Міністерство оборони України

Військовий інститут телекомунікацій та інформатизації

Національного технічного університету України

„Київський політехнічний інститут”

ВОЄННО – НАУКОВА КОНФЕРЕНЦІЯ КУРСАНТІВ (СТУДЕНТІВ)

Факультет інформаційних технологій в системах управління.

(Доповіді та тези доповідей)

21 травня 2008 року

Київ - 2008

ЗМІСТ

Пленарне засідання

Вступне слово

Начальник кафедри № 23

полковник Клименко М.О.

Моніторинг інцидентів безпеки у розподіленій інформаційній системі на основі методу нечіткої ідентифікації
Курсант 231 м навчальної групи,

солдат Драчук О.В.

Загальна характеристика засобів моніторингу і аналізу інформаційних мереж
Курсант 231 м навчальної групи,

солдат Драглюк О.В.

Методика тестування *Web*-ресурсів учбового призначення

Студентка КН – 31 навчальної групи,

Гуненко Л.П.

Система комп'ютерного адаптивного тестування знань
Курсант 231 м навчальної групи ,

солдат Солоний В.А.

Характеристика методів моніторингу і аналізу програмного забезпечення. Мистецтво фазінгу
Курсант 231 м навчальної групи,

солдат Осиченко О.Б.

Дослідження методів кластеризації інформації
Курсант 231 м навчальної групи,

солдат Панченко П.Ю.

Дослідження системи захисту модульного об'єктно-орієнтованого навчального середовища "*Moodle*" 19
Курсант 231 м навчальної групи,
солдат Царенко В.М.

Автоматизована система аналізу захищеності програмного забезпечення з доступним початковим кодом 20
Студент КН – 31 навчальної групи,
Остропіцький Д.О.

Відображення стану зв'язку на місцевості. Оцінка та аналіз технологій, що застосовуються 22
Курсант 231 м навчальної групи,
солдат Назаревич В.В.

Секційне засідання 24
Дослідження систем аналізу захищеності програмного забезпечення з відкритим програмним кодом 25
Курсант 231 м навчальної групи,
мол. сержант Желудєв М.С.

Програмний модуль щодо оцінки захищеності комп'ютерної системи за методом аналізу ієрархії 27
Курсант 231м навчальної групи,
мол. сержант Цибульський С.М.

Синтез способів аутентифікації користувачів *WEB*-ресурсу на основі хешування паролів 29
Студент КН – 31 навчальної групи,
Іщук С.М.

Інтелектуальні технології в системах пошуку інформаційних ресурсів глобальної мережі *Internet* 31
Студент КН – 31 навчальної групи,
Крупкін М.Б.

Автоматизована система оцінки ефективності засобів статичного аналізу захищеності програмного забезпечення 32
Студент КН – 31 навчальної групи,

Безкоровайний Я.О.

Інформаційно-аналітична система по лікарських препаратах 33
Студент КН – 31 навчальної групи,

Артемчук М.С.

Автоматизована система проведення групового експертного оцінювання на базі *Web*-технологій 35
Студент КН – 31 навчальної групи,

Рахімов Ю.Г.

Методи оцінки надійності програмного забезпечення 37
Студент КН – 31 навчальної групи,

Миронюк О.І.

Методика оцінки ефективності комп'ютерних тренажерних систем у навчальному процесі 38

Доцент кафедри №21,

підполковник Любарський С.В.,
Студент КН – 31 навчальної групи,

Вакарук І.В.

Застосування методів інтелектуального аналізу даних у системах виявлення вторгнень 40
Курсант 231 м навчальної групи,

мол. сержант Сімончук О.В.

Інформаційно-аналітична система моніторингу бібліотечно-інформаційних ресурсів 42
Студентка КН – 31 навчальної групи,

Петрище А.В.

Оцінка інформаційних систем з урахуванням кількісних і якісних показників 44
Студент КН – 31 навчальної групи,

Василенко В.В.

Методика оцінки ефективності застосування ПАК „ТЗІТ" СП в 46

навчальному процесі
Студент КН – 31 навчальної групи,
Мужеський К.К.

Методика розробки автоматизованої системи обліку апаратних засобів локальної обчислювальної мережі 47
Студент КН – 31 навчальної групи,
Чабан А.О.

Автоматизована система товарного обліку підприємства 49
Студент КН – 31 навчальної групи,
Шевчик О.Л.

Клименко М.О. (ВІТІ НУТУ „КПІ”)

ВСТУПНЕ СЛОВО

Шановні офіцери, працівники ЗСУ, курсанти та студенти.

Сьогодні, відповідно до річного плану воєнно-наукової роботи курсантів (студентів) факультету, ми проводимо наукову конференцію воєнно-наукового товариства.

Конференція проводиться з метою підбиття підсумків наукової роботи курсантів (студентів) за навчальний рік, популяризації кращих робіт і широкого обміну думками стосовно них на факультеті.

Робота воєнно-наукового товариства на факультеті була організована і проводилася відповідно до вимог керівних документів:

1. Наказу Міністра оборони України № 9 від 13.01.2007 р.
2. Наказу НІ № 68 від 07.09.2007 р. „Про організацію підготовки та проведення наукової і науково-технічної діяльності в інституті на 2007-2008 навчальний рік”.
3. Методичних вказівок про організацію роботи ВНТ курсантів і студентів.
4. Положення про воєнно-наукове товариство курсантів (студентів) (затверджене Вченою радою інституту. Протокол № 10 від 27.02.2008 р.).

Товариші, кожний із вас у свій час виявив бажання самостійно займатися науковою працею і технічною творчістю, добровільно вступивши до воєнно-наукового товариства ВНТ курсантів (студентів) інституту. На протязі року ви підвищували свою методологічну підготовку, розвивали наукове мислення, набували навички дослідницької роботи, творчого підходу до вирішення задач бойового застосування з питань телекомунікацій та інформатизації, а також вивчали основи організації і проведення наукових досліджень.

Пріоритетними напрямками наукової роботи та науково-технічної діяльності роботи факультету є:

– статистичне оцінювання та його застосування на практиці;
– технології функціонування комунікаційних систем в мережах;
– методологія аналізу, синтезу та управління телекомунікаційним мережами;
– системи автоматизації електронного документообігу;
– інформаційні системи та бази даних;
– управління інформаційними мережами;
– захист інформації в інформаційних мережах;
– маршрутизація в територіальних мережах передачі даних;
– підвищення ефективності технічного обслуговування і ремонту військово техніки зв'язку і автоматизації;
– зменшення працезатрат на технічне обслуговування і ремонт військово техніки зв'язку і автоматизації;
– підвищення якості зберігання засобів зв'язку і автоматизації Збройних Си України;
– автоматизація процесів управління технічним забезпеченням зв'язку АУВ на всіх рівнях підпорядкування;
– оптимізація номенклатури засобів вимірювальної техніки з урахуванням її морального стану, фізичного старіння та можливостей поставок дл забезпечення.

