НПК МНІС ІП-2018

ЗБІРНИК НАУКОВИХ ПРАЦЬ МОЛОДИХ НАУКОВЦІВ І СТУДЕНТІВ

ЧАСТИНА 5

ПРИСВЯЧУЄТЬСЯ 30-РІЧЧЮ ПІДГОТОВКИ ІТ-ФАХІВЦІВ В ХМЕЛЬНИЦЬКОМУ НАЦІОНАЛЬНОМУ УНІВЕРСИТЕТІ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Хмельницький національний університет

Військовий інститут Київського національного університету ім.Тараса Шевченка

ПВНЗ "Університет економіки і підприємництва"

Тернопільський інститут агропромислового виробництва

Інтелектуальний потенціал - 2018

збірник наукових праць молодих науковців і студентів

Присвячується 30-річчю підготовки ІТ- фахівців в Хмельницькому національному університеті

сформовано за матеріалами
Всеукраїнської науково-практичної конференції
молодих науковців і студентів «Інтелектуальний потенціал – 2018»

14-16 листопада 2018р.

Частина 5
Актуальні проблеми інформаційних технологій і суспільства

Хмельницький
2018

ББК 74.480.278
С.88

«Інтелектуальний потенціал – 2018» - збірник наукових праць молодих науковців і студентів з нагоди 30-річчя підготовки ІТ- фахівців в ХНУ/ Колектив авторів – Хмельницький: ПВНЗ УЕП, 2018. – Ч.5: Актуальні проблеми інформаційних технологій і суспільства. – 76 с.

ЗМІСТ

Алгоритм паралельного динамічного налаштування комутаційної системи

Барвінський С.С., Кльоц Ю.П., Чешун В.М.
Хмельницький національний університет

Широке поширення мережних технологій та засобів телекомунікацій вимагає постійного вдосконалення засобів і систем, що забезпечують доставку і розподіл повідомлень між пунктами мережі. Для цієї мети використовуються такі пристрої як повторювачі, концентратори, комутатори і т.д.

Однак в останні роки простежується стійка тенденція витіснення комутаторами інших видів активного устаткування. Це пов'язано, перш за все, з розвитком технології виробництва мікроелектронних компонентів, і як наслідок зменшення показника «ціна/якість» для окремого порту комутатора. При зниженні вартості комутаційного обладнання, ринок комутаторів продовжує зростати, і за прогнозами фахівців ця тенденція збережеться ще кілька років. Оцінка динаміки ринку комутаційного обладнання, виконана Dell 'Oro Group, представлена на рисунку 1.

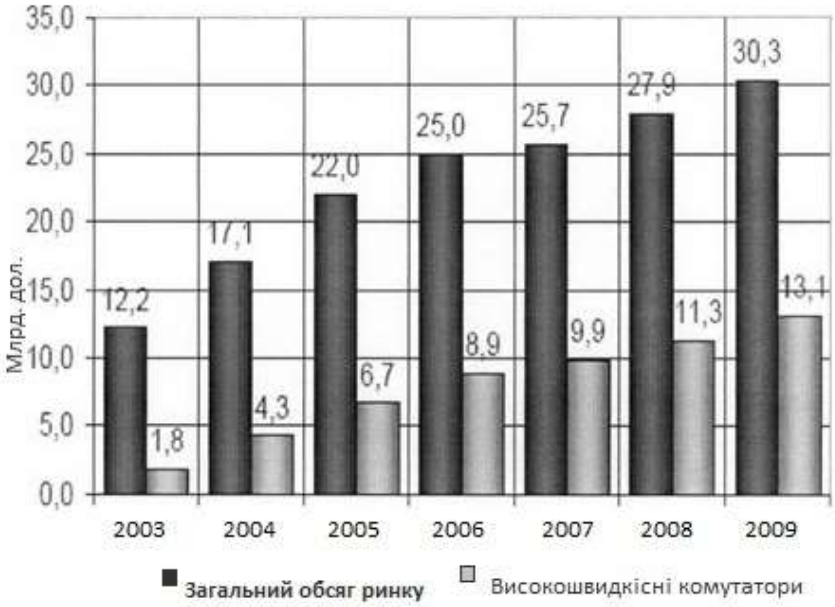


Рисунок 1 – Оцінка динаміки ринку комутаційного обладнання

При таких великих обсягах ринку комутаційного обладнання необхідна розробка способів зменшення втрат в системах комутації, і зокрема способів паралельного динамічного налаштування комутаційних систем. При цьому однією з найважливіших задач є задача розробки методів моделювання подібних пристроїв, що дозволить прогнозувати їх технічні характеристики (ймовірності втрат вимог на з'єднання, пропускну здатність систем і т.д.).

Реалізація паралельного налаштування комутаційних систем дозволить скоротити час налаштування комутаційних систем і підвищити пропускну здатність комутаційних систем за рахунок зниження втрат на центральному керуючому пристрої.

При описі алгоритмів і моделей функціонування систем традиційно використовуються блок-схеми і мови програмування. Останнім часом при описі роботи абстрактних систем широке застосування знаходить теорія множин і псевдо-мови.

Теорія множин дозволяє описувати роботу різних систем, виконання різних операцій, забезпечуючи необхідний рівень абстрагування знань про систему.

Комутаційні системи з паралельною динамічної налаштуванням є складними системами і при описі моделі паралельного налаштування в даній роботі використовуються елементи теорії множин.

З іншого боку комутаційні системи є системами масового обслуговування і тому при побудові математичної (аналітичної) моделі комутаційних систем з паралельною динамічним налаштуванням використовується апарат теорії масового обслуговування.

Реалізація паралельного динамічного налаштування матричних комутаційних систем з просторовим розділенням каналів представляє собою m паралельно працюючих процесів. Кожен такий процес, в свою чергу, описується алгоритмом, наведеному на рисунку 2.

Відповідно до алгоритму джерелами навантаження проводиться генерація вимог на обслуговування (викликів). До настання моменту комутації вимоги що надійшли будуть очікувати його. У момент настання такту комутації вже сформовано множина заявок на встановлення з'єднання в момент часу t. Одночасно формується множина доступних вихідних ліній в даному кванті. Далі проводиться порівняння заголовків вимог з ідентифікаторами доступних каналів. У разі якщо вони збіглися, встановлюється потенційне з'єднання. І, нарешті, після операції виділення пріоритету, який визначається в залежності від просторового розташування вхідної лінії, з якої надійшов запит, встановлюється з'єднання.

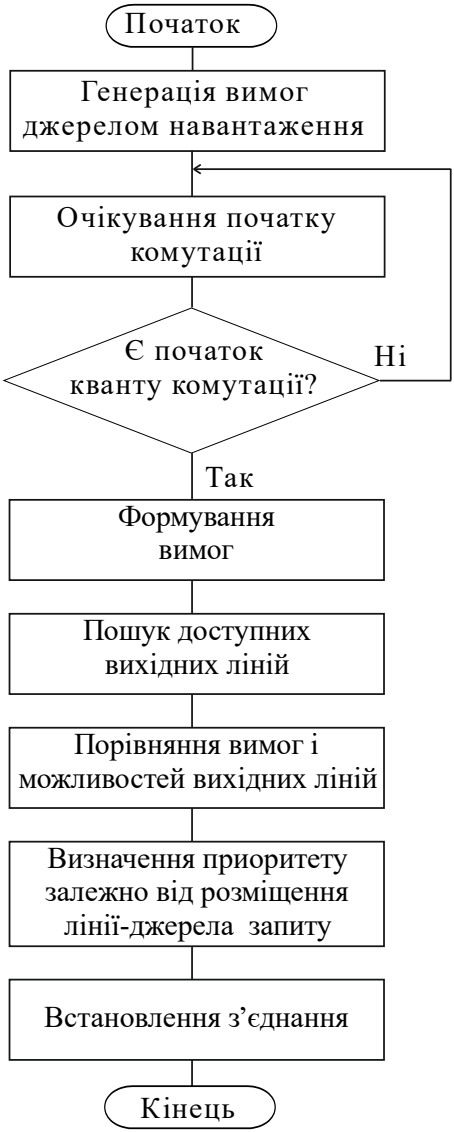


Рисунок 2 – Алгоритм паралельного динамічного налаштування комутаційної системи з просторовим розділенням каналів

В задачі теорії розподілу інформації (телетрафіку) визначається задача знаходження залежності між набором наступних параметрів: потоку

заявок, процесу обслуговування та дисципліни обслуговування, що характеризують якісні показники комутаційної системи:

$$P=f(П,S,Д) \quad (1)$$

де P – якість обслуговування (втрати); $П$ – поступаючий потік заявок; S – процес обслуговування, який визначається схемою комутації; $Д$ – дисципліна обслуговування.

Потік заявок $П$ в загальному випадку залежить від характеру інформаційної системи та його характеристики можуть бути різні для різних систем. Вхідний потік вимог описується розподілом ймовірностей інтервалів часу між сусідніми вимогами. Зазвичай припускають, що ці інтервали часу незалежні і мають однаковий розподіл випадкових величин, які утворюють стаціонарний вхідний потік вимог. Класична теорія масового обслуговування (частиною якої є і теорія телетрафіку) розглядає Пуассонівський (найпростіший) потік вимог, який характеризується:

- стаціонарністю – ймовірність появи k викликів на будь-якому проміжку часу залежить тільки від числа викликів k і від тривалості t проміжку і не залежить від початок його відліку, тобто вважають сталість у часі щільності надходження викликів;
- ординарність - за нескінченно малий проміжок часу одночасно може прийти тільки один виклик;
- відсутністю післядії - незалежність ймовірних характеристик потоку від вже надійшли дзвінки.

Процес обслуговування S – є складною випадково. величиною, з огляду на те, що він може мати багатофазовий характер.

Потік звільнень - послідовність моментів закінчення обслуговування викликів. У загальному випадку властивості і характеристики потоку звільнень залежать від поступаючого потоку викликів, якості обслуговування цих викликів, закону розподілу тривалості обслуговування.

Інтенсивність потоку звільнення β - середня частота обслуговування викликів, вимірювана середнім числом обслужених викликів в одиницю часу. Відповідно, 1/β- середня тривалість обслуговування (середня тривалість зайнятості пристрою).

Дисципліна обслуговування $Д$ - визначає взаємодію потоку викликів з системою розподілу інформації. Її зазвичай характеризують:

- способами обслуговування викликів (з втратами, з очікуванням, комбіноване обслуговування);
- порядком обслуговування викликів (в порядку черговості, у випадковому порядку, обслуговування пакетами тощо);
- режимами шукання виходів схеми (вільне, групове, індивідуальне);
- законами розподілу тривалості обслуговування викликів (показовий закон, постійна або довільна тривалість обслуговування);

- наявністю пріоритетів в обслуговуванні деяких категорій викликів;
- наявністю обмежень при обслуговуванні всіх або деяких категорій викликів (по тривалості очікування, числу викликів, що очікують у черзі, тривалості обслуговування).

Таким чином, наведений алгоритм паралельного динамічного налаштування комутаційної системи, який дає змогу ефективніше передавати дані в систем з множинними обчислювальними елементами. Вказані якісні показники комутаційної системи, на основі яких проводяться оптимізації комутаційних зв'язків.

Література

1. Гольдштейн Б.С. Системы коммутации:Учебник для ВУЗов.2-еизд. / Б.С.Гольдштейн // - СПб.:БХВ-Петербург, 2014. - 314с.

2. Гольдштейн Б.С. Системы связи:Учебник для ВУЗов. - СПб.:БХВ-Петербург, 2014. - 400с.

3. Стеклов В.К. Телекомунікаційні мережі: Підруч. для студ. вищ. навч. закл. за напрямком «Телекомунікації». / В.К.Стеклов, Л.Н. Беркман // – К.: Техніка, 2001. – 392 с.

4. Цифровые системы коммутации для ГТС / под ред. В.Г. Карташевского и А.В. Рослякова. //– М.: Эко-Трендз, 2008. – 352 с.

5. Гайворонская Г.С. Основы построения сетей и систем телефонной связи: Учеб. пособие. / Г.С. Гайворонская // – Одесса: УГАС, 1997. – 128 с.

6. Чумак М.О. Цифрова система комутації 5ESS. Навчальний посібник. / М.О. Чумак // – Одеса: УДАЗ, 1999. – 269с.

7. Комутаційні пристрої систем автоматики [Електронний ресурс] / Портал «Studopedia.com.ua». – Режим доступу: https://studopedia.com.ua/1_129139_komutatsiyni-pristroi-sistem-avtomatiki.html (дата звернення 30.10.2018). – Назва з екрана.

8. Принципи комутації каналів в цифрових системах комутації[Електронний ресурс] / Портал «Studopedia.com.ua». – Режим доступу: https://studopedia.com.ua/1_19153_printsipi-komutatsIyi-kanalIv-v-tsifrovih-sistemah-komutatsIyi.html (дата звернення 30.10.2018). – Назва з екрана.

Модель автомобільного тахографа на мікроконтролері ATmega

Бойко М.І., Чорненький В. І.
Хмельницький національний університет

Здавна у власників транспортних засобів викликало зацікавлення питання контролю за роботою найманих ними працівників на транспорті, адже всім відоме бажання водіїв підзаробити за рахунок виконання «лівих» рейсів, продажу злитих надлишків палива та інших варіантів введення в оману роботодавця.

Спроби ведення контролю за роботою транспортних засобів іншими працівниками не давали бажаного результату через наявність людського фактору з можливістю утворення між контролерами та контрольованими людьми фінансової домовленості. Крім того, потреба виплачувати контролерам заробітну плату за умови недостатньої впевненості в їх порядності призводила до зменшення зацікавленості власників транспортних засобів у створенні подібних служб.

Це зумовило виникнення у власників транспортних фірм бажання оснастити свій транспорт засобами автоматичного відстеження відповідності роботи транспортного засобу до заданого графіку руху, на роботу яких не могли б вплинути водії.

Так з’явились перші замовлення на розробку реєстраторів графіку руху транспортних засобів.

Спочатку вони носили стихійних характер і кожен замовник висував власні вимоги стосовно реєстратора графіку руху транспортного засобу. Враховуючи різні підходи щодо реалізації реєстраторів графіку руху транспортних засобів і розробниками, створювані пристрої були найрізноманітнішими як за можливостями, так і за іншими параметрами.

Незалежно від особливостей реалізації реєстраторів графіку руху транспортних засобів, в тій чи іншій мірі вони виконували основне призначення - дисциплінували роботу водіїв.

Цей фактор зумовив зацікавленість у впровадженні реєстраторів графіку руху транспортних засобів не лише у власників фірм, а і на державному і міждержавному рівні для контролю за графіками роботи водіїв з метою запобігання аваріям через людську втому або порушення графіку.

Поглянувши в історію, можна відзначити наступні етапи впровадження реєстраторів графіку руху транспортних засобів.

Реєстратори графіку руху транспортних засобів у західній Європі почали використовувати з кінця 20-х років одночасно з утворенням автопідприємств з найманими водіями.

В 60-х роках виникла необхідність створення єдиних для Європи правил і норм стосовно дорожнього руху, митного оформлення міжнародних перевезень автотранспортом, часу роботи і відпочинку водіїв, технічних та екологічних вимог тощо.

У 1965 році в Празі було укладено угоду про митне оформлення міжнародних автоперевезень (Угода АВТ).

У 1971 році в Женеві була підписана Конвенція про дорожній рух.

1 липня 1970 року була представлена для підписання розроблена Європейською комісією ООН у Женеві «Європейська угода стосовно праці екіпажів, що виконують міжнародні автоперевезення» (AETR або ЕСТР), яка набрала чинності з 5 січня 1976 року. Угода AETR зазнавала змін та доповнень (1983, 1992, 1995 рр.).

Так було розроблено європейську угоду про роботу екіпажів транспортних засобів, що виконують міжнародні перевезення.

Метою європейської угоди AETR є удосконалення міжнародних автоперевезень пасажирів і вантажів, підвищення безпеки дорожнього руху, врегулювання певних умов праці на міжнародному автотранспорті згідно з принципами Міжнародної організації праці, а також встановлення певних засобів для забезпечення дотримання вимог угоди.

Учасниками угоди AETR одразу стали: Австрія, Бельгія, Білорусь, Боснія-Герцеговина, Хорватія, Данія, Естонія, Росія, Франція, Греція, Іспанія, Голландія, Ірландія, Югославія, Люксембург, Литва, Норвегія, Польща, Португалія, Чехія, Німеччина, Молдова, Словенія, Словаччина, Швеція, Англія, Італія, Румунія, Фінляндія, Угорщина, Швейцарія.

Як бачимо, Україна до списку учасників спочатку не потрапила. Проте наші міжнародні перевізники так чи інакше зобов'язані виконувати вимоги статей 5-10 AETR стосовно віку водіїв, часу керування, відпочинку, а також наявності реєстраторів графіку руху на транспортних засобах з повною допустимою масою більше 3,5 тонни та на пасажирських автобусах з посадочними місцями більше 9. Причому реєстратори графіку руху транспортних засобів повинні відповідати вимогам додатку до угоди AETR, де визначені загальні вимоги до їх характеристик, конструкції, монтажу і контролю.

Ті, хто ігнорує вимоги названих статей AETR на собі відчувають дієвість цього документу, адже штрафні санкції в країнах Західної Європи дуже високі: від 1000$ у Німеччині до 2000$ в Англії.

З 2012 року використання реєстраторів графіку руху транспортних засобів стає обов'язковим в Україні - запроваджуються норми міжнародного права щодо обов'язкового встановлення і використання на транспортних засобах працюючих контрольних пристроїв резидентам України та нерезидентам при здійсненні міжнародних перевезень пасажирів та вантажів автотранспортом. Відповідний Закон України «Про внесення змін до Закону «Про автомобільний транспорт» (щодо упорядкування міжнародних автомобільних перевезень)» ухвалила Верховна Рада на пленарному засіданні 12 січня 2011 року.

На сьогоднішній день весь новий транспорт випускається з заводу тільки з цифровими моделями реєстраторів графіку руху транспортних засобів. Виняток становить тільки транспорт, який продається в державах, що

не входять до складу Євросоюзу.

Пропонована модель реєстратора графіку руху призначена для встановлення на борту транспортних засобів і має наступні властивості.

Тип процесора: мікроконтролер ATmega8515.

Засоби індикації – світлодіодні та LCD-індикатор.

Спосіб спряження з ЕОМ – USB-порт.

Джерело живлення – акумулятор транспортного засобу - 12 V.

Споживаний струм – від джерела живлення +12 В - 0,114 А.

Споживана потужність - 1,368 Вт.

Обсяг сервісної пам’яті – 8 Мбайт.

Обсяг пам’яті накопичення даних – 32 Мбайт.

Час безперервної роботи (накопичення даних) – 132 години (при зменшенні частоти фіксації подій – до 1 місяця).

Датчики, що контролюються:

- ключ запалювання;
- спідометр;
- датчик рівня палива;
- датчик вібрації.

Заміри виконуються від трьох до десяти раз на хвилину, періодичність програмується з урахуванням особливостей виконуваних рейсів (короткочасні по місту або дальній поза межі міста, області або держави).

На рисунку 1 зображено структуру реєстратора графіку руху.

Загалом, в складі електричної структурної схеми реєстратора графіку руху транспортного засобу можна відокремити три групи складових:

1. Обладнання транспортного засобу;
2. Безпосередньо вузли реєстратора відслідковування графіку руху транспортного засобу;
3. ЕОМ.

Обладнання транспортного засобу, в свою чергу, можна поділити на 2 категорії:

1. Контрольовані підсистеми і датчики обладнання транспортного засобу;
2. Автомобільний акумулятор, від якого виконується живлення всіх вузлів реєстратора відслідковування графіку руху транспортного засобу.

Як видно з рисунку 1, сам реєстратор графіку руху транспортного засобу в своїй роботі використовує такі блоки:

1. Мікроконтролер;
2. USB-адаптер;
3. Генератор сигналів переривання;
4. Пам'ять накопичення даних;
5. Сервісна пам'ять;
6. Ключі настроювання;
7. LCD-індикатор;

8. Блок світлодіодів;
9. Перетворювач напруги живлення.

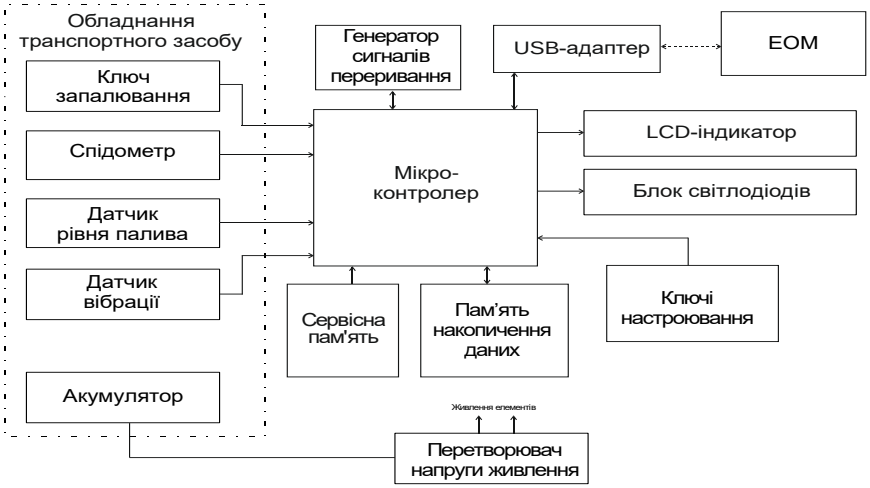


Рисунок 1 – Структурна схема реєстратора графіку руху

Живлення спроектованого реєстратора графіку руху транспортного засобу забезпечується від акумуляторної батареї транспортного засобу. Оскільки напруга живлення акумуляторної батареї залежно від її віку та якості може бути від 10 до 15 В, елементів реєстратора графіку руху транспортного засобу реалізується через перетворювач напруги живлення, який виконує перетворення вхідної напруги з акумуляторної батареї в стабільну напругу +5 вольт, необхідну для роботи блоків пристрою.

При підключенні реєстратора графіку руху транспортного засобу до живлення відбувається ініціалізація мікроконтролера.

