Режим доступа : http://fds.sitis.ru/docs/FDS_5_User_Guide.pdf

Напрям 13

Технології візуалізації даних

IMSMA, ЯК СИСТЕМА ВІЗУАЛІЗАЦІЇ ДАНИХ

Баша К., Нікітчин В.
Львівський державний університет безпеки життєдіяльності

З розвитком інформаційних технологій і зростанням можливостей комп'ютерних систем багато світових дослідників відкрили нові перспективи, які світу відкриває прогрес. Комп'ютер дозволяє оживити статичні дані, зробити їх зручними для аналізу і дослідження, представити інформацію в новому розрізі.

Технології графічного представлення інформації переживають період бурхливого розвитку і на даний момент серед них можна виділити 3 ключових напрямки:

· Візуалізація даних;
· Інфографіка;
· Подання знань.

Візуалізація даних в інформаційних системах підвищує ефективність їх вивчення людиною і знаходить широке застосування в наукових дослідженнях, прогнозуванні, бізнес-аналізі і аналітичних оглядах.

Іншими словами, це - спосіб представлення даних, який спрощує і покращує їх сприйняття людиною. У візуалізації даних може бути два різновиди: дослідницька та презентаційна.

Візуалізація даних щодо досліджень наводить дані у вигляд, що пропонує досліднику нові питання і можливості їх спостереження, а значить, і завдання перед дослідницькою візуалізацією стоять інші:

· Допомогти сформулювати нові питання за наявними даними;
· Показати відносність візуалізованими даних;
· Забезпечити масштабованість від загальних до детальних уявлень даних;
· Уявити дані в прив'язці до контексту.

Одним із пріоритетних напрямків діяльності Державної служби України з надзвичайних ситуацій є виконання робіт, пов'язаних з пошуком, знешкодженням та знищенням вибухонебезпечних предметів на території держави.

Проте, якщо раніше піротехніки Служби порятунку виявляли та знешкоджували лише боєприпаси минулих війн, то у зв’язку з проведенням на Сході України антитерористичної операції, піротехнічні підрозділи розпочали роботи зі знешкодження сучасних та особливо небезпечних боєприпасів. Питання оперативної та безпечної роботи піротехніків та екіпіру-

вання їх сучасними засобами захисту під час роботи на звільнених територіях східних регіонів є нині досить актуальним. Саме тому, в Державній службі України впровадили систему управління інформацією з протимінної діяльності (IMSMA). Вказана система дозволяє підвищити можливість піротехнікам управляти ризиками і загрозами населенню та інфраструктури від вибухонебезпечних предметів, а також оптимізувати збір та обробку інформації стосовно місць розташування боєприпасів, проведення заходів щодо їх знешкодження та встановлення безпечних територій. Кожна піротехнічна група після проведення робіт з розмінування місцевості, звітує про виконання робіт вказуючи GPS координати територій які розміновані та підлягають розмінуванню. Інформація заноситься в загальну базу даних IMSMA після чого керівництво з протимінної діяльності візуально в режимі он-лайн може спостерігати, контролювати та в будь-який момент надати інформацію щодо забруднення територій вибухонебезпечними предметами.

Підбиваючи підсумок, варто сказати, що візуалізація даних за допомогою системи IMSMA, підвищила оперативну діяльність та швидкість донесення інформації щодо територій забруднених вибухонебезпечними предметами.

Література:

1. Електронний ресурс: https://www.mineactionstandards.org

ТЕХНОЛОГІЇ ВІЗУАЛІЗАЦІЇ ДАНИХ

Воврик В., Сторощук О., Яремко З.
Львівський національний університет імені Івана Франка

Візуалізація – це метод подання інформації у вигляді оптичного зображення (наприклад, у вигляді рисунків, фотографій, графіків, структурних схем, діаграм, таблиць, карт тощо). Візуальна інформація краще сприймається і дозволяє швидко й ефективно донести до глядача власні думки та ідеї. Застосування візуалізації даних є також важливою в системі охорони і забезпечення безпеки на підприємствах, заводах та інших закладах. Численні дослідження підтверджують, що:

- 90 % інформації людина сприймає через зір;
- 70 % сенсорних рецепторів знаходяться в очах;
- близько половини нейронів головного мозку людини задіяні в обробці візуальної інформації;
- на 19 % менше при роботі з візуальними даними використовується когнітивна функція мозку, що відповідає за обробку та аналіз інформації;
- на 17 % вища продуктивність людини, що працює з візуальною інформацією;
- на 4,5 % краще згадуються докладні деталі візуальної інформації;
- в 60 000 разів швидше сприймається візуальна інформація в порівнянні з текстовою;
- 10 % людина запам'ятовує з почутого, 20 % – з прочитаного, і 80 % – з побаченого і зробленого;
- на 323 % краще людина виконує інструкцію, якщо вона містить ілюстрації.

Візуалізація є інструментом для показу даних; спонукає глядача замислитися про суть, а не методології; сприяє уникненню спотворення того, що повинні сказати дані; відображення багатьох чисел на невеликому просторі; показу великого набору даних одним цілим; спонукання глядача порівнювати фрагменти даних; служіння досить чітким цілям: опису, дослідженню, упорядкуванню. Особливо ефективно візуалізація використовується при відображенні природно невидимої інформації (наприклад, розподілу густини населення, просторового розподілу електромагнітного поля, температури, густини тощо). Вивчення зображень дозволяє досліджувати просторові структури об'єктів. На візуалізації базується писемність, вона нерозривно пов'язана з розвитком символьного та образного мислення.