Бажаю вам успіхів під час виступів як на пленарному засідання так і під ча роботи наукових секцій та закликаю до плідної творчої праці.

Драчук О.В. (ВІТІ НТУУ „КПІ”)

МОНІТОРИНГ ІНЦИДЕНТІВ БЕЗПЕКИ У РОЗПОДІЛЕНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ НА ОСНОВІ МЕТОДУ НЕЧІТКОЇ ІДЕНТИФІКАЦІЇ

В роботі розглянуто підходи до виконання програмно-апаратних засобів захисту інформації в розподіленій мережі організації та обґрунтовано вибір розподіленої архітектури побудови програмного комплексу ідентифікації інцидентів безпеки в розподіленій інформаційній системі на основі методу нечіткої ідентифікації. Робота є продовженням розгляду тематики розробки програмного модуля ідентифікації інцидентів безпеки на основі експертних знань при централізованій обробці подій.

В огляді актуальності теми роботи наведено існуючі аналоги відповідних рішень захисту інформації. Розподілена архітектура мережних екранів та клієнт-серверна топологія побудови віртуальних захищених мереж обґрунтовують доцільність використання розподіленої архітектури засобів захисту інформації в розподіленій мережі. Динамічний розвиток сучасних засобів проведення мережних атак на захищені розподілені інформаційні мережі зумовлює використання динамічних (адаптивних) засобів захисту – систем виявлення атак та систем централізованої обробки подій. В роботі запропонована типова архітектура побудови системи централізованої обробки подій. Відповідно до цієї архітектури виділено два основних функціональних компоненти: сервер безпеки, як суб’єкт системи та інформаційна система, як об’єкт системи. В основі сервера безпеки визначено менеджер моніторингу, а в основі інформаційної системи – агент моніторингу.

В змісті роботи наведено узагальнені схеми побудови відповідно менеджера і агента моніторингу та відповідне їх математичне наповнення, дано загальну схему програмної реалізації відповідного програмного модуля.

Драглюк О.В. (ВІТІ НТУУ "КПІ")

ЗАГАЛЬНА ХАРАКТЕРИСТИКА ЗАСОБІВ МОНІТОРИНГУ І АНАЛІЗУ ІНФОРМАЦІЙНИХ МЕРЕЖ

Будь-яка система аналізу інформаційної мережі повинна забезпечувати наступні функції:

- управління конфігурацією мережі та її найменуванням;
- обробка помилок;
- аналіз продуктивності і надійності мережі;
- управління безпекою;
- облік роботи мережі.

Відповідно до виконуємих функцій та виду реалізації всі засоби, для моніторингу і аналізу інформаційних мереж, можна розділити на декілька великих класів:

- системи управління мережею (*Network Management Systems*);
- засоби управління системою (*System Management*);
- вбудовані системи діагностики і управління (*Embedded systems*);
- аналізатори протоколів (*Protocol analyzers*);
- устаткування для діагностики і сертифікації кабельних систем;
- експертні системи;
- багатофункціональні пристрої аналізу і діагностики;

Незалежно від класу системи та способу її реалізації, алгоритм роботи системи зводиться до аналізу протоколів, які підтримують мережі. Основним протоколом, що найчастіше використовується в роботі систем є протокол мережного управління *SNMP* (*Simple Network Management Protocol*). Достоїнствами *SNMP* є простота, доступність, незалежність від виробників. *SNMP* офіційно ухвалений *CMIP*, і як протокол, що управляє, за версією *OSI*. Протокол SNMP розроблений для управління маршрутизаторами в мережі Internet

і є частиною стека *TCP/IP*. Інформація, якою керується протокол, знаходиться в комунікаційних пристроях у базі даних *MIB* (*Management Information Base*), що обробляється простими командами протоколу *SNMP*.

Гуненко Л.П. (ВІТІ НТУУ „КПІ”)

МЕТОДИКА ТЕСТУВАННЯ *WEB*-РЕСУРСІВ УЧБОВОГО ПРИЗНАЧЕННЯ

Доповідь присвячена методиці тестування *Web*-ресурсу учбовогс призначення. Тестування *Web*-ресурсів – це складний процес, тому що труднощі примножені всіма розподіленими компонентами системи, які взаємодіють з додатком. Помилка може бути на сервері, у клієнта чи в системі зв’язку між ними (в локальній мережі).

Для того, щоб упевнитися, що сайт працює добре, що він не підведе в критичну хвилину і користувачі залишаться задоволені існують різні методи тестування: тестування функціональності, тестування продуктивності, тестування надійності та доступності, тестування сумісності.

Тестування програми *P* за деяким критерієм *C* означає покриття безл компонентів програми *P* $M = \{m_1, ..., m_k\}$ по елементах або по зв'язках:

$T = \{m_1, ..., m_k\}$ – кортеж ненадмірних тестів t_i.

Тест t_i ненадмірний, якщо існує покритий ним компонент m_i з *M(P, C)*, покритий жодним з попередніх тестів $t_1, ..., t_{i-1}$.

Кожному t_i відповідає ненадмірний шлях p_i – послідовність вершин від вхо до виходу.

V(P, C) – складність тестування *P* за критерієм *C* – вимірюється max числ ненадмірних тестів, що покривають всі елементи множини *M(P, C)*.

DV(P, C, T) – залишкова складність тестування *P* за критерієм *C* – вимірюєт max числом ненадмірних тестів, що покривають елементи множини *M(P, C)*, з залишилися непокритими, після прогону набору тестів *T*. Величина *DV* строг монотонно спадає від *V* до *0*.

$TV(P, C, T) = (V - DV)/V$ – оцінка ступеня тестування P за критерієм C. Критерій закінчення тестування $TV(P, C, T)\ L$, де $(0 \le L \le 10)$. L – рівень тестування, заданий у вимогах до програмного продукту.

Солоний В. А. (ВІТІ НТУУ „КПІ”)

СИСТЕМА КОМП’ЮТЕРНОГО АДАПТИВНОГО ТЕСТУВАННЯ ЗНАНЬ

При вимірюванні рівня знань з неадаптивним тестуванням для кожного навчаємого формується тест певної довжини з вибраних випадковим чином завдань тестового простору. Недоліком такого тестування може бути поява ситуацій, коли слабкому студентові попадається складний тест і як наслідок цього – практична відсутність відповідей. Для забезпечення максимальної інформативності результатів контролю необхідно, щоб середня складність тесту, яка надається студенту, відповідала його гіпотетичному рівню знань. Практично це можна здійснити за допомогою адаптивного тестування.