Апаратну ініціалізацію мікроконтролера при появі живлення забезпечує схема затримки, підключена до RST мікроконтролера, яка на період зарядки її конденсатора утримує нуль на цьому вході (внутрішні схеми та лічильники мікроконтролера переводяться при цьому в початковий стан). Після завершення зарядки конденсатора на вході RST мікроконтролера фіксується неактивний високий рівень сигналу скидання і мікроконтролер може починати працювати за заданою програмою.

Для забезпечення більшої стабільності роботи реєстратора графіку руху транспортного засобу обрано включення мікроконтролера із застосування зовнішньої схеми синхронізації на базі кварцового генератора, яку підключено до входів синхронізації мікроконтролера XTA1 і XTAL2.

Після фіксації на вході RST неактивного високого рівня сигналу скидання і мікроконтролер зчитує базовий програмний код з власної

програмної пам’яті, настроює потрібні режими роботи своїх внутрішніх схем, а також проводить ініціалізацію робочих режимів інших вузлів пристрою.

Оскільки власної програмної пам’яті мікроконтролера недостатньо для зберігання всього програмного коду та службових даних (зокрема, для зберігання всіх текстів повідомлень, що виводяться на LCD-індикатор), в складі реєстратора графіку руху транспортного засобу передбачена сервісна пам'ять, до якої мікроконтролер звертається за потреби. Сервісна пам'ять реалізована на базі мікросхеми FLASH-пам’яті, що дозволяє багатократний перезапис даних та зберігає їх незалежно від наявності напруги живлення. Обраний FLASH-ОЗП підтримує протокол I2C, що дозволяє реалізувати передачу даних між мікроконтролером і сервісною пам'яттю задіявши дві лінії порту D мікроконтролера PD4 і PD5.

Одразу зазначимо, що подібний варіант організації застосовано і для накопичення даних - пам’ять накопичення даних побудована також на мікросхемах FLASH-пам’яті, кожна з яких підтримує протокол I2C. Їх в пам’яті накопичення даних застосовано чотири штуки, керування цими мікросхемами для більшої універсальності і надійності ведеться по різних лініях порту C мікроконтролера.

Для визначення моментів зчитування даних з контрольованих датчиків і забезпечення стабільності інтервалів часу між вимірюваннями в схемі спроектованого реєстратора відслідковування графіку руху транспортного засобу застосовано генератор сигналів переривання, який із заданою періодичністю формує на вході PD2 мікроконтролера сигнали запиту на переривання. За цими сигналами мікроконтролер переходить до виконання процедури обробки переривання, в ході якої опитує датчики за заданим програмою алгоритмом.

Зазначимо, що застосований генератор сигналів переривання забезпечує можливість перепрограмування безпосередньо в схемі (з допомогою мікроконтролера під керуванням ЕОМ). Взаємодія при програмуванні генератора сигналів переривання з мікроконтролером також реалізується за протоколом шини I2C, передачу даних між мікроконтролером і пам'яттю генератора сигналів переривання виконуєтьться також через лінії PD4 і PD5 порту D мікроконтролера (конфлікту з сервісною пам'яттю спроектованого реєстратора відслідковування графіку руху транспортного засобу при цьому не виникає, оскільки ідентифікаційні коди цих схем різні).

Зчитані з датчиків дані фіксуються в пам’яті накопичення даних і можуть переглядатися на LCD-індикаторі.

На LCD-індикатор зазвичай виводяться розширені показники годинника, серед яких поточна дата та час, день тижня, ознака запуску режиму будильника. Також на LCD-індикаторі можна проглядати накопичені. Дані для відображення на LCD-індикатор передаються з лінії PA0-PA7 (порт A) мікроконтролера, а через лінії PB2-PB4 (порт B) на LCD-індикатор мікроконтролер передає сигнали керування. LCD-індикатор

додатково оснащений кнопкою активізації режиму підсвічування його екрану, яку підключено для спеціально призначеного для цього входу LEDA за типовою схемою керування під світкою, що робить більш зручним використання пристрою в темну пору доби. До входу Uee LCD-індикатора підключений регульований резистор, з допомогою якого можна корегувати яскравість і контрастність відображення символів на його екрані.

Для оповіщення про роботу пристрою та справність окремих контрольованих ним вузлів в схемі реєстратора графіку руху транспортного засобу передбачено три світлодіоди, комутовані з ключами ручного управління.

В нормальному режимі роботи всі три наявні в схемі світлодіоди світяться. При замиканні ключа ручного управління відповідний з ним світлодіод гасне – це підтверджує реакцію на кнопку.

При фіксації мікроконтролером відсутності сигналу від одного з контрольованих датчиків (спідометра, датчика рівня палива або вібрації), відповідний з ним світлодіод під управлінням мікроконтролера починає миготіти (миготіння повинне сповістити людину про виявлену несправність і потребу прийняття мір з подальшим сповіщенням про несправність диспетчерської служби).

Світлодіоди мають наступне призначення:

– перший світлодіод (підключений до контакту PB5 порту B мікроконтролера) з'єднаний з ключем вибору режиму настроювань (настроювання годинника, будильника, відображуваних на індикатор даних та інше), стосовно датчиків відповідає за індикацію справної роботи або виходу з ладу спідометра;

– другий світлодіод (підключений до контакту PB6 порту B мікроконтролера) з'єднаний з ключем збільшення значення відповідно до обраного режиму настроювань, стосовно датчиків відповідає за індикацію справної роботи або виходу з ладу вібродатчика;

– третій світлодіод (підключений до контакту PB7 порту B мікроконтролера) з'єднаний з ключем зменшення значення відповідно до обраного режиму настроювань, стосовно датчиків відповідає за індикацію справної роботи або виходу з ладу датчика палива.

Блок ключів управління складається з трьох ключів, які дозволяють виконати деякі функції керування настройками реєстратора графіку руху транспортного засобу (настроювати дані годинника, встановлювати настройки будильника, керувати переглядом накопичених даних та інше).

Зазначені ключі виконують такі функції:

– перший ключ відповідає за вибір режиму (наприклад, настоюваного параметра годинника або типу аналізованих даних);

– другий ключ забезпечує збільшення значення відповідно обраного режиму (наприклад, прокручує відображувані дані вперед, збільшує обраний

часовий параметр годин, хвилин, дати та інше);

– третій ключ забезпечує меншення значення відповідно обраного режиму (наприклад, прокручує відображувані дані назад, зменшує обраний часовий параметр годин, хвилин, дати та інше).

Зазначені ключі не надають змоги змінювати накопичені дані, а також програму роботи реєстратора графіку руху транспортного засобу.

Всі функції загального настроювання реєстратора графіку руху транспортного засобу та зчитування з нього даних зі стиранням їх з пам'яті можливі до реалізації лише з допомогою ЕОМ.

Оскільки застосований мікроконтролер не має можливості комутації до портів ЕОМ безпосередньо, в схемі реєстратора графіку руху транспортного засобу передбачено USB-адаптер. USB-адаптер дає можливість взаємодії реєстратора графіку руху транспортного засобу з ЕОМ із використанням стандартного USB-порту персонального комп'ютера. Мікроконтролер також безпосередньо не має засобів реалізації інтерфейсу USB-порту, тому для цього використовується внутрішня схема UART мікроконтролера (реалізує інтерфейс RS-232, властивий COM-порту ЕОМ, але не узгоджений за рівнями сигналів), що зкомутована з його виводами RXD і TXD (PD0 і PD1 порту D). До цих виводів ззовні мікроконтролера підключено схему USB-адаптера, що узгоджує роботу мікроконтролерного інтерфейсу RS-232 і USB-порту ЕОМ. Окрім підключення USB-адаптера до інтерфейсних контактів схеми UART мікроконтролера, він також має підключення до виходу мікроконтролера PD6, звідки сигнал надходить на вхід SLEEP USB-адаптера для забезпечення переводення цього блоку в режим економі ї енергоспоживання – застосування цього режиму зменшує споживану реєстратором графіку руху транспортного засобу потужність. Оскільки взаємодія з ЕОМ в роботі реєстратора графіку руху транспортного засобу займає малий відсоток, це повністю виправданий крок (для активізації USB-адаптера в достатньо підключити реєстратор графіку руху транспортного засобу до USB-порту ЕОМ або відповідна активізація може виконуватись мікроконтролером при перевірці наявності з'єднання з ЕОМ).

Література

1. Про затвердження Інструкції з використання контрольних пристроїв (тахографів) на автомобільному транспорті. [Електронний ресурс] / Офіційний сайт Міністерства транспорту та зв'язку УКРАЇНИ. – Режим доступу: http://zakon2.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=z0946-10 (дата звернення 30.09.2018). – Назва з екрана.

2. Використання тахографів у вантажних перевезеннях [Електронний ресурс] / Сайт ТзОВ "Кий Авіа Карго" – Режим доступу: https://www.cargo-ukraine.com/uk/vikoristannya-taxografiv-u-vantazhnix-perevezennyax (дата звернення 28.10.2018). – Назва з екрана.

3. При здійсненні міжнародних перевезень українські

автоперевізники мають використовувати тахографи [Електронний ресурс] / Урядовий портал. Єдиний веб-портал органів виконавчої влади України – Режим доступу: http://old.kmu.gov.ua/kmu/control/uk/publish/article?art_id =244865811& cat_id= 248446163 (дата звернення 28.10.2018). – Назва з екрана.

4. Укртрансінспекція: Більшість автомобільних перевізників не використовують тахографи [Електронний ресурс] / Урядовий портал. Єдиний веб-портал органів виконавчої влади України – Режим доступу: https://www.kmu.gov.ua/ua/news/247394736 (дата звернення 28.10.2018). – Назва з екрана.

5. Цифровий тахограф - безпека водія [Електронний ресурс] / Сайт фірми RENAMAX TIR service, м.Рівне – Режим доступу: http://stenck.com/?p=tahografy (дата звернення 30.09.2018). – Назва з екрана.

6. Тахографи цифрові та аналогові [Електронний ресурс] / Сайт фірми RENAMAX TIR service, м.Рівне – Режим доступу: http://goldenpages.rv.ua/svitaho (дата звернення 30.09.2018). – Назва з екрана.

7. Цифровий тахограф Smartach [Електронний ресурс] / Сайт фірми "КАМ"– Режим доступу: http://kam.com.ua/takhografy/digital-tahograf.html (дата звернення 25.10.2018). – Назва з екрана. Фирма

8. Лемешонок С. Все о тахографах [Електронний ресурс] / Веб сайт Лемешонка С – Режим доступу: http://tachograph.su/content/actia-smartach (дата звернення 28.10.2018). – Назва з екрана.

9. Тахограф Flextach [Електронний ресурс] / Сайт фірми RENAMAX TIR service, м.Рівне – Режим доступу: https://svitaho.business-guide.com.ua/ products/unit?pid=182421 (дата звернення 30.09.2018). – Назва з екрана.

10. Цифровой тахограф SmarTach Actia [Електронний ресурс] / Сайт фірми Allbiz, м.Львів – Режим доступу: https://ua.all.biz/cifrovoj-tahograf-smartach-actia-g13313414 (дата звернення 25.10.2018). – Назва з екрана.

11. Міжнародні перевезення: особливості організації [Електронний ресурс] / Веб-портал golovbukh.ua – Режим доступу: https://www.golovbukh.ua/article/6113-qqq-17-m3-03-03-2017-organzatsya-mjnarodnih-perevezen (дата звернення 4.11.2018). – Назва з екрана.

Організація додаткового захисту в компоненті "рс-банкінг" системи ibank 2 ua

Грицаюк Є. С., Тітова В.Ю., Чешун В. М.
Хмельницький національний університет

РС-Банкінг являє собою компоненту системи iBank 2 UA і призначений для обслуговування в режимі офлайн клієнтів – юридичних і фізичних осіб. Дана компонента реалізована у вигляді додатку, що запускається локально на машині клієнта. Модуль РС-Банкінг повністю

аналогічний Internet-Банкінг - різниця в тому, що клієнт працює з фінансовими клієнтами локально, а обмін інформацією між клієнтом і банком відбувається в ході короткочасних сеансів зв'язку по Інтернету – синхронізація. Частота проведення синхронізації обирається клієнтом.

Загалом, синхронізація є обміном інформацією між клієнтом і сервером банку в ході короткочасного з'єднання через Інтернет або модемне з'єднання. В процесі синхронізації відбувається відправка створених і відредагованих клієнтом документів, оновлення статусів документів, довідників системи і отримання виписок по рахунках клієнта, а також оновлення версії РС-банкінг (за наявності такого).

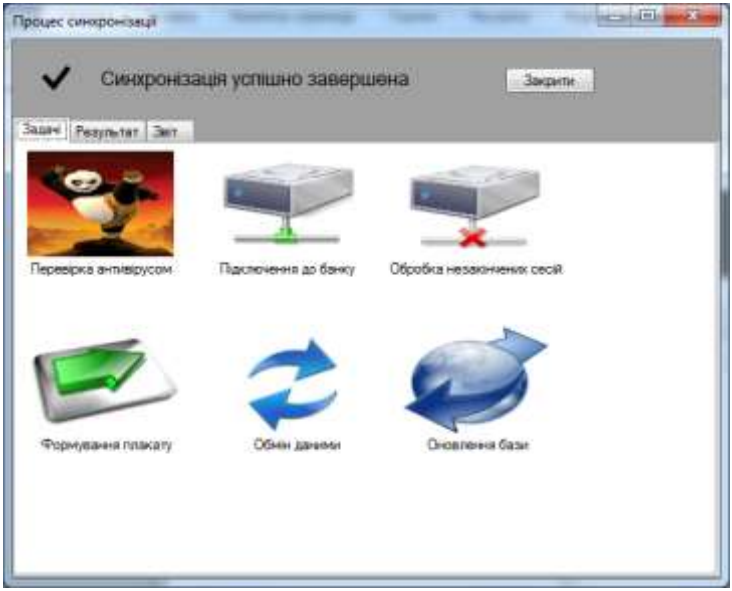
У процесі синхронізації зовнішній носій з секретним ключем ЕЦП повинен знаходитися в комп'ютері користувача.

Для проведення синхронізації слід натиснути кнопку Синхронізація на панелі інструментів. На екрані з’явиться вікно Синхронізація з банком. Зовнішній вигляд АРМа РС-банкінг для корпоративних клієнтів представлений на рисунку 1. Для початку обміну даними у вікні Синхронізація з банком натисніть кнопку Синхронізація. На екрані відкриється вікно Процес синхронізації, в якому відображається процес синхронізації з банком, яке складається з трьох вкладок (рис. 2-3).

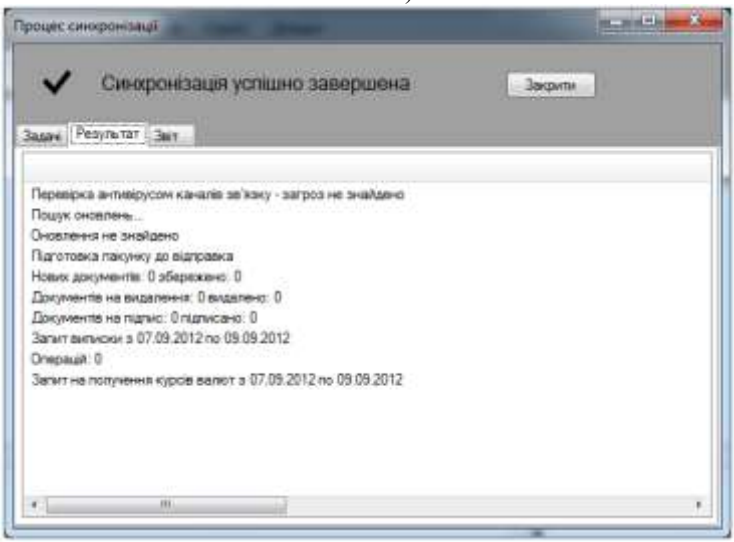
Рисунок 1 - АРМ РС-Банкінг для корпоративних клієнтів

Після завершення обміну даних у вікні Процес синхронізації слід натиснути кнопку Закрити.

Для того, щоб захистити свій комп’ютер від несанкціонованого доступу до ваших даних під час синхронізації потрібно натиснути кнопку Режим посиленої безпеки синхронізації. В результаті цього з’явиться діалогове вікно, в якому ви можете обрати або скасувати Режим посиленої безпеки синхронізації, як показано на рисунку 4.



а)



б)

Рисунок 2 - Вікна процесу синхронізації: а) задачі – перевірка антивірусом каналів зв'язку успішно). б) результат – відображається результат синхронізації окремих документів та звітів;

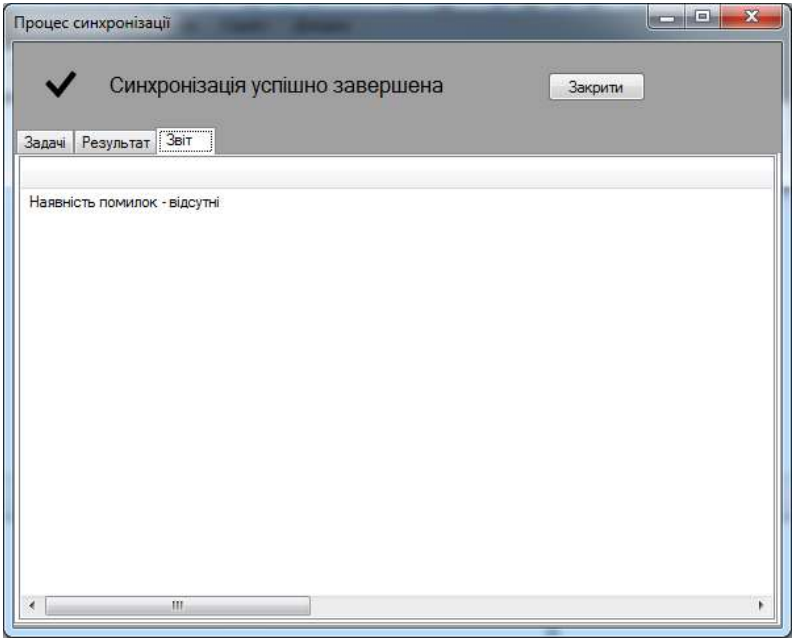


Рисунок 3 - Вікна процесу синхронізації: звіт – відображається інформація про помилки, вхідні листи, відкинуті документи.

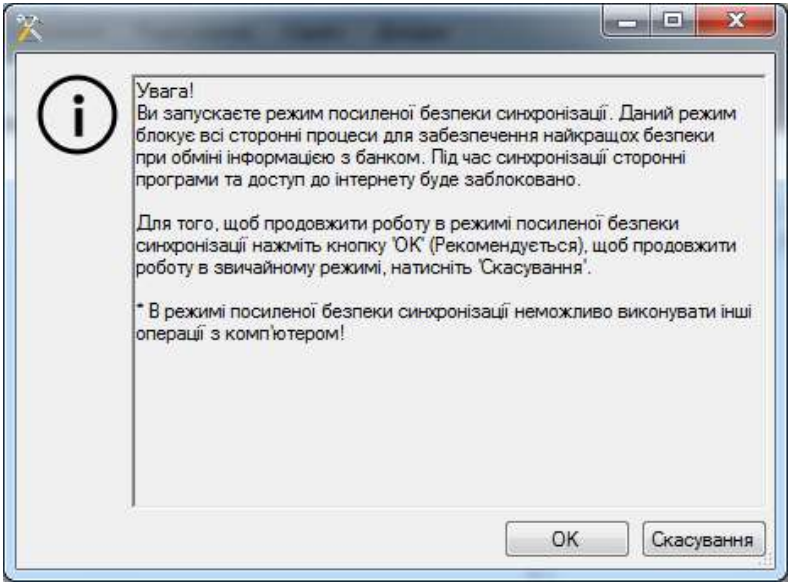


Рисунок 4 - Режим посиленої безпеки синхронізації

Основною відмінністю РС-Банкінгу від Internet-Банкінгу є відсутність необхідності підтримувати постійне з'єднання з сервером банку в процесі роботи і, як наслідок, більш низькі вимоги до каналів зв'язку. Вибір клієнтом моменту синхронізації також дозволяє працювати з iBank 2 UA при низькій або нестійкій якості зв'язку.

Для роботи з модулем РС-Банкінг корпоративні клієнти банку використовують автоматизоване робоче місце (АРМ) РС-Банкінг для корпоративних клієнтів. В АРМі РС-Банкінг для корпоративних клієнтів, що реалізований у вигляді додатку, що локально запускається, здійснюється реєстрація клієнта, адміністрування ключів ЕЦП клієнта і поточна робота клієнтів банку. Крім того, реєстрацію та адміністрування ключів ЕЦП клієнта РС-Банкінгау можна здійснювати за допомогою АРМ Реєстратора, реалізованого у вигляді java-аплету.

Скретч-карти і OTP-токени – засоби додаткової авторизації операцій в Системі «Клієнт-Банк». Вони містять шестизначні одноразові коди, що підтверджують Ваші витратні операції.

При підключенні послуги сервер Системи «Клієнт-Банк» буде підраховувати суму всіх видаткових операцій за Вашим розрахунковому рахунку з моменту останнього введення коду. При перевищенні порогової суми, визначеної Вами в Банку заздалегідь, сервер запросить у Вас в інтерфейсі Системи додатковий одноразовий код (рис. 5).

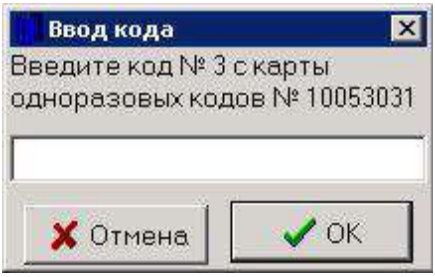


Рисунок 5 – Вікно для введення коду

Кожен код використовується тільки один раз.

Скретч-карта – пластикова картка розміру 8х5 см з 114 кодами, закритими типографічною плівкою (видаються за Вашою заявою безкоштовно), показана на рисунку 6.

При запиті чергового коду Вам необхідно стерти захисний шар з не обхідного коду будь-яким підходящим предметом і ввести його в вікно «Введення коду» в програмі.