Багато сучасних засобів аналізу даних дозволяють будувати сотні типів різних графіків та діаграм. За дотримання умов, вказаних при візуалізації інформації, могли б значно скоротитися травми та інциденти на робочих місцях. Тому вибір методу візуалізації може виявитися доволі склад-

ним завданням для дослідника. Основні принципи компонування візуальних засобів подання інформації:

- принцип лаконічності;
- принцип узагальнення та уніфікації;
- принцип акцентування на основних змістовних елементах;
- принцип автономності;
- принцип структурності;
- принцип стадійності;
- принцип використання звиклих асоціацій та стереотипів.

Аналіз досліджень у галузі візуалізації даних дозволив виокремити такі критерії класифікації технологій візуалізації:

- тривалість даних в часі;
- масштаб явища, що аналізується;
- використана система координат;
- вид зображення;
- формат зображення;
- спосіб обробки даних перед візуалізацією;
- тип даних;
- ступінь віртуалізації;
- активність користувача.

Необхідно зазначити два напрямки розвитку систем візуалізації даних. Перший – розроблення універсальних засобів візуалізації. Другий – спеціалізація за усіма напрямками, включно зі створенням спеціальних графічних станцій з реалізацією графічного алгоритмічного та програмного забезпечення. На сьогодні створено достатньо велику кількість пакетів прикладного програмного забезпечення для моделювання та візуалізації результатів моделювання у фізиці, хімії та інших прикладних областях. Зазвичай ці пакети достатньо складні та великі за об’ємом.

Задачі візуалізації даних зустрічаються практично в усіх предметних областях наукових досліджень. Отже, можна зробити висновок про актуальність та перспективність використання технологій візуалізації даних в охороні праці.

Література:

1. Кожем'яко В. П. Візуалізація як унікальна інформаційно-інтелектуальна технологія, оптико-електронні інформаційно-енергетичні технології. – 2014. – №2(28). – С. 5-16.

2. Гладун О. Візуалізація інформації: інфографіка / Ольга Гладун // Вісник ХДАДМ. – 2012. – №4. С.11-14

3. Edward R. Tufte. The Visual Display of Quantitative Information. – Cheshire, Connecticut: Graphics Press, 2001. – 200 p.

ПОБУДОВА КОМПОЗИЦІЙНОГО ВЕБ-ДОДАТКУ АНІМАЦІЙНОЇ СТУДІЇ

Думич Н.І., Смотр О.О.
Львівський державний університет безпеки життєдіяльності

Роботу присвячено розгляду можливостей композиційних веб-додатків та, зокрема, композиційного веб-додатку анімаційної студії.

Ключові слова: композиційний веб-додаток, mashup, анімаційна студія.

This paper deals with the possibilities of composite web applications and, in particular, the animation studio composite web application.

Key words: composite web application, mashup, animation studio.

В наш час, час – неймовірного темпу життя, час – зростання емоційного навантаження все більш актуальною стає проблема рекреаційної діяльності людини, необхідність у повноцінному відпочинку, що надає змогу відновити фізичні та психологічні сили. При цьому вважається, що рекреаційний ефект досягнуто у випадку, коли людина починає відчувати стан психофізіологічного комфорту та готовність до нових навантажень. Таке завдання на сьогодні вирішують численні анімаційні студії. Сучасна анімація – це діяльність розробки та здійснення спеціальних програм проведення вільного часу [1].

Кількість та різноманіття анімаційних студій на ринку невпинно зростає. Причому, спектр послуг, які вони надають, їх вартість та якість мають широкий розкид по діапазону цін та шкалі якісних характеристик. З огляду на що, клієнту (замовнику анімаційних послуг), доводиться затрачати чимало часу для того, щоб проаналізувати усю інформацію, що надається анімаційними студіями та їх клієнтами (відгуки клієнтів) та обрати саме те, що найбільше влаштовувало б його. Отже, клієнту потрібна можливість швидкого та зручного перегляду пропозицій різних анімаційних студій з можливістю порівняння їх сервісів, цінової політики, якості надання послуг та можливості надання цих послуги в потрібному місці розташування та часовому діапазоні тощо. На нашу думку, надати таку можливість клієнту можна, побудувавши композиційний (mashup) веб-додаток.

Композиційний веб-додаток (mashup) – це додаток, що комбінує в собі контент з різних джерел, такий собі гібрид веб-додатків [2]. Для прикладу, mashup – це синдикація інформаційних каналів (обмін потоками RSS-даних), це – використання Google Map на своєму сайті тощо.

Для специфікації веб-сервісів і їх композицій можна застосовувати графічні, текстові, формальні і ін. способи. Основна відмінність композиційного веб-додатка від веб-сервісів, що використовують динамічну генерацію контенту на стороні сервера технологіями Java, CGI, PHP або ASP, полягає в тому, що mashup контент може генеруватися на стороні браузера клієнта через клієнтські сценарії. Логіка генерації контенту на стороні клієнта – це комбінація коду вбудованого прямо в mashup веб-сторінку [3].

З огляду на наведене вище, ми вважаємо, що створення композиційного веб-додатку анімаційних студій включає в себе рішення одразу декількох проблем, таких як обробка даних одразу з декількох ресурсів, аналіз і вибір необхідного, комбінація отриманої інформації. Комбінуючи різноманітні дані (фото, відео, текстову інформацію) анімаційних студій, щодо їх сервісів, з відгуками людей про отримані послуги від цих студій з використанням карт Google Map та нанесенням на них інформації щодо розташування анімаційних студій можна створити унікальний веб-сервіс з функціональністю, що не передбачало жодне джерело.

Література

1. Килимистий С.М. Класифікація видів анімаційної діяльності. Міжнародний вісник: культурологія, філологія, музикознавство. - 2015. - Вип.II (5). – С.77-83.