Ефективність контрольно-оціночних процедур підвищується при використанні багатокрокової стратегії відбору.

Багатокрокові стратегії адаптивного тестування можна підрозділити на фіксовано-розподілені і варіюючі. Якщо один і той же набір з фіксованим розташуванням завдань на осі складності використовується для всіх випробовуваних, але кожен рухається по набору індивідуальним шляхом, залежно від результатів виконання кожного чергового завдання, то стратегія адаптивного тестування є детерміновано (фіксовано) такою, що гілкується.

Варіююча стратегія адаптивного тестування, припускає відбір завдань безпосередньо з банку за певними алгоритмами, які прогнозують оптимальну складність подальшого завдання та наслідками виконання випробовуваним попереднього завдання адаптивного тесту. Таким чином, з'являється своєрідна послідовність поточних значень рівня підготовленості навчаємого, стосовно яких підбирається складність завдань адаптивних тестів.

Осиченко О. Б. (ВІТІ НТУУ „КПІ

ХАРАКТЕРИСТИКА МЕТОДІВ МОНІТОРИНГУ І АНАЛІЗУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ. МИСТЕЦТВО ФАЗІНГУ

Мета роботи:

Обґрунтувати побудову прототипу автоматизованої системи аналі захищеності програмного забезпечення з недоступним початковим кодом невизначеним інтерфейсом за допомогою використання генетичних алгоритмів.

1. Фаззінг є в даний час досить популярним і ефективним методом аналі захищеності програмного забезпечення, для якого, однак, відсутній вичерпн теоретичний апарат.

2. Ефективність фаззінгу визначається якістю тестового впливу.

3. Існують фактори, що ускладнюють або навіть унеможливлюють практиці вирішення задачі вичерпного покриття поверхні атаки цільового ПЗ:

4. Існує два підходи до вирішення задачі автоматичного розпізнаван протоколів засобами фаззінгу:

– на основі перехоплення й аналізу реальних сеансів роботи;

– на основі вимірювання покриття поверхні атаки цільового програмно забезпечення кожним елементом тестового впливу і скеровування наступн елементів тестового впливу в напрямку, що забезпечує зростання цьо показника.

Другий підхід є більш універсальним і його застосування вимагає менш підготовчих зусиль, хоча жоден із них не є досконально дослідженим.

Панченко П. Ю. (ВІТІ НТУУ „КПІ”

ДОСЛІДЖЕННЯ МЕТОДІВ КЛАСТЕРИЗАЦІЇ ІНФОРМАЦІЇ

Завдання вибору оптимального методу обробки даних часто є дуж важливим, особливо в тих випадках, коли необхідна експрес-оцінка даних, ш приходять з різних ресурсів. Для вирішення даної проблеми почал використовувати спеціальні математичні методи кластерного аналізу.

Методи кластерного аналізу ґрунтуються на розбитті об'єктів на однорід категорії (тобто всі об'єкти в одній групі схожі між собою відповідно до деяк міри), при цьому кожен об'єкт належить тільки одному класу, тобто існує вели число методів кластеризації. Нижче приведені основні з них.

На початку розглянемо ієрархічні методи суть, яких складається послідовному об'єднанні менших кластерів у більші або поділі більших кластер на менші. Вони розподіляються на:

– агломеративні методи: ця група методів характеризується послідовн об'єднанням вихідних елементів і відповідним зменшенням числа кластерів;

– дивізимі (ділені) методи: ці методи є логічною протилежніст агломеративним методам. На початку роботи алгоритму всі об'єкти належа одному кластеру, що на наступних кроках ділиться на менші кластери, результаті утвориться послідовність груп, що розщеплюють.

При великій кількості спостережень ієрархічні методи кластерного аналі непридатні. У таких випадках використовують неієрархічні методи, засновані діленні, які являють собою ітеративні методи дроблення вихідної сукупності. процесі розподілу нові кластери формуються доти, поки не буде викона правило зупинки. До алгоритмів даного типу належать: алгоритм k-серед (k-*means*) та алгоритм *PAM* (*Partitioning around Medoids*).

Однак зараз, у зв'язку з появою великих баз даних, з’явилися нові вимо яким повинен задовольняти алгоритм кластеризації. Основне з них –

масштабованість алгоритму. Відзначимо також інші властивості, яким повинен задовольняти алгоритм кластеризації: незалежність результатів від порядку вхідних даних; незалежність параметрів алгоритму від вхідних даних. Розроблено алгоритми, у яких методи ієрархічної кластеризації інтегровані з іншими методами. До таких алгоритмів відносяться: *BIRCH*, *CURE*, *CLARA*, *Clarans*,

Проведені дослідження різних методів кластеризації дозволяють зробити вивід про їх ефективність, стосовно завдань обробки і аналізу даних з виявленням експрес-оцінок.

Досвід показує, що метод кластеризації неврегульованих записів дає відчутний виграш за часом, за який обробляються дані (що особливо істотно при великій кількості записів).

Проте, враховуючи все вищесказане, приходимо до наступного висновку відносно застосовності розглянутих методів: не існує універсального методу, який дає перевагу економії часу, що при цьому враховує неоднорідність даних. Для кожного завдання слід вибирати свій метод з урахуванням її специфіки.

Царенко В. М. (ВІТІ НТУУ „КПІ”)

АНАЛІЗ СИСТЕМИ ЗАХИЩЕНОСТІ ОБ’ЄКТНО-ОРІЄНТОВАНОГО НАВЧАЛЬНОГО СЕРЕДОВИЩА

При впровадженні систем дистанційного навчання в сучасний навчальний процес, різко постає питання щодо забезпечення безпеки інформації, що зберігається в базах даних таких систем.

В комплект поставки СДО „*Moodle*” включено, *Web*-сервер *Apache*, СКБД *MySQL*, та безпосередньо скрипт СДО написаний на мові програмування PHP.

По-перше: *Web*-сервер *Apache* вважається одним із найбільш захищених *Web*-серверів серед існуючих по рейтенгу використання в світі за 2007–2008 роки. Висновки: мінімальне використання додаткових модулів, перебір URL, фільтрація *SQL*-запитів, захищеність операційної системи.

По-друге: СКБД *MySQL* – найбільш поширена СКБД у мережі інтернет. Висновки: правильна обробка помилок, заборона пересилання системних параметрів, мінімізація привілеїв користувачів, захист схеми.

По-третє: Скрипт PHP. Безпосередньо з адміністративної сторінки СДО „Moodle” передбачено захист інформації, якій відповідає політика безпеки сайту. Висновки: використання *HTTPS*-з’єднання, обмеження використання модулів, реєстрація невдалих спроб входу до сайту, використання антивірусу, фільтрація файлів, використання мережного ключа, автоматичний вихід при бездії користувача.