Після закінчення 114 кодів необхідно отримати наступну карту.

Рисунок 6 - Скретч-картка

Якщо Ви здійснюєте багато операцій по списанню грошових коштів, Ви можете отримати кілька скретч-карт відразу. У цьому випадку для активації подальшої карти, необхідно буде на діючій карті стерти захисний шар над «Кодом активації наступної карти» і ввести його у вікно програми.

OTP-токен (модель – Aladdin eToken PASS) дозволяє не піклуватися про кількість одноразових кодів авторизації. Це брелок з екраном, що формує чер-гові одноразові коди без обмежень по кількості на основі унікального ключа, розміщеного в його мікропроцесорі. Після натискання на кнопку черговий код відображається протягом 20 секунд на екрані, після чого екран вимикається, приклад точену показаний на рисунку 7.

Рисунок 7 - OTP-токен

Для захисту від випадкових натиснень Система зможе прийняти від Вас не тільки поточний код, але і декілька наступних. Брелок видається за додатко-ву плату.

Порогове значення ліміту списань встановлюється за Вашою письмовою заявою і дозволяє гнучко налаштовувати цю перевірку. Якщо Ви залишите по-рогове значення по замовчуванню – 0 руб. – то черговий код буде запитуватися в кожному сеансі з видатковими операціями по Вашому рахунку. Якщо ж Ви направляєте багато доручень на списання невеликих грошових сум окремими сеансами, то Вам, можливо, буде зручно встановити деяке ненульове порогове значення – черговий код Система буде запитувати тільки після того, як сума списань досягне цього порога.

Передбачено два режими роботи модуля РС-Банкінгу для

корпоративних клієнтів – мережевий і звичайний. Робота в мережевому режимі аналогічна роботі в звичайному режимі, головна відмінність – в рамках одного примірника модуля підтримується одночасна робота декількох співробітників корпоратив-ного клієнта.

Механізми безпеки iBank 2 UA наступні.

Для забезпечення інформаційної безпеки в iBank 2 UA використовуються наступні механізми:

1. Електронний цифровий підпис під електронними документами – для забезпечення цілісності та автентичності інформації.

2. Механізм криптографічної аутентифікації сторін – для забезпечення захищеної взаємодії через Інтернет.

3. Шифрування даних – для забезпечення конфіденційності переданої через Інтернет інформації.

Для установки PC-Банкінгу скачайте з сайту банку дистрибутив, в якому вмонтований безкоштовний антивірус Panda. Наступним кроком потрібно запустити файл PC-Banking.exe, він вам встановлює клієнт та безкоштовний хмарний антивірус.

Для запобігання несанкціонованого доступу до Вашого комп'ютера ми пропонуємо скористатися спеціальною послугою і підписатися на антивірусні продукти Panda, які дозволять надійно захистити Ваші комп'ютери від всіх типів загроз з мінімальним впливом на швидкість роботи ПК. Проект реалізова-ний спільно з компанією Panda Security, одним зі світових лідерів в області антивірусного захисту і забезпечення інформаційної безпеки.

Щодо антивірусного ПЗ одним з найкращих варіантів, який можна використати це хмарний антивірус Panda Antivirus Pro 2013. "Хмарна" технологія Panda Security пропонує нову модель захисту, засновану на співтоваристві користувачів, де кожен робить свій внесок. Ваш комп'ютер завжди буде оновлений і захищений. Крім того, Ваш комп'ютер не буде обмежувати можливості виявлення, так як величезна база даних Panda для виявлення вірусів розташована в Інтернеті (в "хмарі").

Як наслідок, отримується покращений всебічний захист:

1. Захист від шпигунів, фішингу (онлайн-шахрайства), руткітів (прихованих технік зараження) і банківських троянів.

2. Захист в режимі реального часу.

3. Новий веб-фільтр для безпечної подорожі в Інтернеті.

4. Повний захист від відомих і невідомих вірусних атак.

5. Захист Ваших USB-пристроїв ("флешок") від інфекцій.

6. Файєрвол. Блокує вторгнення хакерів навіть в бездротовій мережі.

7. Режим посиленої безпеки синхронізації.

Література
1. Модуль РС - Банкинг системы iBank 2 UA: полное руководство (Версия 2.14) / М.: ООО Бифит, 2012. - 93с.
2. Особенности функционирования модуля "РС-Банкинг для корпоративных клиентов в сетевом режиме / М.: ООО Бифит, 2012. - 12с.
3. Общая информация о системе iBank 2 UA / М.: ООО Бифит, 2012. - 18с.
4. РС-Банкинг / електронний ресурс http://www.bifit.ua/decisions/pc-banking/index.html
5. Системи ELECTRONIC-BANKING / електронний ресурс http://pidruchniki.ws/13290305/bankivska_sprava/sistemi_electronic-banking

Кореляційний метод зниження похибки вимірювання потужності сигналів

Гурман І.В.
Хмельницький національний університет

Суть запропонованого підходу полягає у використанні інформації, яка міститься в фазі прийнятих сигналів, для уточнення оцінки різницю часу надходження сигналів з невідомими параметрами і на цій основі уточнення потужності прийнятих сигналів в розподілених точках прийому. У методі вимірювання сигналів [1], за обвідною сигналу або обвідною взаємокореляційної функції, запропоновано момент формування часового інтервалу, внаслідок перевищення сигналом заданого порогу, використовувати в якості попереднього наближення оцінки параметру з наступним уточненням по фазі сигналу. При цьому одночасно на інтервалі автокореляційної функції сигналу вимірюється значення несучої частоти. Подальшим розвитком даного метода є використання отриманого уточнення параметра різниці часу прийому сигналів для уточнення параметра потужності прийнятих сигналів в розподілених точках. При здійсненні попередньої оцінки різниці часу надходження імпульсного радіосигналу по його обвідній, або по максимальному значенню взаємнокореляційної функції з подальшим уточненням результату за даними вимірювання фази в точці попереднього наближення, в умовах апріорної невизначеності несучої частоти сигналу. Одночасно з вимірюванням фази сигналу додатково проводять оцінку середнього значення частоти спектру сигналу шляхом лінійного передбачення на інтервалі автокореляції сигналу [1; 2] і в подальшому визначають потужність сигналу, що відповідає уточненому значенню різниці часу.

Розвинутий метод, з врахуванням даних [1], реалізується наступним чином. Імпульсні радіосигнали, які поступають на входи вимірювача різниці часу прийому сигналу в розподілених точках прийому $U_{\grave{a}}(t)$ і $U_b(t-\tau)$,

перемножуються у змішувачах з сигналом синтезатора опорних частот. Частота вихідного сигналу синтезатора опорних частот вибирається такою, щоб проміжна частота сигналу від приймачів розподілених точок прийому, після відповідної фільтрації і підсилення в своєму підсилювачі проміжної частоти відповідала умові [1]

$$f_{ВПЧ} \le 2 \cdot f_д \tag{1}$$

де $f_{ВПЧ}$ – верхнє граничне значення спектру сигналу проміжної частоти опорного і затриманого сигналів; $f_д$ – гранично можлива в технічній реалізації частота дискретизації сигналу.

Сигнали проміжної частоти приймачів у розподілених точках прийому з виходів підсилювача проміжної частоти перетворюються в аналого-цифровому перетворювачі в цифрову форму. З виходів аналого-цифрового перетворювача оцифровані квадратурні складові сигналу одного з приймачів, затримані в регістрі затримки сигналу, поступають на входи корелятора, на інші входи якого відповідно поступають квадратурні складові сигналу з іншого приймача. В кореляторі здійснюється визначення кореляційного інтегралу [1]

$$R_{ab}(\tau) = \int_0^T U_a(t) \cdot U_b(t-\tau) dt \tag{2}$$

де $U_b(t-\tau)$ і $U_a(t)$ – амплітуди сигналів в цифровій формі, прийняті в розподілених точках прийому, затриманими між собою на часовий інтервал τ; Т – час інтегрування.

Отримані в результаті перемноження і інтегрування в кореляторі відліки дійсних і уявних складових взаємнокореляційної функції, поступають на процесор оцінки початкового наближення різниці часу і далі з нього на процесор оцінки різниці часу надходження сигналу до розподілених точок прийому $\tau_з = \tau_0 - \Delta\varphi / \omega$, на який також подається сигнал з процесору оцінки несучої частоти ω і різниці фази сигналів $\Delta\varphi$, що забезпечує визначення поправки до оцінки різниці часу.

Отримане значення уточненого різниці часу поступає на процесор оцінки потужності прийнятого сигналу в двох розподілених точках прийому $P_a = U_a^2(t)/Z_a$, $P_b = U_b^2(t-\tau_з)/Z_a$.

Слід зазначити, що попередню оцінку можна здійснювати і по обвідній вхідного імпульсного радіосигналу. З точки зору простоти технічної реалізації, перевагу має спосіб вимірювання різниці часу надходження сигналів за їх обвідною. Але даний спосіб неможливо застосувати для оцінки різниці часу надходження псевдошумових та неперервних сигналів. Тому, перевагу слід віддати кореляційному способу, описаному вище.

Середньоквадратична похибка оцінки попереднього наближення залежить від інтервалу дискретизації і співвідношення сигнал/шум [1]

$$\sigma_o = \frac{1}{\Delta\omega_e \sqrt{q}} \tag{3}$$

де q – відношення енергії сигналу до спектральної густини шуму; $\Delta\omega_e$ – еквівалентна ширина смуги спектру сигналу, при умові, що

$$\sigma_o \le \delta t \le \frac{T_o}{2} \tag{4}$$

де δt – час дискретизації кореляційного інтегралу; $\frac{T_o}{2}$ – період несучої частоти сигналу.

За оцінюване значення різниці часу надходження сигналу приймають часовий інтервал появи максимального значення різниці функції $R_{ab}(\tau_o) = \max$ відносно максимального значення автокореляційної функції сигналу, прийнятого в одній точці прийому. Високочастотне заповнення цієї функції містить інформацію про різницю фаз між сигналами. Серед великого спектру можливих варіантів побудови кореляційних вимірювачів, найбільш простими в технічній реалізації є багатоканальний, матричний і спектральний кореляційні вимірювачі [1]. Серед них особливої уваги заслуговує спектральний кореляційний вимірювач, за допомогою якого реалізується просторово–часова селекція прийнятих реалізацій сигналу. В основі принципу його роботи лежить широко відома властивість перетворення Фур'є [1]:

$$R_{ab}(t-\tau) = \int_{-\infty}^{\infty} U_a(t) \cdot U_b(t-\tau) dt = \int_{-\infty}^{\infty} S_a(\omega) \cdot S_b(\omega) \cdot e^{-j\omega\tau} d\omega \tag{5}$$

де $S_a(\omega)$ і $S_b(\omega)$ - пряме перетворення Фур'є часової реалізації сигналів $U_a(t)$, $U_b(t-\tau)$.

В силу короткої тривалості процесу випромінювання сигналу, границі інтегрування в (5) можна суттєво обмежити, що дозволить суттєво спростити технічну реалізацію кореляційного вимірювача. Час інтегрування T і смуга частот $\Delta f_{кор}$ сигналів, що обробляються, відносяться до основних параметрів кореляційних вимірювачів. Від часу інтегрування залежить співвідношення сигнал/шум на виході корелятора впливає на потенційну похибку вимірювання. Час інтегрування потрібно вибирати, виходячи із вимог забезпечення необхідних похибок вимірювання на максимальній дальності при слабких сигналу.

Для апріорно відомих джерел імпульсних радіосигналів немає необхідності час інтегрування вибирати більшим, ніж апріорно відоме максимальне значення різниці часу надходження сигналу до приймачів розподілених точок прийому або значення тривалості імпульсної послідовності радіосигналів, якщо воно перевищує максимальне значення

різниці часу надходження сигналу до приймачів. Отже, час інтегрування може знаходитись в межах від декількох десятків до сотень мікросекунд для об'єктів, які випромінюють надвисокочастотні сигнали.

За структурної схеми цифрового корелятора, який реалізує функцію (5), вибірки вхідних сигналів $U_b(t-\tau)$ і $Ua(t)$, що поступають в цифровому виді після адаптивної просторової фільтрації, накопичуються в оперативних запам'ятовуючих пристроях. Після накопичення N вибірок вхідних сигналів здійснюється швидке перетворення Фур'є, по результатах якого отримують коефіцієнти розкладу цього ряду S_{ak} і S_{bk} (k = 1… N). Після перемноження коефіцієнтів з однаковими індексами k в процесорі оцінки різниці часу надходження сигналу здійснюється оцінка попереднього наближення по максимальному значенню взаємної кореляційної функції та уточнення по фазі.

Для оцінки попереднього наближення після отримання добутків S_{ak} і S_{bk}, необхідно здійснити швидке обернене перетворення Фур'є, обчислити модуль кореляційного інтегралу $|R_{ab}(\tau)|$ і по його максимальному значенню на осі τ визначити попереднє наближення τ_o. Після цього, за даними оцінок проміжної частоти в підсилювачі проміжної частоти, несучої частоти в підсилювачі несучої частоти і по результатах вимірів різниці фази несучої частоти сигналу в процесорі оцінки проміжної частоти і процесорі оцінки фази сигналу, виконується уточнення попередньої оцінки різниці часу надходження сигналу [2]

$$\tau_з = \tau_0 - \Delta\tau_з \tag{6}$$

де $\tau_з$ – оцінка різниці часу надходження сигналу до розподілених точок прийому, виміряна за різницею фази сигналів в даних точках прийому; τ_0 – початкове наближення різниці часу надходження сигналу до розподілених точок прийому, виміряна за обвідною або обвідною взаємокореляційної функції; $\Delta\tau_ç$ – похибка оцінки різниці часу надходження сигналу,

$$\Delta\tau_ç = \frac{\Delta\varphi}{\omega}, \tag{7}$$

де $\Delta\varphi$ – різниця фази сигналу, прийнятого в розподілених точках прийому; ω – оцінка значення несучої кругової частоти сигналу.

Сумарну дисперсію оцінки різниці часу надходження сигналу до приймальних пунктів по результатах оцінки несучої частоти сигналу та результатах фазових вимірів визначають за сумою дисперсій [1]

$$\sigma_{\Delta\tau_y}{}^2 = \left(\frac{\partial\tau_y}{\partial\omega}\right)^2 \cdot \sigma_\omega{}^2 + \left(\frac{\partial\tau_y}{\partial\Delta\varphi}\right)^2 \cdot \sigma_\varphi{}^2 = \frac{1}{\omega^2} \cdot \left(\tau_з{}^2 \cdot \sigma_\omega{}^2 + \sigma_\varphi{}^2\right) \tag{8}$$

де $\sigma_{\Delta\tau_{\acute{o}}}$ – сумарна дисперсія оцінки різниці часу надходження сигналу по даних оцінки несучої частоти сигналу та результатах фазових вимірів; $\sigma_{\omega}{}^2$ – дисперсія оцінки несучої частоти сигналу;

$$\sigma_{\omega}{}^2 = \frac{3}{q \cdot \tau_u{}^2} \tag{9}$$

де $\tau_и$ – інтервал автокореляції сигналу; $\sigma_{\varphi}{}^2$ – дисперсія оцінки фази.

$$\sigma_{\varphi}{}^2 = \frac{1}{q} \tag{10}$$

Підставляючи (10), (9) в (8) отримують:

$$\sigma_{\Delta\tau_{\acute{o}}}{}^2 = \frac{1}{\omega^2 \cdot q} \cdot \left(1 + \frac{3 \cdot \tau_ç{}^2}{\tau_u{}^2}\right) \tag{11}$$

При $q \geq 10$, $\frac{\omega}{2 \cdot \pi} \geq 10^9$ Гц , $\tau_и \geq 10^{-7}$ с, що характерно для сигналів систем радіолокації і $\tau_ç \leq 10^{-6}$, що характерно для когерентних малобазових радіотехнічних систем контролю, в формулі (11) складова

$$\left(\frac{3 \cdot \tau_ç{}^2}{\tau_u{}^2}\right) \ll 1 \tag{12}$$

Це дозволило прийняти [1; 2]:

$$\sigma_{\Delta\tau_{\acute{o}}} \approx \frac{1}{\omega \cdot \sqrt{q}} \tag{13}$$

Отримані оцінки різниці часу надходження сигналу до розподілених точок прийому використовуються на етапі вторинної обробки, при розрахунках дальності до об'єкта. Таким чином, розглянутий підхід дозволяє зменшити похибку вимірювання різниці часу надходження сигналу і наблизити її до потенційно можливого мінімального значення, яке в основному визначається відношенням сигнал/шум.

Література

1. Антонюк В. П. Методи підвищення ефективності пасивних радіотехнічних систем контролю джерел електромагнітного випромінювання : дис. канд. техн. наук : 05.12.17. – Львів, 2010. – 206 с.

2.Пат. UA 73253, МПК G01S 5/00, G01S 13/06, G01S 13/42. Спосіб вимірювання координат об`єктів, що випромінюють радіочастотні сигнали, та пристрій, що його реалізує / Антонюк В. П. та інші, власник Львівський наук.-досл. радіотехн. інститут. – № 20040806871; заявл. 16.08.2004; опубл. 15.06.2005.

3.Вершинин А. С. Экспериментальная оценка увеличения точности измерения задержки сигнала в наземных системах радиомониторинга при многоканальном приеме / А.С. Вершинин, Е.П. Ворошилин, В.П. Денисов /Доклады ТУСУРа, № 2 (22), часть 2, декабрь 2010. – С.32–35.

4.Мархакшинов А. Л. Корреляционное измерение навигационных параметров в сейсмической системе охраны /А.Л. Мархакшинов, М.А. Райфельд, А.А. Спектор/ Научный вестник НГТУ. – 2010. – № 3(40) С.161–166.

Метод планування дій в реальному масштабі часу

Жовнір С.М., Зацепіна О.О.
Науковий керівник: к.т.н. доц. Бойчук В.О.
Хмельницький національний університет

Системи реального часу – це системи, які повинні реагувати на події в зовнішньому по відношенню до системи середовищі або впливати на середовище в рамках необхідних часових обмежень. Кажуть, що система працює в режимі реального часу, якщо для опису роботи цієї системи потрібні кількісні часові характеристики.

Для відображення послідовності дій систем реального часу запропонована модель, яка описує дії направленим графом на основі ланцюга Маркова, де вершини відповідають елементарним діям, а ребра відповідають ступеню сили зв'язку між ними. Ознаки початкової умови прив'язані до першої вершини, з якої починається виконання послідовності дій. Ознаки цілі прив'язані до останьої вершини в послідовності дій. Сила зв'язку між вершинами відображає послідовність дій і може динамічно мінятися в залежності від початкових умов і досягнення цілі.

На основі даної моделі розроблений метод планування дій в реальному масштабі часу, який реалізований на прикладі планування дій в іграх стратегіях.

Ігри-стратегії в режимі реального часу мають кілька характеристик, які ускладнюють застосування традиційних методів планування:

– вони мають величезний набір різних дій, які можуть бути виконані та простір станів

– вони є неповними інформаційними іграми, де гравець може тільки побачити частину карти і включати непередбачуваних супротивників.

– вони функціонують в режимі реального часу. таким чином, поки система вирішує, які дії для виконання, гра продовжується виконуватись і стан гри змінюється постійно

– їх складно визначити, використовуючи класичні формальні методи планування, де постумови для дій легко визначити.

Стандартні стратегії в більшості випадків не є ефективними проти експерта, оскільки люди використовують унікальні особливості кожної карти, щоб придумати цікаві стратегії. Таким чином, класичний змагальний пошук з використанням алгоритму мінімаксного типу - не ефективний.

Традиційне STRIP планування не може бути безпосередньо застосовано, оскільки проблемний простір пошуку занадто великий.

Більш того, навіть якщо б обчислювальна складність алгоритмів планування була низька, застосувати класичні алгоритми планування неможливо. Більшість стратегій в реальному часі не детерміновані. Таким чином, потрібні імовірнісні методи планування. Ймовірнісні методи планування, як правило, ґрунтуються на Марковських ймовірнісних процесах.

Стратегічні ігри в режимі реального часу також є неповністю видимими доменами. У більшості ігор є "туман війни", що робить лише гравця здатний спостерігати лише підмножину карти.

Для вирішення цих проблем розроблено метод планування дій в реальному масшабі часу, який навчається грати в стратегічні ігри, спостерігаючи за грою експертів. Система формує планувальні фрагменти, спостерігаючи людську гру, зберігає їх у системі у вигляді кейзів. Потім такі фрагменти витягуються і складаються разом для отримання повного плану.

Виконання методу можна розділити на два етапи – навчання та виконання. Під час навчання йде спостереження за перебігом гри, щоб навчитися планувальним фрагментам, які будуть зберігатись у базі кейзів. Перебіг гри анотує експерт, пояснюючи цілі він переслідував з діями, які він виконував під час гри. Використовуючи ці анотації, набір фрагментів витягується з перебігу дій і зберігається як набір справ Для кожної справи записується в базі ситуація, в якій вона була виконана, мета, яку вона переслідувала і її успіх або невдачу.

Виконавчий модуль відповідає за виконання поточного плану і оновлення його стану (позначення того, які дії вдалося виконати чи не виконати). Модуль розширення плану відповідає за виявлення відкритих цілей у поточному плані і їх розширення. Для цього він спирається на модуль, який дає відкриту ціль і поточний стан гри та завантажує найбільш відповідний фрагмент програми для виконання відкритої мети.

Модуль адаптації відповідає за адаптацію отриманого фрагменту відповідно до поточного стану гри.

Одним з ключових аспектів методу планування в реальному масштабі часу є то, що він суміщає планування з виконання роботи з динамічними доменами.

Метод може бути адаптований з невеликими змінами для відтворення будь-якої гри в реальному масштабі часу, якщо визначено адекватні структури знань (цілі, дії тощо). Крім того, ті самі ідеї можуть бути застосовані до будь-якого стратегічного завдання в режимі реального часу, для якого дії експертів можуть бути легко зафіксовані та анотовані. Метод не

підходить для доменів, де окремі фрагменти, що складають план, взаємодіють так, що змушують систему виконувати великий пошук, щоб знайти правильні комбінації.