2. Habr. Создаем современное веб приложение. [Електронний ресурс]. – Режим доступу до ресурсу: https://habr.com/ru/post/6586/

3. Головатий Р. Основи графічного дизайну та проекної графіки. – 2019, – 80с.

ВІЗУАЛІЗАЦІЯ ДАНИХ: ОСНОВНІ ПЕРЕВАГИ

Кичма А., Олеха С., Полотай О.
Національний університет «Львівська політехніка»

Використання візуальних елементів, наприклад, діаграм, карт, графіків, забезпечує доступний спосіб бачити та розуміти тенденції, формати та структури даних. Метою даної роботи є дослідження важливості використання інструментів та технологій візуалізації даних для аналізу величезної кількості інформації та прийняття керованих рішень.

Ключові слова: візуалізація даних, структура даних, інформація

The use of visual elements, such as diagrams, maps, graphs provides an accessible way to see and understand trends, formats and data structures. The purpose of this work is to investigate the importance of using data visualization tools and technologies to analyze a wealth of information and make managed decisions.

Keywords: data visualization, data structure, information

Візуалізація даних є іншої формою мистецтва, яка захоплює наш інтерес і зупиняє погляд на певному повідомленні. Візуалізація даних стає все більш ключовим інструментом для осмислення трильйонів рядків даних, що генеруються щодня. Візуалізація даних допомагає розказувати історії, збираючи дані у форму, яка є простішою і цікавішою для розуміння, при цьому підкреслюючи тенденції та передумови. Правильна і хороша візуалізація розказує історії, прибираючи не потрібну інформацію і підкре-

слюючи інформацію, яка є цікавою та корисною. Однак ефективна візуалізація даних має тонку межу балансування між формою та функцією. Дані та візуальні матеріали повинні доповнювати одні одних, при цьому поєднуючи аналіз інформації з чудовою та цікавою розповіддю.

Кожний напрямок професійних галузей має вигоду з розуміння візуалізації даних. Чим краще ви зможете передати свою точку зору візуально, тим краще ви зможете використовувати цю інформацію. Для професіоналів все більш цінним є можливість використовувати дані для прийняття рішень і використовувати візуальні матеріали для розповіді. У той час як традиційна освіта, як правило, виводить чітку межу між творчою розповіддю і технічним аналізом, сучасний професійний світ зараз цінує тих, хто може поєднувати дві: візуалізація даних знаходиться в середині аналізу та візуальної розповіді.

Візуальна інформація краще сприймається і дозволяє швидко та ефективно донести до глядача власні думки та ідеї. Сприйняття візуальної інформації є основною для людини. Дослідження підтверджують, що 90% інформації людина сприймає через зір, і на 17% вищою є продуктивність людини, яка працює з візуальною інформацією. Візуальна інформація зменшує інформаційне перевантаження людини і утримує його увагу. Едвард Тафті, автор одних з найкращих книг по візуалізації, описує її як інструмент для показу даних; спонукання глядача замислитись про суть, а не методології; спонукання глядача порівнювати фрагменти даних.

Правильна візуалізація повинна бути поєднана з правильним набором інформації. Для того, щоб представити дані цікавими та ефективними способами, існує декілька методів візуалізації даних: таблиці, графіки, карти, діаграми, панелі приладів, матриці, гістограми. Приклади декількох методів зображено на рис.1.

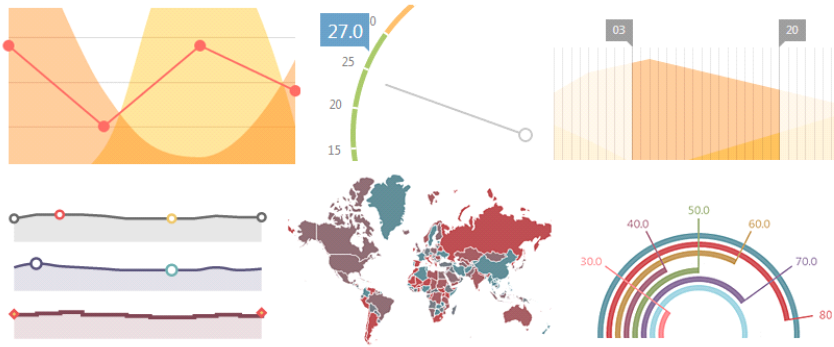


Рис.1. Методи візуалізації

Успіх візуалізації залежить від правильності її застосування, тобто від вибору типу графіка, його оформлення та використання. Відповідно до рис.2, 60% успіху візуалізації даних залежить від вибору типу графіка, 30% - від його правильного використання та 10% - від його оформлення.

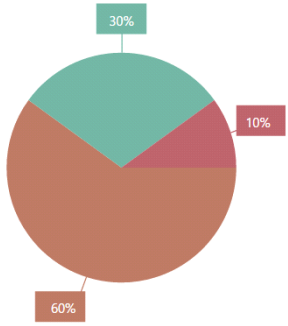


Рис. 2. Структура візуалізації даних

Отже, візуалізація даних – це потужний інструмент донесення думок та ідей до інших людей, який допомагає сприймати та аналізувати дані. При вмілому застосуванні, візуалізація даних дозволяє зробити матеріал цікавим і незабутнім.