Пропозиції щодо вдосконалення системи безпеки СДО „Moodle”:

1. Використання додаткового програмного забезпечення, що стосується безпеки операційної системи.
2. Використання серверу *Apache* версії 2.0 та вище.
3. Використання СКБД версії не нижче *MySQL* 4.0.
4. Правильне налаштування політики безпеки сайту.

Остропіцький Д.О. (ВІТІ НТУУ „КПІ”)

АВТОМАТИЗОВАНА СИСТЕМА АНАЛІЗУ ЗАХИЩЕНОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ З ДОСТУПНИМ ПОЧАТКОВИМ КОДОМ НА ОСНОВІ КОМПЛЕКСНОГО ЗАСТОСУВАННЯ ЗАСОБІВ СТАТИЧНОГО ТА ДИНАМІЧНОГО АНАЛІЗУ

У даній доповіді презентується прототипна реалізація автоматизованої системи аналізу захищеності програмного забезпечення з доступним початковим кодом на основі комплексного застосування засобів статичного та динамічного аналізу, на вже конкретно реалізованому прототипі, із модернізованими алгоритмами роботи.

В своїй реалізації система використовує в якості статичного аналізатора „*ITS*4” , в якості динамічного – систему „*Autodafe*”, поєднуючи переваги обох і нейтралізуючи їх недоліки. Прототип автоматично скеровує проведення динамічного тестування на найбільш вразливі, а точніше з найбільшим ступенем ризику місця, виявлені статичним аналізом.

В даній системі був вдосконалений алгоритм визначення потенційно небезпечних маркерів (елементів тестових впливів) і, пов’язаний із ним, алгоритм визначення послідовності вироблення тестових впливів.

Дана система повинна прискорити виявлення вразливостей програмного забезпечення з доступним початковим кодом (завдяки застосуванню засобів автоматизації статичного аналізу захищеності програмного забезпечення), мінімізувавши при цьому рівень помилкових тривог (завдяки автоматичній верифікації результатів роботи засобів статичного аналізу за допомогою направлених тестових впливів).

Основними компонентами системи є:

– засіб (набір засобів) статичного аналізу захищеності програмного забезпечення;

– модуль (набір модулів) управління засобами динамічного аналізу захищеності програмного забезпечення;

– засіб (набір засобів) динамічного аналізу захищеності програмного забезпечення.

Основні переваги такої побудови системи:

– придатність до розширення, у сенсі додавання підтримки нових засобів статичного й динамічного аналізу захищеності програмного забезпечення, нових мов і технологій програмування;

– застосування вдосконалених алгоритмів дозволяє першочергово виробляти ті тестові впливи, які з найбільшою ймовірністю дозволять виявити вразливості об'єкта тестування, і, завдяки цьому, скоротити середній час пошуку вразливостей.

Назаревич В.В. (ВІТІ НТУУ „КПІ

ВІДОБРАЖЕННЯ СТАНУ ЗВ'ЯЗКУ НА МІСЦЕВОСТІ. ОЦІНКА ТА АНАЛІЗ ТЕХНОЛОГІЙ, ЩО ЗАСТОСОВУЮТЬСЯ

Не буде перебільшенням сказати, що ГІС сьогодні стоять в осно оперативного інформаційного забезпечення військової діяльності, а розробка ГІ та впровадження ГІТ в інформаційне забезпечення військами, це одна найактуальніших задач на сьогодні. Це дасть змогу підвищити оперативніс збору, обробку інформації, збільшити мобільність пунктів бойового управлінн зменшити час на обмін інформації, отриманої від командного пункту нижньо ланцюга і передачі необхідної до вищої ланки, дасть змогу організува підтримку прийняття рішення.

Геоінформаційні системи – це автоматизовані системи, що реалізуєть сукупністю людей і технічних засобів, які ведуть збір, передачу, збереження обробку просторових даних з метою одержання інформації про місцевіст придатної для подальшого використання.

Картографічна інформація – це зафіксоване значення астрономо-геодезични висотних та гравіметричних вимірів, дані топографічного та картографічно характеру, аерокосмічних зйомок.

Геоінформаційні технології – це синтез (логічне поєднання) дан електронної карти з іншими цифровими даними з метою вирішення прикладн інформаційних задач.

Електронна карта – комп'ютерна модель картографічної інформації, в як забезпечується ідентифікація кожної її складової та на основі якої можли застосування автоматизованих методів її обробки.

Векторні карти – це моделі місцевості, при збільшенні яких, в ідеа деталізація збільшується (аж до виду окремих будинків). Суть векторних карт тому, що всі об'єкти на них представлені у вигляді математичних формул

виразів, що з погляду комп'ютера, набагато зручніше, ніж звична класична картинка.

Растрові карти – це фактично зображення у форматі *BMP* або *JPG*, до яких прив'язана географічна координатна сітка.

NGIS компоненти призначені для відображення візуальної інформації в Delphi-проектах.

NGIS Components – допомагають відображати візуальні картографічні дані у ваших програмах, прості в використовуванні і мають можливість настройки властивостей в режимі конструювання.

Секційне засідання

Желудєв М.С. (ВІТІ НТУУ „КПІ”)

ДОСЛІДЖЕННЯ СИСТЕМ АНАЛІЗУ ЗАХИЩЕНОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ З ВІДКРИТИМ ПРОГРАМНИМ КОДОМ

Стан програмного забезпечення ховає в собі певні проблеми, пов’язані з безпекою, актуальною проблемою якої є незахищеність програмного забезпечення від зовнішніх інформаційних впливів, наслідки яких можуть бути фатальними по відношенню до програмного забезпеченя.

Тому проблема розробки систем аналізу захищеності програмного забезпечення дуже широко розглядається програмістами в області безпеки програмного забезпечення.

На сьогоднішній день існує три основних методи аналізу захищеності програмного забезпечення: статичний, динамічний та комбінований, який передбачає символічне та конколічне виконання програмного забезпечення. Для застосування цих методів аналізу необхідно, якимось чином, виробляти руйнівні інформаційні впливи на цільові програми. Для підготовки якісних тестових руйнівних інформаційних впливів необхідний великий обсяг трудомісткої ручної роботи. Ручна розробка базується на ретельному дослідженні інтерфейсів та можливо, початкового коду, об’єкта тестування і потенційно дозволяє забезпечити максимальне охоплення коду об’єкта тестування, однак, є дуже трудомісткою процедурою.