Балансування навантаження додатків в хмарному середовищі

Карун М.Є
Науковий керівник – к.т.н.,доц. Хмельницький Ю.В.
Хмельницький національний університет

У термінології комп'ютерних мереж, балансування навантаження, або вирівнювання навантаження (англ. Load balancing) - метод розподілу завдань між декількома мережевими пристроями (наприклад, серверами) з метою оптимізації використання ресурсів, скорочення часу обслуговування запитів, горизонтального масштабування кластера (динамічне додавання / видалення пристроїв), а також забезпечення відмовостійкості (резервування)

Балансування навантаження може бути використане для розширення можливостей ферми серверів, що складається більш ніж з одного сервера. Воно також може дозволити продовжувати роботу навіть в умовах, коли кілька виконавчих пристроїв (серверів) вийшли з ладу. Завдяки цьому зростає відмовостійкість, і з'являється можливість динамічно регулювати використовувані обчислювальні ресурси, за рахунок додавання / видалення виконавчих пристроїв в кластері.

Балансування навантаження передбачає рівномірне навантаження обчислювальних вузлів. При появі нових завдань програмне забезпечення, що реалізує балансування, має прийняти рішення про те, де (на якому обчислювальному вузлі) слід виконувати обчислення, пов'язані з цим новим завданням. Крім того, балансування передбачає перенос (migration - міграція) частини обчислень з найбільш завантажених обчислювальних вузлів на меншзавантажені вузли.

Проблема балансування обчислювального навантаження виникає з тієї причини, що:

– структура розподіленого додатка неоднорідна, різні логічні процеси вимагають різних обчислювальних потужностей;

– структура обчислювального комплексу (наприклад, кластера), також неоднорідна, тобто різні обчислювальні вузли володіють різною продуктивністю;

– структура міжвузлової взаємодії неоднорідна, тому лінії зв'язку, що з'єднують вузли, можуть мати різні характеристики пропускної здатності.

Слід розрізняти статичне і динамічне балансування. Статичне балансування виконується до початку виконання розподіленого додатка. Дуже часто при розподілі логічних процесів по процесорах використовується

досвід попередніх виконань, застосовуються генетичні алгоритми. Однак попереднє розміщення логічних процесів по процесорах (комп'ютерів) не дає ефекту.

Динамічне балансування передбачає перерозподіл обчислювального навантаження на вузли під час виконання програми. Програмне забезпечення,що реалізує динамічне балансування, визначає:

– завантаження обчислювальних вузлів;

– пропускну спроможність ліній зв'язку;

– частоту обмінів повідомленнями між логічними процесами розподіленого додатка та ін.

На підставі зібраних даних (як по розподіленому додатку, так і по обчислювальному середовищу) приймається рішення про перенесення логічних процесів з одного вузла на інший.

Задачу оптимального розподілу обчислювального навантаження на концептуальному рівні можна порівняти із завданням наповнення поїлок - кількох бочок з різними геометричними характеристиками водою, яка надходить через трубу з вентилями. Один раз в секунду дно бочок відкривається, і вся вода з них потрапляє в поїлки. Вода ж, яка переливається через краї бочок, йде в землю безцільно. Для виключення переливу необхідно вибрати такі регулюють значення вентилів, щоб вода в бочках трималася на однаковому рівні. При збільшенні потоку води рівень води у всіх бочках на момент скидання повинен збільшитися на однакову величину, щоб не допустити переливу води в жодній з бочок (необроблені запити). Саме це дозволить досягти максимального обсягу корисно спожитої води (максимальне значення числа оброблених операцій в багатовузлових системах). Даний процес можна представити на графіку залежності числа оброблених запитів від кількості надійшовших до системи, що складається з двох вузлів А і Б. При оптимальному розподілі навантаження - 1/3 запитів на А і 2/3 запитів на Б (рис 1, а) - величина граничного сумарного числа оброблених запитів, при якому не відбувається скидання, удвічі вище, ніж для варіанту, представленого на рис 1, б (1/3 запитів припадає на Б і 2/3 запитів на А). Причина – швидке досягнення межі можливостей вузла А і деградація продуктивності всієї системи.

Таким чином, одне з найважливіших завдань балансування – визначення оптимальних пропорцій розподілу надходячих запитів і їх подальше динамічне корегування при зміні умов функціонування системи (зміна числа вузлів, складу встановленого і запущених додатків, модернізація апаратної платформи окремих вузлів і т. д.). Оптимальні пропорції в нашому випадку - це таке співвідношення числа оброблених запитів різними вузлами, при якому рівні завантаження цих вузлів приблизно рівні.

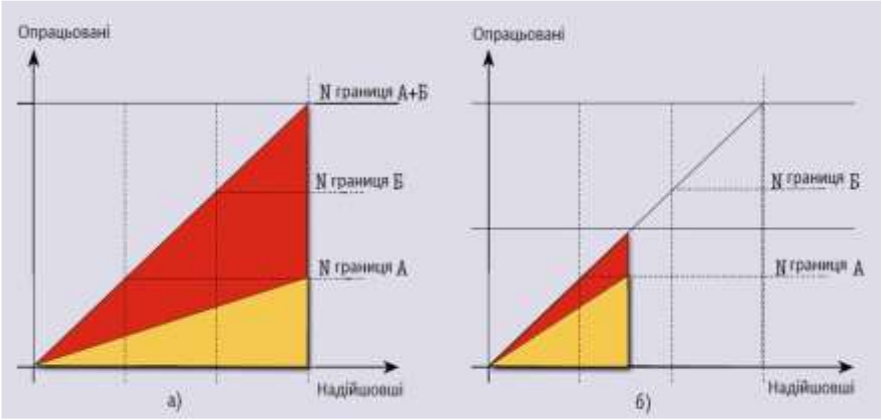


Рисунок 1 – Залежність числа оброблених запитів від числа надійшовши запитів

Література

1. Hoff Ch., Simmonds P. Security guidance for critical areas of focus in cloud computing. Website of Cloud Security Alliance. 2011. С. 12–20. URL: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

2. А.Е. Кононюк Фундаментальная теория облачных технологий // «Освіта України» Київ 2018 С.11-51

3. Батура Т.В., Мурзин Ф.А., Семич Д.Ф. Software & Systems Программные продукты и системы // Облачные технологии: основные модели, приложения, концепции и тенденции развития Сб. – 2014. – №3.

4. Гасюк А.А. Инновации в облачных технологиях - одна из основ экономического роста компаний // Электронный научный журнал. 2016. № 9 (12). С. 88-91.

5. Калягин И.Н., Воронцов А.А. Использование облачных технологий для бизнеса // Международный студ. научный вестник. 2016. № 3-1. С. 79-80.

6. Чесноков А.Н. Особенности использования облачных технологий // Символ науки. 2016. № 4-2. С. 206-209.

Методика побудови корпоративної системи захисту інформації

Красильников С.Р.
Хмельницький національний університет

Характерною ознакою сучасного суспільства є стрімкий розвиток інформаційно-телекомунікаційних технологій, інтенсивне впровадження новітніх інформаційних технологій в усі сфери суспільного життя. Інформація та новітні інформаційно-телекомунікаційні технології дедалі більше визначають розвиток держави і суспільства, сприяють розвитку інформаційного середовища. Стрімкий розвиток інформаційних технологій спричинив нову глобальну проблему – інформаційну безпеку. Багато найважливіших інтересів підприємства в даний час значною мірою визначається станом навколишнього інформаційного середовища. Цілеспрямовані або ненавмисні впливи на інформаційну сферу з боку зовнішніх або внутрішніх джерел можуть завдавати серйозної шкоди цим інтересам і становлять загрози та ризики для безпеки. Тому інформаційна безпека в сучасних умовах є однією з необхідних умов нормального функціонування підприємства.

Серед завдань захисту інформації на підприємстві виділяють такі:

- запобігання витоку, розкраданню, втратам, спотворенню, підробці інформації;
- запобігання несанкціонованим діям щодо знищення, модифікації, спотворення, копіювання, блокування інформації;
- запобігання інших форм незаконного втручання в інформаційні ресурси та інформаційні системи.

Головна мета будь-якої системи інформаційної безпеки полягає в забезпеченні сталого функціонування об'єкта: запобігання загрозам його безпеки, захисту законних інтересів власника інформації від протиправних посягань. Інше завдання зводиться до підвищення якості надання послуг і гарантій безпеки майнових прав та інтересів клієнтів. Для виконання зазначених цілей необхідно:

- віднести інформацію до категорії обмеженого доступу (службової або комерційної таємниці);
- прогнозувати і своєчасно виявляти загрози безпеки інформаційних ресурсів, причини та умови, що сприяють нанесенню фінансового, матеріального і морального збитку, порушення його нормального функціонування і розвитку;
- створити умови функціонування з найменшою вірогідністю реалізації загроз безпеки інформаційних ресурсів і нанесення різних видів шкоди;
- створити механізм і умови оперативного реагування на загрози інформаційної безпеки і прояву негативних тенденцій у функціонуванні,

ефективне припинення зазіхань на ресурси на основі правових, організаційних і технічних заходів і засобів забезпечення безпеки;

- створити умови для максимально можливого відшкодування та локалізації збитку, що наноситься неправомірними діями фізичних і юридичних осіб, і тим самим послабити можливий негативний вплив наслідків порушення інформаційної безпеки. При виконанні робіт можна використовувати наступну модель побудови корпоративної системи захисту інформації (рис.), засновану на адаптації Загальних Критеріїв (ISO 15408) і проведенні аналізу ризику (ISO 17799) і враховує тенденції розвитку вітчизняної нормативної бази з питань захисту інформації, а саме:

- запобігання витоку, розкрадання, втрати, спотворення, підробки інформації;

- запобігання несанкціонованим діям щодо знищення, модифікації, спотворення, копіювання, блокування інформації;

- запобігання інших форм незаконного втручання в інформаційні ресурси та інформаційні системи.

Головна мета будь-якої системи інформаційної безпеки полягає в забезпеченні сталого функціонування об'єкта: запобігання загроз його безпеки, захисту законних інтересів власника інформації від протиправних посягань, у тому числі кримінально караних діянь у даній сфері відносин, , забезпеченні нормальної виробничої діяльності всіх підрозділів об'єкта . Інше завдання зводиться до підвищення якості послуг, що надаються і гарантій безпеки майнових прав та інтересів клієнтів. Для виконання зазначених цілей необхідно:

- віднести інформацію до категорії обмеженого доступу (службової або комерційної таємниці);

- запобігання витоку, розкрадання, втрати, спотворення, підробки інформації;

- запобігання несанкціонованим діям щодо знищення, модифікації, спотворення, копіювання, блокування інформації;

- запобігання інших форм незаконного втручання в інформаційні ресурси та інформаційні системи.

Представлена модель захисту інформації це сукупність об'єктивних зовнішніх і внутрішніх факторів і їх вплив на стан інформаційної безпеки на об'єкті та на збереження матеріальних або інформаційних ресурсів. Розглядаються наступні об'єктивні фактори:

- загрози інформаційної безпеки, які характеризуються ймовірністю виникнення і ймовірністю реалізації;

- уразливості інформаційної системи або системи контрзаходів (системи інформаційної безпеки), що впливають на ймовірність реалізації загрози;

- ризик-фактор, що відображає можливий збиток організації в результаті реалізації загрози інформаційної безпеки: витоку інформації і її

неправомірному використанню (ризик в кінцевому підсумку відображає ймовірні фінансові втрати прямі або непрямі).

Рисунок 1 – Модель побудови корпоративної системи захисту інформації

Для побудови збалансованої системи інформаційної безпеки передбачається спочатку провести аналіз ризиків в області інформаційної безпеки. Потім визначити оптимальний рівень ризику для організації на основі заданого критерію. Систему інформаційної безпеки (контрзаходи) належить побудувати таким чином, щоб досягти заданого рівня ризику. Вже згадана методика проведення аналітичних робіт дозволяє:

- повністю проаналізувати і документально оформити вимоги, пов'язані з забезпеченням інформаційної безпеки;
- уникнути витрат на зайві заходи безпеки, які виникають при суб'єктивній оцінці ризиків;
- надати допомогу в плануванні і здійсненні захисту на всіх стадіях життєвого циклу інформаційних систем;
- забезпечити проведення робіт в стислі терміни;
- представити обґрунтування для вибору заходів протидії;
- оцінити ефективність контрзаходів;
- порівняти різні варіанти контрзаходів.

В ході робіт повинні бути встановлені межі дослідження. Для цього необхідно виділити ресурси інформаційної системи, для яких в подальшому будуть отримані оцінки ризиків. При цьому належить розділити ресурси, що розглядаються і зовнішні елементи, з якими здійснюється взаємодія.

Ресурсами можуть бути засоби обчислювальної техніки, програмне забезпечення, дані, а також інформаційні ресурси - окремі документи, окремі масиви документів, документи і масиви документів в інформаційних системах (бібліотеках, архівах, фондах, банках даних, інших інформаційних системах).

Прикладами зовнішніх елементів є мережі зв'язку, зовнішні сервіси і т.п. При побудові моделі необхідно враховувати взаємозв'язки між ресурсами. Наприклад, вихід з ладу будь-якого обладнання може призвести до втрати даних або виходу з ладу іншого критично важливого елемента системи. Подібні взаємозв'язки визначають основу побудови моделі організації з точки зору інформаційної безпеки. Ця модель, відповідно до запропонованої методики, будується наступним чином: для виділених ресурсів визначається їх цінність, як з точки зору асоційованих з ними можливих фінансових втрат, так і з точки зору шкоди репутації організації, дезорганізації її діяльності, моральної шкоди від розголошення конфіденційної інформації і т.д. Потім описуються взаємозв'язку ресурсів, визначаються загрози безпеки і оцінюються ймовірності їх реалізації.

На основі побудованої моделі можна обґрунтовано вибрати систему контрзаходів, що знижують ризики до допустимих рівнів і володіють найбільшою цінової ефективністю. Частиною системи контрзаходів будуть рекомендації з проведення регулярних перевірок ефективності системи захисту. Забезпечення підвищених вимог до інформаційної безпеки передбачає відповідні заходи на всіх етапах життєвого циклу інформаційних технологій. Планування цих заходів проводиться після завершення етапу аналізу ризиків та вибору контрзаходів. Обов'язковою складовою частиною цих планів є періодична перевірка відповідності існуючого режиму інформаційної безпеки політиці безпеки, сертифікація інформаційної системи (технології) на відповідність вимогам певного стандарту безпеки. По завершенні робіт, можна буде визначити міру гарантії безпеки інформаційного середовища, засновану на оцінці, з якої можна довіряти інформаційному середовищі об'єкта. Даний підхід передбачає, що велика гарантія випливає з застосування великих зусиль при проведенні оцінки безпеки. Адекватність оцінки заснована на залученні в процес оцінки більшого числа елементів інформаційного середовища об'єкта, глибині, що досягається за рахунок використання при проектування системи забезпечення безпеки більшого числа проектів і описів деталей виконання, строгості, яка полягає в застосуванні більшого числа інструментів пошуку і методів, спрямованих на виявлення менш очевидних вразливостей або на зменшення ймовірності їх наявності.

Література

1. Абакумов В. М. Інформаційна безпека підприємництва як об’єкт адміністративно-правової охорони / В. М. Абакумов // Форум права. – 2012. –

№ 4. – С. 10–16 [Електронний ресурс]. – Режим доступу: http://arhive.nbuv.gov.ua/e-journals/FP/2012-4/12avmapo.pdf.

2. Игнатьев В.А. Информационная безопасность современного коммерческого предприятия: Монография. – Старый Оскол: ООО «ТНТ», 2005. – 448 с.

3. Сороківська О. А. Інформаційна безпека підприємства: нові загрози та перспективи / О. А. Сороківська, В. Л. Гевко // Вісник Хмельницького національного університету – 2010. – № 2. – Т. 2. С. 32–35.

Засоби вкладення паралельних програм в кластерні та мультикластерні обчислювальні системи

Огнєвий О.В., Пахар О.В.
Хмельницький національний університет

При побудові кластерних ОС, як правило, використовуються масові апаратно-програмні засоби, що, по суті, є принципом конструювання кластерних ОС та забезпечує їх високу техніко-економічну ефективність [1].

Для створення обчислювальних кластерів використовуються MISD-, SIMD-, MIMD-архітектури, різні функціональні структури і конструктивні рішення.

Основна функціонально-структурна одиниця обчислювальних ресурсів в кластерних ОС - це елементарна машина. Конфігурація ЕМ допускає варіювання в широких межах - від процесорного ядра до ЕОМ, оснащеної засобами комунікацій і зовнішніми пристроями.

Сучасні кластерні ОС переважно конфігуруються з багатопроцесорних вузлів і багатоядерних процесорів.

Комунікаційні середовища кластерних ОС будуються на базі комутаторів і мають ієрархічну організацію. На рис. 1 наведено приклад обчислювального кластера, укомплектованого N обчислювальними вузлами, які об'єднані мережею зв'язку стандарту Gigabit Ethernet. Кожен вузол укомплектований парою двоядерних процесорів AMD Opteron 275, взаємодіють по шині HyperTransport. Кожен процесор має інтегрований контролер пам'яті, через який його ядра маю доступ до їх загальної пам'яті. Видно, що комунікаційне середовище кластера має ієрархічну організацію, в якій перший рівень - це мережа зв'язку стандарту Gigabit Ethernet; другий - шина HyperTransport; третій - спільна пам'ять ядер. Швидкість передачі інформації на різних рівнях комунікаційного середовища істотно різні.

Комунікаційні середовища сучасних кластерних ОС будуються на базі технологій Gigabit Ethernet, InfiniBand, Myrinet. Для об'єднання обчислювальних вузлів в систему використовуються комутатори (switch) з фіксованою кількістю вхідних портів для підключення кінцевих пристроїв (обчислювальних вузлів, комутаторів, систем зберігання даних і т.д.). У цих

умовах для побудови великомасштабних кластерних ОС використовуються різні схеми формування комутаторів. Основна мета - комплексування заданого числа обчислювальних вузлів і забезпечення високої продуктивності комунікаційного середовища.

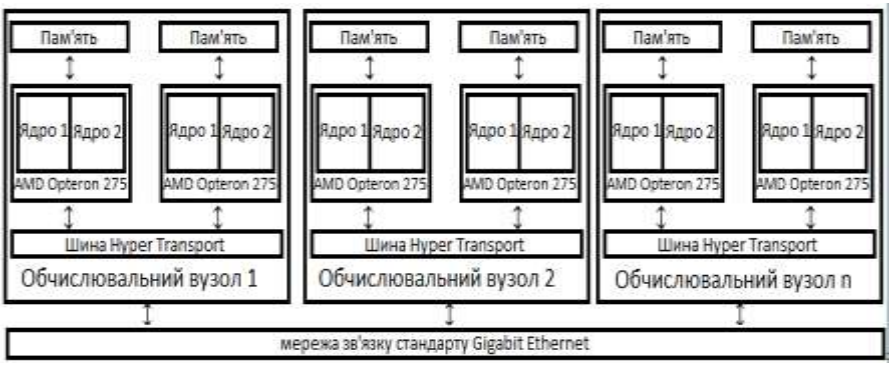


Рисунок 1 - Приклад ієрархічної організації комунікаційного середовища кластерної ОС

З розвитком обчислювальної техніки і телекомунікаційних технологій з'явилася тенденція до побудови розподілених ОС шляхом об'єднання за допомогою локальних і глобальних мереж зв'язку розосереджених обчислювальних ресурсів починаючи від простих ПК і закінчуючи ОС з масовим паралелізмом. Так в кінці XX століття в індустрії обробки інформації отримали розвиток GRID-технології (Global Resource Information Distribution). На основі цих технологій створюються більш масштабні просторово-розподілені системи обробки інформації, здатні реалізувати паралельні алгоритми вирішення суперскладних задач на своїх розсереджених ресурсах. Така GRID-система являє собою композицію множини ЕОМ і ОС, просторово-розподіленої комунікаційної мережі і програмних компонентів для здійснення паралельних обчислень. В GRID-системі можуть використовуватися гетерогенні і не сумісні обчислювальні засоби, однак для їх сумісної роботи над паралельними алгоритмами повині бути застосовані спеціальні механізми (наприклад, стандартизовані протоколи) узгодженої взаємодії. GRID-система - це ні що інше як розподілена ОС в сенсі введеного вище визначення.

Що стосується мультикластерних ОС, то це не окремий клас ОС, а просторово-розподілені системи, що формуються шляхом об'єднання ресурсів розосереджених кластерів.

Обчислювальні кластери належать до класу систем з розподіленою пам'яттю. Паралельні програми для таких ОС розробляються в моделі передачі повідомлень (message passing). Широке розповсюдження отримали

стандарти, бібліотеки і середовища для створення паралельних програм в даній моделі, зокрема стандарт Message Passing Inter face (MPI), система Parallel Virtual Machine (PVM), IBM Message Passing Li brary (MPL), P4 і ін.

В рамках даної моделі паралельні гілки програми синхронізують свою роботу шляхом обміну інформацією по каналах між машинних зв'язків.

Залежно від складності задач і характеру їх надходження в теорії обчислювальних систем виділяють два основні режими функціонування ОС з програмованою структурою: моно- і мультипрограмний режими.

У монопрограмному режимі для вирішення задачі використовуються всі ресурси ОС. Задача представляється у вигляді паралельної програми, число гілок в якій або фіксоване, або допускає варіювання в заданому діапазоні. В якості одиниці ресурсу виступає елементарна машина ОС. Всі машини використовуються для вирішення задачі. Якщо максимальне число гілок в паралельній програмі менше загального числа ЕМ в системі, то «надлишкові» машини використовуються для підвищення надійності функціонування ОС.

До мультипрограмних відносять режими :

1) обробки наборів задач;

2) обслуговування потоків задач.

При роботі ОС в цих режимах одночасно вирішується кілька задач, отже, ресурси системи діляться між ним.