Література

1. What is data visualization? – [Електронний ресурс]. – Режим доступу: https://www.tableau.com/learn/articles/data-visualization
2. Як і для чого використовувати візуалізацію даних? – [Електронний ресурс]. – Режим доступу: http://eidos.org.ua/novyny/yak-i-dlya-choho-vykorystovuvaty-vizualizatsiyu-danyh/
3. 13 Scientific Reason Why Your Brain Craves Infographics. – [Електронний ресурс]. – Режим доступу: https://neomam.com/interactive/13reasons/

РОЗРОБКА ЗАСОБІВ ВІЗУАЛІЗАЦІЇ ОПЕРАЦІЙ НАД ЗВ'ЯЗНИМИ СТРУКТУРАМИ ДАНИХ В СЕРЕДОВИЩІ PHARO

Кормушин Я.К., Ярошко С.А.
Львівський національний університет імені Івана Франка, м. Львів

Ключові слова: розріджена матриця; зв'язна структура даних; відображення даних; відображення операцій над даними; засоби Pharo; мова Smalltalk.
Keywords: sparse matrix; linked data structure; data visualization; data operations visualization; Pharo; Smalltalk.

В інформатиці *зв'язна структура даних* - це структура даних, яка складається з набору записів даних (вузлів), пов'язаних між собою посиланнями. Зв'язні структури даних включають пов'язані списки, дерева пошуку, дерева виразів та багато інших широко використовуваних структур даних. Вони також є ключовими складовими для багатьох ефективних алгоритмів, таких як топологічне сортування [1] та встановлення об'єднання-пошуку. [2]

Розріджена матриця - одна з багатьох зв'язних структур, які використовують для вирішення сучасних задач. Вона корисна в комбінаториці і прикладних областях, таких як мережева теорія, які мають низьку щільність значущих даних або з'єднань. Системи рівнянь з розрідженими матрицями виникають, зокрема, в задачах аналізу міцності конструкцій у цивільному та промисловому будівництві, в авіабудуванні, ракетобудуванні, суднобудуванні, де застосовується метод скінченних елементів.

Вагому роль в таких областях відіграють розріджені матриці, які дозволяють зберігати лише певну частину даних, тим самим зменшуючи час виконання обчислень та обсяг пам'яті, необхідний для їх збереження.

Існує багато способів реалізації зв'язних структур даних, кожен з яких має свої переваги та недоліки. Деякі з них мають доволі складну внутрішню реалізацію, а їх формальний опис зрозуміти важче, ніж їх графічну репрезентацію. Відповідно до збільшення складності внутрішньої структури таких даних зростає складність реалізації операцій над ними, наприклад додавання чи множення для розріджених матриць, або злиття двох дерев пошуку.

Мета завдання полягає в тому, щоб спроектувати і реалізувати пакет, який дозволить виконати наступне:

- надасть змогу візуалізувати будь-яку зв'язну структуру і операції над нею з мінімальними доповненнями до існуючого коду цієї структури;
- допомогти людям, не знайомим з певною зв'язною структурою даних, зрозуміти її внутрішню реалізацію та алгоритми операцій над нею;
- допомогти в пошуку помилок в коді за допомогою наглядного спостереження на його виконанням;
- налагоджувати і оптимізувати існуючі алгоритми.

Візуалізація операцій над цими структурами передбачає відображення на екрані візуалізацій структур даних, над якими відбувається операція, тобто однієї структури для унарних операцій, двох – для бінарних операцій, відповідного результату, а також допоміжних елементів, які використовуються під час обчислень. Допоміжними елементами можуть виступати тимчасові

масиви, в яких зберігаються проміжні результати, інше забарвлення вузлів, які розглядаються в певний момент часу, та допоміжні текстові вказівки.

Pharo — це сучасна повнофункціональна реалізація середовища мовою Smalltalk з відкритим вихідним кодом [5]. *Smalltalk* — об'єктно-орієнтована мова програмування з динамічною типізацією, розроблена у 1970-х роках. Smalltalk продовжує активно розвиватися завдяки співтовариству користувачів і розробників.

Засобів для відображення операцій над зв'язними структурами даних у бібліотеках Pharo Smalltalk немає, а їх наявність покращить вивчення цих структур і алгоритмів, що над ними діють, зокрема додавання, множення тощо.

Roassal – це гнучкий програмний засіб, створений для візуалізації та взаємодії з довільними даними, визначеними на основі об'єктів та їх зв'язків. Roassal зазвичай використовується для створення інтерактивної візуалізації, а діапазон його застосування різноманітний [3, 4].

Smalltalk – рефлексивна мова програмування. Це означає, що програми здатні «відобразити» своє власне виконання та структуру. З програмної точки зору це означає, що метаоб'єкти системи виконання можна змінювати як звичайні об'єкти, які можна зчитувати і перевіряти. І навпаки, у Smalltalk можна модифікувати метаоб'єкти та відобразити ці зміни назад у систему виконання. Це також називається заступництвом (або посередництвом) і підтримується головним чином мовами динамічного програмування і лише в дуже обмеженій мірі статичними мовами. Програма, яка здатна маніпулювати іншими програмами (або навіть собою) називається *метапрограмою*.

Клас *MetaLink* пакету *Reflectivity* в Pharo – це одна з основних складових цілої системи, яка розширює можливості рефлексії в Pharo. За допомогою цього класу та інших допоміжних компонент пакету можна додавати анотації до вузлів абстрактного синтаксичного дерева. Анотований вузол розкривається, компілюється і виконується на льоту.

Таким чином, за допомогою пакету Reflectivity та візуалізаційного двигуна Roassal можна створити відображення операції над зв'язними структурами даних під час її виконання в реальному часу. Більше того, таке поєднання дозволяє нам проводити зміну даних під час виконання операції і впливати на результат.

Література:

1. Donald Knuth. The Art of Computer Programming. – К. : Addison-Wesley, 1968.
2. B.Galler, M.Fisher журнал «Communications of the ACM», №7, 1964.
3. Bergel Alexandre. Agile Visualization: Roassal – http://agilevisualization.com/AgileVisualization/Roassal/0104-Roassal.html.
4. Bergel Alexandre. Agile Visualization First Edition. – К. : Alexandre Bergel, 2016.
5. Bergel Alexandre. Deep into Pharo. – К. : Square Bracket Associates, 2013.
6. Tymchuk Yuriy Concurrent Programming in Pharo. – 4 August 2014 р. – http://pillarhub.pharocloud.com/hub/Uko/concurrentProgrammingInPharo.