Автоматичне ж вироблення тестових впливів за випадковим (псевдовипадковим) алгоритмом, значно простіше реалізується, однак, у випадку більш-менш складних об’єктів тестування не дозволяє забезпечити достатньо повне охоплення коду об’єкта тестування, окрім того, призводить до вироблення значної кількості надлишкових тестових впливів.

Таким чином, досить актуальним є дослідженя шляхів побудови й розробка комплексу таких засобів, орієнтованого на автоматичне вироблення тестових впливів для динамічного аналізу захищеності програмного забезпечення. Пропонується розробити систему, яка, базуючись на комбінованому конкретному й символічному виконанні програмного забезпечення, дозволить максимально автоматизувати процес аналізу його захищеності.

Цибульський С.М. (ВІТІ НТУУ „КПІ”)

ПРОГРАМНИЙ МОДУЛЬ ЩОДО ОЦІНКИ ЗАХИЩЕНОСТІ КОМП’ЮТЕРНОЇ СИСТЕМИ ЗА МЕТОДОМ АНАЛІЗУ ІЄРАРХІЇ

Інформаційні ресурси держави або суспільства в цілому, а також окремих організацій і фізичних осіб являють собою певну цінність, мають відповідне матеріальне вираження і вимагають захисту від різноманітних за своєю сутністю впливів, які можуть призвести до зниження цінності інформаційних ресурсів.

Автоматизація обробки інформаційних ресурсів із застосуванням сучасних інформаційних технологій призвела до появи комп’ютерних систем з різними функціональними профілями захищеності комп’ютерних систем.

Актуальне питання оцінки функціонального профілю комп’ютерної системи є використання єдиної системи нормативних документів технічного захисту інформації.

Функціональний профіль (*functionality profile*) – упорядкований перелік рівнів функціональних послуг, який може використовуватись як формальна специфікація функціональності КС.

Як правило, задача оцінки захищеності комп’ютерної системи покладається на відповідальну посадову особу – „АУДИТОР захищеності комп’ютерної системи”.

Метою програмного модуля саме є розгляд та оцінка функціонального профілю комп’ютерної системи за методом рангових оцінок, визначення головного завдання системи і напрямки діяльності, дати чітку інформацію по її захищеності та функціонуванні.

При виборі методу визначення оцінки комп’ютерної системи необхідно враховувати, як правило, складність отримання експертної інформації, особливо організації і проведення експертизи, достовірність експертної інформації,

Іщук С.М. (ВІТІ НТУУ „КПІ”)

СИНТЕЗ СПОСОБІВ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ *WEB*-РЕСУРСУ НА ОСНОВІ ХЕШУВАННЯ ПАРОЛІВ

У даній доповіді приведено декілька методів хешування паролів аутентифікації при доступі користувачів до *Web*-ресурсів, та розмежуванні їхніх прав.

Розглянуті алгоритми хешування дозволяють надавати безпечність (цілісність паролю, унеможливлення його підміни іншим значенням), при процедурі аутентифікації на доступ до ресурсів користувачам, що надає змогу надати доступ повний чи частковий (без можливості внесення змін в файлах, до яких надається доступ). Таким чином унеможливити несанкціонований доступ до ресурсу.

Основний принцип розмежування повноважень полягає у тому, що повноваження на доступ того чи іншого ресурсу визначаються власником даного ресурсу. При цьому вказується, яким суб’єктам надані права на доступ, та які саме. Така політика розмежування повноважень вважається більш надійною. Процедура аутентифікації передбачає функціональні можливості модуля, який зрівнює пари ім’я – пароль зі строками текстового файла, що зберігається на сервері в вигляді хеш-пароля, котрий кодується за допомогою хеш-функцій. Хеш-функцією називається таке математичне або алгоритмічне перетворення заданого блока даних, яке володіє наступними властивостями:

– хеш-кодування-функція має нескінченну область визначення;

– хеш-кодування-функція має кінцеву область значень;

– вона безоборотна;

– зміна вхідного потоку інформації на один біт міняє близько половини всіх біт вихідного потоку, тобто результату хеш-функції.

Ці властивості дозволяють подавати на вхід хеш-функції паролі, тобто, текстові рядки довільної довжини на будь-якій національній мові і, обмеживши область значень функції діапазоном 0, …, $2^N - 1$, де N – довжина ключа в бітах, отримувати на виході досить рівномірно розподілені по області значення блоки інформації – ключі.

Однак зауважимо, що в комп'ютерних системах, підключених до мереж загального користування, практично неможливо тим чи іншим чином ідентифікувати всіх можливих суб'єктів доступу до ресурсу. Причому користувач повинен зберігати паролі в таємниці від інших користувачів, щоб унеможливити фіктивне використання наданих прав доступу до певного ресурсу, а також при реєстрації на ресурсі чим складніше задавати свої ідентифікатори ім'я-пароль (якщо вони не надаються адміністратором).

Крупкін М.Б. (ВІТІ НУТУ „КПІ")

ІНТЕЛЕКТУАЛЬНІ ТЕХНОЛОГІЇ В СИСТЕМАХ ПОШУКУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ГЛОБАЛЬНОЇ МЕРЕЖІ *INTERNET*

У даній доповіді презентується одна із інтелектуальних технологій яка може бути використана при проектуванні інтелектуальної пошукової системи, а саме класифікація та кластеризація.

При дослідженні автоматичної класифікації надалі (кластеризація) мною було знайдено ряд властивостей які їй характерні та можуть бути використані при інформаційному пошуку, ці властивості задовольняють вимоги до розробленої мною системи для роботи з інформацією:

– фільтрація вхідних документів;

– стиснення інформації (анотування, реферування);

– розширення запитів за рахунок тих, що характеризують тематику класу термінів;

– реалізація зворотного зв'язку по релевантності шляхом попередньої класифікації результатів вибірки по класах і вибору користувачем релевантних класів;

– зняття омонімії шляхом відображення слів в узагальнені концепти.

При виборі кластеризації як методу структурування інформації необхідно враховувати, як правило, складність отримання пошукової інформації, особливо організації і проведення пошуку, достовірність інформації яка шукається більшою мірою залежить від методу індексації інформації, трудомісткості алгоритму обробки інформації при побудові розподіленої системи обробки, класифікації та пошуку інформації.

Безкоровайний Я.О. (ВІТІ НТУУ „КПІ”)

АВТОМАТИЗОВАНА СИСТЕМА ОЦІНКИ ЕФЕКТИВНОСТІ ЗАСОБІВ СТАТИЧНОГО АНАЛІЗУ ЗАХИЩЕНОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

У даній доповіді презентується автоматизована система для оцінки ефективності засобів статичного аналізу захищеності програмного забезпечення.

Дана система дозволяє виробляти оцінку ефективності засобів статичного аналізу захищеності програмного забезпечення на основі тестування їх здатності виявляти вразливості програмного забезпечення на наборі завчасно підготовлених тестових програм.