При організації функціонування ОС у разі обробки набору задач враховується не тільки кількість задач в наборі, але їх параметри: число гілок в програмі (точніше, число машин, на яких вона буде виконуватись), час рішення або імовірнісний закон розподілу часу рішення і ін. Алгоритми організації функціонування ОС задають розподіл задач по машинам і послідовність виконання задач на них. В результаті стає відомим, в якому проміжку часу і на яких машинах (або на який підсистемі) буде вирішуватися будь яка задача набору.

Обслуговування потоку задач на ОС - принципово відрізняється від вибору наборів: задачі надходять у випадкові моменти часу, їх параметри випадкові, отже, детермінований вибір підсистем для вирішення тих чи інших задач виключений. Для режиму потоку задач використовуються методи і алгоритми, що забезпечують оптимальне функціонування обчислювальних систем.

При роботі ОС в будь-якому з мультипрограмних режимів система представляється у вигляді композиції підсистем різних рангів. У міру рішення задачі ця композиція «автоматично» (за допомогою операційної системи) реконфігурується так, щоб забезпечити її адекватність поточної мультипрограмної ситуації. Будь-яка підсистема має всі архітектурні властивості системи, тому її організація при вирішенні виокремленої їй задачі може здійснюватися тими ж методами, якими була організована робота всієї ОС в першому режимі.

Час виконання паралельних програм на розподілених ОС суттєво залежить від того наскільки вони ефективно вкладені в систему .

Під ефективним вкладенням (Task Map, Task Allocation, Task Assign ment) розуміється такий розподіл гілок паралельної програми між ЕМ системи, при якому досягаються мінімуми накладних витрат на міжмашинному обміні інформацією і дисбалансу завантаження ЕМ.

Залежно від того, чим характеризується паралельна програма, яка надійшла в систему, виникають різні постановки задачі вкладення.

Якщо для паралельної програми заданий інформаційний граф, то говорять про задачу вкладення інформаційного графа (структури) програми в ОС. У разі, якщо про паралельну програму відомо лише кількість ЕМ, які необхідно для її реалізації, то розглядається задача формування в межах ОС підсистеми ЕМ, що задовольняє заданим критеріям якості.

Задача оптимального вкладення паралельної програми виникає при організації функціонування ОС в будь-якому з основних режимів: рішення складної задачі, обробки наборів задач, обслуговування потоків задач.

В режимі обслуговування потоків задач в межах ОС формуються підсистеми ЕМ. Для них і надходять паралельні програми для виконання. Елементарні машини, що входять в підсистему, можуть належати різним обчислювальним системам, розміщуватися в різних комутаційних шафах і т. д. Наслідком цього є те, що швидкості передачі інформації між ЕМ можуть бути істотно різними. Тому потрібно не тільки формувати підсистеми з необхідним числом ЕМ, а й ефективно вкладати паралельні програми в них.

Існуючі методи і алгоритми вкладення паралельних програм в ОС розрізняються за типом систем, на які вони орієнтовані, по використовуваних моделях паралельних програм, показниками оптимальності вкладення, точності, централізованості або децентралізованості алгоритмів, по статичній або динамічній схемі формування вкладень.

Ефективне вкладення в ОС паралельної програми вимагає врахування структури інформаційних обмінів і обсягів даних, що передаються між її гілками. Більшість алгоритмів основані лише на структурі інформаційного графа програми і ігнорують обсяги та інтенсивність міжмашиних обмінів. Однак облік таких параметрів практично необхідний. Аналіз популярних вільно розповсюджених паралельних програм, бібліотек і тестів продуктивності High-Performance Linpack, NAS Parallel Benchmarks і SPEC MPI2007 показує, що більшість з них характеризується неоднорідними інформаційними графами. Неоднорідність виражається в обсягах даних, що передаються між гілками, розмірах використовуваних повідомлень, а також в схемах реалізованих обмінів.

Як показники оптимальності вкладення використовують час виконання паралельної програми або функцію, мінімізація якої забезпечує мінімум часу виконання програми.

Алгоритми вкладення спираються на припущення про те, що час

виконання паралельної програми - це сума часу виконання усіх її гілок. Однак практика рішення промислових задач і аналізу їх продуктивності показує, що час виконання програми визначається максимальним часом виконання її гілок. Використання подібних показників ускладнюється вибором коефіцієнтів пропорційності, якими пов'язані функції і найчастіше їх не сумісними розмірностями..

Вкладення в ОС паралельних програм, для яких не задані інформаційні графи, здійснюється шляхом формування підсистеми елементарних машин і розподілу по ній паралельних гілок програми. Сформована підсистема повинна забезпечувати ефективну реалізацію паралельних програм і забезпечувати мінімум часу для їх виконання.

Більшість алгоритмів формування в межах ОС підсистем орієнтовані на системи з певними структурами мереж міжмашинного зв'язку (наприклад, на 2D-решітки, гіперкубічні і тороїдальні структури) і прагнуть зберігати топологічну схожість підсистеми структурі ОС. Можливості застосування таких алгоритмів для ОС з ієрархічною організацією, канали зв'язку в яких мають різну продуктивність, істотно обмежені. Тому актуальною є розробка алгоритмів формування підсистем, що допускають застосування як в системах зі статичною структурою мережі між машинного зв'язку, так і в системах з динамічною структурою.

Задача оптимального вкладення паралельної програми в ОС відноситься до дискретної оптимізації і є складною .

Для великомасштабних розподілених ОС знаходження точного вирішення пов'язане зі значною обчислювальною складністю. Доцільно використання наближених методів і алгоритмів вирішення задачі.

Існуючі методи і алгоритми вкладення паралельних програм в ОС розрізняються за типом систем, на які вони орієнтовані, по використовуваних моделях паралельних програм, показниками оптимальності вкладення, точності, централізованності або децентрализованности алгоритмів, по статичній або динамічній схемі формування вкладень.

Ефективне вкладення в ОС паралельної програми вимагає врахування структури інформаційних обмінів і обсягів даних, що передаються між її гілками.

Аналіз популярних вільно розповсюджених паралельних програм, бібліотек і тестів продуктивності High-Performance Linpack, NAS Parallel Benchmarks і SPEC MPI2007 показує, що більшість з них характеризується не однорідними інформаційними графами. Неоднорідність виражається в обсягах даних, що передаються між гілками, розмірах використовуваних повідомлень, а також в схемами реалізованих обмінів.

Як показники оптимальності вкладення використовують час виконання паралельної програми або функцію, мінімізація якої забезпечує мінімум часу виконання програми.

Зі сказаного випливає, що існуючі алгоритми не дозволяють будувати

ефективні вкладення паралельних програм в ОС з ієрархічною організацією комунікаційних середовищ. Актуальною є разрабка не трудомістких методів і алгоритмів вкладення паралельних програм в ОС з ієрархічною організацією комунікаційних середовищ.

Література

1. Огнєвий О.В., Коваль Б.А., Присяжнюк В.В. Аналіз архітектурних особливостей обчислювальних систем з програмованою структурою / О.В. Огнєвий., В.А. Коваль, В.В.Присяжнюк // Зб. наук. праць Військового інст. Київського НУ ім. Тараса Шевченко. – К.: ВІКНУ, 2018. – Вип. № 48 . – С. 143-148

2. Огнєвий О.В. Особливості управління інформаційними ресурсами в корпоративних інформаційних системах / О.В. Огнєвий., А.М.Огнева, В.А. Коваль, В.В.Присяжнюк // Вісник Хмельницького національного університету. - Хмельницький, 2018, № 6 - С.17-21

Модель опису структури об'єктно-орієнтованої бази даних для інформаційних систем

Поліщук Ю.С., Стопчак О.О.
Науковий керівник: к.т.н. доц. Красильников С.Р.
Хмельницький національний університет

Сучасний світ все більшою мірою набуває вигляд єдиного інформаційного простору. Велику роль в цьому процесі відіграє швидко розвиваючий інформаційний бізнес. Його бурхливий розвиток змушує розробників обчислювальної техніки шукати нові рішення, які дають можливість керувати складними структурами даних і надавати користувачеві доступ до них в кожному куточку земної кулі. Таким чином, інформація в сучасному світі перетворилася в один з найбільш важливих ресурсів. Не є винятком і інформаційні системи (ІС). Різноманітність завдань, що вирішуються за допомогою ІС, привело до появи безлічі різнотипних систем, але жодна з них немислима без використання баз даних.

Одним з основних компонентів ІС є інформаційне забезпечення, яке об'єднує різні складні структури даних. Такі структури зручно описувати у вигляді об'єктів, тому все більшої популярності в цій галузі стали займати об'єктно-орієнтовані бази даних (ООБД). ООБД дозволяють перенести у віртуальний світ об'єкти реального світу з мінімальними втратами. Однак, проектування ООБД є кропітким, трудомістким і динамічним процесом. Цей процес змістився з логічної області до абстрактного рівня, де важливим завданням стало конструювання коректної абстрактної моделі.

При цьому для побудови такої моделі традиційні методи проектування не підходять через наступних недоліків:

1) традиційні моделі даних не достатньо сильні в підтримці складних механізмів моделювання, таких як складові об'єкти і наслідування;

2) залежності обмежень, які використовуються в традиційному підході проектування (функціональні та багатозначні залежності) мають тільки обмежений набір залежностей, який може бути накладено на зв'язки і атрибути для вирішення питання пов'язаного з внутрішньо-об'єктними зв'язками. Крім того, залежність обмежень в плоскій і ущільненій моделях даних можуть бути класифіковані як обмеження, що характеризуються значенням. Сенс, який вони відображають, обумовлений взаємозв'язками між даними та відношенями. На відміну від них, об'єктно-орієнтовані моделі даних підтримують ідею об'єктної ідентифікації, яка ідентифікує об'єкти незалежно від їх значень;

3) вони не підходять для розгляду проблем надмірності і проблем зміни на початку проектування об'єктно-орієнтованої схеми, тому що вирішують питання, пов'язане з отриманням результату, наприклад проблеми продуктивності та зберігання. Об'єктно-орієнтоване проектування даних повинне покладатися на те, що отримання значень не відноситься до діяльності проектування (це інша сторона проекційних дій).

Очевидно, що для вирішення цих проблем потрібно застосування нових методик та інструментів проектування, так як для абстрактної моделі даних, що володіє більш багатими структурними можливостями в порівнянні з реляційною моделлю, потрібно інший метод скорочення надмірності даних або іншими словами метод нормалізації схеми. При цьому загальновизнаного методу нормалізації ООБД не існує, є тільки окремі методи, представлені в різних роботах.

Виходячи з вищевикладеного виникає необхідність дослідження і розробки методу і засобів проектування та контролю схеми ООБД для ІС, які дозволили б повною мірою розкрити всі сторони процесу нормалізації ООБД. При цьому важливо щоб цей метод грунтувався на теоретичній базі, головним елементом якої є модель даних, а схема була виконана на візуально-декларативній мові проектування. Актуальність дослідження обумовлена тим що, в даний час існує колосальний розрив між потенціалом ООБД і інструментальними засобами і методами їх проектування, які дозволили б зробити ООБД загальнодоступними і вивели б їх на новий етап розвитку.

Для усунення деяких недоліків, які властиві ООБД, зокрема відсутність універсальної моделі даних, яка є однією із суттєвих недоліків ООБД, необхідно реалізувати модель представлення структури інформаційного забезпечення, за допомогою якої необхідно вирішити наступні питання:

– проводити контроль правильності структури та взаємозв’язок між об’єктами уже проектованих ООБД;

– проводити контроль правильності структури та взаємозв’язок між

об’єктами на етапі проектування ООБД;

– забезпечити автоматизоване проектування структури та взаємозв’язок між об’єктами ООБД.

Використовуючи математичний апарат теорії формальних граматик та теорії кінцевих автоматів запропоновано формалізовану модель опису структури ООБД. Структуру ООБД представимо як кінцеву множину вершин, для яких задано порядок проходження. Формальна математична модель структури ООБД представлена схемою структури, обумовленої як шістка:

$$S = (K, KE, KT, F, F0, K0),$$

де:

– $K=\{K_{11}\dots K_{1S}\dots K_{21}\dots K_{2S}\dots K_{n1}\dots K_{nS}\dots\}$ – множина класів ООБД;

– $KE=\{K_{e1}\dots K_{e1p}, K_{e2}\dots K_{e2p}, K_{en}\dots K_{np}\}$ – множина екземплярів класів;

– $F: K\times KE \to K$ – функція переходів, що реалізує відображення KE у K: функція F деяким парам основний клас – вхідний екземпляр (K_{si}, K_{epi}) ставить у відповідність деякий клас $K_{si-1} = F(K_{si}, K_{epj})$, $K_{si-1} \in K$;

– $KT = \{K_t,\dots,K_{tp},\dots,K_{tp}\}$ – множина таблиць ООБД;

– $F0: K\times KT \to K$ – функція переходів, що реалізує KT у K; функція $F0$, деяким парам основний клас – вхідна таблиця (K_{si}, K_{tpi}) ставить у відповідність деякий клас $K_{si} -1 = F0(K_{si}, K_{tpi})$;

– $K0 \in K$ – початкова вершина БД.

У загальному вигляді схема ООБД представлена *як* $CH = \{S_i\}_{i=1\dots T}$ – множина підмоделей структур БД, з яких складається ООБД. Структура S_1, використовується для ініціалізації процесу розпізнавання, і називається початковою. Множина таблиць T – це таблиці структури, що описується, які надходять на вхід програми–аналізатора безпосередньо з вхідного потоку. Кожному символу kt_p з множини KT відповідає своя структура S_i, що входить до складу схеми ООБД, тобто:

$$\forall\, kt_p \exists\ S_i\ (kt_p \in KT,\ S_i \in CH).$$

Аналіз структури об'єктно-орієнтованих баз даних виконується в 2 етапи:

І етап – аналізується загальна структура ООБД, на даному етапі аналізуються класи і екземпляри ООБД та зв’язки між ними:

$$kt_p \in KT \exists\ S_i \in CH.$$

ІІ етап – детальний аналіз структури ООБД.

Аналіз структури ООБД еквівалентний побудові дерева розбору методом "нагору": на кожнім кроці алгоритму будується один з рівнів у дереві розбору, "піднімаючись" від листів до кореня. Методика аналізу структури ООБД з використанням формальної математичної моделі полягає в наступному:

1) таблиці a_i розміщені на листках в дереві розбору, замінюються класом A, для якого в формальній моделі є функція $A \rightarrow a$ (іншими словами, робиться "згортка" таблиці a до класу A);

2) потім багаторазово (доти, поки не буде досягнуто вершини ООБД) виконуються наступні кроки: отриманий на попередньому кроці клас A і розташована безпосередньо в даному класі чергова таблиця a_i заміняється класом B, для якого в формальній моделі є функція $B \rightarrow Aa_i$ (i = 2, 3,.., n).

При роботі даного алгоритму можливі наступні ситуації.

1) Прочитана вся структура ООБД, що аналізується; на кожнім кроці знаходилася єдина потрібна "згортка"; на останньому кроці згортка відбулася до вершини $K0$. Це означає, що структура ООБД, яка аналізується, відповідає опису формальній математичній моделі структури ООБД.

2) Прочитана вся структура ООБД, що аналізується; на кожнім кроці знаходилася єдина потрібна "згортка"; на останньому кроці згортка відбулася до символу, відмінному від $K0$. Це означає, що структура ООБД, яка аналізується, не відповідає опису формальної математичної моделі структури ООБД.

3) На деякому кроці не знайшлося потрібної згортки, тобто для отриманого на попередньому кроці класу K і розташованої безпосередньо в ньому таблиці kt_i не знайшлося класу B, для якого в правилах була би функція виводу $B \rightarrow Kkt_i$. Це означає, що структура ООБД, яка аналізується, не відповідає опису формальної математичної моделі структури ООБД.

4) На деякому кроці роботи виявилося, що є більше однієї придатної згортки, тобто в правилах різні класи мають правила виводу з однаковими правими частинами, і тому незрозуміло, до якого з них робити згортку. У даній ситуації необхідно робити згортку в усіх напрямках. Якщо хоча б один з напрямків приведе до символу, відмінному від $K0$, то це означає, що структура ООБД, яка аналізується, не відповідає опису формальної математичної моделі ООБД, у противному випадку відповідає.

Для того, щоб швидше знаходити функцію з необхідною правою частиною, необхідно зафіксувати всі можливі згортки (це визначається тільки правилами і не залежить від виду структури ООБД). Це можна зробити у вигляді таблиці, рядки якої позначені класами структури ООБД, стовпці – таблицями. Значення кожного елемента таблиці – це клас, до якого можна згорнути пари "клас–таблиця", якими позначені відповідні рядок і стовбець.

Отже, розробка методів та засобів на основі запропонованої формальної моделі ООБД дозволить вирішити наступні задачі:

– проводити контроль правильності структури та взаємозв’язок між об’єктами уже проектованих ООБД;

– проводити контроль правильності структури та взаємозв’язок між об’єктами на етапі проектування ООБД;

– забезпечити автоматизоване проектування структури та взаємозв’язок між об’єктами ООБД.

– мінімізувати чи усунути проблеми цілісності даних;
– підвищити загальну продуктивність інформаційної системи;
– зменшити вартість розробки і супроводу бази даних.

Література

1. Курейчик В.М., Гладков Л.А., Курейчик В.В. Дискретная математика. Теория множеств. Учебное пособие. 4.1. — Таганрог: Изд-во ТРТУ, 2005.

2. Джулій В.М. Представлення моделі ООБД інформаційного забезпечення тестового діагностування мікропроцесорних пристроїв / Джулій В. М., Муляр І. В. //Вісник ТУП. – 2004. – No2. Частина 1, том 1.– С.79 -83.

3. Джулій В.М. Гіпертекстова модель представлення інформації в базах діагностичних даних / Джулій В.М., Муляр І.В. // Вісник ТУП. – 2001. – No1. – С.189 -191.

Архітектура програмного комплексу забезпечення безпеки виявлення і протидії DDoS-атакам

Савіцька О.О., Джулій В.М., Муляр І.В.
Хмельницький національний університет

Програмний комплекс виявлення початку атаки в режимі реального часу розраховує середньоквадратичне відхилення з урахуванням актуальних сезонних періодів за кількістю запитів до мережного ресурсу в кожному періоді. Програмний комплекс дає можливість задати розмірність розглянутих періодів: 1 хвилина, 15 хвилин, 1 годину і т.д. А також вести моніторинг відразу по декількох періодів. На підставі розрахованого середньоквадратичного відхилення задається верхня межа кількості запитів до мережного ресурсу відповідного періоду.

Програмний комплекс виявлення початку атаки має гнучкі налаштування, що дозволяють задати чутливість до можливої атаки (лістинг 1). Конфігураційні дані виділені в окремий php-файл, що дає додаткові можливості як з точки зору зручності, так і з точки зору безпеки. Чутливість варіюється за допомогою корекції границі, а також порушенням границі відразу в декількох періодах різного розміру. Наприклад, при порушенні границі на хвилинних інтервалах засіб може тільки сповістити зацікавлених осіб про збільшення активності. У разі порушення границі також на п'ятихвилинному інтервалі відбувається повне включення механізму захисту.

Лістинг 1 - Фрагмент конфігураційного файлу

```
//час періоду мережевої активності в секундах, 86400 добу, 604800 тиждень
    $Loop = 40400;
//період для дослідження в секундах
```

```
$User_per = 300;
//кількість періодів для аналізу
$Count_user_per = 100;
//період, який необхідно відступити від початку атаки для позначки
//легітивного трафіку
$Safe_per = 600;
//число в процентах, на яке благополучний трафік повинен відрізнятися від
//шкідливого
$Pogresnost = 10.
```

У разі виявлення початку атаки виконуються наступні дії:

1. Розсилка повідомлень. В автоматичному режимі відбувається розсилка повідомлень електронною поштою.

2. Виконання скриптів. Запускаються скрипти або сторонні програми, підготовлені для виконання системним адміністратором. Це можуть бути як скрипти, що включають додаткові рівні кешування або ж відключають модулі web-ресурсу, що генерують підвищене навантаження, так і системні скрипти та програми.

3. Активація засобів фільтрації трафіка.

Засіб фільтрації трафіка. На підставі розробленого алгоритму засіб фільтрації трафіку проводить первинну кластеризацію. В результаті первинної кластеризації в базі даних створюються дві таблиці, що характеризують шкідливий і легітивний трафік. Отримані таблиці використовуються в якості навчальних вибірок при класифікації запитів, що надходять. В процесі роботи таблиці уточнюються і доповнюються.

Дані, які містяться в таблиці, що характеризує шкідливий трафік, використовуються для блокування трафіку. У розробляємому програмному засобі передбачена можливість вилучення з таблиці, відповідно шкідливому трафіку, клієнтських IP адрес і створення на їх основі заборонних правил. Крім цього, на підставі даних про шкідливий трафік можливо реалізувати додаткові механізми захисту. Наприклад, при надходженні шкідливих запитів до конкретної сторінки можна в автоматичному режимі тимчасово заблокувати цю сторінку або ж підмінити її статичної або кеш-версією. В цьому випадку шкідливий трафік, який був некоректно класифікований і не був заблокований на попередньому рівні, завдасть меншої шкоди.

Блокування шкідливих запитів. Для блокування шкідливих запитів передбачено два варіанти. В першому варіанті блокування здійснюється за допомогою створення відповідних забороняючих правил для iptables. Другий варіант буде актуальний якщо засіб функціонує у вузьких рамках віртуального хостингу, в цьому випадку блокування шкідливого трафіку здійснюється за допомогою заборонних правил, зазначених у файлі .htaccess (Лістинг 2).

В обох випадках блокування трафіку здійснюється повністю в автоматичному режимі. Також передбачений механізм експорту даних про

шкідливий трафік для блокування його в різних програмних файерволах або ж на вищих мережевих вузлах.

Лістинг 2 - Приклад блокування IP-адрес у файлі .htaccess

```
order allow, deny
deny from 192.168.0.1
deny from 192.168.0.2
allow from all
```

Архітектура програмного комплексу представлена на рис. 1.