УДК 004.032.26; 004.855.5.

ПЕРЕТВОРЕННЯ НЕЙРОННИХ МЕРЕЖ ДЛЯ ЗАПУСКУ НА МІКРОКОНТРОЛЕРАХ СІМЕЙСТВА STM32

Протасеня П., Малець Р.
Львівський національний університет імені Івана Франка, Львів

Задача запуску об'ємної нейронної мережі на пристрої з малою ємністю, такому як мікроконтролер, потребує в свою чергу вирішення такої задачі як перетворення моделі мережі на значно меншу, аналогічну до неї. Для досягнення цього необхідна квантизація усіх операцій чи ваг, прунинг та стиснення ваг мережі. Варто врахувати, що кожна операція може негативно вплинути на точність мережі. Також існує похибка переходу від сучасних, 64-розрядних процесорів до 32-розрядних серії ARM Cortex M4 або M7, котрі присутні у мікроконтролерах серії STM32. Такий перехід приводить до втрати продуктивності, котру можна компенсувати квантизацією мережі.

У процесі розробки TensorFlow Lite постало питання запуску та використання технології нейронних мереж на мобільних пристроях,. Власне такі нейронні системи дозволили б виконувати задачі, для котрих важлива точність припущень та котрі можуть вирішувати такі повсякденні проблеми, як розпізнавання об'єктів на фото. Назагал, це можна звести до доволі простого процесу: зняти фото та обробити його ж на місці. Проте, сучасні мобільні пристрої не є найкращими претендентами для виконання таких задач через те, що не кожен такий пристрій може похвалитись довгим терміном роботи акумулятора. Тому постає задача переносу цих нейронних систем на менш енерговитратні пристрої — мікроконтролери. Для використання нейронних систем на пристроях з малим обсягом пам'яті необхідно стиснути такі мережі до достатньо малого розміру.

Варто зазначити, що при трансформації мережі у сумісну з мікроконтролерами, може з'явитись похибка порядку 10^{-8}. Вона зумовлена переходом від 64-розрядної розмірності дійсного числа моделі до 32-розрядної розмірності такого числа. Для моделей з більшою розрядністю, похибка припущень без стиснення ваг може сягати і 10^{-6}.

Одним із способів скорочення та підвищення продуктивності нейронної моделі є квантизація — зведення операцій над дійсним числом до операцій над 8-розрядним цілим. Такий метод можна використати як над усіма математичними операціями в моделі, так і лише над вагами мережі. У випадку повної квантизації передбачається вкорочення розміру мережі в чотири рази та зріст продуктивності у понад три рази, у випадку виконання операції лише над вагами зріст продуктивності значно менший - приблизно від двох до трьох разів.

Другим способом є прунинг нейронних мереж — викидання маловагомих зв'язків та ваг. Недоліком такого методу є, очевидно, втрата точності, проте таким чином можна вкоротити кількість ваг з 24 мільйонів до 3 мільйонів, втративши притому 4% точності.

Стиснути та перетворити нейронну мережу до достатньо малих розмірів також допоможе пакет програмного забезпечення X-Cube-AI. Перевага цього пакету полягає у підтримці ним усіх пристроїв сімейства STM32, що містять у собі процесор Cortex M7 або Cortex M4, та фізично можуть запустити обрану нейронну модель (тобто, достатньо оперативної та flash-пам'яті). X-Cube-AI дозволяє стиснути мережі Keras (до версії 2.2.4), Caffe (версії 1.0), Lasagne (версії 0.2-dev), ConvnetJS (версії 0.3 з npm) та TensorFlow Lite.

Пакет пропонує наступні підходи до оптимізації нейронної системи:

- Стиснення ваг. Підхід виконання такої оптимізації не використовує жодних тестових наборів даних, і відповідно може привести до втрати точності порівняно з вихідною моделлю. Звісно, якщо стиснення не відбувається, то, ймовірно, точність отриманих припущень буде складати щонайменше 10^{-8}. Застосовують алгоритм спільного використання ваг. Стиснення накладається лише на щільний тип шару (у Keras, шар "Dense"). Перевагою цього підходу є його швидкість, проте може втрачатись точність моделі.
- Злиття шарів тензорів. При генерації оптимізованої мережі, деякі операції зливають одне з іншим. Наприклад, операції pool та conv.
- Єдиний буфер функцій. Для зменшення навантаження на RAM, пакет вводить в згенеровану бібліотеку роботу з єдиним буфером функцій. Він використовується у виконанні операцій з кожного шару мережі, і відповідно, його розмір визначає максимальна необхідна для обчислення припущень кількість ресурсів.

Для демонстрації роботи пакета, було натренована проста мережа на основі набору даних MNIST, на основі технології Keras. Таку мережу, із максимально допустимим стисненням ваг (до 1/8 розміру), можна було встановити на мікроконтролер Nucleo F401RE. У порівнянні з такою ж у повному обсязі та на ПК, було втрачено приблизно 2% від точності припущень, а швидкість обчислення припущень складала 485 мс на Nucleo F401RE, та 17 мс на ПК.