Тестові програми вибрані для двох класів вразливостей програмного забезпечення:

- переповнення буфера;
- помилки у форматуванні строк.

Аналізуються засоби статичного аналізу захищеності програмного забезпечення з відкритим вихідним кодом: *Flawfinder*, *Splint*, *Rats*, *Its* 4.

Оцінка ефективності виконується за наступними показниками:

- коефіцієнт покриття заданих класів вразливостей (обчислюється як доля тестових програм, що правильно ідентифіковані як уразливі, серед загальної кількості тестових програм, що моделюють уразливості заданих класів);
- рівень помилкових тривог для заданих класів вразливостей (обчислюється як доля тестових програм, що неправильно ідентифіковані як уразливі, серед загальної кількості тестових програм, що імітують уразливості заданих класів (але не є вразливими)).

Артемчук М.С. (ВІТІ НТУУ „КПІ”)

ІНФОРМАЦІЙНО-АНАЛІТИЧНА СИСТЕМА ПО ЛІКАРСЬКИХ ПРЕПАРАТАХ

Поставлено завдання обґрунтувати необхідність створення „Інформаційно-аналітичної системи по лікарських препаратах», яка приведе до пришвидшення і покращення лікування хворих в закладах медичного профілю. Навести фінансову і трудомістку сторони розробки такої системи в зв’язку з великим обсягом інформації і її поганою структурованістю.

У процесі дослідження проаналізовано проблеми, пов’язані з розробкою інформаційно аналітичної системи.

1. Інформатизація медицини. Технічне забезпечення медичних закладів „бажає” кращого. Персонал має низький і невелику кількість – середній рівень знань в інформаційних технологіях.

2. Використання великої кількості людських ресурсів. Побудова системи вимагає, з однієї сторони, спеціалістів в області програмування, з іншої фахівців-експертів. Крім того, спільну роботу обох сторін необхідно узгодити та логістично забезпечити.

3. Архітектура системи. Які апаратні та програмні засоби повинні бути використані?

4. Оновлення інформації. Інформація має властивість застарівати. Хто, коли, і за які кошти має здійснювати оновлення інформації?

Затрати на створення системи можна поділити за такими напрямками: фінансові затрати (оплата обладнання і праці), часові затрати, витрати на нормативне забезпечення, створення умов функціонування системи, затрати на оновлення інформації.

Інформаційно-аналітична система розглядатися в двох аспектах:

1. Медичний аспект. Необхідно врахувати та узгодити роботу всіх медичних підрозділів, інформаційну підтримку користувачів медичних послуг, сімейні стосунки тощо. В центрі має бути пацієнт.

2. Інформаційний аспект. Необхідно використати доцільні технології обробки та передачі інформації.

В ході дослідження нами були зроблені такі висновки:

1. „Інформаційно-аналітична система по лікарських препаратах" дозволить підібрати найоптимальніші лікарські засоби для лікування хворих в закладах медичного профілю.

2. Розробка є фінансовою і трудомісткою. Для створення потрібно залучити відповідних спеціалістів з різних наукових галузей та створити їм належні умови для ефективної розробки системи.

Рахімов Ю.Г. (ВІТІ НТУУ „КПІ”)

АВТОМАТИЗОВАНА СИСТЕМА ПРОВЕДЕННЯ ГРУПОВОГО ЕКСПЕРТНОГО ОЦІНЮВАННЯ НА БАЗІ *WEB*-ТЕХНОЛОГІЙ

Істотним чинником підвищення наукового рівня управління є застосування при підготовці рішень математичних методів та моделей. Проте, повна математична формалізація техніко-економічних завдань часто нездійсненна внаслідок їх якісної новизни та складності. У зв’язку з цим, все ширше використовуються експертні методи, під якими розуміють комплекс логічних та математико-статистичних методів і процедур, направлених на отримання від фахівців інформації, необхідної для підготовки і вибору раціональних рішень.

Експертні методи застосовують зараз в ситуаціях, коли вибір, обґрунтування і оцінка наслідків рішень не можуть бути виконані на основі точних розрахунків. Такі ситуації нерідко виникають при рішенні сучасних проблем управління суспільним виробництвом і, особливо, при прогнозуванні та довгостроковому плануванні. Останніми роками експертні оцінки знаходять широке застосування в соціально-політичному і науково-технічному прогнозуванні, в плануванні народного господарства, галузей, об’єднань, в розробці крупних науково-технічних, економічних і соціальних програм, у вирішенні окремих проблем управління.

Методи експертних оцінок – це методи організації роботи з фахівцями-експертами і обробки думок експертів. Ці думки, зазвичай, висловлені частково в кількісній, частково в якісній формі. Експертні дослідження проводять з метою підготовки інформації для ухвалення рішень особою, що приймає рішення. Для проведення роботи за методом експертних оцінок створюють робочу групу, яка й організовує за дорученням діяльність експертів, об’єднаних в експертну комісію.

В теперішній час застосовуються різні різновиди методу експертних оцінок. До основних видів відносяться: анкетування і інтерн’ювання; мозковий штурм,

метод Дельфі, дискусія; нарада, оперативна гра; сценарій. Кожен з цих видів експертного оцінювання має свої переваги та недоліки, що визначають раціональну сферу застосування. У багатьох випадках найбільший ефект дає комплексне застосування декількох видів експертизи.

Для реалізації експертного оцінювання добре підходять Web-технології. Основними причинами цього є сьогоднішнє поширення Інтернету на планеті, оперативність проведення оцінювання, практично моментальна обробка результатів, зручність проведення оцінювання для експертів, залучення більшої кількості експертів, наочність та інтерактивність.

Сьогодні експертні оцінки у поєднанні з іншими математико-статистичними методами є важливим інструментом вдосконалення управління на всіх рівнях виробництва.

Миронюк О.І. (ВІТІ НТУУ „КПІ”)

МЕТОДИ ОЦІНКИ НАДІЙНОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

У даній доповіді розглядаються методи оцінки надійності програмного забезпечення, що базуються на негомогенному пуасонівському процесі.

Основною метою доповіді є провести дослідження моделей оцінювання надійності програмного забезпечення, виявити недоліки та підвищити показники надійності.

Існує декілька моделей оцінки надійності програмного забезпечення, що базуються на негомогенному пуасонівському процесі:

- модель Гоеля-Окумото;
- модель Шнайдевінда;
- модель Муси;
- S-подібна модель зростання надійності.

Були розглянуті основні відомі моделі, що базуються на негомогенному пуасонівському процесі – моделі Гоеля-Окумото, Шнайдевінда, Муси та S-подібну модель. Якість роботи розглянутих моделей була перевірена на практиці на базі реальних даних про кількість виявлених несправностей та їхній розподіл у часі.