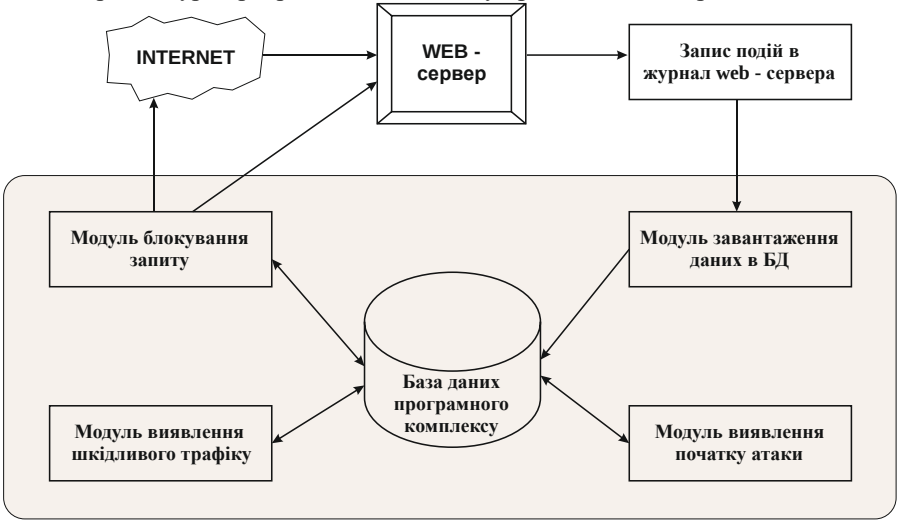


Рисунок 1 - Архітектура програмного комплексу

Взаємодія модулів програмного комплексу, один з одним і з WEB-сервером, відбувається за наступною схемою:

1. В результаті обробки запитів, що приходять до WEB-сервера з мережі інтернет, в журнал WEB-сервера додаються відповідні події.

2. Модуль завантаження даних з заданим інтервалом часу зчитує нові дані з журналу і завантажує їх в базу даних.

3. Модуль виявлення початку атаки, аналізує дані про запити, що містяться в базі даних. У разі виявлення початку атаки, цей модуль створює в базі даних дві порожні таблиці. Одну для легітимних запитів, другу для шкідливих.

4. Модуль виявлення шкідливого трафіку відстежує появу і стан зазначених вище таблиць БД. Якщо таблиці незаповнені, модуль проводить кластеризацію і первинне заповнення таблиць. Якщо в таблицях вже є дані, модуль аналізує запити, шо надійшли на предмет приналежності до груп легітивних або шкідливих запитів, і додає дані про запит в відповідну таблицю.

5. Модуль блокування запиту отримує список IP-адрес з таблиці, що містить шкідливі запити і вносить їх в «чорні списки» брандмауера або передає для блокування на вищестоящий мережевий сегмент.

Розроблений програмний засіб повністю відповідає поставленим завданням. Основні риси створеного програмного комплексу для виявлення і протидії DDoS-атакам це кроссплатформенність, універсальність і масштабованість.

Програмний комплекс може застосовуватися в якості засобу забезпечення безпеки так званої «останньої милі». Основною спеціалізацією комплексу є забезпечення безпеки web-серверів від DDoS-атак типу http-flood. Програмний комплекс підтримує різні операційні системи, він може бути використаний з більшістю сучасних web-серверів. При цьому інсталяція комплексу може здійснюватися як в рамках фізичного сервера, так і в рамках віртуального хостингу.

Універсальність програмного комплексу виявлення і протидії DDoS-атакам полягає в можливості його використання не тільки для виявлення http-flood'a, а й інших DDoS - атак різних типів. При незначних змінах, що не відносяться до основного модуля, програмний засіб може аналізувати різні дані, що містяться в log-файлах різних мережевих сервісах, або ж використовувати дані, отримані від мережевих локаторів.

У даній реалізації весь програмний комплекс, що складається з трьох модулів, розміщується на кінцевому мережевому ресурсі. В разі необхідності, модулі програми можуть бути розміщені в різних місцях мережі. Так, наприклад, на кінцевому сервері може знаходитися тільки засіб завантаження даних. Засоби виявлення атаки і фільтрації трафіку можуть бути встановлені на окремому сервері, недоступному для атаки з зовнішньої мережі. При такій установці програмний засіб зможе нормально функціонувати і проводити класифікацію трафіку навіть в випадку відмови атакуємого сервера.

Можливий варіант інсталяції, коли на вузлі, безпеку якого потрібно підтримувати, взагалі не встановлено ніяких модулів програмного засобу. У цьому випадку дані для аналізу можуть бути отримані від мережевих локаторів або вищестоящих маршрутизаторів. Блокування трафіку може бути здійснена на вищому вузлі.

Також програмний комплекс підтримує мультиінсталляцію при одночасному запуску декількох однойменних модулів. Так наприклад, дані для аналізу можуть надходити в базу даних з декількох джерел. Дані про шкідливий трафік можуть бути передані для блокування на різні рівні.

Література

1. Бабаш, А.В. Криптографические методы защиты информации: учебник / А. В. Бабаш, Е. К. Баранова. - М. : КНОРУС, 2016. - 190 с.

2. Батурин, Ю.М. Компьютерная преступность и компьютерная безопасность / Ю.М. Батурин, А.М. Жодзинский. – М.: Юридическая литература, 2006. – 160 с.

3. Борисов, М.А. Основы программно-аппаратной защиты информации: учеб. пособие для вузов / М. А. Борисов, И. В. Заводцев, И. В. Чижов. - 4-е изд., перераб. и доп. - М. : ЛЕНАНД, 2016. - 416 с.

4. Васильева, И.Н. Криптографические методы защиты информации : учебник и практикум для академ. бакалавриата / И. Н. Васильева. - Санкт-Петерб. гос. эконом. ун-т . - М. : Юрайт, 2017. - 349 с.

5. Нестеров, С.А. Основы информационной безопасности : учебник / С. А. Нестеров. - СПб. : Лань, 2017. – 423 с.

Екологічні проблеми Баранівського району Житомирської області

Свінтіцький П. В.
Науковий керівник к. пед. н Дячук А. О.
Хмельницький національний університет

Проблема охорони природи для Баранівського району зараз є дуже актуальною. Природні умови та ресурси Баранівщини своєрідні, і на сьогодні ще недостатньо досліджене питання раціонального їх використання. Збереження сучасної природи, збільшення її багатств, неможливі без детального знання історії. Саме знання минулого допомагають нам краще пізнати сучасне та прогнозувати майбутній стан природи регіону, можливості його реконструкції не тільки шляхом збереження, але і створення нових природоохоронних об'єктів. Сучасний розвиток людської діяльності часто виявляється шкідливим для навколишнього середовища внаслідок зростання містобудування, промислового виробництва, дорожнього руху. Тому відбувається забруднення води, повітря, грунтів, що негативно впливає на стан здоров'я населення, викликає загрозу навколишньому середовищу, загострює екологічні проблеми.

До основних антропогенних джерел забруднення атмосфери належать: теплове та енергетичне устаткування; промислові підприємства, добувна та обробна галузь господарства, всі види транспорту.

Однією з основних причин забруднення атмосферного повітря є низький рівень оснащення джерел викидів пилогазоочисним обладнанням. Значно впливає на забруднення атмосфери відсутність установок по вловлюванню газоподібних сполук, а саме: діоксиду сірки, діоксиду азоту, оксиду вуглецю, летючих органічних сполук та інших [1].

Зазначені речовини надходять в повітря від котелень, які працюють на кам'яному вугіллі, добування та переробки корисних копалин, виробництва мінеральної продукції, діяльності виробництва та оброблення деревини та ін.

Основними напрямами зменшення надходження забруднюючих речовин в атмосферне повітря є, насамперед виконання природоохоронних заходів та впровадження сучасних технологій очищення промислових викидів.

Зменшення шкідливих викидів від пересувних джерел можливе за рахунок збільшення використання неетильованого бензину, посилення контролю за токсичністю відпрацьованих газів автомобільних двигунів, будівництва об'їзних автошляхів для транзитного транспорту.

Аналізуючи показники забруднення повітряного басейну, що включає обсяг викидів шкідливих речовин стаціонарних та пересувних джерел забруднення потрібно відмітити зменшення загальної кількості викидів в атмосферне повітря в 2017 році у порівнянні з попереднім (на 11,02 тис. т або на 14,2 % менше) і склало 77,42 тис. т.

Протягом 2016 року в атмосферу Баранівського району надійшло 77,42 тис. т забруднюючих речовин, що на 12,46 % (на 11,02 тис. т) менше ніж у 2015 році.

На стаціонарні джерела викидів забруднюючих речовин в атмосферне повітря в 2016 році припало майже 14,12 % сумарних обсягів забруднення повітря області, на пересувні (автомобільний, залізничний, авіаційний, водний транспорт та виробнича техніка) – 85,88 % .

Спостерігається значне зменшення обсягу викидів забруднюючих речовин в атмосферне повітря від стаціонарних джерел викидів, який в 2016 році склав 10,9 тис. т, що на 36,5 % (або 6,3 тис. т) менше ніж у 2015 році (17,21 тис. т).

В 2016 році дещо зменшився обсяг викидів забруднюючих речовин в атмосферне повітря від пересувних джерел викидів. Так, в порівнянні з 2015 роком, обсяг викидів зменшився на 4,74 тис. т (на 6,7 %) і склав 66,49 тис. т.[1]

Однією з найважливіших умов успішної боротьби з транскордонним забрудненням повітря є наявність достовірної і повної інформації про стан навколишнього середовища і руху потоків забруднювачів.

Конвенція про транскордонне забруднення повітря на великі відстані вимагає від сторін здійснення обміну наявною інформацією про викиди забруднювачів повітря, що були здійснені з площ (за узгодженою мережею квадратів 50 км на 50 км), дані про потоки забруднювачів повітря через національні кордони і за узгоджені періоди .

Керівним органом Спільної програми спостережень та оцінки розповсюдження забруднювачів повітря на великі відстані у Європі (Програма ЕМЕП) до Конвенції 1979 року розроблені та направлені Сторонам Конвенції Керівні принципи оцінки та представлення даних про викиди забруднюючих речовин в регіоні ЕМЕП [5].

Щорічно в поверхневі водойми району відводиться близько 10 млн. $м^3$ зворотних вод. Всього в районі експлуатується 23 комплекси очисних

споруд, з них 16 зі скидом в поверхневі водні об'єкти загальною потужністю 18,35 млн.м^3. Більшість комплексів очисних споруд перевантажена і працює неефективно, спрацьована і потребує заміни переважна більшість технологічного обладнання. Зменшення скиду забруднюючих речовин у водні об'єкти можливе за рахунок поліпшення ефективності роботи очисних споруд шляхом проведення реконструкції очисних споруд, заміни насосного та технологічного обладнання, що використало свої технічні можливості.

Із загального обсягу скидів зворотних вод скиди нормативно очищених вод і таких, що не потребують очистки становлять понад 85 %, недостатньо очищених і не очищених – близько 10 %, близько 3 % стічних вод скидаються в накопичувачі та на рельєф місцевості [6].

Найбільшу кількість забруднених зворотних вод у водні об'єкти скидають підприємства комунального господарства – понад 90 %. На сьогодні вода основної річки – Случ з її притоками – за більшістю показників відповідає встановленим нормам. Вміст більшості забруднюючих речовин не перевищує ГДК для водойм господарсько-побутового призначення.

Через відсутність фінансування, прибережні захисні смуги малих річок Баранівщини в натуру практично не виносилися. В межах населених пунктів, де ширина смуги встановлюється проектом, такий проект було розроблено тільки для м. Житомира. Це значно ускладнює здійснення контролю за дотриманням вимог природоохоронного законодавства на землях водного фонду.

Вода р. Случ природна із слабким річковим запахом, середньою мінералізацією (сухий залишок знаходився в межах від 438,0 мг/дм^3 до 492,3 мг/дм^3, ГДК = 1000 мг/дм^3), із задовільним кисневим режимом (вміст розчиненого кисню становив від 8,4 O_2/дм^3 до 9,16 O_2/дм^3, при нормі не менше 4 мг O_2/дм^3), жорсткість води середня (від 5,2 моль/дм^3 до 5,9 моль/дм^3).

Вміст амонію сольового знаходився у межах від 0,16 мг/дм^3 до 0,93 мг/дм^3, нітритів від 0,049 мг/дм^3 до 0,138 мг/дм^3, нітратів від 1,17 мг/дм^3 до 1,89 мг/дм^3, що нижче встановлених ГДК. Вміст заліза знаходився нижче ГДК і становив від 0,02 мг/дм^3 до 0,07 мг/дм^3.

Вміст органічних сполук залишився на рівні 2015 р., разові значення показника $БСК_5$ знаходились в межах від 2,05 мг/дм^3 до 3,62 мг/дм^3. Вміст сульфатів, хлоридів, кальцію та магнію є стабільним. АПАР, нафтопродукти не виявлені. Солі важких металів знаходяться в нормі або нижче норми для водойм господарсько-побутового призначення [4]

Контроль за станом води у р. Случ проводився щоквартально по трьом створам.

Показники якості води річок Случ та Хомора у 2015 р. відповідали нормативам. У порівнянні з іншими роками стан води в цих річках залишився практично незмінним.

Стан води характеризувався такими показниками: мінералізація середня (разові концентрації сухого залишку знаходились в межах від 258,6 мг/дм^3 до 497,6 мг/дм^3), кисневий режим задовільний (вміст розчиненого кисню становив від 8,07 мг/дм^3 до 9,08 мг/дм^3), вода середньої жорсткості (від 5,2 моль/дм^3 до 7,7 моль/дм^3).

Вміст забруднюючих речовин групи азоту знаходиться нижче встановлених нормативів, залишився на рівні попереднього року: вміст сольового амонію знаходився в межах від 0,51 мг/дм^3 до 1,17 мг/дм^3, нітритів від 0,02 мг/дм^3 до 0,05 мг/дм^3, нітратів від 0,44 мг/дм^3 до 2,03 мг/дм^3.

Вміст сульфатів, хлоридів, кальцію та магнію є стабільним. АПАР, нафтопродукти не виявлені. Солі важких металів знаходяться в нормі або нижче норми для водойм господарсько-побутового призначення [3].

Контроль за станом води у р. Случ, Хомора проводився щоквартально.

Основним чинником антропогенного впливу на земельні ресурси району являється ведення сільського господарства. Екологічну стійкість земельних ресурсів характеризує ступінь розораності земель. Найбільш нестійкими в екологічному відношенні є ті території Баранівщини, в яких розорані землі значно переважають над умовно стабільними угіддями (сіножаті, пасовища, землі вкриті лісом і чагарниками, болота) [4].

Основним критерієм оцінки екологічного стану сільськогосподарських угідь є рівень родючості ґрунтів, як основа функціонування цієї категорії земель. Важливим показником рівня родючості ґрунтів є вміст гумусу, середній вміст якого в ґрунтах району станом на 01.01.2017 року становить 2,7 %, в порівнянні з аналогічними показниками обстеження площ в 1995 році, вміст гумусу зменшився на 0,06 %. Найвищий вміст його мають ґрунти Баранівського району (3,3 %).

В Баранівському районі розташовані перезволожені грунти. Тут ґрунтоутворюючими є щільні дочетвертинні глини або ж оглеєні леси підстелені ними, утворилися чорноземні-лучні мочаристі та мочарні ґрунти. В місцях розміщення таких ґрунтів на схилах більше 70 в роки надмірної кількості опадів, виникають зсуви, які спричиняють руйнування поверхні ґрунту. На таких площах частково проводиться заліснення [1].

Сучасний стан навколишнього природного середовища у Баранівському районі можна охарактеризувати як відносно стабільний. У порівнянні з іншими регіонами Житомирської області не відзначається високим промисловим потенціалом, але екологічних проблем, які потребують термінового вирішення, є чимало. Основні екологічні проблеми району:

– забруднення атмосферного повітря внаслідок викидів шкідливих речовин;

– забруднення водних ресурсів;

– забруднення грунтів і земельних ресурсів;

– зростання захворювання населення;

– погіршення стану природного середовища;

– неконтрольоване знищення і пошкодження тварин, рослин, лісів.

Основні заходи з покращення екологічного стану району:

– запровадження водозберігаючих форм розвитку економіки області;

– зменшення скидів забруднюючих речовин у водойми, повітря, грунти;

– підвищення розмірів зборів за користування та забруднення природних ресурсів;

– впровадження екологічного виховання населення;

– збільшення витрат бюджетів на природоохороннну діяльність [2].

Проблема раціонального використання водних ресурсів. Основними проблемами використання водних ресурсів району є забруднення поверхневих і підземних вод, поганий стан очисних споруд, складний стан каналізаційного господарства, спричинений застарілим та зношеним обладнанням, незадовільним технічним станом, відсутністю ефективних споруд попередньої очистки промислових стічних вод.

Проблема раціонального використання земельних ресурсів. Основними проблемами використання земельних ресурсів є: інтенсифікація землеробства, збільшення техногенного навантаження на земельні ресурси, безконтрольне застосування засобів хімізації в умовах низької технологічної культури та інші впливи призводять до погіршення якості ґрунтів, зниження їх родючості. Ерозія ґрунтів є основним і найнебезпечнішим дестабілізуючим фактором екологічної ситуації в ландшафтах, призводить до забруднення та замулення струмків, річок, ставків, посилення евтрофікації водойм. Великої шкоди ґрунтам завдає багаторазове механічне оброблення: оранка, культивування, боронування тощо. Все це посилює вітрову та водну ерозію. Важливу роль у боротьбі з ерозією ґрунтів відіграють ґрунтозахисні сівозміни, агротехнічні та лісомеліоративні заходи, будівництво гідротехнічних споруд.

Також ще є не вирішена проблема подальшого функціонування очисних споруд каналізації м. Полонного в с. Понінка Полонського району. В даний час ці очисні споруди взагалі не працюють, неочищені стоки з міста без будь-якої очистки скидаються у водні об’єкти. Заборгованість Полонського підприємства «Водоканал» перед Баранівськими РЕМ складає близько 100 тис. грн, що є однією з причин припинення роботи очисних споруд, поряд з незавершеним ремонтом напірного колектора. Згідно домовленостей між цими районами, сторона зобов`язувалась розпочати будівництво очисних споруд, однак жодних даних про початок цього будівництва немає, а на період їх будівництва за будь яких умов має здійснювати безпечна експлуатація споруд, наявних у с. Понінка Полонського району.

Екологічне становище Баранівського району Житомирської області досить складне. Це пояснюється тим, що протягом багатьох років не було комплексного підходу у вирішенні питань охорони природи.

Наразі проводиться робота щодо налагодження в Баранівці роздільного збирання побутових відходів (їх корисних компонентів). Так, розроблений міськвиконкомом у 2013 році інвестиційний проект «Підвищення екологічної безпеки населення міста Баранівки Житомирської області шляхом запровадження інноваційних механізмів збору, вивозу та утилізації (переробки) сміття» став переможцем Всеукраїнського конкурсу проектів та програм розвитку місцевого самоврядування. Як результат – у 2014 році міська рада повинна була одержати з державного бюджету грант у сумі 199 тис. грн. на його реалізацію. Проектом передбачалося придбання за рахунок коштів Конкурсу та спів фінансування з міського бюджету сміттєвоза із заднім навантаженням та 15 євро контейнерів для роздільного збирання твердих побутових відходів. У зв'язку із складною суспільно-політичною ситуацією в країні Верховною Радою України було внесено зміни до закону України «Про Державний бюджет України на 2014 рік», внаслідок чого було призупинено фінансування грантів для переможців Всеукраїнського конкурсу проектів та програм розвитку місцевого самоврядування. Тож наразі це питання залишається невирішеним [5].

Щоб діяльність відділу давала кращі результати потрібно збільшити, як штат службовців, так і штат працівників лабораторії.

В кожного службовця має бути транспортний засіб для виїзду на перевірки. Фахівці повинні мати вищу екологічну освіту та навики роботи.

Працівники інспекції повинні доповідати населенню про екологічну ситуацію в регіоні.

На підприємствах можна встановити повітроочисні та водоочисні споруди, а за надмірні викиди не погоджені з інспекцією накладати штрафи.

Необхідно продовжити роботу та зосередити зусилля на прибиранні та вивезенні побутових відходів і сміття, приведенні в належний санітарний стан полігонів твердих побутових відходів, кладовищ, місць поховань, ринків та закріплених територій (вулиць, тротуарів, комунальних доріг).

Можна також організовувати різні заходи щодо охорони навколишнього середовища з залученням школярів, студентів та бажаючого населення. Працівникам екологічного відділу доводити до свідомості населення про негативний вплив їхньої діяльності на навколишнє природне середовище (наприклад, спалювання листя, складування відходів у не відведених для цього місцях та інше) та подальшу негативну дію на організм людини.

Пріоритетними напрямками в екологічній освіті та вихованні є створення учнівських студій, екологічних клубів за інтересами. Методичні підходи до організації навчально-пізнавальної діяльності учнів під час занять з екології сприяють упровадженню неперервної екологічної освіти,

формуванню наукового світогляду, викликають стійке бажання подолати екологічні проблеми, активізують участь у природоохоронному русі, змушують школярів уважно придивлятися до того, що відбувається навколо.

Отже, основними шляхами покращення стану навколишнього природного середовища на території Баранівського району повинні стати такі:

– зменшення енергоємності стаціонарних джерел забруднення, переведення автомобільного парку на більш екологічно чисті види пального, екологорежимна наладка котелень;

– будівництво і реконструкція каналізаційних очисних споруд, насосних станцій і колекторів, поліпшення пропускної спроможності річок Хомори та Случ;

– дотримання технологічних норм споживання води через систему дозволів на спеціальне використання водних ресурсів то контролю за дотримання водоспоживачами умов дозволу;

– консервації деградованих і малопродуктивних земель, вапнування земель;

– проведення завершального етапу інвентаризації непридатних до використання та заборонених до застосування хімічних засобів захисту рослин та подальшого перезатарення та вивезення на місця тимчасового зберігання до знешкодження;

– паспортизація місць видалення відходів, будівництво сміттєзвалищ;

– вдосконалення системи екологічної освіти та виховання.