Література:

1. ST. Getting started with X-CUBE-AI Expansion Package for Arti_cial Intelligence (AI) / ST // User Manual UM2526 Режим доступу до ресурсу: https://www.st.com/en/embedded-software/x-cube-ai.html#resource

2. Goodfellow-et-al-2016. Deep Learning / Ian Goodfellow and Yoshua Bengio and Aaron Courville // MIT Press 2016 Режим доступу до ресурсу: http://www.deeplearningbook.org

3. Google Research. TensorFlow:Large-Scale Machine Learning on Heter-

ogeneous Distributed Systems / Mart__n Abadi, Ashish Agarwal, Paul Barham, Eugene Brevdo, Zhifeng Chen, Craig Citro,Greg S. Corrado, Andy Davis, Je_rey Dean, Matthieu Devin, Sanjay Ghemawat, Ian Goodfellow,Andrew Harp, Geo_rey Irving, Michael Isard, Yangqing Jia, Rafal Jozefowicz, Lukasz Kaiser,Manjunath Kudlur, Josh Levenberg, Dan Man_e, Rajat Monga, Sherry Moore, Derek Murray,Chris Olah, Mike Schuster, Jonathon Shlens, Benoit Steiner, Ilya Sutskever, Kunal Talwar,Paul Tucker, Vincent Vanhoucke, Vijay Vasudevan, Fernanda Vi_egas, Oriol Vinyals,Pete Warden, Martin Wattenberg, Martin Wicke, Yuan Yu, and Xiaoqiang ZhengGoogle Research // Preliminary White Paper _ 9 листопада 2015. Режим доступу до ресурсу: http://download.tensor_ow.org/paper/whitepaper2015.pdf

4. Chollet. Keras / Chollet, Fran_cois and others // Режим доступу до ресурсу: https://keras.io – 2015

5. Alex Clark. Pillow (PIL Fork) / Alex Clark та вкладники (PIL зроблено Fredrik Lundh та вкладники) // Режим доступу до ресурсу: https://pillow.readthedocs.io/en/stable/index.html

6. LeCun, Yann and Cortes, Corinna. MNIST handwritten digit database / LeCun, Yann and Cortes, Corinna // Режим доступу до ресурсу: http://yann.lecun.com/exdb/mnist/ _ 28 червня 2010

7. ST. Neural Networks on STM32 Arti_cial Intelligence Solutions / ST // Режим доступу до ресурсу: https://www.st.com/resource/en/product_presentation/stm32cubeai_press_pres.pdf – версія 1.1 _ 2019

8. ST. STM32 and STM8 embedded software solutions / ST // Режим доступу до ресурсу: https://www.st.com/resource/en/product_presentation/stm32-stm8_embedded_software_solutions.pdf – версія 7.7 – лютий 2019

ПРОЕКТ ІНТЕЛЕКТУАЛЬНОЇ РЕКОМЕНДАЦІЙНОЇ СИСТЕМЫ ВІЗУАЛІЗАЦІЇ БАГАТОМІРНИХ ДАНИХ

Рудніченко М.Д., Тіщенко С.Є., Ярчук О. О., Войцеховський А. С.
Одеський національний політехнічний університет, Одеса

Анотація. В роботі наведено опис концепції проекту рекомендаційної системи для вибору інструментів візуалізації даних, розробленої на базі нейронних мереж з використанням машинного навчання
Ключові слова: візуалізація даних**,** рекомендаційна система, аналіз даних.

Abstract. The paper describes the concept of the project of recommendation system for selecting data visualization tools developed based on the neural networks using machine learning.
Keywords: data visualization, recommendation system, data analysis.

В умовах швидкого збільшення кількості інформації, її урізноманітнення та загального пришвидшення життя актуальності набрало питання представлення даних, їх сприйняття та засвоєння. Зокрема, як у науковій, так і у інформаційній областях набула ваги тематика візуалізації багатомірних даних великих обсягів[1]. Відповідно до проведених досліджень, 90% інформації людина сприймає через очі. Зорова інформація запам'ятовується на 80%, тоді як, наприклад, слухова – лише на 10%. До того ж, продуктивність працівника при використанні візуальної інформації підвищується на 17% [2].

Однак, поширеність використання графічно представлених даних призвела до появи значної кількості способів їх зображення, а також програм та веб-сайтів, що програмно реалізують відповідні функції, однак не поєднують ряд необхідних функцій автоматизації підтримки прийняття рішень аналітиком. У зв'язку з цим виникає необхідність розробки власного програмного застосування, що буде рекомендувати типи й методи реалізації візуального представлення наданого набору даних. Ця програма повинна містити наступні компоненти: модуль аналізу взаємозв'язків набору даних; модуль аналізу проблем та задач, для розв'язання яких використовуються дані; модуль відстеження та аналізу відповідних застосувань та веб-сайтів для реалізації візуалізації даних. Пропонований проект реалізації рекомендаційної системи щодо обрання методів візуалізації даних ґрунтується на використанні мов програмування Python та JavaScript, а також використанні логіки програмування нейронних мереж, машинного навчання та реляційних систем управління базами даних. Основні сервіси розробленого застосування: створення й доповнення бази наданих даних; аналіз даних за алгоритмом Б. Шнейдермана «Overview first, zoom and filter, then details-on-demand» та технологіями фільтрації даних, брашингу, кластеризації, моделювання потоку даних, автоматичних обчислень, а також задачами користувача[3]; аналіз існуючих програм та веб-сайтів для візуалізації даних; надання

рекомендацій щодо обрання методів візуалізації та відповідних програмних застосувань чи веб-сайтів.

Висновки. Розроблений проект рекомендаційної системи щодо обрання методів візуалізації даних є основою для подальшої програмної реалізації відповідного застосування. Воно може бути використане як фізичними, так і юридичними особами для підвищення ефективності засвоєння інформації, проведення наочних досліджень та відображення наведених аргументів щодо виконання певних дій, планів, проведення заходів тощо.