В ході проведення дослідження було запропоноване узагальнення та розширення моделей, що базуються на пуасонівському процесі.

Любарський С.В. (ВІТІ НТУУ „КПІ”)
Вакарук І.В. (ВІТІ НТУУ „КПІ”)

МЕТОДИКА ОЦІНКИ ЕФЕКТИВНОСТІ КОМП’ЮТЕРНИХ ТРЕНАЖНИХ СИСТЕМ У НАВЧАЛЬНОМУ ПРОЦЕСІ

У даній доповіді презентується методика оцінки ефективності комп’ютерних тренажерних систем у навчальному процесі.

Основною метою її є вироблення необхідної методики для оцінювання тренажерних систем.

В якості найбільш поширених форм комп’ютерного навчання, можна зазначити:

– електронні підручники;
– засоби віртуальної реальності;
– системи дистанційного навчання;
– імітаційні тренажерні системи;
– експертні системи навчального характеру.

Однією з найпопулярніших серед вищезгаданих форм на сьогоднішній день є імітаційні тренажерні системи.

Кожна тренажерна система по сутті є ІС. Тому логічно розглянути для початку основні підходи щодо оцінки якості інформаційних систем.

До характеристик якості інформаційних систем можна віднести:

– загальну корисність;
– початкову корисність;
– зручність експлуатації.

Основними критеріями якості навчальних програм є:

– ефективність комп’ютерної підтримки;
– методичні властивості;

– якість екранного дизайну;

– економічна обґрунтованість.

Основним критерієм оцінки ефективності є загальноприйнятий критерій економічної ефективності капітальних витрат на організацію процесу навчання, який визначається наступним виразом:

$$E = \frac{\Delta C}{S}$$

де ΔC – загальний економічний ефект, S – сумарні витрати на проектування.

Сімончук О.В. (ВІТІ НТУУ „КПІ”)

ЗАСТОСУВАННЯ МЕТОДІВ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ДАНИХ У СИСТЕМАХ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Виявлення вторгнень залишається областю активних досліджень вже протягом тривалого часу. Вважається, що початок цьому напряму був покладений в 1980 р. статтею Джеймса Андерсона „Моніторинг погроз комп’ютерній безпеці”.

Існує дві основні категорії методів виявлення вторгнень: виявлення аномалій і виявлення зловживань. На практиці найчастіше використовується комбінація цих підходів.

Виявлення аномалій використовує моделі передбачуваної поведінки користувачів і додатків, інтерпретуючи відхилення від „нормальної” поведінки як потенційне порушення захисту .

Системи виявлення зловживань, по суті, визначають, що йде не так, як повинно. Вони містять описи атак („сигнатури”) і шукають відповідність цих описів в потоці даних, що перевіряються, з метою виявити прояв відомої атаки.

Для виявлення аномалій, можна використати інформаційно-теоретичну міру – ентропію. Класифікаційні правила індуктивно навчаються за даними аудиту (або за мережевими даними) і використовуються як модель виявлення вторгнень. Головна вимога до правил – створити ефективну модель виявлення, тобто в першу чергу, повинна бути створена відповідна множина особливостей. Основна ідея полягає в автоматичній конструкції особливостей. Надалі, застосувавши алгоритми добування даних, можна обчислити шаблони частотної діяльності системи або мережі, автоматично аналізуючи які можливо генерувати додаткову множину особливостей для виявлення вторгнень.

Петрище А.В. (ВІТІ НТУУ „КПІ”)

ІНФОРМАЦІЙНО-АНАЛІТИЧНА СИСТЕМА МОНІТОРИНГУ БІБЛІОТЕЧНО-ІНФОРМАЦІЙНИХ РЕСУРСІВ

Зі збільшенням фондів великих бібліотек актуальною стає необхідність якісного і об’єктивного аналізу інформаційних потоків, зокрема, потоку читацьких запитів, рівень задоволення яких є важливою характеристикою діяльності бібліотеки. Сам по собі такий аналіз виявився б трудомістким, тому доцільніше аналізувати не вимоги читачів, а відповіді книгосховища, що дозволяє відтворити не менш реальну картину. Поява негативних відповідей інформаційно-аналітичної системи (ІАС) книгосховища неминуча, оскільки певна кількість видань завжди знаходиться на бронеполицях, в ремонті, або екземплярність не відповідає попиту. Саме моніторинг потоку відповідей ІАС книгосховища може дати відповіді на питання, з якої причини найчастіше залишається незадоволеним запит читача. Результатом такого моніторингу стане підготовка рекомендацій для прийняття обґрунтованих управлінських рішень з оптимізації топології зберігання фондів та коригування політики комплектування літературою бібліотек.

Оскільки потік запитів користувачів, а, отже, і відповідей книгосховища, є рівномірним, немає потреби аналізувати всі відповіді. Достовірну оцінку з допустимою помилкою можна отримати, аналізуючи лише невелику вибірку (до 3 % відповідей). Дані будуть більш достовірні, якщо аналіз проводити в різні дні тижня і в різні години.

У доповіді розглядаються питання розробки інформаційно-аналітичної системи моніторингу бібліотечно-інформаційних ресурсів, де аналізу підлягають тільки запити на видання, занесені до електронного каталогу. Відбір карток відповідей для аналізу здійснює відповідальна особа, або оператор.

Методика, яка пропонується в даній роботі, реалізує наступну схему:

Етап 1. Ведення бази даних відповідей книгосховища. Відповіді книгосховища відбираються без певного правила. Єдиний критерій відбору

відповідей для автоматизованої обробки – це наявність видання в електронному каталозі бібліотеки.

Етап 2. Аналізування бази даних відповідей книгосховища. Доцільно проводити аналіз отриманих даних за однією або декількома категоріями аналізу. Кожна категорія аналізу виконується за відповідним алгоритмом, кожний з яких використовує певні поля з повної бази відповідей книгосховища. Результатом аналізу за кожною категорією буде відповідна відомість (звіт), яка дозволить спеціалістам зробити належні висновки і допоможе виробити рекомендації для прийняття управлінських рішень.

У результаті застосування запропонованої методики буде здійснений моніторинг інформаційного потоку відповідей книгосховища, результатом якого стане підготовка рекомендацій для прийняття обґрунтованих управлінських рішень з оптимізації зберігання фондів та коригування політики комплектування літературою бібліотек.