Отже, проаналізувавши екологічний стан Баранівського району, за даними обласної Держекоінспекції, Департаментом екології та природних ресурсів, а також за власними спостереженнями встановлено, що найбільш екологічними проблемами району є: забруднення атмосфери відпрацьованими газами, забруднення водойм та водних об'єктів примисловими скидами, а також ерозія грунтів.

Література

1. Агрокліматичний довідник Житомирської області. – К.: Держсільгоспвидав УРСР, 1959. – 92 с.

2. Еколого-економічні проблеми довкілля Житомирщини / В. І. Карпов, С. П. Сіренький, В. К. Данилко та ін.; Під заг. ред. П. П. Михайленка. – Житомир: НДІ статистики, 2001. – 320 с.

3. Житомирська область: Географічний атлас: Моя мала Батьківщина – 3-є вид., випр. і доп. / Відп. ред. М. Ю. Кострица. – К.: ТОВ Видавництво «Мапа», 2003. – 24 с.

4. Литвак П. В., Малиновський А. С, Таргонський П. Н., Бруцький Ю. В. Дикорослі лікарські рослини Полісся. – Житомир: «Державний агроекологічний університет», 2007. – 279 с.

5. http://baranivkarda.gov.ua/index.php/pro-raion
6. http://www.ecology.zt.gov.ua/ND2014-ND14.html

Аналіз сучасного стану управління інформаційними ресурсами корпоративних інформаційних систем

Струбчевська М. С.
Науковий керівник к.т.н., доц. Огнева А.М.
Хмельницький національний університет

Сучасні ІС зазвичай є комбінаціями декількох типів інформаційних систем. ІС системи розрізняються не лише функціональними можливостями і інформаційним вмістом, але і їх організаційним і апаратним виконанням. У міру розвитку інформаційних систем (ІС) з'явилася тенденція до узагальнення їх функцій і структур оброблюваних документів. Залежно від структури і розміру підприємства і особливостей його бізнесу ІС їм може функціонувати як на єдиній ЕОМ, так і у рамках локальної або розподіленої мережі. Крім того, інформаційно-обчислювальні системи розрізняються за призначенням, по територіальному розташуванню і взаємодії технічних засобів, за способом організації і обробки завдань, по розміщенню даних в компонентах мережі, за способом доступу користувачів до ресурсів і абонентів мережі і ряду інших ознак [1].

В розвинутих країнах поширені такі концепції інформаційних систем на підприємствах [3] :

– Управління ресурсами підприємства.

1. MRP (Material Retirements Planning) - планування матеріальних потреб.

2. MRP II (Manufacturing Resource Planning) - планування ресурсів виробництва.

3. ERP (Enterprise Resource Planning) - планування ресурсів підприємства.

– Управління логістикою (SCM - Supply Chain Management).

– Управління даними про вироби (PDM - Product Development Management).

– ІС автоматизованого проектування та виробництва (CAD/CAM - Computer-Aided Design/ Manufacturing).

– ІС документообігу (docflow).

Сучасний етап розвитку ІС в економіці України характеризується створенням інформаційних систем нового покоління, до яких належать експертні системи, системи підтримки прийняття рішень, інформаційно-пошукові системи, системи зі штучним інтелектом. Основою створення таких систем є децентралізація структури ІС та організація розподільної обробки

інформації.

Розвиток ІС визначив стрімкий розвиток інформаційних технологій і вдосконалення концепцій управління підприємством. Він характеризується збільшенням і ускладненням завдань, що стоять перед ІС, а також визнанням важливості ролі інформаційних ресурсів для підвищення ефективності функціонування будь-якого підприємства, інтенсифікації і розвитку управлінських і інноваційних процесів.

Ресурс – це запас, джерело чого-небудь. Розглядаючи народне господарство країни, будь-яку галузь, підприємство можна виділити такі економічні категорії: матеріальні, природні, трудові, фінансові, енергетичні ресурси. Для нормального функціонування організації будь-якого масштабу недостатньо мати ресурси – необхідно знати технології їх використання. Тому інформаційні ресурси розглядаються як окрема економічна категорія, як особливий вид ресурсу, що ґрунтується на ідеях і знаннях, нагромаджених у результаті науково-технічної діяльності людей і поданий у формі, придатній для збирання, реалізації та відтворення [3].

Саме інформація дозволяє визначати стратегічні, тактичні й оперативні цілі і завдання підприємства; здійснювати контроль поточного стану підприємства, його підрозділів і процесів в них; приймати обґрунтовані і своєчасні управлінські рішення; координувати діяльність, як окремих співробітників, так і підрозділів, спрямовуючи їх зусилля на досягнення загальних цілей.

Законодавчо інформаційні ресурси (ІР) – це «окремі документи і окремі масиви документів, документи і масиви в інформаційних системах. Іншими словами, ІР – це особливий вид ресурсу, оснований на ідеях і знаннях, нагромаджений у результаті науково-технічної діяльності людей і поданий у формі, придатній для накопичення, реалізації та відтворення [2].

В більшості випадків інформаційний ресурс розглядають як сукупність документів що циркулюють на підприємстві [1].

Оскільки інформаційні ресурси можуть зберігати інформацію різного типу: дані, знання, графічну і текстову інформацію, інформацію про об’єкти реального і віртуального світів, то для обробки кожного типу інформації застосовуються конкретні інформаційні технології. Так для цих цілей виявився затребуваним увесь спектр ключових технологій управління інформацією, що використовуються в сучасних ІС - технології баз даних, технології текстового пошуку, WEB- технології тощо [4].

У будь-якій організації інформаційні ресурси є початковою сировиною для інформаційно-обчислювальних систем, які підтримують практично усі аспекти управлінської діяльності в таких функціональних областях, як бухгалтерський облік, фінанси, управління трудовими ресурсами, маркетинг, управління виробництвом.

Сучасні корпоративні інформаційні системи (КІС) за своєю природою завжди є розподіленими (багатомашинними) системами. Щоб досягти мети

свого існування розподілена система повинна задовольняти наступним необхідним вимогам: відкритість, безпека, масштабованість, стійкість, підтримка логічної цілісності даних, ефективність.

Корпоративна інформаційна система являє собою багаторівневу структуру, кожен рівень якої виконує конкретні функції і вирішує власне безліч завдань [5]. Робочі станції користувачів, сервери додатків, сервери баз даних та інші мережеві вузли КІС розподілені по великій території. У великій компанії офіси і майданчики з'єднані різними видами комунікацій, що використовують різні технології і мережеві пристрої.

Головним завданням ІТ-персоналу КІС є забезпечення надійної, безперебійної, продуктивної і безпечної роботи всієї цієї складної системи. Для цього необхідно організувати захист інформаційних ресурсів, які формують основу всієї діяльності корпорації. Отже особливістю КІС є неоднорідність інформаційних ресурсів, яка проявляється: в різноманітті видів ІР (текстова, аудіо тощо); у різній структурованості даних (неструктуровані, слабоструктуровані, структуровані); у відмінності способів формалізованого представлення даних (реляційна модель, об'єктна модель); у відмінності використовуваних програмних систем і інтерпретації змісту даних тощо [5].

Таким чином, для ефективного управління інформаційними ресурсами корпоративна система повинна володіти наступним інструментарієм: інтегрованими програмними продуктами; засобами автоматизованої підготовки складних аналітичних звітів і візуалізації даних; надійною інформацією про характер використання ІР; вичерпною поточною інформацією про стан усіх компонентів КІС.

Для забезпечення максимальної рентабельності і отримання конкурентних переваг ІТ-послуги, що надаються, мають бути погоджені з потребами бізнесу, що постійно змінюються, та доступні корпоративним користувачам на усіх рівнях підприємства. Різноманіття і складність завдань управління інформаційними ресурсами КІС вимагає їх комплексного рішення, а саме створення інтегрованої системи управління інформаційними ресурсами як у рамках окремої КІС, так і в масштабі усієї країни [4].

Література

1. Ситник В.Ф. Системи підтримки прийняття рішень: навч . посіб / В.Ф. Ситник. – К.: КНЕУ, 2004. – 614 с.

2. Закон України «Про національну програму інформатизації» N 74/98-ВР від 04.02.98 р. [Електронний ресурс]. – Режим доступу: http://www.rada.gov.ua

3. Плескач В. Л. Інформаційні системи і технології на підприємствах : підручник / В. Л. Плескач, Т. Г. Затонацька. – К. : Знання, 2011. – 718 с.

4. Різніченко Л.В., Ткаченко Н.В. Досвід упровадження корпоративних інформаційних систем управління на вітчизняних підприємствах / Вісник КДПУ імені Михайла Остроградського. Випуск

4/2009 (57). Частина 2, с-184-189.
5. Інформаційні технології та моделювання бізнес-процесів : навч. посіб. / О. М. Томашевський, Г. Г. Цегелик, М. Б.Вітер, В. І. Дубук. - К. : ЦУЛ, 2012. - 296 с.

Аналіз моделей та алгоритмів функціонування мереж SDN

Хмельницький Ю.В.
Хмельницький національний університет

Аналіз методів, моделей та алгоритмів управління програмно-керованими мережами показав, що проблема забезпечення якості обслуговування займає досить важливе місце у наукових працях закордонних і вітчизняних дослідників. Значна увага науковців приділяється до адаптивності програмно - керованої мережі в умовах обслуговування мультисервісного потоку даних, яка реалізується завдяки можливостям протоколу Open-Flow. На відміну від традиційного застосування мережевої операційної системи як операційної системи інтегрованої зі стеком мережевих протоколів, в даному випадку будемо розглядати програмну система, що забезпечує моніторинг, доступ, керування ресурсами всієї мережі, а не конкретного вузла. Об'єктом керування мережевої операційної системи є один або кілька комутаторів. Контролер забезпечує набір інтерфейсів для створення, редагування, видалення, керування конфігурацією таблиць потоків у комутаторах. Комутатором керує програмний процес, який виконується на контролері. Контролер повинен завжди володіти інформацією про топологію мережі. Інформація про топологію мережі також містить інформацію про розміщення користувачів та серверів, інших елементів та сервісів мережі, а також, прив'язку між іменами та їх адресами.

Використання стандартизованого відкритого інтерфейсу площини передачі даних дає можливість впроваджувати інновації набагато оперативніше, ніж це відбувається сьогодні. Це дає можливість здійснювати оперативний моніторинг функціональних параметрів пристроїв передачі даних у мережах і можливість їх динамічно їх програмувати. В рамках дослідження та аналізу складових елементів системи управління SDN архітектури, що забезпечують якість обслуговування потоків у програмно - керованими мережах є деякі недоліки. Різнорідність самої апаратної реалізації пристроїв передачі даних мережі призводить до того, що різні види комутаторів можуть не підтримувати деякі функції чи підтримувати їх із обмеженою продуктивністю. У процесі роботи мережі це може суттєво вплинути на пропускну здатність окремих потоків передачі даних чи цілих доменів мережі. Сама маршрутизація потоків передачі здійснюється за критерієм якості обслуговування чи за критерієм рівномірного завантаження мережевих ресурсів мережі. Підвищення якості обслуговування здійснюється із врахуванням класифікації потоку передачі згідно ITU-T, що досить суттєво

обмежує можливість управління потоком даних. Більшість моделей не враховують характеристик мультисервісного потоку даних, що призводить до погіршення якості обслуговування та підвищення ймовірності блокування каналів передачі мережі.

Ще одна категорія методів базується на потокових аналітичних моделях для оптимізації мережі. Ці методи використовують моделі балансування навантаження потоків передачі даних, які не враховують чутливості потоку даних до перемішування порядку пакетів, погіршення затримки та тимчасового розриву з'єднання. Відсутність можливості здійснювати диференційоване управління для окремих потоків даних окремих клієнтів мережі та врахувати їхні вимоги щодо якості, призводить до низької ефективності каналу маршрутизації, неоптимального розподілу навантаження мережі, погіршення якості обслуговування високо пріоритетних потоків даних. Самі ж засоби контролю за процесом передачі окремих потоків передачі даних відсутні, внаслідок чого система управління мережею не має змогу визначити погіршення якості обслуговування для цих потоків даних, а тому не зможе гарантувати рівень якості, узгоджений у сервісі обслуговування.

Проведений аналіз показує, що існуючі моделі управління інформаційним потоком у програмно - конфігуруємо мережах не завжди враховують вимоги окремого клієнта, а диференціюють потоки лише за класами потоку інформації. Не використовують актуальні параметри управління та обслуговування як окремих каналів, так й індивідуальних потоків окремого клієнта мережі та не завжди можуть справитися із перевантаження елементів телекомунікаційної мережі, вузлів чи каналів. Проводить маршрутизацію потоків даних мережі, не диференціюючи їх за чутливістю до перемішування порядку пакетів та розриву з'єднання [1]. Розглянемо архітектуру SDN (рис. 1), що складається із рівня програми, рівня мережевого устаткування та рівня даних.

Мережеві комутатори стають простими пристроями переадресації, а логіка управління в архітектурі SDN реалізована в централізованому контролері. При аналізі моделей та алгоритмів функціонування системи управління SDN архітектури розглянемо співвідношення до її традиційних мереж.

Усі сучасні інформаційні технології висувають досить великі вимоги до гнучкості та масштабованості комп'ютерних мереж і очікується, що SDN мережі допоможуть вирішити цілий ряд наявних проблем, сприятимуть створенню автоматизованих, програмованих, гнучких та економічних мережевих інфраструктур, однак ця стратегія у різних провідних виробників помітно розрізняється.

Нові тенденції – це віртуалізація, хмарні обчислення, мобільність користувачів, зростання обсягів передачі - змінюють вимоги до мережевих інфраструктур. Будуть виникати питання чи зможуть сьогодні мережеві продукти забезпечити підтримку майбутніх додатків і сервісів, якою мірою

розвиток мережі буде прив'язаний до продуктів обраного виробника тощо. Пріоритетність рішень, архітектура традиційного мережевого обладнання робить цю прив'язку дуже міцною. Деякі виробники навіть характеризують поточну ситуацію у мережевий галузі як революційну.

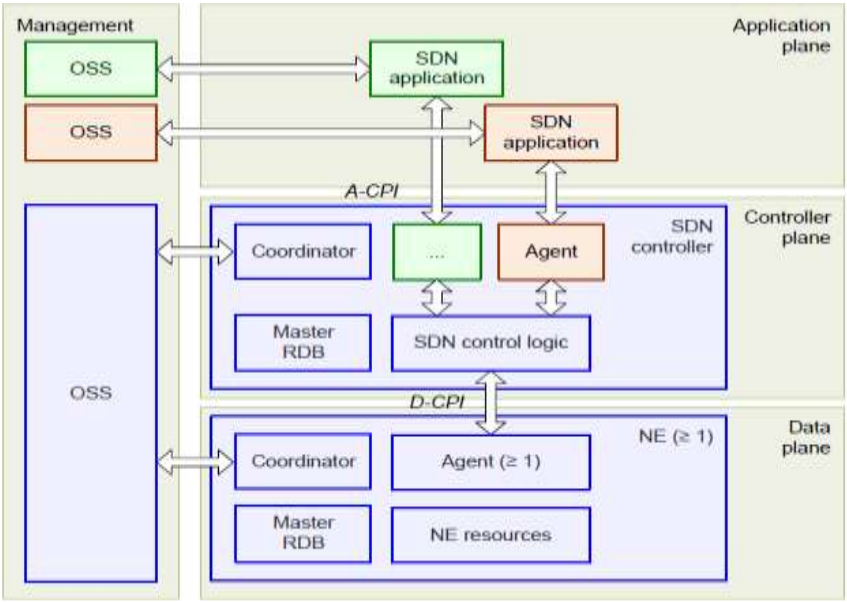


Рисунок 1 – Класична модель архітектура SDN мережі

Ряд експертів [2] у якості рецепту усунення розкритих в мережах проблем називають перехід до архітектури програмно-керованих мереж (Software-Defined-Networking, SDN). Архітектура SDN обіцяє істотно послабити залежність від замовників технологій конкретного виробника.

В архітектурі SDN вся логіка управління мережевими пристроями виноситься в так звану «площину управління», яка реалізується програмним чином. Конструктивно контролери в архітектурі SDN можуть будуватися на базі фізичних або віртуальних вузлів. В архітектурі SDN управління мережевими пристроями, як правило, здійснюється по протоколу Open-Flow.

Ідея архітектури SDN - відділення функцій передачі даних від функцій управління. У традиційних комутаторах та маршрутизаторах ці процеси зв’язані. У архітектурі SDN мережа, що складається із безлічі пристроїв різних виробників, постає для застосування як один логічний комутатор. Архітектура SDN дозволяє адміністраторам програмувати мережу як єдине ціле, а не займатися окремими комутаторами, які можуть просто виконувати інструкції контролера. Реалізація такої концепції значно спрощує експлуатацію та функціонування мережі, її конфігурацію. Комутатори

можуть бути простими та дешевими. Характеристики мережі можна оперативно змінювати у режимі реального часу, скорочуються терміни впровадження нових додатків та сервісів. Програмні інтерфейси (API), контролери дозволяють розробникам створювати додатки для управління такою мережею. Ці програми можуть виконувати найрізноманітніші функції, причому для цього не потрібно знати особливості роботи конкретних мережевих пристроїв.

Із точки зору виробників, такий підхід не повинен викликати ентузіазму у розробників мережевого устаткування, які багато років удосконалювали унікальні функції своїх комутаторів та маршрутизаторів. Можливість використання простих та дешевих комутаторів, створення додатків сторонніми розробниками за рахунок відкритих API підриває бізнес таких компаній, позбавляє їх джерела додаткової вартості. Проте великі замовники, включаючи провідних операторів зв'язку та провайдерів, вже перейнялися ідеями архітектури SDN, а виробники мікросхем комутаторів оголосили про підтримку Open-Flow, тому поставники не можуть залишатися осторонь.

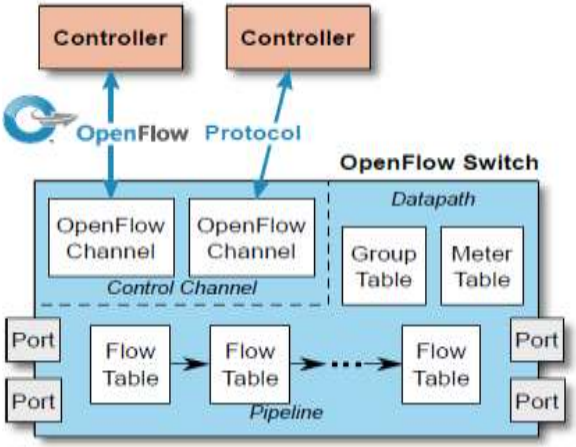


Рисунок 2 – Алгоритм функціонування Open-Flow маршрутизатора

Структура Open-Flow маршрутизатора представлена на рис. 2. Open-Flow маршрутизатор складається із однієї або декількох таблиць потоків. Маршрутизатор обмінюється повідомленнями з контролером за допомогою протоколу Open-Flow. За допомогою протоколу Open-Flow, контролер виконує такі дії з записами потоків в таблицях як додавати, оновлювати, видаляти. У таблицях потоків маршрутизатора містяться набори записів, а усі записи визначаються полями порівнянь, лічильниками та набором інструкцій, які застосовуються до пакету та співпали із полями. При передачі, заголовки пакетів порівнюються із полями порівнянь записів в порядку пріоритету, а це

одне із полів порівняння. Якщо знайдені відповідні записи, то до пакету застосовуються інструкції, асоційовані із цим записом. Якщо не знайдено жодного запису, то пакет скидається або передається для аналізу прийняття рішення контролеру.

Робочі інструкції у відповідних записах Open-Flow маршрутизатора містять дії, які застосовуються до пакету та визначають безпосередньо самі правила пересилання, чи визначають подальшу обробку пакета, у наступних таблицях потоків - конвеєрна обробка. Конвеєрна обробка дозволяє передавати аналіз пакета із однієї таблиці в іншу, додатково пересилаючи спеціальні метадані. Обробка закінчується, коли відповідні інструкції не містять команд пересилання в наступну таблицю у цей момент виконується модифікація пакету, виконання "накопичених" дій. Завдяки такій моделі, Open-Flow комутатор може функціонувати як простий комутатор, маршрутизатор, мережевий екран чи як інше мережевий пристрій. Все визначається за таблицею передачі. Така модель обробки пакета відкриває унікальні можливості. Пристрій може використовуватися в ролі як комутатора, так і маршрутизатора чи мережевого екрану. Групова таблиця містить записи груп, а кожен запис містить також список інструкцій зі специфічною семантикою, що залежить від типу групи. Дії в одній застосовуються для всіх пакетів, що посилаються до цієї групи. Збір статистики реалізується за допомогою лічильників. Лічильники можуть бути призначені для кожної таблиці, потоку, порту, черги, групи чи набори лічильників, визначені спеціалізацією Open-Flow.

Всі Open-Flow сумісні лічильники можуть бути реалізовані в програмному забезпеченні та відображають інформацію на основі опитування апаратних лічильників, які мають обмежений діапазон значень. Любий потоковий запис містить набір інструкцій, які виконуються в тому разі, коли пакет відповідає правилу. Усі інструкції діляться на наступні типи: для негайного виконання, для очищення списку інструкцій, для додавання нової інструкції, для запису метаданих, для переходу до наступної таблиці. Інструкції для негайного виконання дають вказівку застосувати певні дії негайно, без будь - яких змін у наборі дій. Така інструкція може бути використана для модифікації пакета при передачі його до іншої таблиці. Інструкції для очищення видаляють всі інструкції з набору інструкцій для окремого потоку. Інструкції для додавання нової інструкції доповнюють наявний набір інструкцій для окремого правила новими інструкціями. Інструкція переходу до наступної таблиці містить номер таблиці, в яку пакет буде переданий після обробки в поточній таблиці. Номер наступної таблиці обов’язково повинен бути більшим від номера поточної таблиці.