Література:

1. Авербух В.Л. Анализ и визуализация "больших данных / В.Л. Авербух, Д.В. Манаков // Труды международной научной конференции “Параллельные Вычислительные Технологии” (ПаВТ'2015). – Екатеринбург: ЮУрГУ, 2015. – С.332-340.

2. Зачем и как использовать визуализацию данных? [Електроний ресурс]. – Режим доступу: https://infogra.ru/infographics/zachem-i-kak-ispolzovat-vizualizatsiyu-dannyh. – Дата доступу: 01.11.2019.

3. Авербух В.Л. Задачи визуализации параллельных вычислений / Авербух В.Л., Байдалин А.Ю., Васев П.А // Вопросы атомной науки и техники. – № 3. – 2002. – С. 40-52.

ТЕХНОЛОГІЯ CDMA: ФУНКЦІОНАЛЬНА СТРУКТУРА, ЕВОЛЮЦІЯ

Дудикевич В., Микитин Г., Бабенцов Г., Васильєв Д.
Національний університет “Львівська політехніка”, м.Львів

Анотація: розглянуто технологію CDMA. було зроблено порівняння з іншими технологіями множинного доступу. Приведено еволюцію CDMA за швидкістю.

Ключові слова — CDMA, множинний доступ, технологія,FDMA, TDMA.

Summary: CDMA technology was considered and compared with other multiple access technologies. The evolution of CDMA in terms of speed was given.

Key words — CDMA, multiple access , technology ,FDMA, TDMA.

Структура CDMA. CDMA - стандарт бездротового зв'язку множинного доступу з кодовим розділенням каналів. CDMA можна розглядати як вдосконалену версію технології TDMA та її заміну. Також на цій технології базується перехід до цифрового радіо. Розглянемо принцип функціонування CDMA (рис. 1). Мобільна станція (MS)- це абонентський пристрій. Мережа радіо доступу (RAN) - є вхідною точкою абонента у всю мережу оператора. Базова станція (BTS)- служить інтерфейсом між мережею та мобільними пристроями. Контролер базових станцій (BSC) - передає повідомлення та голосові дані між сотами і MSC. Пристрій контролю пакетних з'єднань (PCF) головним завданням якого є маршрутизація пакетів між BTS і PDSN. Мережа

комутації (NSS). MSC- відповідає за встановлення голосових з'єднань в системі. Регістри (HLR, VLR) - в них зберігається інформація про абонентів. Мережа пакетної комутації (PCN)- відповідає за передачу користувацьких пакетів з / в зовнішні мережі. Обслуговуючий вузол пакетної мережі, об'єднаний із зовнішнім агентом (PDSN / FA) - це шлюз між мережею радіо доступу та зовнішніми пакетними мережами. AAA - сервер використовується для аутентифікації і авторизації абонентів, для зберігання абонентських даних. Домашній агент (HA) надає безшовний роумінг до інших мереж стандарту CDMA2000.

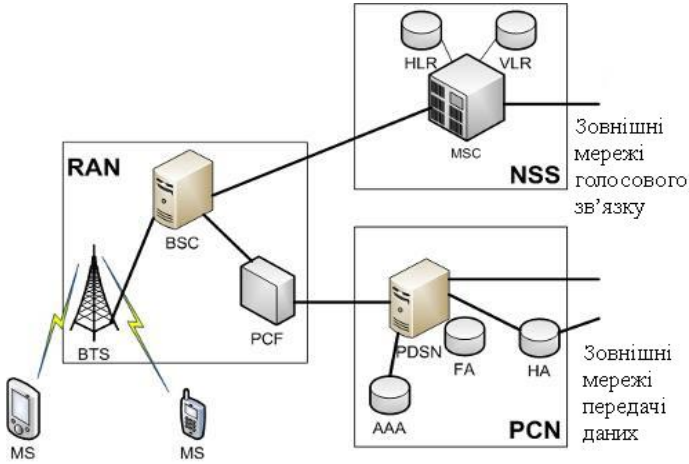


Рис.1. Структура технології CDMA

Порівняння технологій множинного доступу CDMA, FDMA, TDMA (рис. 2). Принцип FDMA полягає в тому, що весь частотний спектр поділяється між користувачами на рівні або нерівні частотні смуги. У стільниковому зв'язку FDMA застосовується у всіх стандартах: NMT ,GSM ,UMTS ,LTE , Mobile WIMAX. Максимальною швидкістю передачі при використанні даної технології є 1200 б/с у стандарті NMT-900 . Основний принцип TDMA полягає в тому, що наявний ресурс поділяється між учасниками інформаційного обміну на циклічно повторюються проміжки часу. TDMA широко застосовується в стандартах другого покоління стільникового зв'язку . TDMA в комбінації із CDMA у стандарті UMTS (UTRAN) має швидкість до 2 Мб/с . Принцип CDMA полягає в тому, що кожному джерелу інформації призначається індивідуальний код, за допомогою якого він кодує передане повідомлення.

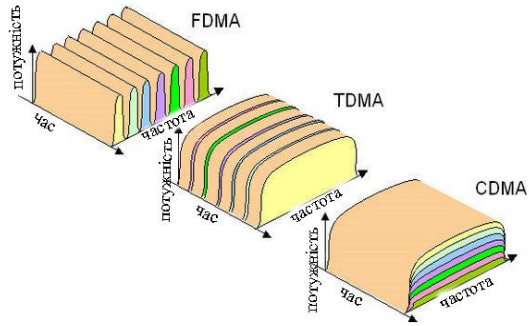


Рис. 2. Структура технологій множинного доступ

Метод CDMA використовується в основному в системах радіодоступу. У стільниковому зв'язку принцип CDMA знайшов застосування в стандартах 2G і 3G. Максимальною швидкістю у стандарті EV-DO Rev.B, який заснований CDMA, є 14.7 Мб/с.