Василенко В.В. (ВІТІ НТУУ „КПІ”)

ОЦІНКА ІНФОРМАЦІЙНИХ СИСТЕМ З УРАХУВАННЯМ КІЛЬКІСНИХ І ЯКІСНИХ ПОКАЗНИКІВ

Істотним чинником підвищення наукового рівня управління є застосування при підготовці рішень математичних методів та моделей. Проте, повна математична формалізація техніко-економічних завдань часто нездійсненна внаслідок їх якісної новизни та складності. У зв’язку з цим все ширше використовуються експертні методи, під якими розуміють комплекс логічних та математико-статистичних методів і процедур, направлених на отримання від фахівців інформації, необхідної для підготовки і вибору раціональних рішень.

Експертні методи застосовують зараз в ситуаціях, коли вибір, обґрунтування і оцінка наслідків рішень не можуть бути виконані на основі точних розрахунків. Такі ситуації нерідко виникають при рішенні сучасних проблем управління суспільним виробництвом і, особливо, при прогнозуванні та довгостроковому плануванні. Останніми роками експертні системи знаходять широке застосування в соціально-політичному і науково-технічному прогнозуванні, в плануванні народного господарства, в розробці крупних науково-технічних, економічних і соціальних програм, у вирішенні окремих проблем управління.

Системи підтримки прийняття рішення – комп’ютерна інформаційна система, що використовується для різних видів діяльності при прийнятті рішення в ситуаціях, де неможливо або небажано мати автоматичну систему, повністю виконуючи весь процес рішення

Методи експертних оцінок – це методи організації роботи з фахівцями-експертами і обробки думок експертів. Ці думки, зазвичай, висловлені частково в кількісній, частково в якісній формі. Експертні дослідження проводять з метою підготовки інформації для ухвалення рішень особою, що приймає рішення.

Сьогодні застосовуються різні методи добування експертної інформації. До основних видів відносяться: анкетування і інтерв'ювання; мозковий штурм, метод Дельфі, дискусія; нарада, оперативна гра; сценарій. Кожен з цих видів експертного оцінювання має свої переваги та недоліки, що визначають раціональну сферу застосування, та метод обробки цих оцінок. У багатьох випадках найбільший ефект дає комплексне застосування декількох методів.

Для реалізації експертного оцінювання добре підходять системи підтримки прийняття рішення. Основними причинами цього є оперативність проведення оцінювання, швидка обробка результатів, зручність проведення оцінювання для експертів та звичайних користувачів, можливість донавчання системи.

Сьогодні експертні оцінки у поєднанні з іншими математико-статистичними методами є важливим інструментом вдосконалення управління на всіх рівнях виробництва.

Мужеський К.К. (ВІТІ НТУУ „КПІ”)

МЕТОДИКА ОЦІНКИ ЕФЕКТИВНОСТІ ЗАСТОСУВАННЯ ПАК „ТЗІТ” СП В НАВЧАЛЬНОМУ ПРОЦЕСІ

У даній роботі розглянуто методики оцінки ефективності даної системи за визначеними параметрами, зроблено оцінку ефективності впровадження розробленого програмного продукту, а також описана інструкція з використання інформаційно-довідкової системи.

Провівши аналіз підходів до створення програмно-апаратного комплексу для підтримки учбового процесу з проведення занять з дисципліни „Технічне забезпечення інформаційних технологій”, створено систему управління активними візуальними засобами, та дистанційне керування комплексом.

З точки зору ергономічної оцінки програмний продукт характеризується якісним та придатним до експлуатації. Ергономічні показники визначають пристосованість даного програмного продукту до забезпечення оптимальних умов праці працівника навчальної лабораторії кафедри № 21.

Чабан А.О. (ВІТІ НТУУ „КПІ”)

МЕТОДИКА РОЗРОБКИ АВТОМАТИЗОВАНОЇ СИСТЕМИ ОБЛІКУ АПАРАТНИХ ЗАСОБІВ ЛОКАЛЬНОЇ ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ

У даній доповіді презентуються актуальність та шляхи рішення розробки обліку апаратних засобів локальної обчислювальної мережі.

Актуальність роботи полягає в тому, що на сьогодні ще не існує програми обліку апаратних засобів, яка б відповідала ряду вимог, а саме: була безкоштовною, підтримувала нові апаратні засоби в повній мірі, мала блок ведення бази даних апаратних засобів, які знаходяться в локальній обчислювальній мережі підприємства, мала мережеву підтримку і інтерфейс українською мовою. До того ж не існує повного огляду програм обліку апаратних засобів, в якому вони порівнюються і виділяються їх переваги і недоліки. Існуючі огляди виділяють одну, або дві програми і які постають для кінцевих користувачів без альтернативи вибору.

Для вирішення задачі автоматизації обліку апаратних засобів локальної обчислювальної мережі виробниками програмного забезпечення створено ряд програм. На створення та процес налагодження до стабільно працюючих версій витрачається від 8 до 12 місяців. Багато часу займає налагодження стосунків з виробниками апаратних засобів, які повинні надавати інформацію про вже існуючі апаратні засоби. Зокрема, з виходом нових апаратних засобів потрібно було випускати нові версії програм, які б їх підтримували. Колективи підрозділів, зайнятих розробкою програм автоматизації обліку апаратних засобів, налічують не менше 6–10 осіб, також в тестуванні нових версій програм бере участь велика кількість бета-тестерів, які знаходять помилки в розроблених програмах, та повідомляють про це розробників. Частина осіб займається розробкою інтерфейса програми, частина – пише код програми. Велика увага приділяється рекламі

Шевчик О.Л. (ВІТІ НТУУ „КПІ”)

АВТОМАТИЗОВАНА СИСТЕМА ТОВАРНОГО ОБЛІКУ ПІДПРИЄМСТВА

У даній доповіді розглядається спосіб вирішення проблеми співробітників торгівельного підприємства. У наш час обсяги інформації стрімко збільшуюються, у зв’язку з чим з’являється нагальна потреба у структуруванні інформації та у автоматизації доступу до неї, а також введення у роботу свого наукового підходу по даному проекту.

Основною метою даної системи є автоматизація роботи торгівельного підприємства, що значно спрощує роботу логістів, щодо пошуку необхідної інформації. Ця система була розроблена з урахуванням усіх потреб користувачів. В першу чергу, враховувались вимоги до швидкодії та до користувальницького інтерфейсу. У ході проектування було проведено ретельні дослідження щодо вибору засобів та технологій для реалізації. Виробничий процес являє собою:

– затвердження плану реалізації системи;
– узгодження періодів звітності у замовника;
– об’єднання підсистем у єдину систему;
– фінальне тестування;
– фінальне звітування;
– впровадження системи на виробництві.

Таким чином, торгівельне підприємство отримає досконалу та практичну в роботі програму, оскільки вона являє у собі:

- швидкий доступ до необхідних файлів;
- повний набір необхідного функціоналу;
- надійність у використанні.