Дослідження та аналіз моделей і алгоритмів забезпечення функціонування й процесів управління мережею, побудованою за принципами SDN, показує, що спочатку необхідно здійснити модернізацію механізмів моніторингу стану її ресурсів, по скільки при використанні

стандартного механізму спостерігається генерація надлишкової службової інформації для елементів, що простоюють. Це може мати досить негативний вплив на ефективність роботи через завантаженість каналів передачі. Тому при аналізі моделей та алгоритмів функціонування системи управління SDN архітектури, у зв'язку із недоліками існуючих систем моніторингу, у багатьох публікаціях [3] пропонується використовувати метод динамічної адаптації параметрів системи моніторингу, наприклад, зміну інтенсивності моніторингу стану мережевого елемента залежно від його поточної завантаженості. Інтелектуальний моніторинг в мережі на основі SDN реалізується шляхом встановлення головного додатку моніторингу на контролер та відповідних підконтрольних йому агентів на кожен комутатор.

Тому аналіз моніторингу виконує додаток, встановлений на контролері, а підконтрольні йому агенти виконують функції збору інформації, модифікацію та відправлення на контролер. Розподіл інтенсивності моніторингу окремих сегментів мережі дає можливість усунути надлишкові процеси моніторингу та обробки даних про стан мережі, виконуючи необхідну інтенсивність лише на тих вузлах, де все це необхідно робити. На основі інтенсивності моніторингу можна збільшувати гнучкість управління елементами мережі на основі SDN, та ефективніше використовувати обчислювальні ресурси пристроїв рівня управління. Володіючи поточною службовою інформацією, можна здійснювати оптимальний розподіл навантаження на мережі, попереджуючи таким чином негативні явища перевантаження мережевих вузлів. Можна переводити елементи, що простоюють, у режим очікування, зберігаючи при цьому можливість надійного та швидкого їх відновлення до нормального режиму роботи. Це значно зменшить витрати та збільшує час «життя» мережевих пристроїв. Повністю відключати обладнання не завжди доцільно, по скільки його ввімкнення потребує певного часу для відновлення таблиць комутації, запуску усіх апаратних та програмних процесів комутатора, що впливає на час перебудови топології мережі та спричиняє стрибок службової інформації між контролером та комутатором. Особливістю розглянутого механізму є зміна інтенсивності моніторингу лише конкретного мережевого вузла, який цього потребує, однак це не впливає на інтенсивність моніторингу інших вузлів.

Такий алгоритм функціонування системи управління SDN архітектури та пропонований механізм є адаптованим до сучасного динамічного потоку даних та забезпечує хорошу базу для подальшого процесу балансування навантаження. Чим вище миттєве значення завантаження каналу, тим швидше відбудеться наступне опитування, тому чим більше завантаження каналу, тим частіше система моніторингу здійснює опитування щодо кількості переданої інформації. Такий метод можна використовувати стосовно усіх параметрів комутатора у випадку, коли підвищення інтенсивності їхнього опитування не впливає негативно на характеристики

продуктивності та якості функціонування мережі. Ще важливим параметром процесу моніторингу є кількість інформації, що генерується цим процесом. При роботі мережі, у випадку підвищення інтенсивності моніторингу кількість службової інформації, навантаження на інформаційний канал зростає, що загалом призводить до часткового зниження ефективності використання інформаційного каналу. Функція зміни інтенсивності моніторингу буде різною для кожного окремого параметру мережі, а її максимальне значення залежатиме від рівня навантаження процесу моніторингу на мережеві елементи. Обмеження щодо частоти моніторингу деяких параметрів часто встановлюють виробники, вказуючи критичне значення у документації до пристроїв.

Спрощені підходи до аналізу потоків даних і спроби отримання інформації про мережеві додатки на підставі легкодоступних атрибутів та характеристик потоків найчастіше виявляються непродуктивними. У більшості програм обміну файлами активно використовуються прийоми, що ускладнює достовірну ідентифікацію таких додатків - динамічне призначення портів, децентралізовані сховища, використання поширених прикладних протоколів як транспортних, а також криптографічні методи приховування та маскування потоку даних. Ці обставини вимагають використання додаткових технічних, програмних та алгоритмічних засобів і математичних моделей досліджуваних процесів. Характеристики функціонування програмно - керованої мережі, що складається з різнорідних Open-Flow комутаторів, залежать від апаратних характеристик кожного комутатора. З метою зменшення складності та вартості комутатора постачальники можуть обмежити функціональні можливості Open-Flow, наприклад, розмір апаратної таблиці потоків чи можливостей цієї таблиці щодо пошуку за певними полями, виконання певних дій над пакетами. Додатки, що встановлюються на контролері, повинні враховувати ці обмеження, щоб уникнути можливих проблем, пов’язаних із погіршенням продуктивності мережі в процесі її роботи.

Використання нових моделей та алгоритмів дозволяє забезпечити централізований моніторинг параметрів мережевих пристроїв та формувати характеристики функціонування програмно – керованої мережі на виході. Результати моніторингу можуть бути додатково використані при плануванні роботи мережі чи для динамічної оптимізації мережі - встановлення правил із врахуванням апаратних характеристик комутатора та передачі потоку даних через різні шляхи для уникнення вузьких місць у такій мережі. Специфікація Open-Flow визначає необхідну функціональність, яка повинна бути реалізована у кожному комутаторі Open-Flow. Основною метою цієї специфікації є забезпечення уніфікованих процесів контролю та управління програмно – керованою мережею, що складається із пристроїв різних моделей від різних виробників. Реалізація необхідної функціональності є індивідуальною та змінюється від одного виробника до іншого та може

привести до змін продуктивності у реальній мережі. Проблеми виникають уже тоді, коли програмно - керована мережа налаштована та окремі комутатори починають створювати вузькі місця, погіршуючи продуктивність та якість обслуговування мережі. Тому необхідно, щоб розробники додатків для програмно – керованих мереж змогли отримати інформацію про обмеження продуктивності конкретного комутатора із метою забезпечення стабільної та надійної роботи мережі. Комутатор, залежно від апаратної реалізації, може надавати доступ до окремих параметрів. Специфікація Open-Flow містить загальний алгоритм роботи та список параметрів доступних для моніторингу:

– аналіз потоків передачі - тривалість існування, пріоритет, кількість оброблених пакетів, байт;

– аналіз таблиць потоків даних - кількість правил, кількість оброблених пакетів, байт;

– аналіз портів передачі - кількість переданих чи відкинутих пакетів, байт, помилок передачі та колізій;

– аналіз черг передачі - довжина черги, кількість переданих пакетів, байт, кількість відкинутих пакетів через переповнення.

Розглянута система дозволяє здійснювати моніторинг як Open-Flow параметрів, так і параметрів якості, пов'язаних із роботою комутатора. Параметри Open-Flow - максимальна кількість правил із конкретною структурою, тривалість встановлення правил, тривалість опитування статистики таблиці потоків, тривалість обробки пакетів із використанням програмних таблиць потоків даних, тривалість зчитування інформації із лічильників, а також завантаження центрального процесора пристрою. Основним компонентом розглянутої системи моніторингу є додаток моніторингу, який встановлюється на фізичному сервері. Цей додаток виконує ключову роль збору, форматування та представлення інформації у форматі, зручному для користувача і для подальшої обробки цієї інформації іншими додатками. База даних зберігає інформацію, необхідну для роботи додатка, наприклад, для налаштування комутаторів, моделі та технічні особливостей того чи іншого комутатора. Ці дані заносяться в базу даних адміністратор програмно – керованої мережі. У базі даних зберігаються зібрані дані моніторингу та оброблені статистичні характеристики поведінки мережі в певні періоди.

Відсутність можливості здійснювати диференційоване управління для окремих потоків даних окремих клієнтів мережі та врахувати їхні вимоги щодо якості, призводить до низької ефективності каналу маршрутизації, неоптимального розподілу навантаження мережі, погіршення якості обслуговування високо пріоритетних потоків даних. Засоби контролю за процесом передачі окремих потоків передачі даних відсутні, внаслідок чого система управління мережею не має змогу визначити погіршення якості

функціонування для цих потоків даних. Розробники ставлять за мету формування такої архітектури мережі та устаткування, що припускає відділення площини управління від площини передачі та докладають значних зусиль до подолання виникаючих проблем, пов'язаних із складнощами міграції від традиційних мереж до архітектури SDN. Це в подальшому надасть можливість користувачам отримувати послуги із необхідною якістю, надійністю та достовірністю.

Література

1. Орлов Є.В. Програмно - конфігуровані мережі (SDN): архітектура, міжнародна стандартизація / Є. В. Орлов // Наукові записки УНДІЗ. - 2014. - №4(32). - С. 85-91.

2. Толубко В.Б. Багатокритеріальна оптимізація параметрів програмно – конфігурованих мереж(SDN)/В.Б.Толубко, Л.Н.Беркман,Л.О.Комарова, Є.В. Орлов // Телекомунікаційні та інформаційні технології - 2014. - №4.- С.5-11

3. Стрихалюк Б.М. Метод балансування навантаження на основі інтегрованої архітектури управління з використанням функції NVF / Б.М.Стрихалюк, О.М.Шпур, М.О.Селюченко // IX Міжнародна науково-технічна конференція «Проблеми телекомунікацій» ПТ-2015: Збірник матеріалів конференції (м. Київ, 21-24 квітня 2015 р.). - К.: НТТУ «КПІ», 2015. - С.322-325

Дослідження методів тестування додатка для мобільних пристроїв

Чешун К.А., Орленко В.С., Джулій В.М.
Хмельницький національний університет

Процес розробки додатків для мобільних пристроїв являє собою ітеративну схему, її застосування доцільно в проектах розробки додатка для мобільних пристроїв, загальною тривалістю до одного року. Особливість ітеративної схеми полягає в прискореному просуванні до готового продукту внаслідок кількох ітерацій повного циклу розробки (рис. 1).

В результаті визначення функціональних вимог починається цикл з декількох етапів розробки готових альфа-версій продукту. На кожному етапі відбувається повна збірка додатка, системне тестування нового функціоналу і етап регресійного тестування. Після кількох ітерацій приймається рішення, що подальше доопрацювання додатка не є доцільним і відбувається вихід з циклу з додатком, готовим до випуску. Процес визначення вимог вимагає попереднього аналізу цільової аудиторії і ринку аналогічної продукції. Можливі кілька варіантів визначення бізнес вимог до продукту: «мозковий штурм» за участю всіх залучених до процесу розробки людей; зустрічі з замовником і формування високорівневих вимог. Основна особливість отриманих вимог - високий рівень абстракції. Вимоги повинні бути зрозумілі будь-якій людині, залученій в процес розробки, і не повинні залежати від конкретної технології розробки. Існує кілька способів подання і зберігання бізнесі вимог:

- набір шаблонів - паперових або електронних. Кожен шаблон описує певну частину програми. Шаблони статичні і ніяк не взаємодіють між собою. Очевидні плюси шаблонів - їх швидка розробка і наочність. Шаблони можна розробити таким чином, щоб вони дуже точно описували призначений для користувача інтерфейс продукту, що розробляється;

- модель додатка, написана на формальній мові. Для розробки формальних моделей необхідне знання відповідних інструментів моделювання, наприклад, UniTESK. Подібні формальні моделі дозволяють точно описувати внутрішню структуру програми, наприклад, ООП класи. Також формальні моделі дозволяють генерувати функціональні специфікації та тестові сценарії на основі побудованих моделей. Тестові сценарії, що генеруються, можуть застосовуватися для тестування методом «білого ящика», оскільки формальна модель описує внутрішню структуру програми. Такі моделі не дозволяють «побачити» готовий додаток, оскільки описують тільки функціонал, але не призначений для користувача інтерфейс;

- модель додатка, створена за допомогою спеціальних інструментів прототипіювання інтерфейса для користувача. Прототипи дозволяють точно описати поведінку додатки на системному рівні, тобто інтерфейс для користувача. При цьому прототипи ніяк не описують внутрішню структуру програми. Прототипи дозволяють генерувати функціональні специфікації та

тестові сценарії, придатні для тестування методом «чорного ящика».

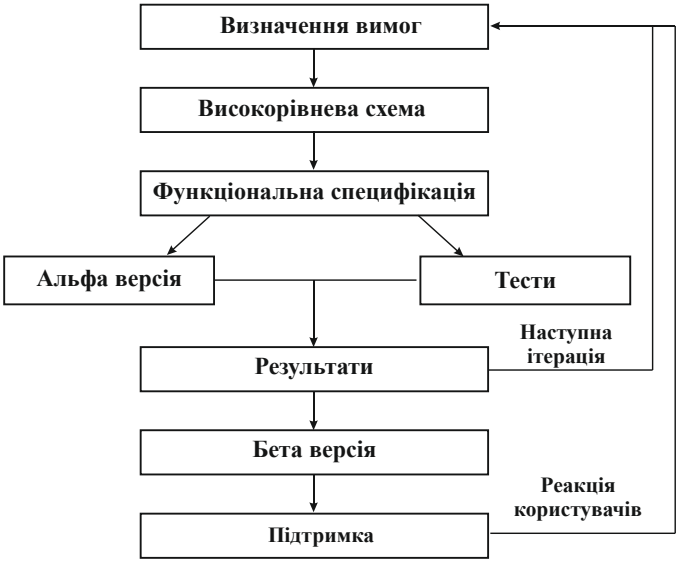


Рисунок 1 - Ітеративна схема розробки додатка для мобільних пристроїв

Проведений аналіз процесу розробки додатка для мобільних пристроїв дозволяє виділити наступні особливості: процес розробки розглянутих додатків швидкоплинний, загальна тривалість проектів по впровадженню програми - не більше одного року; розробка відбувається по ітеративній схемі, тому вимагає оптимізації інтегрованих процесів функціонального тестування за часовим параметром; розробка високорівневого прототипу додатка з подальшою генерацією тестових сценаріїв, імовірно, дозволить оптимізувати процес впровадження додатків.

В ітеративній схемі, в процесі розробки додатків для мобільних пристроїв, додаток надходить на тестування на системній стадії, минаючи процеси модульного і інтеграційного тестування. Таким чином, процес функціонального тестування зводиться до перевірки функціональності програми на рівні призначеного для користувача інтерфейсу. У загальному випадку взаємодія користувача з додатком відбувається за наступною схемою:

1. Користувач бачить на екрані мобільного пристрою деякий «вид» додатка. Цей вид містить елементи призначеного для користувача інтерфейсу (кнопки, поля введення і ін.), які дозволяють здійснювати різні дії (запити користувача).

2. Запит, що генерується користувачем, надходить в «логічну» частину

додатка, яка обробляє запит і, можливо, звертається до бази даних за необхідними даними.

3. Отримавши дані, «логічна» частина генерує наступний «вид», який побачить користувач - як результат свого запиту.

4. Далі процес повторюється.

В схемі, зображеній на рис. 2, на кожному етапі розробки можна вибрати один із способів переходу до наступного етапу. Залежно від обраного переходу змінюється час досягнення наступного етапу. Сумарний час розробки залежить від шляху проходження зі стану 1 схеми в стан 7 і від кількості ітерацій циклу 1-7. Зі стану 1 в стан 7 можна прийти різними шляхами, але в кожному стані вибір наступного маршруту залежить від попереднього стану процесу розробки. Кожен з можливих маршрутів визначає метод тестування програми. Розглянемо найбільш поширені шляхи переходу з 1 в 7.

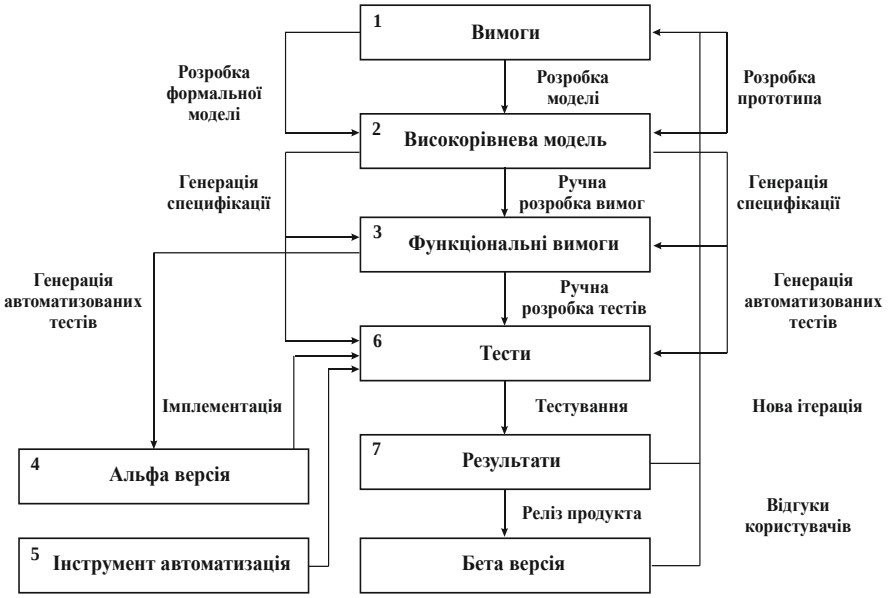


Рисунок 2 - Детальна ітеративна схема розробки додатка для мобільних пристроїв

Ручне тестування з документації: визначення вимог; розробка шаблонів; ручна розробка текстової функціональної специфікації; ручна розробка тестових сценаріїв; ручне тестування. Метод ручної розробки документів і тестів (*PP* метод) дуже гнучкий і дозволяє досягти будь-якого рівня тестового покриття. Однак цей метод вимагає великих часових витрат.

Автоматизація ручних тестів: визначення вимог; розробка шаблонів;

ручна розробка текстової функціональної специфікації; ручна розробка тестових сценаріїв в текстовому вигляді; автоматизація тестових сценаріїв; автоматизоване тестування.

Метод автоматичної розробки тестів (*РА* метод) вимагає текстового опису тестових сценаріїв. По суті, створюються тестові сценарії в текстовому вигляді, як і в випадку *РР* методу, а на основі даних тестових сценаріїв розробляються автоматизовані тести. Такий підхід вимагає значно більше часу на розробку тестів, але значно скорочує час проведення тестування. Отже, такий підхід ефективний при збільшенні кількості циклів розробки.

Тестування на основі формальної моделі (*ФМ* метод): визначення вимог; розробка формальної моделі; генерація специфікації; генерація тестових сценаріїв; автоматизоване тестування. Даний метод підлягає автоматизації, але не досить гнучкий в області розробки додатків для мобільних пристроїв, оскільки за допомогою формальних моделей важко описувати призначені для користувача інтерфейси, отже, важко отримати необхідне тестове покриття.

Тестування на основі прототипу: визначення вимог; розробка прототипу; генерація специфікації; генерація тестових сценаріїв; ручне та автоматизоване тестування. Метод розробки на основі прототипу (*ПР* метод) дозволяє добре описувати призначені для користувача інтерфейси, отже, отримати необхідне покриття. Метод також дозволяє генерувати різні типи тестових сценаріїв при наявності відповідних інструментів генерації і особливі правила побудови прототипів, що надає додаткову гнучкість в проведенні тестування.

Для мобільних додатків існують різні інструменти автоматизації тестування. У загальному випадку можна виділити два основні підходи до автоматизації тестів.

Програмний метод автоматизації. Метод, який передбачає використання певних бібліотек деякої мови програмування. Автоматизація тестів зводиться до написання допоміжних модулів тестування і написання тестових скриптів на мові програмування. Основний мінус цього підходу - значні часові витрати на реалізацію тестових скриптів.

Метод автоматизації з використанням playback інструментів. Такий підхід вимагає мінімальних навичок в програмуванні. Автоматизація тесту відбувається за допомогою проведення тестового сценарію на цільовому пристрої з пропущенням впливів через спеціальну програму (проксі-сервер), що записує вплив і дані. Після запису ця програма представляє отриману інформацію у вигляді автоматичного тесту. При такому підході автоматизація тесту зводиться до його виконання. Основний мінус цього підходу - будь-яка зміна в тестовому додатку вимагає перезапису тестових сценаріїв, пов'язаних зі зміненим функціоналом.

Виходячи з проведеного дослідження, можна зробити наступні висновки щодо методів тестування додатка для мобільних пристроїв: ефективність методу тестування додатка для мобільних пристроїв безпосередньо залежить від кількості ітерацій розробки, тому оптимізація методів тестування за часом зводиться до автоматизації процесів створення тестових сценаріїв і автоматизації їх виконання; найбільшу ефективність надає метод тестування на основі прототипів, при цьому тестові сценарії для тестування додатка для мобільних пристроїв генеруються з побудованого прототипу; необхідно мати можливість генерувати тестові сценарії таким чином, щоб використовувати їх в програмному методі автоматизації тестування з найменшими доопрацюваннями.

Література

1. Ханссон Д. Х., Томас, Д. Гибкая разработка веб-приложений в среде Rails / Д. Томас, Д. Х. Ханссон — Санкт-Петербур - Питер, 2008.

2. Салмре Иво Конечный автомат для пользовательского интерфейса. Программирование мобильных устройств на платформе .NET Compact Framework / Иво Салмре – Изд-во: Издательский дом "Вильямс", 2006.

3. Джулій В.М. Методи та алгоритми розробки web-додатків / В.М. Джулій, Ю.О. Гунченко, Д.В. Чешун // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2017. – Вип. № 56. – С.107-115

4. Роберт Мартин Быстрая разработка программ. Принципы, примеры, практика. /Роберт Мартин, Джеймс Ньюкирк, Роберт Косс — Изд-во: Диалектика-Вильямс, 2004. — 752 с.

Наукове видання

«Інтелектуальний потенціал – 2018» - збірник наукових праць молодих науковців і студентів з нагоди 30-річчя підготовки ІТ- фахівців в ХНУ/ Колектив авторів – Хмельницький: ПВНЗ УЕП, 2018. – Ч.2: Математичне моделювання та інженерія програмного забезпечення – 76 с.

Відповідальність за зміст текстів і якість редагування матеріалів покладена на авторів і наукових керівників.

Комп'ютерна верстка: Чешун В.М.
Дизайн: Муляр І.В.

Здано до складання 5.11.18. Підписано до друку 10.11.18. Формат 60x84/16. Папір друкарський. Тираж 50 прим. Умовних друкованих аркушів – 4,38. Обліково-видавничих аркушів –1.

Редакційний відділ ПВНЗ УЕП 29016, м. Хмельницький, вул. Львівське шосе, 51/2.

ББК 74.480.278
С.88