Еволюція технології CDMA. На рис. 3 подано етапи еволюції технології CDMA за параметром швидкості передавання інформації на інтервалі часу.

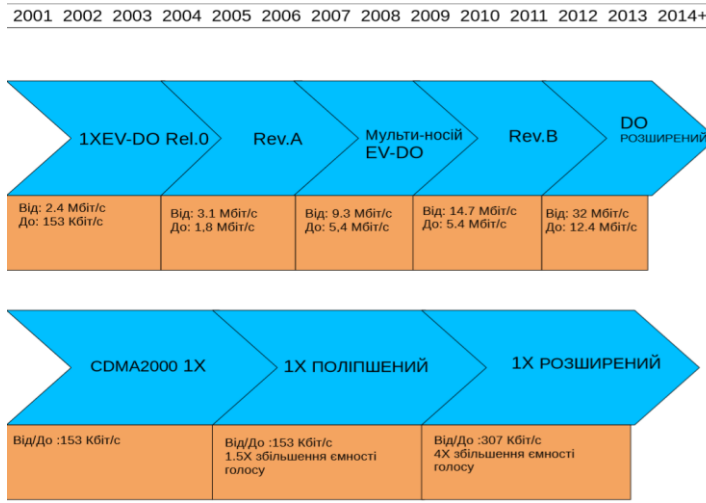


Рис. 3. Етапи еволюці технології CDMA

Висновок: Розглянуто структуру технології CDMA, принцип її функціонування, порівняння з іншими технологіями множинного доступу, а також розвиток.

ІНТЕРНЕТ РЕЧЕЙ У СИСТЕМІ “РОЗУМНЕ МІСТО”

Микитин А.
Івано-Франківський національний технічний університет нафти і газу

Анотація. Розглянуто Інтернет речей у контексті функціонування “розумного міста” та елементи інформаційної безпеки.
Ключові слова: “розумне місто”, технологіїі, Інтернет речей, давачі, безпека.

Summary: The Internet of things was considered within the context of “smart city” functioning and information security elements.
Key words: “smart city”, technologies, Internet of things, sensor, security.

Розумне місто: технології. Національна програма інформатизації та Концепція 4.0 в Україні розгортають впровадження інформаційно-комунікаційних технологій в процеси інтелектуалізації предметних сфер суспільства. Серед актуальних напрямків – проектування інформаційних систем “Розумне місто”, що грунтується на знаннях та інноваційних технологіях. Інтелектуальні компоненти розумного міста – це енергосистеми, виробництво, транспортні, екологічні та медичні системи т. і. Технології системи “Розумне місто” повязані з процесами автоматизації, роботизації, управління. До основних технологій відносяться: Інтернет речей, Smart Grid, машинне навчання (штучні нейронні мережі). Інтернет речей (*поняття запропонував Кевін Ештон, 1999*) – мережі фізичних об’єктів з вбудованими давачами для реєстрації та передавання даних про стан різнорідних об’єктів, середовища та структури взаємодії “об’єкт – середовище” (рис. 1).

Рис.1. Інтернет речей як мережа мереж

Інтернет речей функціонує з спеціальними та МЕМС-давачами. Спеціальні давачі, вбудовані у пристрої – електронної та аерокосмічної розвідки, дистанціного моніторингу параметрів екосистем планети, спостереження стану надзвичайних ситуацій, виявлення рухомих і нерухомих об'єктів у воєнних ситуаціях; пошук об'єктів т.і. MEMS-давачі – мікроелектромеханічні системи (*швейцарська компанія STMicroelectronics*) застосовуються в системах безпеки і є особливими у контексті: шкали, самотестування, цифрової технології, високої стабільності параметрів. Основними вимоги до параметрів цифрових давачів є: забезпечення інформаційної безпеки відбору, реєстрації, передавання інформації мережами для подальшого оброблення і прийняття рішення на управління розумними об'єктами. Безпечне функціонуваня системи "розумного міста' забезпечує вибір алгоритму побудови архітектури ПЗ, зокрема у частині Інтернету речей можна виділити два аспекти – безпеку давачів, що забезпечує безпечний контроль (відбір інформації) розумних об'єктів та безпечне збереження і обмін інформацією. З метою забезпечення безпечного збереження та обміну інформації використовують: методи оптимального шифрування передавання даних, коди аутентифікації повідомлень на основі хеш-функції

Висновок: Проаналізовано Інтернет речей як технологію системи "Розумне місто".

З М І С Т

Секція 1

КІБЕРБЕЗПЕКА

Напрям 1. УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Напрям 2. ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Напрям 3. ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

Напрям 4. БЕЗПЕКА ІНФОРМАЦІЇ У ХМАРНИХ СХОВИЩАХ

Секція 2

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Напрям 7. Інформаційні технології управління проєктами

Напрям 8. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ

Напрям 9. Прикладне та системне програмування

Напрям 13. ТЕХНОЛОГІЇ ВІЗУАЛІЗАЦІЇ ДАНИХ

Наукове видання

ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

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

Відповідальні за випуск **Олександр Придатко**
Назарій Бурак

Оригінал-макет **Олександр Хлевной**

Друк на різографі **Маріанна Климус**

Підписано до друку 12.11.2019 р.
Формат 60×84/16. Гарнітура Times New Roman.
Друк на різографі. Папір офсетний.
Ум. друк. арк. 17,8.

Друк ЛДУ БЖД
79007, Україна, м. Львів, вул. Клепарівська, 35
тел./факс: (032) 233-32-40, 233-24-79.